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

Кваліфікаційна наукова праця
На правах рукопису

**ГАВЕЛЬ СЕРГІЙ МИКОЛАЙОВИЧ**

УДК 004.056.53:621.391.7

**ДИСЕРТАЦІЯ**

# ПІДВИЩЕННЯ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛЬНИХ КОНСТРУКЦІЙ

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
_____ Гавель Сергій Миколайович
(*підпис*)

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

Одеса – 2026

# АНОТАЦІЯ

Гавель С. М. Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій – 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 наведено наукове обґрунтування та нове вирішення актуального науково-технічного завдання захисту інформації від несанкціонованого доступу в інформаційно-комунікаційних системах, що функціонують в умовах радіоелектронного протиборства, шляхом підвищення прихованості її передавання. Запропоновані рішення базуються на сумісному використанні непозиційних таймерних сигнальних конструкцій і прямого розширення спектра за допомогою псевдовипадкових послідовностей для формування широкосмугових шумоподібних сигналів з урахуванням енергетичних, частотних та інформаційних обмежень каналу зв'язку.

У роботі розроблено метод підвищення захищеності інформації на фізичному рівні за рахунок одночасного забезпечення структурної та енергетичної прихованості сигнально-кодових конструкцій. Для оцінювання рівня захисту інформації запропоновано методику кількісного визначення показників структурної та енергетичної прихованості широкосмугових таймерних сигналів. Підвищення прихованості досягається шляхом адаптації параметрів формування таймерних сигнальних конструкцій, вибору бази розширення спектра та використання псевдовипадкових і хаотичних послідовностей в умовах нестаціонарного функціонування каналу зв'язку.

*Метою дисертаційної роботи* є розроблення методу захисту інформації в інформаційно-комунікаційних системах шляхом підвищення структурної та енергетичної прихованості передавання сигнально-кодових конструкцій на основі

прямого розширення спектра таймерних сигналів псевдовипадковими послідовностями.

*Об'єкт дослідження* – процеси захисту інформації в інформаційно-комунікаційних системах на фізичному рівні шляхом формування та передавання широкосмугових шумоподібних сигнально-кодових конструкцій в умовах радіоелектронної протидії.

*Предмет дослідження* – метод прямого розширення спектра таймерних сигнальних конструкцій на основі псевдовипадкових послідовностей Уолша та послідовностей, сформованих на основі хаотичних коливань, а також методи оцінювання їх структурної та енергетичної прихованості.

У вступі обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача. Подано відомості про апробацію результатів роботи, особистий внесок здобувача та його публікації.

*У першому розділі* дисертаційної роботи проведено аналіз сучасного стану наукових досліджень у сфері захисту інформації та забезпечення прихованості її передавання в інформаційно-комунікаційних системах, що функціонують в умовах радіоелектронного протиборства. Розглянуто основні загрози інформаційній безпеці, пов'язані з можливістю виявлення, перехоплення, аналізу та відновлення переданих повідомлень засобами радіоелектронної розвідки, радіомоніторингу та активного радіоелектронного впливу.

Проаналізовано поняття прихованості передавання інформації як одного з напрямів її захисту на фізичному рівні та визначено основні показники оцінювання захищеності інформації, зокрема енергетичну та структурну прихованість сигналів. Встановлено, що ефективність виявлення та розпізнавання сигнально-кодових конструкцій значною мірою визначається їх спектральними, часовими та кореляційними характеристиками.

Здійснено аналіз існуючих методів захисту інформації під час передавання, зокрема криптографічних методів, завадостійкого кодування, методів модуляції та розширення спектра сигналів. Показано, що зазначені методи не повною мірою забезпечують необхідний рівень структурної та енергетичної прихованості в умовах сучасної радіоелектронної протидії.

Досліджено методи прямого розширення спектра та особливості використання псевдовипадкових, ортогональних і квазіортогональних послідовностей для формування широкосмугових шумоподібних сигналів. Визначено обмеження класичних DSSS-систем щодо забезпечення структурної прихованості та протидії засобам кореляційного аналізу.

Розглянуто принципи побудови таймерних сигнальних конструкцій як засобу підвищення структурної прихованості сигнально-кодових конструкцій. Показано, що використання непозиційного представлення інформації дозволяє суттєво збільшити ансамбль можливих реалізацій сигналів та ускладнити їх виявлення і відновлення структури.

За результатами аналізу встановлено, що недостатньо дослідженими залишаються питання інтеграції таймерних сигнальних конструкцій із методами прямого розширення спектра для забезпечення комплексного захисту інформації на фізичному рівні. Це обумовлює необхідність розроблення методів формування широкосмугових таймерних сигналів із підвищеними показниками структурної та енергетичної прихованості.

На основі проведеного аналізу сформульовано наукове завдання дисертаційного дослідження, яке полягає у розробленні методів захисту інформації шляхом підвищення прихованості передавання сигнально-кодових конструкцій на основі прямого розширення спектра таймерних сигналів псевдовипадковими послідовностями.

*У другому розділі* проведено комплексне дослідження таймерних сигнальних конструкцій як перспективної основи побудови захищених інформаційно-комунікаційних систем, призначених для забезпечення захисту інформації від несанкціонованого доступу, виявлення та перехоплення в умовах

радіоелектронного протиборства. Основну увагу зосереджено на аналізі принципів формування таймерних сигналів, їх інформаційних характеристик та оцінюванні можливостей використання для забезпечення структурної прихованості, завадостійкості та підвищення рівня кіберзахисту каналів зв'язку.

Розглянуто метод таймерного кодування, за якого інформація передавалася не фіксованими позиціями імпульсів, а тривалостями часових інтервалів між значущими моментами модуляції. Показано, що такий метод забезпечує суттєве розширення множини можливих сигнальних реалізацій порівняно з класичними позиційними та розрядно-цифровими кодами, створюючи додатковий рівень невизначеності структури сигналу для стороннього спостерігача та засобів радіоелектронної розвідки.

Проведено аналіз інформаційних властивостей таймерних сигналів із використанням ентропійного аналізу та положень теорії інформації. На основі співвідношень Шеннона та Хартлі досліджено взаємозв'язок між кількістю можливих сигнальних реалізацій, інформаційною ємністю сигналу та рівнем структурної прихованості. Показано, що зростання ансамблю сигнальних конструкцій призводить до збільшення ентропії сигналу та ускладнює процедури його виявлення, класифікації, аналізу та дешифрування.

Проведено оцінювання взаємної інформації в захищених каналах зв'язку з урахуванням впливу шумових факторів, навмисних завад та засобів радіоелектронної боротьби. Показано, що використання таймерного кодування сприяє зменшенню інформаційної доступності сигналу для засобів перехоплення, підвищуючи рівень захисту інформації та стійкість систем передавання даних до кіберзагроз.

Досліджено вплив параметрів побудови таймерних сигналів на кількість реалізацій, показник структурної прихованості та ймовірність розкриття структури сигналу. Розглянуто можливість формування таймерних сигналів на основі системи залишкових класів. Показано, що поєднання властивостей завадостійкого кодування, спектрального розширення та таймерного подання інформації створює передумови для побудови комбінованих сигнально-кодових конструкцій із

підвищеним рівнем захищеності інформації, структурної прихованості та достовірності передавання.

Отримані результати підтвердили ефективність використання таймерних сигнальних конструкцій як основи побудови захищених інформаційно-комунікаційних систем та сформували теоретичне підґрунтя для подальшого розроблення методів комбінованого забезпечення структурної прихованості, завадостійкості та захисту інформації в умовах радіоелектронного протиборства.

*У третьому розділі* досліджено теоретичні та прикладні аспекти розширення спектра таймерних сигналів на основі псевдовипадкових послідовностей для забезпечення захисту інформації в інформаційно-комунікаційних системах. Розглянуто принципи прямого розширення спектра та особливості їх адаптації до таймерних сигнальних конструкцій, у яких інформаційні ознаки визначаються часовими параметрами сигналу. Проведено аналіз кореляційних, структурних і статистичних властивостей класичних псевдовипадкових послідовностей, зокрема М-послідовностей, кодів Голда, Касамі та Уолша, а також досліджено їх придатність для формування широкосмугових сигналів із підвищеним рівнем структурної та енергетичної прихованості.

Показано обмеження класичних лінійних псевдовипадкових послідовностей, пов’язані з передбачуваністю механізмів їх генерації та недостатнім рівнем структурної прихованості, що створює передумови для виявлення й аналізу сигналів засобами радіоелектронної розвідки. Обґрунтовано доцільність використання хаотичних генераторів як джерела псевдовипадкових послідовностей для формування шумоподібних сигналів із підвищеним рівнем захисту інформації. Досліджено методи підвищення криптостійкості хаотичних послідовностей, спрямовані на покращення їх статистичних і кореляційних характеристик та наближення властивостей сформованих сигналів до білого шуму.

Досліджено вплив бази сигналу на рівень енергетичної прихованості, завадостійкість, частотну та енергетичну ефективність систем передавання інформації. Встановлено, що збільшення бази сигналу забезпечує зменшення спектральної щільності потужності, підвищує виграш від кореляційної обробки та

знижує ймовірність помилки приймання, хоча одночасно супроводжується зменшенням частотної ефективності каналу.

Отримані результати підтвердили перспективність застосування широкосмугових таймерних сигналів, сформованих із використанням хаотичних псевдовипадкових послідовностей та системи залишкових класів, для побудови захищених інформаційно-комунікаційних систем, що забезпечують підвищення рівня захисту інформації від виявлення, перехоплення та несанкціонованого доступу в умовах радіоелектронного протиборства.

*У четвертому розділі* досліджено кореляційні властивості широкосмугових таймерних сигнальних конструкцій та виконано оцінювання їх ефективності щодо забезпечення захисту інформації в умовах радіоелектронного протиборства та кіберзагроз. Розглянуто особливості інтерпретації бази широкосмугових таймерних сигналів з урахуванням особливості таймерного кодування та змінної часової структури сигнальних конструкцій. Обґрунтовано необхідність адаптації класичних методів прямого розширення спектра до умов формування таймерних сигналів як механізму підвищення енергетичної та структурної прихованості передавання інформації.

Досліджено процес синтезу широкосмугових таймерних сигналів із використанням псевдовипадкових послідовностей та показано принципи узгодження параметрів таймерних конструкцій і послідовностей розширення спектра. Встановлено, що використання псевдовипадкових послідовностей забезпечує формування шумоподібних сигналів із керованими спектральними характеристиками, що сприяє підвищенню рівня захисту інформації від виявлення, перехоплення та аналізу засобами радіоелектронної розвідки.

Розглянуто особливості кореляційного приймання широкосмугових таймерних сигналів та відновлення їх часової структури. Показано відмінності між кореляційним прийманням таймерних і класичних позиційних широкосмугових сигналів, які полягають у необхідності визначення значущих моментів відновлення імпульсів сигнальної конструкції. Проаналізовано вплив кореляційного стискання спектра на завадостійкість та ефективність приймання сигналів за низьких значень

відношення сигнал/шум, що є важливим для забезпечення достовірності передавання інформації в умовах навмисних завад.

Окрему увагу приділено оцінюванню структурної прихованості широкосмугових таймерних сигналів. Досліджено вплив параметрів таймерних конструкцій, бази розширення спектра та типу модуляції на загальний рівень структурної невизначеності сигналу. Доведено, що структурна прихованість забезпечується внаслідок комплексної взаємодії непозиційної часової структури сигналу, псевдовипадкового спектрального маскування та властивостей системи модуляції, що ускладнює виявлення й ідентифікацію сигнальних конструкцій сторонніми засобами спостереження.

Проведено аналіз кореляційних властивостей шумоподібних таймерних сигналів, сформованих на основі різних псевдовипадкових послідовностей, та досліджено вплив часової структури таймерних конструкцій на значення кореляційних показників. Визначено, що використання таймерного кодування змінює кореляційні властивості широкосмугових сигналів, підвищує складність їх прогнозування та ускладнює відновлення структури сигналу засобами радіоелектронної розвідки, що сприяє підвищенню рівня захисту інформації в інформаційно-комунікаційних системах.

Отримані результати підтверджують перспективність використання широкосмугових таймерних сигнальних конструкцій для побудови захищених систем передавання інформації, у яких поєднуються властивості спектрального розширення, кореляційного виділення та структурного маскування сигналів, забезпечуючи підвищення стійкості до кіберзагроз, перехоплення та несанкціонованого доступу.

У висновках дисертаційної роботи викладено основні результати та рекомендації, що випливають із проведених досліджень, а також наведено кількісні оцінки ефективності запропонованих рішень.

У додатках до дисертації наведено акти впровадження результатів дослідження, а також перелік наукових праць і матеріалів апробації за темою дисертації.

**Ключові слова:** інформаційно-комунікаційні системи, прихованість передавання, таймерні сигнальні конструкції, широкосмугові таймерні сигнали, розширення спектра, шумоподібні сигнали, псевдовипадкові послідовності, послідовності Уолша, хаотичні коливання, кореляційні характеристики, автокореляція, взаємна кореляція, інтерпретація бази сигналу, структурна прихованість, енергетична прихованість, радіоелектронне протиборство, спектральний аналіз, імітаційне моделювання.

## SUMMARY

**Havel S. M.** Enhancement of Information Transmission Concealment Based on Direct Spread Spectrum Timer Signal Constructions – 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 scientific justification and a novel solution to the pressing scientific and technical problem of protecting information from unauthorized access in information and communication systems operating under conditions of electronic warfare, by enhancing the concealment of its transmission. The proposed solutions are based on the combined use of non-positional timer signal constructions and direct spread spectrum with pseudorandom sequences to form broadband noise-like signals, taking into account the energy, frequency, and informational constraints of the communication channel.

The work develops a method for improving information security at the physical layer by simultaneously ensuring structural and energy concealment of signal-code constructions. To assess the level of information protection, approaches are proposed for the quantitative determination of indicators of structural and energy concealment of broadband timer signals. The enhancement of concealment is achieved through the adaptation of parameters for forming timer signal constructions, the choice of the spreading basis, and the use of pseudorandom and chaotic sequences under non-stationary conditions of the communication channel.

*The aim of the dissertation* is to develop a method for information protection in information and communication systems by enhancing the structural and energy concealment of signal-code constructions transmission based on direct spread spectrum of timer signals using pseudorandom sequences.

*The object of the research* is the processes of information protection in information and communication systems at the physical layer through the formation and transmission

of broadband noise-like signal-code constructions under conditions of electronic countermeasures.

*The subject of the research* is the method of direct spread spectrum of timer signal constructions based on Walsh pseudorandom sequences and sequences formed on the basis of chaotic oscillations, as well as methods for evaluating their structural and energy concealment.

**In the introduction**, the relevance of the dissertation topic is justified, the research purpose and scientific-applied tasks necessary for its achievement are formulated, the connection of the research with scientific programs and topics is demonstrated, the scientific novelty of the obtained results, their practical value, and the personal contribution of the applicant are presented. Information about the approbation of the work's results, the personal contribution of the applicant, and their publications is provided.

In the **first chapter** of the dissertation, an analysis of the current state of scientific research in the field of ensuring the concealment of information transmission in information and communication systems operating under conditions of electronic warfare is conducted. The main threats to information and communication systems from electronic intelligence, radio monitoring, and active radio suppression means, which can lead to interception, detection, or disruption of signal construct transmission processes, are considered.

The concept of information transmission concealment is analyzed, and the main indicators for its evaluation are defined, including energy, spectral, and structural concealment of signals. It is established that the effectiveness of signal detection is largely determined by their spectral, temporal, and correlation characteristics, which are used by electronic intelligence means for signal analysis and identification in the communication channel.

An analysis of classical methods for enhancing the concealment of signal constructs is carried out, including modulation methods, cryptographic protection, noise-resistant coding, and frequency-time transformations of signals. It is shown that although these methods allow for improving the security of information transmission, they have

limitations in terms of ensuring an adequate level of spectral and correlation concealment of signals under modern conditions of electronic warfare.

Methods of signal spectrum spreading, widely used to enhance concealment and noise immunity of information transmission, are analyzed. The principles of using pseudorandom, orthogonal, and quasi-orthogonal sequences for forming spread spectrum signals are investigated, and the limitations of traditional DSSS approaches regarding their detection by correlation analysis means are determined.

The principles of construction and application features of timer signal constructs in covert information transmission systems are considered. Their advantages in enhancing the structural concealment of signals are demonstrated, and potential vulnerabilities of such constructs in the case of using classical methods of spectral and correlation analysis are identified.

Based on the analysis of modern approaches to the formation of noise-like signals, it was established that the issue of spectrum spreading of timer signal constructs and the management of their correlation properties has been insufficiently studied. This necessitates the development of new methods for synthesizing spread spectrum timer signal constructs capable of providing an enhanced level of concealment for information transmission under conditions of electronic warfare.

Based on the results of the analysis, the scientific task of the dissertation research was formulated, which consists in developing methods for forming spread spectrum timer signal constructs with controlled spectral and correlation properties to enhance the concealment of information transmission.

In the **second chapter**, a comprehensive study of timer signal constructions as a promising foundation for building secure information and communication systems designed to protect information from unauthorized access, detection, and interception under conditions of electronic warfare is carried out. The main focus is placed on the analysis of the principles of timer signal formation, their informational characteristics, and the evaluation of their potential use for ensuring structural concealment, noise immunity, and enhancing the level of cybersecurity of communication channels.

The method of timer coding is considered, in which information is transmitted not by fixed pulse positions but by the durations of time intervals between significant modulation moments. It is shown that this method provides a substantial expansion of the set of possible signal realizations compared to classical positional and digit-based codes, creating an additional level of uncertainty in the signal structure for external observers and electronic intelligence means.

An analysis of the informational characteristics of timer signals based on the entropy approach and the principles of information theory is conducted. Using Shannon and Hartley relations, the relationship between the number of possible signal realizations, the information capacity of the signal, and the level of structural concealment is investigated. It is demonstrated that the growth of the ensemble of signal constructions leads to an increase in signal entropy and complicates the procedures of detection, classification, analysis, and decryption.

An evaluation of mutual information in secure communication channels is performed, taking into account the influence of noise factors, intentional interference, and electronic warfare means. It is shown that the use of timer coding reduces the informational accessibility of the signal for interception means, thereby increasing the level of information protection and the resilience of data transmission systems to cyber threats.

The influence of timer signal construction parameters on the number of realizations, the indicator of structural concealment, and the probability of revealing the signal structure is studied. The possibility of forming timer signals based on the system of residual classes is considered. It is shown that the combination of properties of noise-resistant coding, spectral spreading, and timer-based information representation creates prerequisites for the development of combined signal-code constructions with enhanced levels of information security, structural concealment, and transmission reliability.

The obtained results confirmed the effectiveness of using timer signal constructions as a basis for building secure information and communication systems and formed the theoretical foundation for further development of methods for combined provision of

structural concealment, noise immunity, and information protection under conditions of electronic warfare.

In the **third chapter**, theoretical and applied aspects of timer signal spectrum spreading based on pseudorandom sequences for ensuring information protection in information and communication systems are investigated. The principles of direct spread spectrum and the features of their adaptation to timer signal constructions, in which informational features are determined by the temporal parameters of the signal, are considered. An analysis of the correlation, structural, and statistical properties of classical pseudorandom sequences, including M-sequences, Gold codes, Kasami codes, and Walsh sequences, is carried out, and their suitability for forming broadband signals with an enhanced level of structural and energy concealment is examined.

The limitations of traditional linear pseudorandom sequences are demonstrated, associated with the predictability of their generation mechanisms and insufficient structural concealment, which creates prerequisites for the detection and analysis of signals by electronic intelligence means. The expediency of using chaotic generators as sources of pseudorandom sequences for forming noise-like signals with an increased level of information protection is substantiated. Methods for enhancing the cryptographic resistance of chaotic sequences are studied, aimed at improving their statistical and correlation characteristics and approximating the properties of the generated signals to white noise.

The influence of the signal base on the level of energy concealment, noise immunity, frequency, and energy efficiency of information transmission systems is investigated. It is established that increasing the signal base reduces the spectral power density, enhances the gain from correlation processing, and decreases the probability of reception error, although it is simultaneously accompanied by a reduction in the frequency efficiency of the channel.

The obtained results confirmed the prospects of applying broadband timer signals formed using chaotic pseudorandom sequences and the system of residual classes for building secure information and communication systems that ensure an increased level of

information protection against detection, interception, and unauthorized access under conditions of electronic warfare.

In the **fourth chapter**, the correlation properties of broadband timer signal constructions are investigated, and their effectiveness in ensuring information protection under conditions of electronic warfare and cyber threats is evaluated. The peculiarities of interpreting the base of broadband timer signals are considered, taking into account the specifics of timer coding and the variable temporal structure of signal constructions. The necessity of adapting classical direct spread spectrum methods to the conditions of timer signal formation as a mechanism for enhancing the energy and structural concealment of information transmission is substantiated.

The process of synthesizing broadband timer signals using pseudorandom sequences is studied, and the principles of matching the parameters of timer constructions and spreading sequences are demonstrated. It is established that the use of pseudorandom sequences enables the formation of noise-like signals with controlled spectral characteristics, which contributes to increasing the level of information protection against detection, interception, and analysis by electronic intelligence means.

The peculiarities of correlation reception of broadband timer signals and the restoration of their temporal structure are examined. The differences between correlation reception of timer and classical positional broadband signals are shown, consisting in the necessity of determining significant moments for restoring the pulses of the signal construction. The influence of correlation compression of the spectrum on noise immunity and the effectiveness of signal reception at low signal-to-noise ratios is analyzed, which is important for ensuring the reliability of information transmission under conditions of intentional interference.

Special attention is paid to the evaluation of structural concealment of broadband timer signals. The influence of timer construction parameters, spreading base, and modulation type on the overall level of structural uncertainty of the signal is investigated. It is proven that structural concealment is ensured as a result of the complex interaction of the non-positional temporal structure of the signal, pseudorandom spectral masking,

and the properties of the modulation system, which complicates the detection and identification of signal constructions by external observation means.

An analysis of the correlation properties of noise-like timer signals formed on the basis of different pseudorandom sequences is carried out, and the influence of the temporal structure of timer constructions on the values of correlation indicators is studied. It is determined that the use of timer coding changes the correlation properties of broadband signals, increases the complexity of their prediction, and complicates the restoration of the signal structure by electronic intelligence means, thereby contributing to the enhancement of information protection in information and communication systems.

The obtained results confirm the prospects of using broadband timer signal constructions for building secure information transmission systems, in which the properties of spectral spreading, correlation extraction, and structural masking of signals are combined, ensuring increased resilience to cyber threats, interception, and unauthorized access.

In the **conclusions** of the dissertation, the main results and recommendations derived from the conducted research are presented, and quantitative assessments of efficiency indicators under the conditions of using the proposed solutions are provided.

In the **appendices** to the dissertation, the acts of implementation of the dissertation results, as well as the list of scientific works and approbations of the author on the dissertation topic, are included.

**Keywords:** information and communication systems, transmission concealment, timer signal constructions, broadband timer signals, spread spectrum, noise-like signals, pseudorandom sequences, Walsh sequences, chaotic oscillations, correlation characteristics, autocorrelation, cross-correlation, signal base interpretation, structural concealment, energy concealment, electronic warfare, spectral analysis, simulation modeling.

## ПЕРЕЛІК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

***Наукові праці, в яких опубліковано наукові результати дисертації:***

1. 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. https://doi.org/10.15587/2706-5448.2026.353067 **(Scopus)**

2. Zaharchenko , M. ., Hadzhyiev , M. ., Salmanov , N. ., Shvets , N., & Havel , S. . (2021). Аналіз і оцінка якісних і кількісних показників інформації при вирішенні завдань побудови систем передачі і перетворення даних. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 3(11), 136–143. https://doi.org/10.28925/2663-4023.2021.11.136143

3. Корчинський, В., Гавель, С., Сєдов, К., Севастєєв, Є., & Лімарь, І. (2025). Метод захисту інформації на основі системи залишкових класів при формуванні таймерних сигналів. Measuring and computing devices in technological processes, (3), 204–209. https://doi.org/10.31891/2219-9365-2025-83-37

4. Корчинський, В., Рябуха, О., Халед, А.-Ф., Гавель, С., Міненко, В., & Криштафор, З. (2023). Дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей. *Measuring and computing devices in technological processes*, (1), 180–186. https://doi.org/10.31891/2219-9365-2023-73-1-24

5. 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

6. 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. Lviv Polytechnic National University, Vol. 11, No. 11, 50-55. https://doi.org/10.23939/acps2026.01.050

***Наукові праці, які засвідчують апробацію матеріалів дисертації:***

7. Гавель С.М., Славич В.О., Петровський Р.І., Комісар В.В. Методи формування шумоподібного сигналу на основі дискретних генераторів хаосу. 80-та ювілейна Міжнародна науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів і студентів. 26 листопада 2025 року. ДУТІЗ. С.308-311.

8. Корчинський, В., Рябуха, О., Бєлова, Ю., Степанов, В., & Гавель, С. (2024). Методи захисту інформації на основі розширення спектра сигналу. Scientific Collection «InterConf», (208), 216–220. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/6685

9. Гавель С. М., Беспятенко С. В. Захист інформації від несанкціонованого доступу в умовах радіоелектронного конфлікту. Матеріали 78-ї Міжнародної науково-технічної конференції професорсько-викладацького складу, науковців, аспірантів та студентів (Одеса, 21–23 листопада 2023 р.). Одеса : ДУІТЗ, 2023. С. 111–113.

10. Гавель С.М., Мар'ян М.О., Перун І.П. Перспективи використання динамічного хаосу в системах захисту інформації Impact of Artificial Intelligence and Other Technologies on Sustainable Development: Proceedings of the 1st International Scientific and Practical Internet Conference, December 28-29, 2023. FOP Marenichenko V.V., Dnipro, Ukraine, p. 48-50. http://www.wayscience.com/wp-content/uploads/2024/01/Conference-Proceedings-December-28-29-2023.pdf

11. Корчинський В.В., Гавель С.М., Донкогло А.С., Галиця О.Т. Аналіз і дослідження методів підвищення захисту передаваної інформації на основі хаотичних коливань 79-а науково-технічна конференція професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів. Одеса 2023. (21-23 листопада 2024). С. 94-96.

12. Гавель С.М., Славич В. О., Мар'ян М. О., Прилуцький А. О., Гавреш І.Р. Методи підвищення криптостійкості псевдовипадкових послідовностей, що формуються на основі генераторів хаосу. 1 Міжнародна науково-практична інтернет-конференція Reimagining the future: collaborative solutions for global problems 9-10 жовтня 2025 року. С. 66-68.

http://www.wayscience.com/wp-content/uploads/2025/10/Conference-Proceedings-October-9-10-2025-1.pdf

13. Serhii Havel, Yevhen Vasiliu, Nikolaos Bardis, Sergii Staikutsa. Eavesdropping Attack of Two Eavesdroppers on the Ping-Pong Protocol with GHZ triplets. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 4-6 September, 2025, Gliwice, Poland P. 329-335/ **(SCOPUS)** ISSN 1424-8220

https://ieeexplore.ieee.org/xpl/conhome/11321922/proceeding

14. 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.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

НСД – несанкціонований доступ

РЕБ – радіоелектронна боротьба

СКК – сигнально-кодова конструкція

РЦК – розрядно-цифровий код;

ТСК – таймерна сигнальна конструкція

ІКС – інфокомунікаційна система

ЕОМ – електронна обчислювальна машина;

ЗММ – значущий момент модуляції;

ЗМВ – значущий момент відтворення;

ПД – передавання даних;

ППС – пристрій перетворення сигналів;

СПД – система передавання даних;

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

ПРС-ПВП – пряме розширення спектра за допомогою псевдовипадкових послідовностей;

ППРЧ – псевдовипадкове перелаштування робочої частоти;

ЧМ – частотна модуляція;

ФМ – фазова модуляція;

АФМ – амплітудно-фазова модуляція;

КК – кодова комбінація;

ПВП – псевдовипадкова послідовність;

ВО – виграш при обробці;

ВКФ – взаємо-кореляційна функція;

АКФ – автокореляційна функція;

ЕМС – електромагнітна сумісність;

# ВСТУП

**Актуальність.** Розвиток інформаційно-комунікаційних систем супроводжується постійним зростанням обсягів інформації, що передається бездротовими каналами зв'язку. Водночас підвищуються можливості засобів радіоелектронної розвідки, технічного моніторингу та аналізу сигналів, що створює додаткові загрози перехоплення інформації та отримання несанкціонованого доступу до інформаційних ресурсів. За таких умов особливого значення набуває захист інформації на фізичному рівні шляхом підвищення прихованості передавання сигнально-кодових конструкцій.

Одним із перспективних напрямів забезпечення захисту інформації є використання сигнальних конструкцій зі складною часовою структурою та широкосмугових шумоподібних сигналів, параметри яких ускладнюють виявлення факту передавання інформації, визначення структури сигналу та відновлення переданих даних засобами радіоелектронної розвідки. У цьому контексті значний науковий інтерес становлять таймерні сигнальні конструкції, в яких інформація передається за рахунок часових параметрів сигналу, що забезпечує додатковий рівень структурної прихованості.

Вагомий внесок у розвиток методів захисту інформації, теорії сигналів, завадостійкого кодування та технологій розширення спектра зробили М. Захарченко, В. Кільдішев, Л. Політанський, А. Семенко, А. Зюко, В. Банкет, Б. Радзімовський, К. Шеннон, А. Камінський, В. Гордійчук, Аль-Файюмі Халед та інші науковці. Разом із тим питання забезпечення структурної та енергетичної прихованості інформації на основі широкосмугових таймерних сигнальних конструкцій залишаються недостатньо дослідженими.

Існуючі методи захисту інформації на фізичному рівні, зокрема класичні методи модуляції та прямого розширення спектра, переважно орієнтовані на забезпечення завадостійкості та енергетичної прихованості. При цьому структура використовуваних сигналів і псевдовипадкових послідовностей часто залишається

передбачуваною, що створює можливість їх виявлення та аналізу сучасними засобами радіоелектронної розвідки. Це зумовлює необхідність розроблення нових методів формування сигнально-кодових конструкцій із підвищеним рівнем структурної прихованості.

Перспективним напрямом розв’язання зазначеної проблеми є поєднання таймерних сигнальних конструкцій із технологією прямого розширення спектра на основі псевдовипадкових послідовностей. Такий метод дозволяє формувати широкосмугові шумоподібні сигнали зі складною часовою, спектральною та кореляційною структурою, що ускладнює їх виявлення, класифікацію та відновлення параметрів передавання.

Особливий інтерес становить використання ортогональних послідовностей Уолша та псевдовипадкових послідовностей, сформованих на основі хаотичних коливань. Властивості динамічного хаосу, зокрема чутливість до початкових умов, непередбачуваність та висока структурна складність, створюють передумови для синтезу широкосмугових сигналів із підвищеним рівнем структурної прихованості та низькою кореляційною детектованістю.

У зв’язку з цим актуальним науковим завданням є розроблення методів захисту інформації від несанкціонованого доступу шляхом підвищення структурної та енергетичної прихованості сигнально-кодових конструкцій на основі прямого розширення спектра таймерних сигналів псевдовипадковими послідовностями, а також розроблення методів оцінювання рівня такого захисту за показниками прихованості.

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

Дисертаційна робота підготовлена у відповідності до основних положень Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах», Стратегії кібербезпеки України. Тема дослідження пов’язана з науковими напрямами, сформульованими в п. 1.2.9 та п. 1.2.9.5 – теорія та комп’ютерні технології інформаційної безпеки "Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і

гуманітарних наук національної академії наук України на 2024–2028 роки", затверджених постановою Президії НАН України від 10.01.2024 №8. Тематика дисертаційного дослідження відповідає стандарту та фаховим компетентностям освітньо-наукової програми підготовки докторів філософії з кібербезпеки Державного університету інтелектуальних технологій і зв'язку Міністерства освіти і науки України та спрямована на проведення фундаментальних і прикладних наукових досліджень у галузі захисту інформації, зокрема щодо розробки методів підвищення прихованості передавання даних з використанням таймерних сигнальних конструкцій, широкосмугових шумоподібних сигналів та псевдовипадкових послідовностей. Результати досліджень дисертаційної роботи увійшли до складу науково-технічного звіту з держбюджетної науково-дослідною роботою за темою: «Розроблення методів підвищення захищеності передавання інформації в інформаційно-комунікаційних системах на основі інтегрованих сигнально-кодових перетворень» (державний реєстраційний номер 0126U002946).

**Метою дисертаційної роботи** є розроблення методу захисту інформації в інформаційно-комунікаційних системах шляхом підвищення структурної та енергетичної прихованості передавання сигнально-кодових конструкцій на основі прямого розширення спектра таймерних сигналів псевдовипадковими послідовностями.

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

1) провести аналіз сучасних методів захисту інформації шляхом забезпечення прихованості передавання інформації та визначити обмеження існуючих позиційних сигнальних конструкцій і методу прямого розширення спектра щодо забезпечення енергетичної та структурної прихованості;

2) розробити інтегрований метод захисту інформації на основі формування широкосмугових шумоподібних таймерних сигналів із використанням таймерних сигнальних конструкцій та прямого розширення спектра псевдовипадковими послідовностями, а також дослідити їх спектральні й кореляційні характеристики

щодо забезпечення структурної та енергетичної прихованості передавання інформації;

3) розробити метод визначення інтерпретованої бази для розширення спектра непозиційних таймерних сигналів та дослідити її вплив на показники енергетичної прихованості, завадостійкості й ефективності захисту інформації від виявлення та перехоплення;

4) розробити метод формування та розширення спектра таймерних сигналів на основі системи залишкових класів, послідовностей Уолша та хаотичних псевдовипадкових послідовностей для забезпечення захисту інформації шляхом поєднання властивостей завадостійкого кодування і структурної прихованості;

5) розробити методику оцінювання структурної прихованості широкосмугових шумоподібних таймерних сигналів як показника захищеності інформації від виявлення та несанкціонованого доступу, а також виконати порівняльне оцінювання ефективності запропонованих методів відносно позиційних сигнальних конструкцій;

6) провести математичне та імітаційне моделювання процесів формування і передавання широкосмугових таймерних сигнальних конструкцій та оцінити ефективність запропонованих методів захисту інформації за показниками структурної й енергетичної прихованості та завадостійкості.

*Об'єкт дослідження* – процеси захисту інформації в інформаційно-комунікаційних системах на фізичному рівні шляхом формування та передавання широкосмугових шумоподібних сигнально-кодових конструкцій в умовах радіоелектронної протидії.

*Предмет дослідження* – метод прямого розширення спектра таймерних сигнальних конструкцій на основі псевдовипадкових послідовностей Уолша та послідовностей, сформованих на основі хаотичних коливань, а також методи оцінювання їх структурної та енергетичної прихованості.

**Методи дослідження**. У дисертаційній роботі використано методи теорії інформації, теорії сигналів і систем, теорії кодування, теорії ймовірностей та теорії випадкових процесів. Методи системного аналізу застосовано для дослідження

інформаційно-комунікаційних систем в умовах радіоелектронного протиборства та забезпечення захисту інформації від несанкціонованого доступу. Методи математичного та імітаційного моделювання використано для аналізу процесів формування таймерних сигнально-кодових конструкцій, синтезу широкосмугових шумоподібних сигналів і дослідження їх характеристик. Методи спектрального, кореляційного та статистичного аналізу застосовано для оцінювання енергетичної та структурної прихованості сигналів, а також визначення ефективності захисту інформації від виявлення, перехоплення та відновлення структури повідомлень. Методи теорії оптимального приймання сигналів використано для дослідження процесів кореляційного приймання широкосмугових таймерних сигналів. Методи чисельного експерименту та порівняльного аналізу застосовано для перевірки достовірності отриманих результатів і оцінювання ефективності запропонованих методів порівняно з відомими сигнальними конструкціями.

**Наукова новизна одержаних результатів полягає в наступному:**

1. *Вперше* розроблено інтегрований метод захисту інформації на основі підвищення прихованості передавання сигнально-кодових конструкцій шляхом формування широкосмугових шумоподібних таймерних сигналів із використанням псевдовипадкових послідовностей. На відміну від існуючих методів прямого розширення спектра, запропонований метод забезпечує керовані кореляційні та спектральні властивості сигналів завдяки адаптивному вибору параметрів таймерних сигнальних конструкцій, що підвищує їхню стійкість до кіберзагроз.

2. *Удосконалено* інтегровану методику оцінювання структурної прихованості шумоподібного таймерного сигналу, яка, на відміну від існуючих методів оцінювання, враховує сумарний внесок структурної прихованості таймерних сигнально-кодових конструкцій, псевдовипадкових послідовностей прямого розширення спектра та використаної системи модуляції. Це дозволяє комплексно визначати рівень ефективності сигналів у забезпеченні захисту інформації, завадостійкості та стійкості до кіберзагроз.

3. *Вперше* запропоновано поняття інтерпретованої бази широкосмугового таймерного сигналу, яке, на відміну від класичного поняття бази позиційного

сигналу, враховує розширення спектра на інтервалі формування всієї таймерної комбінації, а не окремого позиційного імпульсу. Це забезпечує новий метод оцінювання прихованості та завадостійкості сигнально-кодових конструкцій як механізму захисту інформації в інформаційно-комунікаційних системах.

4. *Набув подальшого розвитку* метод розширення спектра таймерних сигналів, сформованих на основі системи залишкових класів, який поєднує функції завадостійкого кодування та структурної прихованості. На відміну від існуючих методів позиційного завадостійкого кодування, запропонований метод таймерного кодування не потребує введення додаткових перевірочних елементів і забезпечує підвищення рівня захисту інформації та стійкості систем до кіберзагроз.

5. *Удосконалено* метод розширення спектра таймерних сигналів за допомогою послідовностей Уолша та псевдовипадкових послідовностей, сформованих на основі хаотичних коливань. На відміну від класичних DSSS-методів, запропонований метод забезпечує динамічну зміну кореляційних властивостей шумоподібного сигналу під час передавання, що пояснюється впливом непозиційної структури таймерної комбінації на процес спектрального розширення. Це дозволяє підвищити рівень структурної прихованості та ефективність захисту інформації порівняно з позиційними сигналами, а також забезпечує стійкість систем до кіберзагроз.

**Практична значимість отриманих результатів** полягає у розробленні методів формування широкосмугових шумоподібних таймерних сигналів, які можуть бути використані під час створення та модернізації захищених інформаційно-комунікаційних систем, що функціонують в умовах радіоелектронного протиборства та кіберзагроз.

1. Розроблено інтегрований метод формування широкосмугових таймерних сигналів із використанням псевдовипадкових послідовностей, який забезпечує керування спектральними та кореляційними характеристиками сигналів, що дозволяє підвищити рівень їх енергетичної та структурної прихованості. Аналіз кореляційних властивостей показав, що коефіцієнт кореляції змінювався в межах $K_{\text{су}} = 0{,}125 \div 0{,}516$, що свідчить про низьку передбачуваність сигналів і високу

стійкість до кореляційного аналізу. Встановлено, що при базі сигналу $B > 64$ та відношенні сигнал/шум $h = 0{,}7$ забезпечується достатній рівень структурної прихованості за ймовірності спотворення таймерної сигнальної конструкції $p < 1{,}7482 \cdot 10^{-20}$.

2. Запропоновано метод визначення інтерпретованої бази широкосмугового таймерного сигналу, який може бути використаний під час проєктування систем із прямим розширенням спектра для обґрунтованого вибору параметрів сигналів залежно від вимог щодо прихованості, завадостійкості та ефективного використання частотного ресурсу. Використання співвідношення $B_{\text{ТСК}} = B(t_0) \cdot m$дозволяє враховувати особливості розширення спектра всієї непозиційної структури таймерної комбінації та забезпечує підвищення рівня захисту інформації в інформаційно-комунікаційних системах.

3. Запропонований метод розширення спектра таймерних сигналів, сформованих на основі системи залишкових класів, поєднує функції завадостійкого кодування та структурної прихованості. На відміну від позиційого завадостійкого кодування, запропонований метод не потребує введення додаткових перевірочних елементів і забезпечує збільшення кількості допустимих сигнальних комбінацій у 2,56 рази порівняно з кодом Хемінга $(7, 4)$ на однаковому інтервалі формування сигналу $T = 7t_0$. Це дозволяє підвищити рівень структурної прихованості, ефективність використання сигнального простору та стійкість інформаційно-комунікаційних систем до кіберзагроз у процесі передавання інформації.

4. Запропоновано інтегровану методику оцінювання структурної прихованості широкосмугових таймерних сигналів, яка враховує сумарний внесок таймерних сигнальних конструкцій, псевдовипадкових послідовностей розширення спектра та використаної системи модуляції. Методика базується на використанні інтегрального показника структурної прихованості $S_{\text{ТСК-ПВП}} = \log_2 N_{\text{ТСК}} + \log_2 N_{\text{ПВП}} + \log_2 N_{\text{см}}$, що дозволяє комплексно оцінювати рівень прихованості сигналів та ефективність їх застосування для захисту інформації.

4. Запропонована інтегрована методика оцінювання структурної прихованості шумоподібного таймерного сигналу враховує сумарний внесок структурної прихованості таймерних сигнальних конструкцій, псевдовипадкових послідовностей розширення та використаної системи модуляції. Інтегральний показник структурної прихованості широкосмугового таймерного сигналу може бути представлений як $S_{\text{ТСК}-\text{ПВП}} = \log_2 N_{\text{ТСК}} + \log_2 N_{\text{ПВП}} + \log_2 N_{\text{см}}$, що дозволяє комплексно оцінювати рівень прихованості сигналів та їхню ефективність у забезпеченні захисту інформації й стійкості до кіберзагроз.

5. Розроблений метод прямого розширення спектра таймерних сигналів, у якому для формування широкосмугових шумоподібних сигналів використовуються послідовності Уолша, хаотичні псевдовипадкові послідовності та сигнальні конструкції, сформовані на основі системи залишкових класів, дозволяє реалізувати комбінований механізм захисту інформації без суттєвого ускладнення структури сигнально-кодових конструкцій і може бути використаний під час побудови захищених каналів зв'язку та систем спеціального призначення. Так, для параметрів таймерних сигналів $m = 4$, $s = 5$, $i = 2$ кількість реалізацій становила 66, а при $i = 3$– 286, що відповідно у 4,1 та 17,9 раза перевищує кількість реалізацій еквівалентного розрядно-цифрового коду. Для параметрів $m = 10$, $s = 6$, $i = 4$, $B(t_0) = 128$та використанні ФМ-4 структурна прихованість при застосуванні кодів Уолша становила 25 дв. вим., тоді як при використанні хаотичних псевдовипадкових послідовностей вона досягала 146 дв. вим., що еквівалентно близько $2^{146}$ операціям перебору для відновлення структури сигналу. Це підтверджує високий рівень прихованості та стійкості до кіберзагроз у процесі передавання інформації.

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 полягає в тому, що розроблені методи формування та розширення спектра широкосмугових шумоподібних таймерних сигналів придатні для інженерного проєктування захищених радіотехнічних і

телекомунікаційних систем, що функціонують в умовах радіоелектронного протиборства та кіберзагроз. Це підтверджено актом впровадження основних результатів досліджень на підприємстві ТОВ «Технологічні Інноваційні Рішення».

**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 сигналів за допомогою псевдовипадкових послідовностей; [2] – оцінка якісних і кількісних показників інформації при вирішенні завдань побудови систем передавання і перетворення даних; [3] – розробка алгоритму побудови структури таймерних сигналі на основі системи залишкових класів; [4] – аналіз якісних характеристик послідовностей в залежності від початкових параметрів початкових параметрів програмних генераторів хаосу; [5] – проведення експериментальної частини роботи, аналіз та обговорення результатів дослідження; [6] – аналіз методів розширення спектра на основі хаотичних коливань, аналіз та обговорення результатів дослідження.

**Апробація результатів дисертації**. Основні положення та результати дисертаційної роботи доповідалися, обговорювалися та отримали позитивну оцінку на міжнародних і всеукраїнських науково-практичних конференціях, зокрема: на 78-й Міжнародній науково-технічній конференції професорсько-викладацького складу, науковців, аспірантів та студентів (Одеса, ДУІТЗ, 2023 р.); 1-й Міжнародній науково-практичній інтернет-конференції «Impact of Artificial Intelligence and Other Technologies on Sustainable Development» (Дніпро, 2023 р.); міжнародній науково-практичній конференції InterConf (2024 р.); 79-й Міжнародній науково-технічній конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів (Одеса, ДУІТЗ, 2024 р.); 80-й

ювілейній Міжнародній науково-технічній конференції професорсько-викладацького складу, науковців, аспірантів і студентів (Одеса, ДУІТЗ, 2025 р.); 1-й Міжнародній науково-практичній інтернет-конференції «Reimagining the Future: Collaborative Solutions for Global Problems» (2025 р.); 13-й Міжнародній конференції IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2025) (Глівіце, Польща, 2025 р.). Окремі результати дослідження також висвітлено у колективній монографії «Сталий розвиток і цифрові інновації» (Одеса, 2024 р.).

**Публікації.** За результатами досліджень по темі дисертаційної роботи опубліковано 14 наукових праць, у тому числі: 6 наукових статей у періодичних виданнях України [1-6], що включені до переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів, у тому числі одна стаття [1] у журналі, який цитується у наукометричній базі даних Scopus; 9 тез доповідей [7-14] в матеріалах наукових конференцій. Одна наукова праця включена до складу монографії [14]. Загальна кількість наукових праць у виданнях, які цитуються у наукометричних базах даних Scopus складає 2, з яких – 1 стаття та 1 теза до конференції [13].

**Структура та обсяг дисертації.** Дисертація складається зі вступу, чотирьох розділів, висновків, двох додатків і списку використаних джерел. Загальний обсяг роботи становить 181 сторінку, з яких 136 сторінок — основний текст, 8 сторінок – додатки, 14 сторінок – список використаних джерел, що містить 102 найменування. Робота містить 18 рисунків і 12 таблиць.

Під час виконання дисертаційного дослідження використовувалися інструменти штучного інтелекту, зокрема ChatGPT, для інформаційного пошуку, опрацювання літературних джерел і мовного редагування тексту. Остаточне формулювання змісту роботи, інтерпретація результатів досліджень, наукові положення та висновки виконані автором самостійно.

# РОЗДІЛ 1
# АНАЛІЗ СУЧАСНИХ МЕТОДІВ ПІДВИЩЕННЯ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ СИГНАЛЬНИХ КОНСТРУКЦІЙ В УМОВАХ РАДІОЕЛЕКТРОННОГО ПРОТИБОРСТВА

У першому розділі проведено аналіз сучасних загроз інформаційно-комунікаційним системам в умовах радіоелектронного протиборства та досліджено методи захисту інформації шляхом забезпечення прихованості передавання сигнально-кодових конструкцій. Проаналізовано спектральні, часові та кореляційні характеристики сигналів, що використовуються засобами радіоелектронної розвідки для їх виявлення й перехоплення. Виконано аналіз існуючих методів підвищення прихованості та визначено їх переваги й обмеження щодо забезпечення захисту інформації в інформаційно-комунікаційних системах. За результатами дослідження сформульовано наукову задачу розроблення широкосмугових таймерних сигнальних конструкцій з керованими спектральними та кореляційними властивостями для підвищення структурної та енергетичної прихованості передавання інформації.

## 1.1 Загрози інформаційно-комунікаційним системам в умовах радіоелектронного протиборства

Одним із напрямів захисту інформації від несанкціонованого доступу в інформаційно-комунікаційних системах (ІКС) є забезпечення прихованості передавання сигнально-кодових конструкцій фізичними каналами зв’язку [1-4]. ІКС, що використовують радіоканали передавання, у сучасних умовах функціонують під постійним впливом засобів радіоелектронного протиборства (РЕП), до складу яких належать системи радіоелектронної розвідки (РЕР), радіоелектронного перехоплення, радіомоніторингу та активного радіоелектронного подавлення [5, 6]. Зазначені засоби спрямовані як на порушення

працездатності каналів зв’язку, так і на виявлення, ідентифікацію та аналіз передаваних сигнальних конструкцій [7-11].

Завдання виявлення передаваного сигналу зводиться до задачі статистичної перевірки гіпотез [11]:

$$\begin{aligned} H_0 &: r(t) = n(t), \\ H_1 &: r(t) = s(t) + n(t), \end{aligned} \tag{1.1}$$

де: $r(t)$ – прийнятий сигнал на вході приймача або засобу радіорозвідки; $s(t)$ – корисний (інформаційний) сигнал, який намагаються передати; $n(t)$ – шум (як правило, адитивний білий гаусівський шум); $H_0$ – нульова гіпотеза: сигнал відсутній, приймається лише шум; $H_1$ – альтернативна гіпотеза: у прийнятому сигналі присутній корисний сигнал на фоні шуму.

Одним з ключових інструментів виявлення є спектральний аналіз, який ґрунтується на оцінюванні спектральної щільності потужності сигналу [11,12]:

$$S_x(f) = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} x(t)\ e^{-j2\pi ft}\, dt\ |^2, \tag{1.2}$$

Наявність виражених спектральних максимумів, вузькосмугових компонент або періодичних складових істотно полегшує виявлення сигналів засобами радіомоніторингу та радіоелектронної розвідки. У цьому контексті рівень енергетичної прихованості сигналу зазвичай оцінюється за відношенням сигнал/шум [12]:

$$\text{SNR} = \frac{P_s}{P_n}, \tag{1.3}$$

де $P_s$ – середня потужність корисного сигналу, $P_n$ – середня потужність шуму на вході приймального пристрою.

Для вузькосмугового передаваного сигналу зменшення значення SNR призводить до зниження енергетичної помітності сигналу та підвищення його прихованості, однак водночас це негативно впливає на завадостійкість і ймовірність безпомилкового приймання інформації.

Наявність виражених кореляційних піків або регулярної структури автокореляційної функції дозволяє ідентифікувати тип сигнальної конструкції, параметри кодування та використані псевдовипадкові послідовності. Таким чином, структурна прихованість сигналу визначається ступенем складності його кореляційної структури та відсутністю інформативних ознак у часовій і кореляційній областях.

В умовах радіоелектронного протиборства значну загрозу становлять також методи часово-частотного аналізу, зокрема вейвлет-перетворення та короткочасне перетворення Фур'є [13]:

$$X(t,f) = \int_{-\infty}^{\infty} x(\tau)\, w(\tau - t)\; e^{-j2\pi f\tau}\, d\tau, \qquad (1.4)$$

де: $x(\tau)$ – сигнал, $w(\tau - t)$ – вікно аналізу, $f$ – частота, $t$ – час. Використання цих методів дозволяє виявляти сигнали зі змінними параметрами та локальними часовими особливостями. Це є особливо актуальним для сигналів з непозиційною структурою, до яких належать таймерні сигнальні конструкції.

Активні засоби радіоелектронного придушення створюють додаткові загрози, оскільки примушують збільшувати потужність сигналу або вводити надлишковість для забезпечення завадостійкості. Це, у свою чергу, призводить до зростання енергетичної помітності сигналу та збільшує ймовірність його виявлення. Таким чином, виникає фундаментальне протиріччя між вимогами до завадостійкості та прихованості передавання.

Класичні позиційні сигнали та сигнали з фіксованими часовими інтервалами мають обмежені можливості щодо маскування в умовах сучасних засобів РЕР. Слід відзначити, що навіть класичні методи розширення спектра (DSSS), що використовують детерміновані або ортогональні псевдовипадкові послідовності,

можуть бути ідентифіковані за рахунок характерних кореляційних властивостей та стабільності спектральної структури [11-13].

У зв’язку з цим особливої уваги потребують таймерні сигнальні конструкції (ТСК), які формуються на основі змінних часових інтервалів між елементами сигналу [14]. Такі конструкції ускладнюють синхронізацію, кореляційний аналіз і часову локалізацію сигналів. Поєднання таймерних сигналів із методами спектрального розширення та псевдовипадковими послідовностями дозволяє формувати шумоподібні сигнали з низькою спектральною щільністю та складною кореляційною структурою [15-20].

Отже, аналіз загроз ІКС в умовах радіоелектронного протиборства показує, що подальший розвиток методів прихованого передавання інформації має бути спрямований на формування широкосмугових таймерних сигнальних конструкцій з керованими спектральними та кореляційними властивостями, що ускладнюють виявлення, ідентифікацію та аналіз сигналів сучасними засобами радіоелектронної розвідки.

## 1.2 Поняття прихованості передавання інформації та основні показники її оцінювання

У сучасних інформаційно-комунікаційних системах прихованість передавання інформації [21-23] визначається як здатність системи зв’язку забезпечувати конфіденційність даних шляхом зменшення ймовірності виявлення, перехоплення, ідентифікації або декодування повідомлення сторонніми спостерігачами, зокрема в умовах радіоелектронного протиборства [24, 25]. Забезпечення прихованості є одним із ключових завдань побудови захищених систем зв’язку, оскільки ефективність функціонування таких систем значною мірою залежить не лише від достовірності передавання інформації, але й від здатності протидіяти засобам радіоелектронної розвідки [26, 27].

Прихованість [21, 22] є складовою поняття завадозахищеності системи зв’язку, до складу якої також входить завадостійкість. При цьому

завадостійкість [14] характеризує здатність системи забезпечувати необхідну якість передавання інформації в умовах впливу випадкових чи навмисних завад, тоді як прихованість [21, 22] визначає рівень захисту сигналу від несанкціонованого виявлення, аналізу та відтворення.

У загальному випадку завадозахищеність характеризує комплексне завдання [20] забезпечення ефективного функціонування системи зв'язку в умовах радіоелектронної протидії та несанкціонованого доступу до інформації. Для оцінювання рівня захисту сигналів використовуються різні показники прихованості, серед яких основними є енергетична, структурна та інформаційна прихованість [21, 22]. Зазначені види прихованості визначають ефективність протидії засобам радіоелектронної розвідки на різних етапах обробки сигналу – від його виявлення до аналізу структури та дешифрування перехопленого повідомлення.

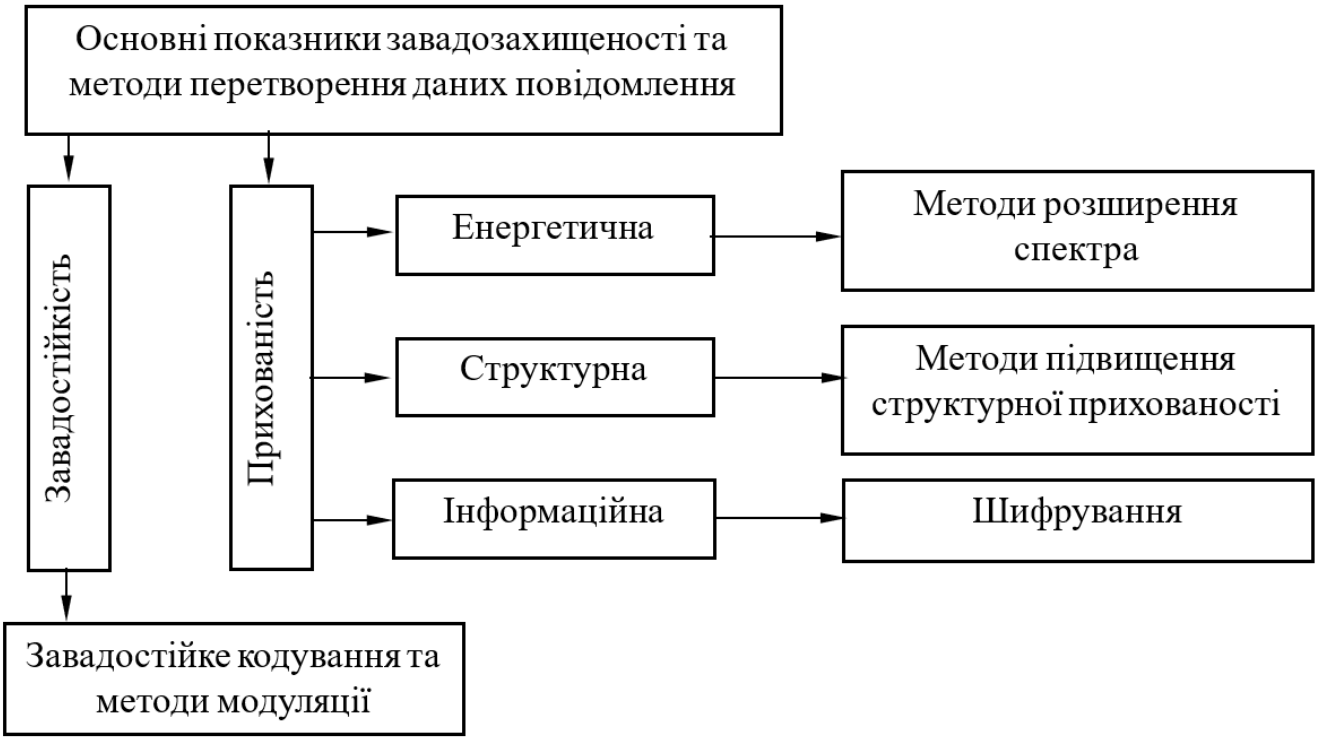



Рис. 1.1. Узагальнена модель забезпечення захисту інформації від засобів радіоелектронної розвідки

На рис. 1.1 наведено узагальнену модель забезпечення захисту інформації від засобів радіоелектронної розвідки, яка відображає взаємозв'язок між основними складовими завадозахищеності та методами формування і перетворення сигнально-кодових конструкцій. Представлена модель демонструє, що забезпечення захищеного передавання інформації в сучасних системах радіозв'язку є комплексним завданням, яке включає одночасне підвищення завадостійкості, енергетичної, структурної та інформаційної прихованості.

У моделі показано, що завадозахищеність системи формується за рахунок двох основних напрямів: забезпечення стійкості до впливу завад та прихованості передавання інформації від засобів радіоелектронної розвідки. При цьому завадостійкість спрямована на забезпечення необхідної достовірності приймання повідомлень в умовах дії випадкових, індустріальних або навмисних завад. Для цього використовуються методи завадостійкого кодування, адаптивної обробки сигналів, рознесення каналів, фільтрації та компенсації перешкод.

Другим важливим напрямом є забезпечення різних видів прихованості сигналу. Енергетична прихованість [21] базується на зменшенні ймовірності виявлення сигналу шляхом зниження його спектральної щільності потужності або маскування сигналу під шумові процеси. Для цього застосовуються методи розширення спектра, псевдовипадкового перестрибування робочих частот, хаотичні сигнали та інші широкосмугові технології.

Структурна прихованість пов'язана [21] з ускладненням аналізу структури сигнально-кодових конструкцій. Вона забезпечується за рахунок використання багатопозиційних та непозиційних методів кодування, псевдовипадкових послідовностей, таймерних сигнальних конструкцій, комбінованих методів маніпуляції та багатовимірного перетворення параметрів сигналу. У результаті для стороннього спостерігача суттєво ускладнюється процес синхронізації, класифікації та розпізнавання структури сигналу.

Інформаційна прихованість [21, 28-30] орієнтована безпосередньо на захист змісту повідомлення та досягається шляхом використання криптографічних методів перетворення інформації. При цьому навіть у випадку перехоплення

сигналу противник не має можливості відновити зміст повідомлення без знання криптографічного ключа або алгоритму шифрування.

Отже, наведена на рис. 1.1 модель свідчить, що сучасні системи захищеного радіозв'язку повинні реалізовувати комплексний метод забезпечення захисту інформації, який передбачає одночасне використання засобів підвищення завадостійкості, енергетичної, структурної та інформаційної прихованості залежно від умов функціонування системи та рівня радіоелектронної протидії.

## 1.3 Забезпечення енергетичної прихованості сигнально-кодових конструкцій

Енергетична прихованість сигналу характеризується його здатністю залишатися невиявленими на фоні шумів і завад завдяки оптимізації енергетичних параметрів. Основним показником тут є спектральна щільність потужності (СЩП) сигналу $S(f)$, яка визначається як розподіл потужності сигналу $x(t)$ по частоті $f$ [27]:

$$S(f) = \int_{-\infty}^{\infty} R_{xx}(\tau) e^{-j2\pi f\tau} d\tau, \tag{1.5}$$

де $R_{xx}(\tau)$ – автокореляційна функція сигналу, що описується виразом [27]:

$$R_{xx}(\tau) = \int_{-\infty}^{\infty} x(t)x(t+\tau)dt. \tag{1.6}$$

Енергетична прихованість безпосередньо залежить від рівня потужності сигналу $P_s$ та ширини смуги частот $B$. Чим нижча спектральна щільність потужності $S(f)$, тим складніше виявити сигнал на тлі шумів з спектральною щільністю $N_0$. Відношення сигнал/шум (SNR) визначається як [27]:

$$\text{SNR} = \frac{P_s}{N_0 B}. \tag{1.7}$$

Низьке значення SNR зменшує ймовірність виявлення сигналу $P_d$, яка залежить від порогового рівня виявлення $\gamma$та розподілу ймовірностей шумів і сигналу. Енергетична помітність сигналу оцінюється через відношення його потужності до рівня шумів у каналі передачі, а ймовірність виявлення $P_d$може бути виражена через функцію помилок [27]:

$$P_d = Q\left(\frac{\gamma-\sqrt{P_s}}{\sigma}\right), \tag{1.8}$$

де $Q$ – функція доповнювального розподілу нормального закону, $\sigma$ – середньоквадратичне відхилення шуму.

Структурна прихованість сигналу визначається складністю його кореляційної, спектральної та часової структури. Кореляційна структура сигналу описується автокореляційною функцією $R_{xx}(\tau)$, яка для сигналів з хорошою прихованістю повинна мати мінімальні виражені піки за винятком $\tau = 0$. Це ускладнює синхронізацію та виявлення сигналу противником. Спектральна структура сигналу повинна бути рівномірною, без характерних піків, що описується рівнянням:

$$S(f) \approx \text{const.} \tag{1.9}$$

Часова структура сигналу, особливо для таймерних сигнальних конструкцій, базується на використанні змінних часових інтервалів $\{T_i\}$ між елементами сигналу, що ускладнює часову локалізацію та аналіз. Такі сигнали можуть бути описані як [14]:

$$x(t) = \sum_{i=0}^{N-1} a_i\, p(t - t_i), \tag{1.10}$$

де $a_i$ – амплітуда $i$-го елементу сигналу, $p(t)$ – базовий імпульс, $t_i$ – випадкові або псевдовипадкові моменти появи імпульсів.

Спектральні, часові та кореляційні ознаки сигналів є ключовими факторами їх виявлення. Спектральні ознаки включають стабільність спектральної структури, наприклад, для сигналів з прямим розширенням спектру (ПРС-ПВП), де спектр $S(f)$ має характерні піки на певних частотах. Часові ознаки пов'язані з періодичністю або регулярністю часових інтервалів між елементами сигналу, що може бути описано як [14]:

$$T_i = T_0 + \Delta T_i, \tag{1.11}$$

де $T_0$ – базовий інтервал, $\Delta T_i$ – випадкова або псевдовипадкова зміна інтервалу. Кореляційні ознаки включають наявність виражених піків у автокореляційній функції $R_{xx}(\tau)$, що характерно для сигналів з детермінованими псевдовипадковими послідовностями. Для підвищення прихованості необхідно мінімізувати інформативність цих ознак. Це досягається шляхом використання широкосмугових сигналів з рівномірним спектром $S(f)$, таймерних сигнальних конструкцій зі змінними часовими інтервалами $\{T_i\}$, а також складних псевдовипадкових послідовностей з низькою автокореляцією. Застосування зазначених методів дозволяє ускладнити виявлення та аналіз сигналів системами радіоелектронної розвідки, забезпечуючи ефективну прихованість передавання інформації в умовах радіоелектронного протиборства.

Перспективним рішенням є розширення спектра таймерних сигналів [15-17], що поєднує переваги часового кодування, структурної прихованості та широкосмугового маскування. Це дозволить формувати новий клас шумоподібних сигналів із підвищеним рівнем енергетичної та структурної прихованості.

Теоретичне поєднання умов забезпечення енергетичної прихованості з показниками частотної та енергетичної ефективності базується на взаємозв'язку між потужністю сигналу, шириною спектра, швидкістю передавання інформації та імовірністю виявлення сигналу.

Енергетична прихованість досягається тоді, коли спектральна щільність потужності сигналу наближається до рівня шумового фону каналу зв'язку. Для цього середня потужність сигналу повинна задовольняти умову [21, 22]:

$$\frac{P_s}{\Delta f} \leq N_0, \tag{1.12}$$

де $P_s$ – потужність сигналу, $\Delta f$ – ширина спектра сигналу, $N_0$ – спектральна щільність шуму.

З наведеного виразу видно, що підвищення енергетичної прихованості може бути досягнуте двома шляхами: зменшенням потужності сигналу $P_s$ або збільшенням смуги частот $\Delta f$. Однак кожний із цих способів впливає на ефективність системи передавання.

Частотна ефективність характеризує кількість переданої інформації в одиниці смуги частот [20]:

$$\eta_f = \frac{R}{\Delta f}, \tag{1.13}$$

де $R$ – швидкість передавання інформації.

При розширенні спектра ($\Delta f \uparrow$) для забезпечення прихованості значення $\eta_f$ зменшується. Отже, зростання прихованості досягається ціною зниження частотної ефективності.

Енергетична ефективність визначається витратами енергії на передавання одного біта інформації [20, 21]:

$$\eta_E = \frac{E_b}{N_0} = \frac{P_s}{RN_0}, \tag{1.14}$$

де $E_b$ – енергія на біт.

Якщо потужність сигналу зменшується для підвищення прихованості, то знижується і відношення $E_b/N_0$, що може призвести до погіршення достовірності приймання та зростання ймовірності помилки.

Отже, можна відзначити, що між цими показниками показниками існує суперечливий взаємозв'язок:

– збільшення $\Delta f$ підвищує прихованість, але зменшує частотну ефективність;

– зменшення $P_s$ підвищує прихованість, але погіршує енергетичну ефективність;

– збільшення швидкості $R$ покращує частотну ефективність, але потребує більшого $E_b/N_0$.

З урахуванням цього умову забезпечення енергетичної прихованості доцільно розглядати як задачу компромісної оптимізації [22]:

$$\max\ K_{\text{пр}} \text{ за умов } \eta_f \geq \eta_{f\,min}, \eta_E \geq \eta_{E\,min}, \tag{1.15}$$

де $K_{\text{пр}}$ – коефіцієнт прихованості.

Для широкосмугових таймерних сигналів це означає, що збільшення бази сигналу [21]

$$B = \Delta f \cdot T \tag{1.16}$$

дозволяє одночасно знизити спектральну помітність та зберегти необхідну завадостійкість за рахунок кореляційного накопичення енергії на приймальній стороні.

Отже, забезпечення енергетичної прихованості неможливе без урахування частотної та енергетичної ефективності. Оптимальний режим функціонування досягається шляхом вибору таких параметрів сигналу, при яких рівень їх виявлення мінімальний, а пропускна здатність і достовірність передавання залишаються в допустимих межах.

На рис. 1.2 представлено класифікацію методів забезпечення енергетичної прихованості сигналів у системах захищеного радіозв'язку. Показано, що основним методом маскування сигналу є використання методів розширення спектра, до яких належать: пряме розширення спектра за допомогою псевдовипадкових послідовностей (ПРС–ПВП), псевдовипадкове перелаштування робочих частот (ППРЧ), лінійна частотна модуляція (ЛЧМ) та хаотичні сигнальні конструкції (ХСК). Особливу увагу приділено можливості застосування зазначених методів як для позиційних, так і для непозиційних таймерних сигнальних конструкцій.


Рис. 1.2. Класифікація методів забезпечення енергетичної прихованості сигналів у системах захищеного радіозв'язку

Використання методу ПРС–ПВП забезпечує розширення спектра сигналу зі зменшенням його спектральної щільності потужності та амплітуди. У результаті

сигнал набуває шумоподібного характеру, що суттєво ускладнює його виявлення, класифікацію та синхронізацію засобами радіоелектронної розвідки.

Підвищення енергетичної прихованості також може бути реалізоване на основі хаотичних сигнальних конструкцій [31-33]. Особливістю таких сигналів є використання хаотичних коливань, які характеризуються широкосмуговістю, неперіодичністю та високою чутливістю до початкових умов формування [34, 35]. Завдяки цьому хаотичні сигнали мають складну спектрально-часову структуру та статистичні характеристики, наближені до шумових процесів [36-38]. Це дозволяє ефективно маскувати передавання інформації на фоні шумів каналу та ускладнює процес прогнозування параметрів сигналу для несанкціонованого приймача.

На відміну від ПРС–ПВП і хаотичних сигналів [38-40], методи ППРЧ та ЛЧМ [41-44] забезпечують енергетичну прихованість переважно за рахунок динамічної зміни частотних параметрів сигналу без суттєвого зменшення його амплітуди. При цьому комбіноване використання зазначених методів дозволяє формувати багатовимірні шумоподібні сигнальні конструкції з підвищеним рівнем прихованості та завадостійкості.

## 1.4 Вплив структурної прихованості сигнально-кодових конструкцій на захист інформації

Однією з ключових вимог до сучасних інформаційно-комунікаційних систем, особливо в умовах радіоелектронної боротьби [39, 40], є забезпечення не лише криптографічного захисту, але й прихованості самого факту та структури передавання інформації [45-48]. У цьому контексті особливого значення набуває поняття структурної прихованості, яке характеризує здатність системи ускладнювати або унеможливлювати визначення параметрів сигналу, алгоритмів модуляції та закономірностей формування передаваних повідомлень.

На відміну від енергетичної прихованості, яка досягається шляхом маскування сигналу на фоні шумів, структурна прихованість [48-49] базується на формуванні складної, непередбачуваної та багатовимірної структури сигналу.

Рівень структурної прихованості значною мірою визначається кількістю можливих сигнально-кодових конструкцій $A_{\text{СКК}}$, які можуть бути використані системою зв'язку під час передавання інформації [14, 49]. Зі збільшенням кількості можливих реалізацій сигналу [50] зростає невизначеність для стороннього спостерігача, що ускладнює процес аналізу структури сигналу, синхронізації та відновлення переданої інформації без знання алгоритмів формування СКК. З ймовірнісної точки зору потенційна структурна прихованість визначається як імовірність правильного розпізнавання структури сигналу [49]:

$$p_{\text{стр}} = \frac{1}{A_{\text{СКК}}}, \tag{1.17}$$

де $A_{\text{СКК}}$ – кількість можливих сигнально-кодових конструкцій.

Для кількісної оцінки структурної прихованості доцільно використовувати логарифмічний показник, що характеризує інформаційну невизначеність структури сигналу [49]:

$$S_{\text{стр}} = \log_2 A_{\text{СКК}}, \tag{1.18}$$

де $S_{\text{стр}}$ визначає рівень структурної прихованості у двійкових одиницях.

Слід відзначити, що структурна прихованість може оцінюватися на різних рівнях еталонної моделі взаємодії відкритих систем OSI. На фізичному рівні вона визначається параметрами сигнальної конструкції, видом маніпуляції, способом розширення спектра, частотними та часовими характеристиками сигналу [51-55]. Зокрема, використання багатопозиційної маніпуляції, псевдовипадкових послідовностей, таймерного кодування або хаотичних сигналів дозволяє суттєво підвищити кількість можливих станів сигналу та ускладнити його аналіз [56].

На канальному рівні структурна прихованість залежить від методів кодування, структури кадрів, алгоритмів формування кодових комбінацій та способів організації передавання даних. Додаткове застосування непозиційних

таймерних сигнальних конструкцій забезпечує формування багатовимірної часової структури сигналу, що підвищує рівень інформаційної невизначеності для засобів радіоелектронної розвідки [20, 21]. Структурна прихованість є комплексною характеристикою системи зв'язку [23], яка визначається сукупністю часових, частотних, кодових та сигнальних параметрів і безпосередньо впливає на стійкість системи до виявлення та аналізу в умовах радіоелектронної протидії.

На відміну від класичної теорії інформації, основною метою якої є оцінювання кількості переданої інформації, у задачах забезпечення прихованості важливого значення набуває аналіз інформаційних характеристик з позицій їх впливу на ймовірність виявлення та ідентифікації сигналів. У цьому випадку ключовим показником виступає невизначеність спостерігача, яка може бути формалізована на основі ентропійних характеристик. Нехай множина можливих структур сигналів описується як:

$$S = \{s_1, s_2, \ldots, s_n\}, \tag{1.19}$$

де кожен елемент відповідає певній сигнально-кодовій конструкції. У загальному випадку апріорна невизначеність щодо структури сигналу визначається ентропією [57]:

$$H_0 = -\sum_{i=1}^{n} P(s_i)\log_2 P(s_i). \tag{1.20}$$

У випадку рівноймовірних структур сигнальних конструкцій [57]:

$$H_0 = \log_2 n, \tag{1.21}$$

що відповідає максимальному рівню невизначеності та, відповідно, максимальній структурній прихованості. Після проведення спостереження або аналізу сигналу противником невизначеність зменшується і визначається апостеріорною ентропією [57]:

$$H_1 = -\sum_{i=1}^{n} P(s_i \mid Y)\log_2 P(s_i \mid Y), \quad (1.22)$$

де $Y$ – прийнятий сигнал.

Зменшення невизначеності характеризує кількість інформації, отриманої спостерігачем [57]:

$$I = H_0 - H_1. \quad (1.23)$$

З позицій забезпечення структурної прихованості необхідно мінімізувати величину $I$, тобто забезпечити умови, за яких апостеріорні ймовірності максимально наближені до апріорних [14]:

$$P(s_i \mid Y) \approx P(s_i). \quad (1.24)$$

У цьому випадку спостерігач не отримує додаткової інформації про структуру сигналу, що відповідає максимальному рівню прихованості. Для кількісної оцінки рівня структурної прихованості доцільно ввести коефіцієнт:

$$K_{sp} = \frac{H_1}{H_0}, \quad (1.25)$$

де $K_{sp} \to 1$ – високий рівень прихованості; $K_{sp} \to 0$ – низький рівень прихованості.

Важливим показником є також взаємна інформація між переданим сигналом $X$ та прийнятим сигналом $Y$ [14]:

$$I(X;Y) = H(X) - H(X \mid Y). \quad (1.26)$$

З точки зору структурної прихованості ця величина визначає ступінь залежності між сигналами та можливість відновлення структури передавання.

Мінімізація взаємної інформації є одним із основних критеріїв підвищення прихованості [14]:

$$I(X;Y) \to 0. \tag{1.27}$$

Це означає, що прийнятий сигнал не містить достатньої інформації для ідентифікації структури переданого сигналу. Аналіз ентропійних характеристик показує, що максимальна структурна прихованість досягається у випадку:

1) рівномірного розподілу ймовірностей сигналів;

2) високої варіативності сигнально-кодових конструкцій;

3) відсутності статистичних залежностей між елементами сигналу.

Практична реалізація таких умов можлива шляхом використання:

1) хаотичних сигналів;

2) псевдовипадкових послідовностей;

3) технологій розширення спектра;

4) адаптивних методів модуляції;

5) комбінованих сигнально-кодових конструкцій.

Особливо ефективними є методи, засновані на використанні хаотичних коливань, які забезпечують високу ентропію сигналу та ускладнюють його аналіз навіть при наявності сучасних засобів радіоелектронної розвідки.

Отже, структурна прихованість може бути формалізована як властивість інформаційної системи, що визначається рівнем ентропії сигналів, величиною взаємної інформації та ступенем збереження невизначеності спостерігача. Використання запропонованих показників дозволяє здійснювати кількісну оцінку ефективності методів маскування та обґрунтовувати вибір сигнально-кодових конструкцій при проєктуванні захищених систем передачі даних.

Отримані результати є теоретичною основою для подальшого розроблення методів підвищення структурної прихованості інформації на основі інтегрованого використання статистичного шифрування, таймерного кодування та технологій спектрального розширення сигналів.

На рис. 1.3 наведено узагальнену класифікацію основних методів забезпечення структурної прихованості сигнально-кодових конструкцій систем зв’язку. Структурна прихованість характеризує здатність сигналу протидіяти виявленню його внутрішньої структурі, типу модуляції, закономірностей побудови та способів кодування засобами радіоелектронної розвідки.


Рис. 1.3. Забезпечення структурної прихованості

До першої групи належать адаптивні методи модуляції [12-14], які передбачають зміну параметрів сигналу залежно від умов каналу зв’язку, рівня завад або вимог до прихованості. Використання адаптивної зміни виду модуляції, швидкості передавання чи потужності сигналу ускладнює ідентифікацію сигнальної структури противником.

Другий напрям представлений таймерними сигналами [14, 49], у яких інформація передається за рахунок часових параметрів імпульсів, пауз або інтервалів між ними. Такі сигнали мають непозиційний характер, забезпечують значну кількість можливих сигнальних станів і підвищують складність структурного аналізу.

Третю групу становлять хаотичні сигнальні конструкції, що формуються на основі детермінованих хаотичних процесів. Їх використання дозволяє створювати

сигнали з шумоподібною структурою, широким спектром та високою чутливістю до початкових параметрів, що істотно підвищує рівень прихованості.

Окремим напрямом є розширення спектра позиційних сигналів, яке реалізується шляхом застосування ПВП або частотних перестрибувань. Це дозволяє зменшити спектральну щільність потужності сигналу та ускладнити його виявлення.

Перспективним рішенням є розширення спектра непозиційних сигнально-кодових конструкцій, зокрема таймерних сигналів, що поєднує переваги часового кодування та широкосмугового маскування.

Найбільш складними та ефективними є комбіновані методи розширення спектра, які базуються на сумісному використанні кількох механізмів прихованості: таймерного кодування, хаотичних послідовностей, адаптивної модуляції та псевдовипадкового спектрального розширення.

Отже, рис. 1.3 демонструє, що забезпечення структурної прихованості досягається як за рахунок ускладнення внутрішньої структури сигналу, так і шляхом інтеграції часових, частотних та стохастичних методів формування сигнально-кодових конструкцій.

Окремим напрямом є розширення спектра позиційних сигналів, яке реалізується на основі відомих класичних методів, зокрема шляхом застосування псевдовипадкових послідовностей, прямого розширення спектра або частотних перестрибувань [59-63]. Такі методи орієнтовані переважно на сигнали, інформація в яких передається зміною амплітуди, частоти або фази несучого коливання [60]. Їх використання дозволяє зменшити спектральну щільність потужності сигналу, підвищити завадостійкість та ускладнити його виявлення засобами радіомоніторингу.

Разом з тим, непозиційні сигнально-кодові конструкції [14], прикладом яких є таймерні сигнали, мають інший алгоритм формування інформаційних ознак, оскільки передавання даних здійснюється через часові параметри імпульсів та інтервалів між ними. У зв’язку з цим застосування класичних методів розширення спектра для таких сигналів є обмеженим або недостатньо ефективним. Це

обумовлює необхідність розроблення альтернативних методів розширення спектра непозиційних сигналів, які повинні враховувати особливості таймерного кодування, часову структуру сигналу та вимоги до збереження інформаційної місткості.

## 1.5 Аналіз методів підвищення прихованості сигнальних конструкцій

### 1.5.1 Методи підвищення прихованості сигнальних конструкцій

Класичні методи підвищення прихованості сигнальних конструкцій є основою для забезпечення захисту інформації в умовах радіоелектронного протиборства [61-63]. Ці методи включають модуляцію, шифрування, завадостійке кодування та частотно-часові перетворення, кожен з яких має свої особливості, переваги та обмеження, особливо на фізичному рівні передачі даних. Отже, можна стверджувати, що сукупність різних методів перетворення складових сигнального представлення інформаційного повідомлення в той або іншій мірі впливають на різні показники прихованості. Також важливим є визначення пріоритетних методів, які є особливо важливим для захисту передаваної інформації в умовах РЕБ [21, 22, 39, 40]. З цього приводу доцільно окремо розглянути ці методи перетворення інформаційного сигналу, що впливають на певні показники прихованості.

### 1.5.2 Вплив модуляції на процес виявлення сигнальних конструкцій

Модуляція сигналів забезпечує узгодження передаваної цифрової або аналогової інформації з середою розповсюдження за допомогою певних сигнально-кодових конструкцій [14, 58]. Існують різні види модуляції, які впливають як на завадостійкість, та і прихованість сигналів в каналі .

Амплітудна модуляція (AM, Amplitude Modulation) характеризується простотою реалізації (рис. 1.4), однак має низький рівень прихованості передавання

сигнальних конструкцій. Це обумовлено тим, що амплітудно-модульований сигнал має чітко виражену огинаючу, яка безпосередньо відтворює інформаційний сигнал [14]:

$$s(t) = A_c[1 + \mu m(t)]\cos(2\pi f_c t), \quad (1.28)$$

де $m(t)$ – нормований модулюючий сигнал; $\mu$ – коефіцієнт модуляції; $A_c$– амплітуда несучої; $f_c$– частота несучого коливання.

Для даного виду модуляції доцільно оцінювати енергетичну та структурну прихованість. Енергетична прихованість визначається рівнем спектральної щільності потужності сигналу та співвідношенням сигнал/шум у каналі зв'язку, тоді як структурна прихованість характеризується складністю виявлення внутрішньої організації сигналу, його параметрів та способу модуляції.

Для АМ-сигналу характерна наявність виражених демаскувальних факторів, до яких належать потужна несуча складова на частоті $f_c$, симетричні бічні смуги спектра на частотах $f_c \pm f_m$, чітко виражена огинаюча, що повторює форму передаваного повідомлення, стабільна спектральна структура сигналу, а також висока кореляція між інформаційним сигналом та огинаючою. Наявність зазначених ознак значно спрощує виявлення, класифікацію та перехоплення сигналу засобами радіоелектронної розвідки і спектрального моніторингу.

Зазначені ознаки значно спрощує виявлення сигналу засобами радіомоніторингу, спектрального аналізу та несанкціонованого перехоплення. Таким чином, амплітудна модуляція не забезпечує достатнього рівня енергетичної та структурної прихованості, особливо в умовах радіоелектронного протиборства, що обмежує її використання в захищених системах зв'язку. Наявність огинаючої $A_c[1 + \mu m(t)]$ призводить до того, що інформаційна складова сигнально-кодової конструкцій може бути відновлена за допомогою простих детекторів огинаючої, без необхідності складної обробки сигналу, що значно спрощує її перехоплення. У спектральній області АМ-сигнал (рис. 1.5) має дискретну структуру [14]:

$$S(f) = \frac{A_c}{2}\delta(f - f_c) + \frac{A_c}{2}\delta(f + f_c) + \frac{A_c\mu}{4}[\delta(f - f_c - f_m) + \delta(f - f_c + f_m)] + \cdots (1.29)$$

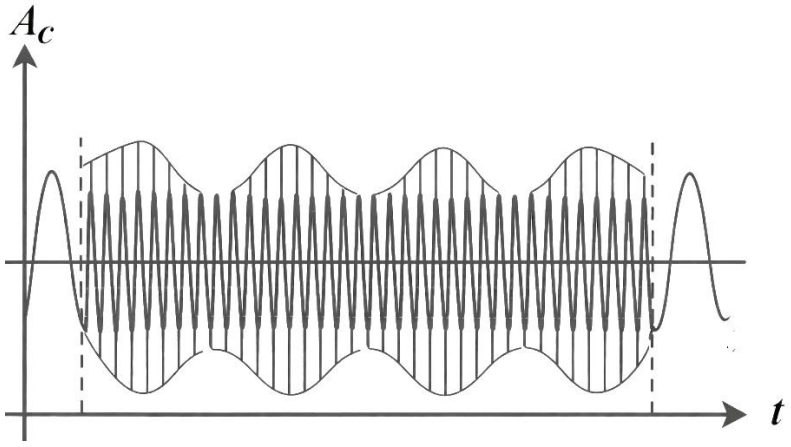



Рисунок 1.4 – Амплітудно-модульований сигнал

З (1.29) бачимо, що в спектрі сигналу є потужна несуча складова $f_c$ та симетричні бічні смуги $f_c \pm f_m$. Наявність виражених спектральних піків призводить до високої ймовірності виявлення сигналу засобами радіомоніторингу, оскільки такі сигнали легко ідентифікуються навіть при низьких значеннях відношення сигнал/шум. Крім того, автокореляційна функція АМ-сигналу має регулярну періодичну структуру, що додатково спрощує його виявлення за допомогою кореляційних методів аналізу.

Отже, амплітудна модуляція не забезпечує достатнього рівня енергетичної та структурної прихованості, що обмежує її застосування в системах захищеного передавання інформації, особливо в умовах радіоелектронного протиборства.

Частотна маніпуляція (ЧМ, FSK, Frequency Shift Keying) є цифровим методом модуляції, при якому передавання інформації здійснюється шляхом зміни частоти несучого сигналу відповідно до значень бінарної послідовності. Для двійкового випадку (BFSK) сигнал формується як гармонічне коливання з однією з двох фіксованих частот: $f_1$ – для передачі логічної «1» та $f_2$ – для передачі логічного «0», що може бути описано виразом [14]:

$$s(t) = A_c\cos(2\pi f_1 t) \text{або} s(t) = A_c\cos(2\pi f_2 t). \quad (1.30)$$

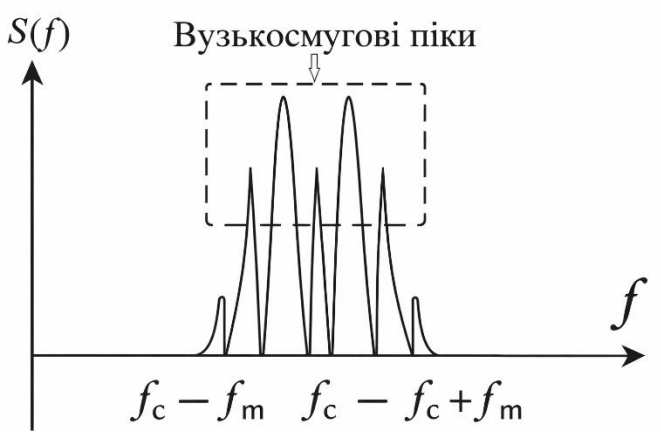



Рисунок 1.5 – Спектр АМ сигналу

Завдяки такому принципу формування сигналу ЧМ забезпечує відносно високу завадостійкість, оскільки використання різних частот дозволяє ефективно розділяти сигнали навіть у присутності шумів та завад. Проте з точки зору забезпечення прихованості передавання інформації цей метод має суттєві обмеження.

У спектральній області FSK-сигнал характеризується наявністю дискретних частотних компонент, що відповідають використовуваним частотам $f_1$ та $f_2$. Навіть з урахуванням розширення спектра через скінченну тривалість символів, у спектрі зберігаються виражені максимуми, що формують характерний «частотний підпис» сигналу. Така структура спектра легко виявляється засобами радіомоніторингу та радіоелектронної розвідки за допомогою спектрального аналізу або вузькосмугової фільтрації.

Крім того, регулярність перемикання між обмеженою кількістю частот зумовлює високу кореляційну визначеність сигналу, що спрощує процеси його синхронізації та демодуляції навіть за низьких значень відношення сигнал/шум. Це, у свою чергу, підвищує ймовірність виявлення та ідентифікації сигналу противником. Обмежена кількість станів також знижує ентропію сигнальної конструкції, що негативно впливає на рівень її структурної прихованості.

Таким чином, незважаючи на переваги частотної маніпуляції з точки зору завадостійкості, її застосування в системах прихованого передавання інформації є

обмеженим, оскільки дискретна та передбачувана частотна структура сигналу забезпечує високу ймовірність його виявлення засобами радіоелектронної розвідки.

Фазова маніпуляція (ФМ, PSK, Phase Shift Keying) є цифровим методом модуляції, при якому передавання інформації здійснюється шляхом зміни фази несучого сигналу відповідно до значень передаваних символів. У найпростішому випадку двійкової фазової маніпуляції (BPSK) сигнал може бути поданий у вигляді [14, 58]:

$$s(t) = A_c \cos(2\pi f_c t + \varphi_i), \tag{1.31}$$

де $\varphi_i \in \{0, \pi\}$ – фаза, що відповідає логічним символам «1» та «0».

Застосування фазової маніпуляції забезпечує високу енергетичну ефективність і завадостійкість, оскільки інформація передається через фазу сигналу при незмінній амплітуді. Це дозволяє зменшити вплив амплітудних завад та ефективно використовувати енергетичні ресурси каналу зв'язку.

Разом з тим, з точки зору забезпечення прихованості передавання інформації, фазова маніпуляція має низку обмежень. У спектральній області PSK-сигнал зберігає вузькосмуговий характер із концентрацією енергії навколо несучої частоти $f_c$. Незважаючи на відсутність вираженої огинаючої, як у випадку амплітудної модуляції, спектр сигналу містить характерні компоненти, що дозволяють його виявлення за допомогою енергетичних та спектральних методів аналізу.

Крім того, фазові стрибки, які виникають у моменти зміни передаваних символів, формують специфічну часову та кореляційну структуру сигналу. Автокореляційна функція ФМ-сигналу має регулярні властивості, що спрощує його синхронізацію та демодуляцію, а також підвищує ефективність застосування кореляційних методів виявлення. Це, у свою чергу, знижує рівень структурної прихованості сигналу.

Додатковим фактором є те, що кількість можливих фазових станів (наприклад, у BPSK або QPSK) є обмеженою, що призводить до відносно низької

ентропії сигнальної конструкції. У результаті сигнал має передбачувану структуру, яка може бути ідентифікована сучасними засобами радіоелектронної розвідки навіть за умов низького відношення сигнал/шум.

Таким чином, незважаючи на високі показники завадостійкості та енергетичної ефективності, фазова маніпуляція не забезпечує достатнього рівня прихованості передавання інформації, оскільки її спектральні та кореляційні характеристики залишаються детермінованими та придатними для виявлення. Це обґрунтовує необхідність застосування більш складних методів формування сигналів, зокрема широкосмугових та шумоподібних сигнальних конструкцій із керованими спектральними та кореляційними властивостями.

Квадратурна амплітудна маніпуляція (КАМ, QAM, Quadrature Amplitude Modulation) є цифровим методом модуляції, при якому передавання інформації здійснюється шляхом одночасної зміни амплітуди та фази несучого сигналу. Сигнал QAM може бути представлений у вигляді суми двох ортогональних компонент:

$$s(t) = I(t)\cos(2\pi f_c t) - Q(t)\sin(2\pi f_c t), \qquad (1.32)$$

де $I(t)$та $Q(t)$ – квадратурні складові, які формують сигнальні точки сузір'я.

Використання КАМ дозволяє значно підвищити спектральну ефективність передавання інформації за рахунок передачі декількох бітів за один символ (наприклад, 16-QAM, 64-QAM), що забезпечує високу пропускну здатність каналу зв'язку. Однак така ефективність досягається ціною підвищеної чутливості до завад і спотворень, а також ускладнення структури сигналу.

Для даного виду модуляції доцільно оцінювати енергетичну та структурну прихованість. Енергетична прихованість визначається рівнем спектральної щільності потужності сигналу, характером розподілу енергії в частотній області та можливістю виявлення сигналу на фоні шуму. Структурна прихованість характеризується складністю встановлення типу модуляції, параметрів сигнального сузір'я, закономірностей зміни символів та внутрішньої організації сигнальної конструкції.

З точки зору забезпечення прихованості передавання інформації, КАМ має ряд суттєвих обмежень. У спектральній області сигнал залишається вузькосмуговим із концентрацією енергії поблизу несучої частоти $f_c$, що знижує рівень енергетичної прихованості та дозволяє його виявлення засобами спектрального аналізу. Незважаючи на більш складну структуру порівняно з ФМ або ЧМ, спектр КАМ-сигналу має характерні ознаки, що формуються регулярною зміною амплітудно-фазових станів.

Крім того, структура сигнального сузір'я є дискретною та детермінованою. Це означає, що навіть при великій кількості точок (наприклад, у 64-КАМ або 256-КАМ) сигнал має обмежену множину станів, що знижує його структурну прихованість. Засоби радіоелектронної розвідки можуть використовувати статистичний аналіз розподілу амплітуд та фаз, а також кореляційні методи для ідентифікації типу модуляції, порядку сузір'я та параметрів сигналу.

Додатково автокореляційні та взаємно-кореляційні властивості КАМ-сигналів мають регулярний характер, що полегшує процеси синхронізації та демодуляції. Це підвищує ймовірність виявлення сигналу навіть за умов низького відношення сигнал/шум, особливо при використанні сучасних алгоритмів цифрової обробки сигналів.

Отже, незважаючи на високу спектральну ефективність та широке застосування в сучасних телекомунікаційних системах, квадратурна амплітудна маніпуляція не забезпечує достатнього рівня енергетичної та структурної прихованості передавання інформації. Її вузькосмугова структура, дискретність сигнального сузір'я та детерміновані спектрально-кореляційні характеристики зумовлюють можливість ефективного виявлення та ідентифікації сигналу засобами радіоелектронної розвідки. Це обґрунтовує необхідність переходу до використання широкосмугових та шумоподібних сигнальних конструкцій, зокрема на основі таймерних сигналів і псевдовипадкових послідовностей, що дозволяють підвищити рівень прихованості передавання інформації.

Це обґрунтовує необхідність пошуку нових методів формування сигналів, зокрема використання широкосмугових та шумоподібних сигнальних конструкцій із керованими спектральними та кореляційними властивостями.

### 1.5.3 Забезпечення прихованості даних на основі криптографічного захисту інформації

Криптографічний захист даних є одним із базових і найбільш поширених методів забезпечення захисту інформації від несанкціонованого доступу, який реалізується на основі шифрування [30, 65-67]. Основною метою шифрування є перетворення відкритих даних у форму, недоступну для розуміння без наявності спеціального ключа або алгоритму дешифрування. У сучасних інформаційно-комунікаційних системах криптографічний захист використовується практично на всіх рівнях моделі OSI та забезпечує конфіденційність, цілісність і автентичність інформації. У загальному випадку процес шифрування можна описати співвідношенням [30]:

$$C = E_K(M), \tag{1.33}$$

де $M$ – відкрите повідомлення; $C$ – зашифроване повідомлення; $E_K$ – функція шифрування з ключем $K$. Процес розшифрування визначається виразом [30]:

$$M = D_K(C), \tag{1.34}$$

де $D_K$ – функція розшифрування. Сучасні криптографічні системи умовно поділяються на: симетричні; асиметричні; потокові; блочні; гібридні. У системах передавання інформації найчастіше застосовуються симетричні потокові та блочні алгоритми, оскільки вони мають високу швидкодію та можуть працювати в режимі реального часу.

У потокових системах шифрування кожен біт або символ повідомлення комбінується з псевдовипадковою ключовою послідовністю :

$$C_i = M_i \oplus K_i, \tag{1.35}$$

де $M_i$ – біт повідомлення; $K_i$ – елемент ключової послідовності; $\oplus$ – операція XOR.

Основною перевагою потокового шифрування є висока швидкість роботи та можливість інтеграції з широкосмуговими сигналами. Водночас ефективність захисту значною мірою залежить від статистичних властивостей ключової послідовності. Якщо послідовність має періодичну або передбачувану структуру, вона може бути виявлена за допомогою статистичного або кореляційного аналізу.

Блочні алгоритми шифрування здійснюють перетворення фіксованих блоків даних:

$$C = E_K(M_1, M_2, \dots, M_n). \tag{1.36}$$

До найбільш відомих алгоритмів належать AES, DES, IDEA та інші. Блочне шифрування забезпечує високий рівень криптостійкості, однак у системах реального часу може створювати додаткові затримки та потребувати значних обчислювальних ресурсів.

Криптографічний захист ефективно забезпечує інформаційну прихованість, тобто унеможливлює відновлення змісту повідомлення без знання ключа. При цьому статистичні властивості зашифрованих даних наближаються до випадкових.

Рівень ентропії зашифрованого повідомлення оцінюється виразом Шеннона (1,20). Для криптостійких систем значення ентропії повинно бути максимальним, що ускладнює статистичний аналіз. Незважаючи на високий рівень криптографічного захисту, шифрування не забезпечує повної прихованості процесу передавання інформації. Основним недоліком є те, що криптографічний захист приховує лише зміст повідомлення, але не маскує сам факт передавання сигналу. У

більшості випадків сигнал залишається: спектрально помітним; енергетично виявлюваним; структурно детермінованим.

Навіть якщо інформація зашифрована, засоби радіоелектронної розвідки можуть:

- виявити наявність передавання;
- визначити частоту роботи системи;
- оцінити параметри сигналу;
- виконати класифікацію типу модуляції;
- встановити часову активність каналу зв’язку.

### 1.5.4 Інтеграції шифрування з методами розширення спектра для забезпечення інформаційної, структурної та енергетичної прихованості

Для систем захищеного зв’язку важливою є не лише інформаційна, а й енергетична та структурна прихованість. Енергетична прихованість визначається можливістю виявлення сигналу за його потужністю та спектральною щільністю (1.12)).

Структурна прихованість характеризує складність визначення типу сигналу, його внутрішньої організації та закономірностей формування. Шифрування практично не впливає на ці характеристики. Для забезпечення комплексної прихованості сучасні системи зв’язку використовують поєднання: криптографічного захисту; шумоподібних сигналів; псевдовипадкових послідовностей; методів DSSS; таймерних сигнальних конструкцій; хаотичних сигналів. У такому випадку шифрування забезпечує інформаційну прихованість, а широкосмугові та таймерні сигнали – енергетичну й структурну прихованість.

Особливий інтерес для сучасних систем захисту інформації становить використання псевдовипадкових послідовностей [74-76], хаотичних коливань [68-70 ] та широкосмугових таймерних сигналів [71-73]. Застосування таких методів дозволяє формувати шумоподібні сигнальні конструкції, спектральні та часові характеристики яких наближаються до природних шумів каналу зв’язку.

Це забезпечує маскування сигналу на фоні шумів, зниження спектральної щільності потужності та ускладнення його виявлення засобами радіоелектронної розвідки. Крім того, використання хаотичних та псевдовипадкових послідовностей дозволяє змінювати часову структуру сигналу, погіршувати його кореляційні властивості та зменшувати ефективність кореляційного аналізу. У результаті забезпечується підвищення енергетичної та структурної прихованості передавання інформації.

Отже, шифрування є ефективним засобом забезпечення конфіденційності та інформаційної прихованості даних, однак не гарантує енергетичної та структурної прихованості самого процесу передавання сигналу. Незважаючи на криптографічну стійкість повідомлення, сигнал може бути виявлений та класифікований засобами радіоелектронної розвідки за його спектральними, часовими та кореляційними ознаками. Це обґрунтовує необхідність інтеграції криптографічних методів із широкосмуговими, шумоподібними та таймерними сигнальними конструкціями, що дозволяє забезпечити комплексний захист інформації в умовах радіоелектронного протиборства.

### 1.5.5 Забезпечення інформаційної та структурної прихованості даних на основі завадостійкого кодування

Одним із важливих напрямів підвищення захищеності інформаційно-комунікаційних систем є використання методів завадостійкого кодування [14, 76], які забезпечують не лише підвищення достовірності передавання інформації, але й можуть застосовуватися для формування додаткових механізмів інформаційної та структурної прихованості сигналів. У сучасних системах зв’язку завадостійке кодування використовується для захисту даних від помилок, що виникають у результаті впливу шумів, завад, багатопроменевого поширення сигналів та навмисної радіоелектронної протидії .

Основною задачею завадостійкого кодування є введення контрольної надлишковості з $r$ біт до складу інформаційного повідомлення з $k$ розрядів, що

дозволяє виявляти та виправляти помилки при прийманні сигналу. Це призводить до збільшення розрядності кодового блоку [14]:

$$n = k + r. \tag{1.37}$$

Принцип побудови завадостійких кодів базується на використання дозволених та недозволених кодових комбінацій. Мінімальна кодова відстань $d_{min}$ між сусідніми дозволеними кодовими комбінаціями визначає коригувальну здатність коду. Здатність виявлення помилок визначається з урахуванням значення $d_{min}$ [14]:

$$d_{min} = t_{\text{вияв}} + 1, \tag{1.38}$$

де $t_{\text{вияв}}$ – максимальна кратність виявлення помилок у кодовому блоку.

Здатність виявлення помилок також визначається з урахуванням значення $d_{min}$ [14]:

$$t_{\text{вип}} = \frac{d_{min}-1(2)}{2}. \tag{1.39}$$

Слід зазначити, що більш сучасних завадостійких кодів є роздільними, тобто відомо розташування інформаційних та перевірочних елементів. Це не дозволяє їх використовувати для завдання захисту інформації від НСД. Важливим показником завадостійких кодів є кодова швидкість, яка визнає долю корисної передаваної інформації в кодовому блоку [14]:

$$\gamma_{\text{к}} = \frac{k}{n}. \tag{1.40}$$

До найбільш поширених методів належать коди Хеммінга, циклічні коди, коди БЧХ, коди Ріда–Соломона, турбо-коди та коди з низькою щільністю перевірок

на парність (LDPC). Наприклад, для всіх кодів Хеммінга мінімальна кодова відстань $d_{min} = 3$. Такі коди забезпечують обмежену кратність виявлення та виправлення помилок при відносно невеликій складності реалізації. Для всіх кодів Хеммінга мінімальна кодова відстань $d_{min} = 3$, що забезпечує $t_{\text{вияв}} = 2$ та $t_{\text{вип}} = 1$.

Коди Ріда–Соломона широко використовуються у цифрових системах зв'язку та накопичення даних завдяки високій ефективності виправлення пакетних помилок [76]. LDPC-коди характеризуються високою завадостійкістю в умовах значного рівня шумів та наближаються до межі Шеннона за ефективністю передавання інформації. Турбо-коди забезпечують високу якість корекції помилок, однак потребують значних обчислювальних ресурсів і складних алгоритмів ітераційного декодування.

Перевагою використання завадостійкого кодування є суттєве підвищення надійності передавання інформації в зашумлених каналах зв'язку та зменшення ймовірності втрати даних. Водночас введення надлишковості призводить до збільшення тривалості передавання або ширини смуги сигналу, що може підвищувати його енергетичну помітність для засобів радіоелектронної розвідки. Крім того, використання складних кодових конструкцій супроводжується зростанням вимог до швидкодії та обчислювальних можливостей апаратури.

Незважаючи на різне функціональне призначення завадостійкості та прихованості, під час побудови комплексних систем захисту інформації виникає необхідність спільного вирішення взаємопов'язаних задач, які враховують алгоритми роботи системи зв'язку, методи захисту від помилок, параметри каналу передавання, процедури доступу до ресурсів мережі та криптографічні алгоритми захисту інформації. У зв'язку з цим методи завадостійкого кодування та криптографічного перетворення інформації дедалі частіше розглядаються як взаємодоповнюючі складові єдиного процесу захисту інформації.

Слід відзначити, що між завадостійким кодуванням і криптографічним шифруванням існує певна функціональна подібність. В обох випадках інформаційне повідомлення після обробки певним алгоритмом змінює форму свого представлення, але зберігає зміст, який може бути відновлений лише за умови

використання відповідного алгоритму декодування або розшифрування. Комплексне використання цих методів дозволяє одночасно забезпечувати достовірність передавання даних та їх захист від несанкціонованого доступу.

Одним із перспективних напрямів є об’єднання процедур криптографічного шифрування та завадостійкого кодування в єдину систему перетворення інформації. Це дозволить зменшити затримки обробки даних, підвищити швидкодію системи та оптимізувати використання частотного ресурсу каналу зв’язку. У теорії криптографічних систем з відкритим ключем відомими прикладами використання методів завадостійкого кодування є криптосистеми МакЕліса та Нідеррайтера, побудовані на основі лінійних кодів.

Криптосистема МакЕліса, запропонована у 1978 році, базується на використанні коду Гоппи та належить до класу постквантових криптографічних систем [77]. Її основна ідея полягає у перетворенні інформаційного повідомлення в кодову послідовність без явної структурної закономірності. Висока криптостійкість системи визначається складністю задачі декодування довільного лінійного коду без знання секретних параметрів. Перевагою криптосистеми МакЕліса є висока швидкодія шифрування та розшифрування, яка значно перевищує швидкодію класичних асиметричних алгоритмів, зокрема RSA [77]. Слід відзначити, що під шифруванням та розшифрування потрібно розуміти одночасний відповідний процес, який пов’язаний з кодуванням та декодуванням.

Можна побачити, що при використання криптосистеми МакЕліс для забезпечення високої криптостійкості шифру визначаються мінімальні значення розміру інформаційного та загального кодового блоку ($n$=1024, k=524) та кратності виправлення помилок ($t_{\text{вип}} = 50$) [77]. Так криптосистема забезпечує швидкодію на кілька порядків вище, чим у криптосистеми з відкритим ключем RSA. Разом із тим одним із основних недоліків криптосистеми МакЕліса є значна надлишковість шифрованих повідомлень, тобто $\gamma_{\text{к}} = 524/1024 = 0{,}512$. У ряді випадків довжина шифрованого кодового блоку може майже вдвічі перевищувати довжину вихідного інформаційного повідомлення. Для компенсації цієї надлишковості доцільним є використання таймерних сигнальних конструкцій, які дозволяють формувати

значно більшу кількість сигнальних реалізацій на заданому часовому інтервалі порівняно з класичними позиційними кодами.

Використання таймерного кодування у поєднанні з криптосистемою МакЕліса дозволяє формувати багатовимірні сигнальні конструкції зі змінною часовою структурою [14]. Зміна параметрів таймерного кодування, зокрема кількості базових елементів, тривалості часових інтервалів та кількості інформаційних переходів, забезпечує можливість формування великої кількості різних реалізацій сигналу. Це дозволяє підвищити структурну прихованість системи та ускладнити процес аналізу сигнальних конструкцій засобами радіоелектронної розвідки.

Додатковою перевагою таймерного кодування є можливість адаптивної зміни структури сигналу залежно від умов функціонування каналу зв’язку та рівня радіоелектронної протидії. Варіювання параметрів таймерних сигнальних конструкцій дозволяє формувати множини сигналів із різними часовими та структурними характеристиками, що підвищує рівень інформаційної невизначеності для несанкціонованого приймача.

Отже, сумісне використання методів завадостійкого кодування, криптографічного шифрування та таймерного кодування створює передумови для побудови комплексних систем захисту інформації з підвищеним рівнем завадостійкості, інформаційної та структурної прихованості. Застосування таймерних сигнальних конструкцій дозволяє не лише компенсувати надлишковість криптографічного перетворення, але й суттєво ускладнює процес виявлення, класифікації та дешифрування переданих повідомлень в умовах радіоелектронного протиборства.

### 1.5.6 Забезпечення прихованості даних на основі частотно-часового перетворення сигналів

Частотно-часові перетворення використовуються для формування сигналів, які важко виявити та проаналізувати. Одним з найпоширеніших методів є пряме

розширення спектру з використанням псевдовипадкових послідовностей (ПРС-ПВП), де сигнал розповсюджується по широкій смузі частот за допомогою псевдовипадкових послідовностей $c(t)$ [26, 27]:

$$s(t) = A \cdot c(t) \cdot d(t)\cos(2\pi f_0 t), \quad (1.41)$$

де $A$ – амплітуда, $c(t)$ – псевдовипадкова послідовність, $d(t)$ – інформаційний сигнал, $f_0$ – несуча частота. Це ускладнює виявлення сигналу. Метод ППРЧ передбачає періодичну зміну робочої частоти сигналу за псевдовипадковим законом [43]:

$$f(t) = f_0 + \Delta f_k, k = 1,2, \dots, N, \quad (1.42)$$

де $\Delta f_k$ – випадкова зміна частоти. Це робить сигнал важко виявляним. Ультраширокосмугові сигнали використовують надзвичайно короткі імпульси, які займають велику смугу частот, що також ускладнює їх виявлення. Переваги частотно-часових перетворень полягають у підвищенні прихованості сигналу завдяки розподілу енергії по широкій смузі частот та ускладненні його виявлення противником. Однак використання широкої смуги частот може обмежуватися регуляторними нормами, а складність синхронізації та обробки сигналів вимагає додаткових ресурсів.

Отже, класичні методи підвищення прихованості сигналів мають свої переваги та обмеження. Оптимальний вибір методів залежить від конкретних умов експлуатації, вимог до системи зв’язку та необхідного рівня захисту інформації. Поєднання широкосмугових сигналів, складної структури та динамічних змін параметрів дозволяє досягти максимальної прихованості, але вимагає ретельного врахування технічних та регуляторних обмежень.

## 1.6 Обґрунтування шляхів підвищення прихованості шумоподібних сигналів, що формуються на основі псевдовипадкових послідовностей

Сутність методу розширенням спектра на основі ПВП полягає у штучному збільшенні займаної смуги частот сигналу порівняно з мінімально необхідною для передавання інформації. У результаті енергія сигналу розподіляється в ширшому частотному діапазоні, що знижує спектральну щільність потужності та ускладнює його виявлення засобами радіоелектронної розвідки. Загальна база сигналу визначається співвідношенням:

$$B = \Delta f \cdot T, \tag{1.43}$$

де $\Delta f$ – ширина спектра сигналу, $T$ – тривалість символу або сигнальної конструкції. Зі збільшенням бази сигналу підвищується його завадостійкість, енергетична прихованість та потенційна стійкість до вузькосмугових завад.

Найбільш поширеним методом є пряме розширення спектра (DSSS – Direct Sequence Spread Spectrum), при якому інформаційна послідовність множиться на високошвидкісну псевдовипадкову послідовність (ПВП):

$$s(t) = m(t) \cdot c(t), \tag{1.44}$$

де $m(t)$ – інформаційний сигнал, $c(t) \in \{-1, +1\}$ – кодова псевдовипадкова послідовність.

Унаслідок цього тривалість одного інформаційного біта розбивається на $N$коротших елементів (чіпів), а спектр сигналу розширюється приблизно у $N$разів. Коефіцієнт розширення визначається як:

$$G_p = \frac{R_c}{R_b}, \tag{1.45}$$

де $R_c$ – швидкість чіпів, $R_b$ – швидкість передавання інформаційних бітів.

Чим більший коефіцієнт $G_p$, тим нижча спектральна щільність потужності сигналу та вищий рівень його енергетичної прихованості.

Для реалізації ПРС-ПВП застосовуються спеціальні кодові послідовності, які мають наближені до шуму властивості. Основними вимогами до таких послідовностей є:

– низький рівень автокореляційних бічних пелюсток;
– мала взаємна кореляція між різними кодами;
– велика кількість можливих кодових комбінацій;
– простота апаратної реалізації.

До класичних ПВП належать:

– m-послідовності;
– коди Голда;
– коди Касамі;
– послідовності Баркера;
– послідовності Уолша.

Автокореляційна функція кодової послідовності визначається як (1.6). Ідеальним є випадок, коли:

$$R_{cc}(0) = N, R_{cc}(\tau) \approx 0,\ \tau \neq 0. \tag{1.46}$$

Особливе місце займають ортогональні коди, зокрема послідовності Уолша. Для двох різних кодів $c_i$та $c_j$виконується умова:

$$\sum_{k=1}^{N} c_i\,(k)c_j(k) = 0, i \neq j. \tag{1.47}$$

Це дозволяє використовувати такі коди для багатокористувацьких систем зв’язку та кодового розділення каналів.

До переваг кодів Уолша належать:

– ортогональність;

– простота синтезу;

– ефективність у синхронних системах.

Разом з тим, в асинхронних каналах ортогональність частково втрачається, що призводить до взаємних завад.

Квазіортогональні коди мають малі, але ненульові значення взаємної кореляції. Вони забезпечують більшу кількість кодових послідовностей, проте поступаються ортогональним за стійкістю до взаємного впливу.

Методи прямого розширення спектра за допомогою ПВП (ПРС-ПВП, DSSS – Direct Sequence Spread Spectrum) є одним із найбільш поширених по забезпеченню енергетичної прихованості та завадостійкості сигналів у системах захищеного зв'язку. Їхня ефективність ґрунтується на перемноженні інформаційного сигналу з високошвидкісною псевдовипадковою кодовою послідовністю, що призводить до суттєвого розширення спектра передаваного сигналу. При цьому спектральна щільність потужності сигналу зменшується відповідно до співвідношення $S(f) \approx P_s/\Delta f$, де $P_s$– потужність сигналу, а $\Delta f$– ширина його спектра. Збільшення смуги частот $\Delta f$ знижує рівень сигналу в одиниці смуги частот, наближаючи його спектральні характеристики до фонового шуму. Це ускладнює виявлення сигналу засобами радіоелектронної розвідки та підвищує рівень енергетичної прихованості. Крім того, ПРС-ПВП забезпечує маскування сигналу шумом, коли його спектральний рівень наближається до рівня фонового шуму, а також захист від вузькосмугових завад, які займають лише частину широкого спектра.

Важливою перевагою ПРС-ПВП є підвищення завадостійкості системи зв'язку: після кореляційного стискання на приймальній стороні енергія сигналу концентрується, тоді як енергія завад розподіляється по всій смузі спектра. Це дозволяє ефективно протидіяти вузькосмуговим і навмисним завадам, вплив яких обмежується лише частиною широкосмугового сигналу. Додатково метод ПРС-ПВП забезпечує можливість багатокористувацького доступу завдяки використанню різних кодових послідовностей.

Разом із тим класичні системи з ПРС-ПВП мають низку обмежень з точки зору забезпечення структурної прихованості. Кореляційна виявлюваність є одним із основних недоліків: якщо противнику відома структура псевдовипадкової послідовності (ПВП) або клас використовуваних кодів, сигнал може бути виявлений за допомогою кореляційного приймача. Наприклад, значення кореляційної суми

$$Z = \sum_{i-1}^{N} r_i \times c_i, \tag{1.48}$$

де $r_i$ – прийнятий сигнал, а $c_i$ – кодова послідовність різко зростає за наявності сигналу, що дозволяє виявити факт передавання навіть при низькому відношенні сигнал/шум (SNR). Крім того, більшість класичних ПВП генеруються лінійними регістрами зсуву та мають детерміновану структуру, що дозволяє відновити кодову послідовність за достатньої довжини перехопленого сигналу. Обмежена кількість ортогональних або квазіортогональних кодів призводить до появи взаємних кореляційних завад у багатокористувацьких системах. Також стаціонарність статистичних характеристик класичних сигналів на основі ПРС-ПВП формує характерні спектральні ознаки, які можуть бути використані засобами радіомоніторингу для класифікації та виявлення типу сигналу.

Для усунення цих недоліків перспективним є використання адаптивних псевдовипадкових послідовностей, хаотичних кодів, таймерних сигнальних конструкцій, а також комбінованих методів часово-частотного розширення спектра. Особливий інтерес становить інтеграція ПРС-ПВП із таймерними сигналами, що дозволяє одночасно забезпечити енергетичну та структурну приховання передавання інформації. Використання хаотичних сигнальних конструкцій додатково підвищує рівень непередбачуваності сигналу завдяки складним нелінійним закономірностям формування часової та спектральної структури, наближаючи його статистичні характеристики до шумоподібного процесу.

Отже, методи розширення спектра, зокрема ПРС-ПВП, є ефективним інструментом забезпечення прихованості передавання інформації завдяки

зниженню спектральної щільності потужності, формуванню шумоподібних сигналів та підвищенню завадостійкості. Водночас класичні ПРС-ПВП системи мають обмеження, пов’язані з кореляційною виявлюваністю, передбачуваністю структури кодів, обмеженою кількістю ортогональних кодів та стаціонарністю статистичних характеристик. Це обґрунтовує необхідність розроблення нових методів формування широкосмугових сигнальних конструкцій, зокрема на основі таймерних сигналів, хаотичних послідовностей та комбінованих методів розширення спектра.

## 1.7 Постановка наукового завдання

Аналіз сучасних методів забезпечення прихованості передавання інформації показує, що існує суперечність між вимогами до високої прихованості сигналу та практичною складністю його формування, синхронізації й обробки в реальних системах зв’язку. Класичні системи прямого розширення спектра забезпечують достатньо високий рівень енергетичної прихованості та завадостійкості, однак характеризуються наявністю кореляційних ознак, які можуть бути використані засобами радіоелектронної розвідки для виявлення та класифікації сигналів. У свою чергу, таймерні сигнальні конструкції дозволяють підвищити структурну прихованість за рахунок непозиційного принципу формування сигналу, проте потребують додаткового спектрального маскування та удосконалення методів синхронізації.

У зв’язку з цим актуальним напрямом наукових досліджень є розроблення широкосмугових таймерних сигнальних конструкцій, у яких поєднуються:

– переваги таймерного кодування;

– методи прямого та комбінованого розширення спектра;

– використання псевдовипадкових, ортогональних і хаотичних послідовностей;

– адаптивне керування параметрами сигналу;

– керовані кореляційні та спектральні властивості сигналів.

Методи формування шумоподібних сигналів на основі таймерних конструкцій мають значний потенціал для забезпечення прихованого передавання інформації в умовах радіоелектронної протидії. Найбільш перспективними є комбіновані методи, що поєднують часову, кодову та частотну області розширення спектра. Це дозволяє формувати багатовимірні сигнальні конструкції зі зниженою спектральною щільністю потужності, підвищеною ентропією та складною структурою, що ускладнює їх виявлення, синхронізацію та відтворення несанкціонованим приймачем.

Разом із тим недостатньо дослідженими залишаються питання:

– синтезу широкосмугових таймерних сигналів із заданими кореляційними характеристиками;

– оцінювання структурної, енергетичної та інформаційної прихованості комбінованих сигнальних конструкцій;

– вибору параметрів таймерного кодування залежно від умов функціонування каналу зв’язку;

– інтеграції таймерних сигналів із методами прямого розширення спектра, псевдовипадкового перелаштування робочих частот та хаотичними сигналами;

– забезпечення компромісу між прихованістю, завадостійкістю, енергоефективністю та складністю технічної реалізації системи.

Таким чином, науковим завданням дисертаційної роботи є розроблення методів формування та обробки широкосмугових таймерних сигнальних конструкцій на основі комбінованого розширення спектра, які забезпечують підвищення структурної, енергетичної та інформаційної прихованості передавання даних в умовах радіоелектронної протидії при збереженні необхідної завадостійкості та ефективності використання частотного ресурсу.

## 1.8 Висновки до розділу 1

У першому розділі дисертаційної роботи проведено комплексний аналіз сучасного стану проблеми забезпечення прихованості передавання інформації в інформаційно-комунікаційних системах в умовах радіоелектронного протиборства.

1. Розглянуто основні загрози, пов’язані із застосуванням засобів радіоелектронної розвідки, радіомоніторингу, навмисних завад та технічних засобів несанкціонованого доступу, що підтверджує актуальність удосконалення методів захисту інформації на фізичному рівні.

2. Уточнено зміст поняття прихованості передавання інформації як сукупності енергетичної, структурної та інформаційної прихованості. Встановлено, що рівень прихованості визначається спектральними, часовими, статистичними та кореляційними характеристиками сигнальних конструкцій, які можуть бути використані для їх виявлення, класифікації та відновлення структури засобами радіоелектронної розвідки.

3. Проведений аналіз класичних методів модуляції та маніпуляції сигналів показав, що вони, незважаючи на широке практичне застосування, не забезпечують достатнього рівня прихованості через наявність характерних спектральних ознак, обмеженої кількості сигнальних станів та можливості використання кореляційних способів виявлення сигналів.

4. Досліджено сучасні методи розширення спектра, зокрема системи прямого розширення спектра із застосуванням псевдовипадкових, ортогональних та квазіортогональних кодів. Встановлено, що такі методи дозволяють знизити спектральну щільність потужності сигналу, підвищити завадостійкість та наблизити сигнал до шумоподібної форми. Разом із тим виявлено їх обмеження, пов’язані з передбачуваністю структури кодів, кореляційною виявлюваністю та обмеженою кількістю кодових комбінацій.

5. Приділено аналізу таймерних сигнальних конструкцій як перспективного класу непозиційних сигналів. Показано, що використання таймерного кодування дозволяє формувати значну кількість сигнальних реалізацій за рахунок варіювання

часових параметрів імпульсних послідовностей, що забезпечує підвищення структурної прихованості та адаптивності системи зв’язку. Водночас встановлено, що при статичній структурі таймерні сигнали можуть виявлятися засобами спектрального та кореляційного аналізу, що обумовлює необхідність їх додаткового спектрального маскування.

6. Виконаний аналіз методів формування шумоподібних сигналів показав, що найбільш перспективними є комбіновані методи, які поєднують таймерне кодування з прямим розширенням спектра, псевдовипадковими, ортогональними та хаотичними послідовностями. Запропонований метод дозволяє одночасно підвищити енергетичну, структурну та інформаційну прихованість сигналів, а також забезпечити керовані спектральні та кореляційні властивості сигнальних конструкцій.

7. У результаті проведеного аналізу виявлено науково-технічне протиріччя між необхідністю забезпечення високого рівня прихованості передавання інформації та обмеженими можливостями існуючих методів формування сигналів щодо маскування їх спектральних, часових і кореляційних ознак. Встановлено, що існуючі системи недостатньо враховують можливість інтеграції таймерного кодування з комбінованими методами розширення спектра та адаптивного керування параметрами сигналів залежно від умов функціонування каналу зв’язку.

8. На підставі проведених досліджень сформульовано наукове завдання дисертаційної роботи, яке полягає у розробленні методів підвищення прихованості передавання інформації шляхом синтезу широкосмугових таймерних сигнальних конструкцій із використанням псевдовипадкових, ортогональних та хаотичних послідовностей, що забезпечують адаптивне керування спектральними та кореляційними характеристиками сигналів в умовах радіоелектронної протидії.

# РОЗДІЛ 2
# ТАЙМЕРНІ СИГНАЛЬНІ КОНСТРУКЦІЇ ЯК ОСНОВА ФОРМУВАННЯ ПРИХОВАНИХ СИСТЕМ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

У другому розділі досліджено таймерні сигнальні конструкції як основу побудови захищених інформаційно-комунікаційних систем, призначених для забезпечення захисту інформації від виявлення, перехоплення та несанкціонованого доступу в умовах радіоелектронного протиборства. Проаналізовано принципи формування таймерних сигналів, їх інформаційні характеристики та особливості забезпечення структурної прихованості. Досліджено вплив параметрів таймерного кодування на кількість сигнальних реалізацій, ентропійні характеристики та рівень захищеності передавання інформації. Показано, що використання непозиційних таймерних сигнальних конструкцій сприяє підвищенню структурної прихованості та завадостійкості каналів зв'язку, що створює передумови для побудови інформаційно-комунікаційних систем із підвищеним рівнем кіберзахисту. За результатами досліджень обґрунтовано доцільність використання таймерних сигнальних конструкцій як базової складової методів захисту інформації на фізичному рівні передавання.

## 2.1 Основні інформаційні характеристики сигналів для забезпечення структурної прихованості

У сучасних інформаційно-комунікаційних системах, особливо в умовах необхідності забезпечення структурної прихованості [21, 22] та завадостійкості [14, 76], важливе значення мають якісні та кількісні характеристики інформації. Ефективність процесів передавання даних значною мірою визначається інформаційними параметрами сигналів, їх статистичними властивостями, рівнем

невизначеності та можливістю достовірного відновлення повідомлень в умовах впливу шумів, завад і засобів радіоелектронної протидії.

У теорії інформації поняття інформації пов'язують зі зменшенням невизначеності щодо стану системи або результату певної події [14, 57, 76]. До моменту отримання повідомлення приймальна сторона має лише деякі апріорні уявлення про можливі стани або сигнали. Після приймання повідомлення рівень невизначеності зменшується, що і характеризує кількість отриманої інформації.

Кількість інформації залежить від імовірності появи повідомлення або сигналу [57]. Чим менш імовірною є подія, тим більшу кількість інформації несе повідомлення про її появу. Це є основою статистичної теорії інформації та широко використовується при аналізі систем передавання даних.

Однією з перших кількісних оцінок інформації є формула Хартлі, яка застосовується для рівноймовірних подій [57]. Якщо система може перебувати у $n$рівноймовірних станах, то кількість інформації визначається виразом [14]:

$$I = \log_2 m, \tag{2.1}$$

де $I$ – кількість інформації, біт; $m$ – кількість можливих станів або повідомлень.

Відповідно до даного виразу збільшення кількості можливих станів призводить до зростання кількості інформації. Логарифмічна залежність дозволяє оцінювати інформацію у двійкових одиницях – бітах. Отримання одного біта інформації відповідає вибору одного з двох рівноймовірних станів.

Однак у реальних системах зв'язку сигнали та повідомлення зазвичай мають різні ймовірності появи. Для таких випадків використовується статистичний метод К. Шеннона, відповідно до якого кількість інформації для окремого повідомлення визначається співвідношенням [57]:

$$I(x_i) = \log_2 \frac{1}{P(x_i)}, \tag{2.2}$$

де $I(x_i)$ – кількість інформації, що міститься у повідомленні $x_i$; $P(x_i)$ – імовірність появи повідомлення $x_i$.

З наведеного виразу випливає, що повідомлення з меншою ймовірністю виникнення несуть більшу кількість інформації. Якщо подія є достовірною, тобто її ймовірність дорівнює одиниці, кількість інформації дорівнює нулю, оскільки така подія не зменшує невизначеність.

Для оцінювання інформаційних процесів у системах передавання даних важливим є поняття невизначеності, яка характеризує ступінь непередбачуваності стану системи до моменту приймання повідомлення. Кількісною мірою невизначеності є ентропія, яка визначає середню кількість інформації, що припадає на одне повідомлення ансамблю сигналів.

Для ансамблю повідомлень $X = \{x_1, x_2, \ldots, x_n\}$з відповідними імовірностями $P(x_i)$ ентропія визначається за формулою Шеннона (1.20) [57]. Ентропія характеризує середню невизначеність системи та є важливим показником при оцінюванні інформаційної ефективності сигнальних конструкцій. Максимальне значення ентропії досягається у випадку рівноймовірних повідомлень, що відповідає найбільшій невизначеності та, відповідно, найвищому рівню структурної прихованості сигналів.

Для захищених систем передавання даних ентропійні характеристики мають особливе значення, оскільки збільшення невизначеності параметрів сигналу ускладнює його виявлення, розпізнавання та аналіз засобами радіоелектронної розвідки. У системах, що використовують таймерні сигнальні конструкції, хаотичні процеси або технології розширення спектра, підвищення ентропії дозволяє забезпечити додатковий рівень структурної прихованості та завадостійкості.

Отже, кількість інформації, імовірнісні характеристики сигналів та ентропійні параметри є основними інформаційними показниками, які визначають ефективність функціонування захищених систем передавання даних і створюють теоретичне підґрунтя для подальшого дослідження таймерних сигнальних конструкцій.

## 2.2 Ентропійне оцінювання сигнальних конструкцій для задачі для аналізу структурної прихованості

Ентропійне оцінювання сигнальних конструкцій є ключовим інструментом для аналізу структурної прихованості та завадозахищеності в системах передавання інформації, зокрема тих, що базуються на таймерних сигналах. Ентропія, як кількісна міра невизначеності, дозволяє оцінити рівень непередбачуваності сигналів, що є критично важливим для забезпечення їхньої прихованості від засобів радіоелектронної розвідки. У контексті захисту інформації ентропія визначає, наскільки важко противнику виявити або відновити структуру сигналу, особливо в умовах обмеженої апріорної інформації.

Властивості ентропії безпосередньо пов'язані з її роллю в оцінюванні сигнальних конструкцій. Згідно з формулою Шеннона для ансамблю повідомлень $X = \{x_1, x_2, \dots, x_n\}$ з імовірностями $P(x_i)$, ентропія обчислюється як:

$$H = -\sum_i p_i \log_2 p_i, \tag{2.3}$$

і характеризує ступінь невизначеності або випадковості сигналу. В цій формулі $p_i$ – ймовірність $i$-ї СКК, яка визначається конкретною комбінацією параметрів. Наприклад, при комбінованому використання різних методів формування сигнально-кодових конструкцій у просторі  це можна представити як «час-частота-код».

Формула (2.3) ілюструє, що ентропія досягає максимального значення за умови рівноймовірності всіх повідомлень, що відповідає максимальній невизначеності системи. Для таймерних сигналів, які характеризуються високим рівнем непередбачуваності, це означає підвищену структурну прихованість, оскільки противник не може легко передбачити або відтворити сигнальну послідовність.

Структурна прихованість сигналів тісно корелює з їхньою ентропією. Чим вища ентропія, тим складніше виявити сигнал на тлі шуму або відрізнити його від

інших сигналів. У системах з таймерними сигнальними конструкціями це особливо актуально, адже їхня часова та спектральна структура формується з урахуванням максимальної невизначеності. Наприклад, використання хаотичних або адаптивних кодових послідовностей дозволяє досягти високої ентропії, що ускладнює кореляційний аналіз і виявлення сигналу засобами радіомоніторингу.

Сигнальні ансамблі – це сукупність можливих сигналів, які можуть бути використані в системі передавання даних. У контексті ентропійного оцінювання ансамбль сигналів аналізується з точки зору розподілу імовірностей їхньої появи. Для таймерних сигналів ансамблі часто формуються з урахуванням вимог до структурної прихованості, що передбачає використання сигналів з високою ентропією. Це дозволяє не лише підвищити рівень прихованості, а й забезпечити стійкість до вузькосмугових завад та навмисних впливів.

Отже, ентропійне оцінювання сигнальних конструкцій є невід'ємною частиною аналізу захищених систем передавання даних. Використання ентропії як міри невизначеності дозволяє оцінити ефективність таймерних сигналів у забезпеченні структурної прихованості, а також оптимізувати вибір сигнальних ансамблів для підвищення завадозахищеності. Це створює теоретичне підґрунтя для розробки нових методів формування сигналів, які поєднують високі ентропійні характеристики з можливістю ефективного передавання інформації в умовах впливу завад.

## 2.3 Оцінювання взаємної інформації в захищених каналах зв'язку

У захищених каналах зв'язку взаємна інформація є ключовим показником, який характеризує кількість інформації, що передається від джерела до приймача, з урахуванням впливу завад, шумів та засобів РЕБ [39, 40]. Вона визначає ефективність передавання даних в умовах структурної прихованості та завадостійкості, особливо в системах, що використовують таймерні сигнальні конструкції або методи розширення спектра.

Взаємна інформація між двома випадковими величинами $X$(вхідний сигнал) та $Y$(вихідний сигнал) визначається як різниця між ентропією джерела повідомлень та умовною ентропією після приймання сигналу [14, 76]:

$$I(X;Y) = H(X) - H(X \mid Y), \tag{2.5}$$

де $H(X)$ – ентропія вхідного сигналу, що характеризує невизначеність до передавання; $H(X \mid Y)$ – умовна ентропія вхідного сигналу за умови отримання вихідного сигналу $Y$, що характеризує залишкову невизначеність після передавання.

Еквівалентно взаємна інформація може бути представлена через спільний розподіл імовірностей [14, 76]:

$$(X;Y) = \sum_i \sum_j P(x_i, y_j) \log_2 \left( \frac{P(x_i, y_j)}{P(x_i)\, P(y_j)} \right), \tag{2.6}$$

де $P(x_i, y_j)$ – спільна імовірність появи сигналів $x_i$та $y_j$; $P(x_i)$ – імовірність появи вхідного сигналу $x_i$; $P(y_j)$ – імовірність появи вихідного сигналу $y_j$.

Взаємна інформація показує, наскільки зменшується невизначеність щодо вхідного сигналу $X$після отримання вихідного сигналу $Y$. В ідеальному каналі без завад і шумів виконується умова:

$$I(X;Y) = H(X), \tag{2.7}$$

тобто вся інформація передається без втрат. Однак у реальних умовах, особливо в захищених каналах зв’язку, на величину взаємної інформації суттєво впливають завадостійкість, рівень шумів та дія засобів РЕБ.

Завадостійкість визначає здатність системи передавання даних протидіяти зовнішнім впливам, таким як вузькосмугові або широкосмугові завади. У системах з таймерними сигналами або сигналами з розширенням спектра завадостійкість досягається за рахунок розподілу енергії сигналу по широкій смузі частот. Це

ускладнює виявлення сигналу противником та знижує вплив вузькосмугових завад, які займають лише частину спектра. При цьому взаємна інформація залишається достатньо високою завдяки використанню кореляційної обробки сигналів на приймальній стороні.

Вплив шумів на взаємну інформацію проявляється у зменшенні кількості достовірно переданої інформації через викривлення сигналу. Шум може бути адитивним, мультиплікативним або імпульсним, а його вплив безпосередньо залежить від відношення сигнал/шум $\mathrm{SNR} = P_s/P_n$.

Зі зменшенням значення SNR взаємна інформація знижується, що може призводити до втрати або викривлення даних. Для компенсації цього використовуються методи завадостійкого кодування та корекції помилок, зокрема коди Ріда–Соломона, турбо-коди та LDPC-коди [14, 76].

Вплив засобів радіоелектронної боротьби є одним із найбільш критичних факторів для захищених каналів зв’язку. Засоби РЕБ можуть створювати навмисні завади, здійснювати імітацію сигналів або перехоплення інформації. У таких умовах взаємна інформація може суттєво знижуватися, особливо у випадках, коли структура сигналу є прогнозованою або відомою противнику.

Для підвищення структурної прихованості та зменшення ефективності засобів РЕБ використовуються [74, 75]: адаптивні псевдовипадкові послідовності; хаотичні сигнали; таймерні сигнальні конструкції; методи розширення спектра; комбіновані сигнально-кодові структури.

Таймерні сигнали [14, 46, 78] забезпечують додатковий рівень невизначеності за рахунок зміни часових параметрів передавання сигналів, що ускладнює їх виявлення та аналіз. У поєднанні з методами спектрального розширення [15, 71, 73] це дозволяє підвищити як структурну прихованість, так і завадостійкість систем передавання даних.

Отже, оцінювання взаємної інформації у захищених каналах зв’язку є важливим етапом аналізу ефективності систем передавання даних [21, 22]. Врахування впливу шумів, завад та засобів РЕБ дозволяє оптимізувати параметри сигнальних конструкцій для забезпечення високої достовірності передавання,

структурної прихованості та стійкості до зовнішніх впливів. Це створює теоретичне підґрунтя для подальшого дослідження таймерних сигнальних конструкцій та комбінованих методів захисту інформації.

## 2.4 Оцінка впливу інформаційних характеристик таймерних сигнальних конструкцій на структурну приховність

Таймерні сигнали [14, 46, 47, 49] становлять значний науковий і практичний інтерес у задачах побудови сучасних захищених систем передавання інформації, оскільки забезпечують підвищений рівень структурної та інформаційної прихованості, завадостійкості й стійкості до впливу засобів радіоелектронної боротьби. На відміну від класичних методів передавання даних, у яких інформація визначається переважно амплітудними, фазовими або частотними параметрами сигналу, у ТСК основним інформаційним параметром виступає часове положення сигнальних елементів.

Особливістю ТСК є те, що інформація передається не окремими двійковими елементами фіксованої тривалості, а часовими інтервалами між інформаційно значущими моментами модуляції та їх взаємним розташуванням на інтервалі формування сигналу. Це дозволяє значно збільшити кількість допустимих сигнальних реалізацій навіть при незначній зміні параметрів формування сигналу.

Ансамбль бінарних ТСК формується на часовому інтервалі [14]:

$$T_c = mt_0, \tag{2.8}$$

де $n$ – кількість елементарних посилок; $t_0$ – тривалість елементарної посилки.

При цьому базовий часовий елемент $\Delta$ визначається співвідношенням

$$\Delta = \frac{t_0}{s}, \tag{2.9}$$

де $s$ – коефіцієнт часової дискретизації.

На відміну від розрядно-цифрового кодування, де інформація визначається рівнем сигналу в межах окремого розряду, у таймерних сигналах інформація в межах комбінації міститься у значущих моментах модуляції (ЗММ) імпульсів:

$$t_c = t_0 + k\Delta, \tag{2.10}$$

де $k = 0,1,2,\dots,s(m-2)$. Це означає, що кожна сигнальна конструкція визначається не лише послідовністю інформаційних символів, а й структурою часових позицій імпульсів у межах інтервалу формування сигналу. Це створює додатковий ступінь невизначеності для стороннього спостерігача та значно ускладнює процес виявлення і розпізнавання сигналів.

Якщо для формування одного інформаційного символу використовується $M$ можливих часових позицій, кількість інформації, що передається одним таймерним сигналом, визначається виразом

$$I = \log_2 M, \tag{2.11}$$

де $I$ – кількість інформації, біт; $M$ – кількість можливих часових позицій.

Збільшення кількості допустимих часових позицій приводить до суттєвого зростання інформаційної ємності сигнальної конструкції та підвищення структурної прихованості.

Важливою перевагою ТСК є значно більша кількість можливих реалізацій сигналів у порівнянні з розрядно-цифровими кодами. Якщо у класичному двійковому коді число реалізацій визначається як

$$N = 2^m, \tag{2.12}$$

то для таймерних сигналів кількість можливих реалізацій може суттєво перевищувати це значення. При використанні ТСК з фіксованим числом інформаційно ЗММ $i$ число реалізацій визначається співвідношенням [14]:

$$N_p = \frac{[ms-(s-1)i]!}{i!([ms-(s-1)i]-i)!}, \quad (2.13)$$

де $N_p$ – кількість реалізацій ТСК; $i$ – число ЗММ.

На рис. 2.1 (a) наведено приклад цифрового сигналу з розрядно-цифровим кодуванням, сформованого у вигляді послідовності з чотирьох імпульсів $t_0$. Кожний імпульс кодується чотирирозрядним двійковим кодом та складається з елементарних імпульсів Найквіста тривалістю $t_0$. У такій системі інформація передається лише рівнями сигналу, тоді як у ТСК додатково використовується часовий ресурс каналу зв'язку. Наведені приклади побудови ТКС (рис. 2.1 b, c) мають наступні параметри: *i*=2, $m$=4, *s*=4. У наведених таймерних сигналах кількість інформаційно ЗММ $i$ визначається числом зміни полярності імпульсу при переходах між часовими інтервалами. Для розглянутого прикладу зміна полярності відбувається при переході від $t_{c1}$ до $t_{c2}$ та від $t_{c2}$до $t_{c3}$, тому $i = 2$.

З рис. 2.1 бачимо, що у структурі ТСК інформація передається не лише значенням двійкових елементів, а й часовими інтервалами між інформаційно ЗММ, що забезпечує додатковий ступінь структурної прихованості сигналу. Тривалість побудови ТСК $T_c = 4t_0$, що дає змогу згідно формули (2.13) створити $N_p = 45$ комбінацій. На цьому ж інтервалі для РЦК можна створити усього 16 комбінацій.

Для наведеної першої ТСК (рис. 2.1 b) часові інтервали між імпульсами визначаються як: $t_{c1} = 4\Delta, t_{c2} = 5\Delta, t_{c3} = 7\Delta$. Загальна тривалість інтервалу формування сигналу становить:

$$T_c = t_{c1} + t_{c2} + t_{c3} = 4\Delta + 5\Delta + 7\Delta = 16\Delta = nt_0.$$

Для таймерного сигналу, що надано на рис. 2.1 (c), значення імпульсів будуть наступними: $t_{c1} = 5\Delta, t_{c2} = 5\Delta, t_{c3} = 6\Delta$. Для *i*=3 кількість імпульсів $t_c$ буде усього три.

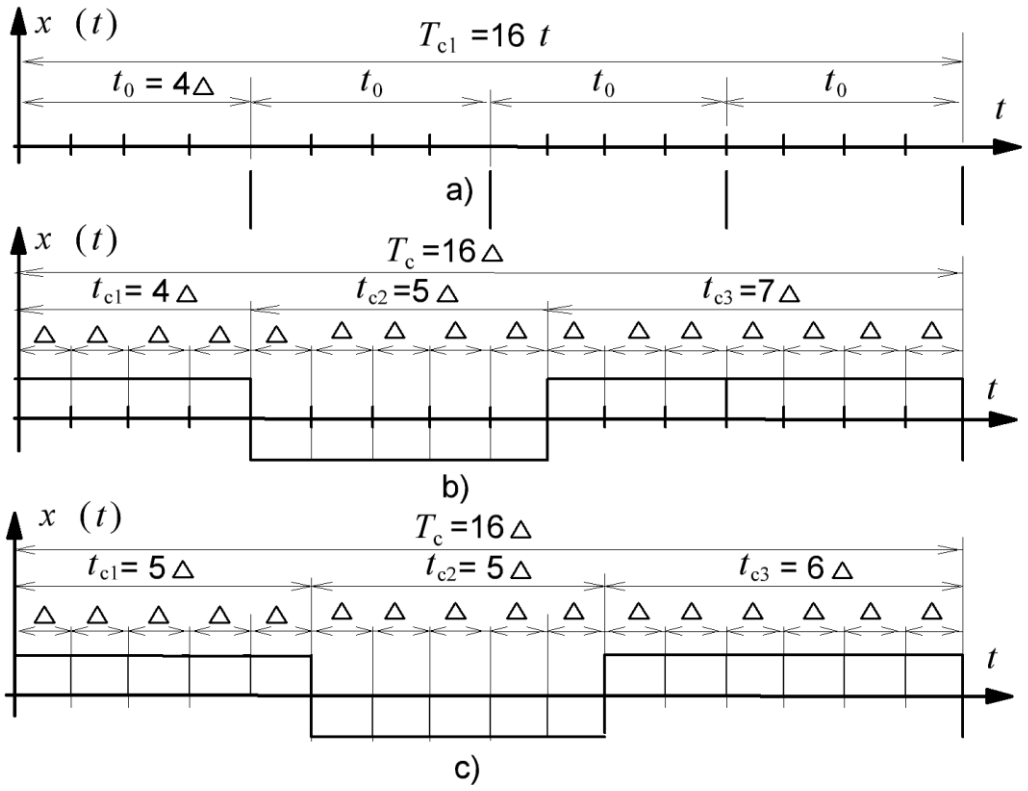



Рис. 2.1. Приклад формування таймерних сигналів
з параметрами $m$=4, $s$=4, $i$=2

Збільшимо інтервал побудови $T_c$ та кількість ЗММ і покажемо вид таймерних сигналів. На рис. 2.2 наведено приклади ТСК для наступних параметрах їх формування: $i$=3, $m$=8, $s$=5. Згідно формули (2.13) кількість реалізацій для ТСК $N_p = 561$, що більше ніж у 2 рази у порівнянні з РЦК – $N_{p\text{рцк}} = 256$. З рисунку бачимо, що при $i$=3 кількість імпульсів $t_{c1}$ вже буде чотири.

Однією з важливих характеристик таймерних сигналів є практична ширина спектра сигналу, яка визначається мінімальною тривалістю інформаційного інтервалу:

$$\Delta f_{\text{ТСК min}} = \frac{1}{t_{c\min}}, \tag{2.14}$$

де $\Delta f_{\text{ТСК}}$ – практична ширина спектра таймерного сигналу; $t_{c\min}$ – мінімальна тривалість імпульсу в межах комбінації тривалістю $T_c$.

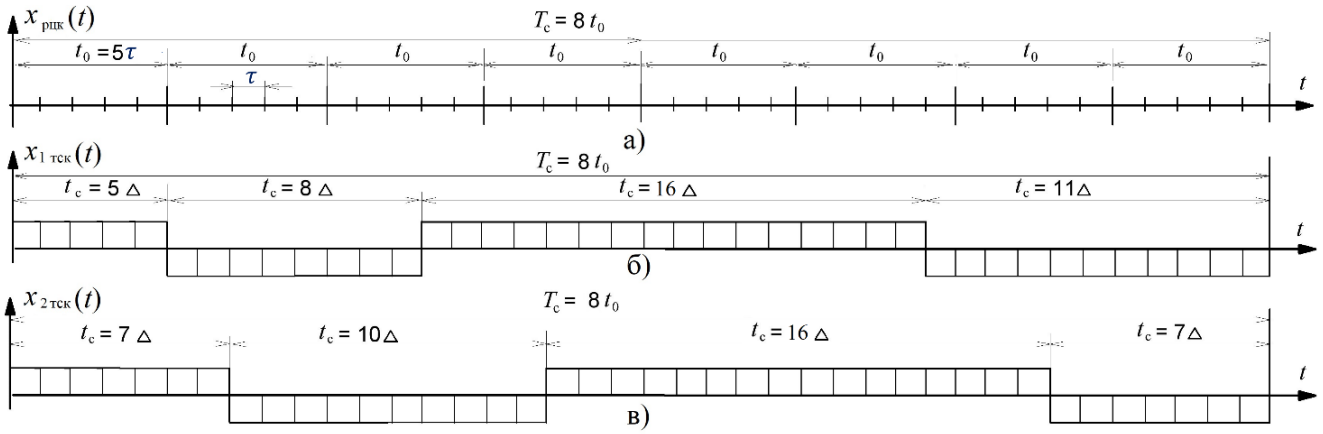



Рис. 2.2. Приклад формування таймерних сигналів
з параметрами $m$=8, $s$=5, $i$=3

Аналіз показує, що практична ширина спектра сигналів з таймерними сигналами може бути меншою або дорівнювати ширині спектра сигналів з РЦК, тобто:

$$\Delta f_{\text{ТСК}} \geq \frac{1}{t_c} = \frac{1}{t_0 + k\Delta}. \qquad (2.15)$$

Такий спосіб формування сигнальних конструкцій дозволяє більш ефективно використовувати часові структури сигналу та можливістю формування інформаційних послідовностей без збільшення швидкості зміни елементарних імпульсів.

Таким чином, використання таймерних сигналів дозволяє не лише збільшити кількість можливих сигнальних реалізацій та підвищити структурну прихованість сигналу, а й покращити спектральні та енергетичні характеристики системи передавання даних. Це забезпечує підвищення завадостійкості та ефективності функціонування каналів зв’язку в умовах впливу шумів і засобів радіоелектронної протидії.

У випадку використання конструкцій із різним числом ЗММ $i$ загальна кількість реалізацій визначається як [14]:

$$N_{p\Sigma} = \sum_{i=1}^{n} \frac{[ns-(s-1)i]!}{i!([ns-(s-1)i]-i)!}. \quad (2.16)$$

Аналіз наведених співвідношень показує, що навіть при відносно невеликих значеннях параметрів $m$ та $s$ кількість допустимих реалізацій ТСК значно перевищує кількість реалізацій двійкових кодів. Наприклад, при $m = 5$ та $s = 7$ число реалізацій ТСК може досягати $N_p = 1293$, тоді як для двійкового коду на тому самому часовому інтервалі кількість реалізацій становить лише $N = 2^5 = 32$.

Це свідчить про значно більші варіаційні можливості таймерних сигналів та їх високу ефективність у задачах структурного маскування сигналів.

Однією з основних характеристик ТСК є їх висока ентропія, яка визначається невизначеністю часового положення сигнальних елементів. Для ансамблю таймерних сигналів ентропія визначається формулою Шеннона (1.20). Максимальне значення ентропії досягається при рівноймовірному використанні всіх часових позицій:

$$P(x_i) = \frac{1}{M}. \quad (2.18)$$

тоді

$$H_{\max} = \log_2 M. \quad (2.19)$$

Зростання ентропії приводить до підвищення інформаційної невизначеності сигналу та ускладнює його аналіз засобами радіоелектронної розвідки.

Для оцінювання потенційної структурної прихованості ТСК вводиться ансамбль реалізацій сигналів, який необхідно проаналізувати при несанкціонованому доступі:

$$A_{\text{тск}} = \sum_n \sum_s \sum_{i=1}^{n} \frac{[(n\cdot s)-[(s-1)\cdot i]]!}{i!\cdot[[(n\cdot s)-[(s-1)\cdot i]]-i]!}, \quad (2.20)$$

Тоді показник структурної прихованості таймерних сигналів $S_{\text{тск}}$ може бути визначений як

$$S_{\text{тск}} = \log_2 A_{\text{тск}} \tag{2.21}$$

Імовірність розкриття структури сигналу при несанкціонованому доступі визначається виразом

$$p_{\text{стр}} = \frac{1}{A_{\text{ТСК}}}, \tag{2.22}$$

з якого випливає, що збільшення ансамблю можливих реалізацій призводить до суттєвого зменшення ймовірності розкриття структури сигналу.

Табл. 2.1 відображає залежність кількості можливих реалізацій таймерних сигналів $N_p$ та показника структурної прихованості $S_{\text{ТСК}}$ від параметрів формування сигналу $m$, $s$ та $i$. У проведених розрахунках довжина інтервалу формування сигналу $T_c$ була фіксованою та становила $m = 4$, а кількість інформаційно ЗММ приймалась фіксованою – $i = 2$. Змінним параметром виступав коефіцієнт часової дискретизації $s$, який визначає кількість базових часових елементів $\Delta$ усередині інтервалу Найквіста $t_0$.

Аналіз результатів, наведених у табл. 2.1, показує, що зі збільшенням параметра $s$ відбувається суттєве зростання кількості можливих реалізацій таймерних сигналів $N_p$. Так, при $s = 2$ кількість реалізацій становить лише $N_p = 15$, тоді як при $s = 8$ отримаємо вже $N_p = 231$.

Це пояснюється тим, що збільшення параметра $s$ призводить до підвищення кількості допустимих часових позицій для формування інформаційно ЗММ. У результаті розширюється ансамбль можливих сигнальних конструкцій $N_p$ та зростає варіативність часової структури сигналів. Зростання кількості допустимих реалізацій $N_p$ безпосередньо впливає на підвищення структурної прихованості

ТСК, оскільки ускладнюється процес аналізу та розпізнавання структури сигналу засобами радіоелектронної розвідки.

*Таблиця 2.1*

Показники $N_p$ та $S_{\text{тск}}$ на інтервалі часу $T_c = 4t_0$ в залежності від параметрів побудови ТСК *n*, *s* та *i*=2

| № | $m$ | $s$ | $i$ | $N_p$ | $S_{\text{тск}}$ |
|---|---|---|---|---|---|
| 1 | 4 | 2 | 2 | 15 | 3,91 |
| 2 | 4 | 3 | 2 | 28 | 4,81 |
| 3 | 4 | 4 | 2 | 45 | 5,49 |
| 4 | 4 | 5 | 2 | 66 | 6,04 |
| 5 | 4 | 6 | 2 | 91 | 6,51 |
| 6 | 4 | 7 | 2 | 120 | 6,91 |
| 7 | 4 | 8 | 2 | 153 | 7,26 |
| 8 | 4 | 9 | 2 | 190 | 7,57 |
| 9 | 4 | 10 | 2 | 231 | 7,85 |

Разом із тим збільшення параметра $s$ породжує певне протиріччя між рівнем структурної прихованості $S_{\text{тск}}$ та завадостійкістю системи передавання інформації. З одного боку, підвищення часової роздільної здатності дозволяє формувати більшу кількість сигнальних конструкцій $N_p$ і покращує прихованість сигналу $S_{\text{тск}}$. З іншого боку, зменшення значення $\Delta = t_0/s$ призводить до скорочення тривалості окремих часових інтервалів та підвищення чутливості системи до впливу шумів, фазових нестабільностей, часових флуктуацій і похибок синхронізації. У таких умовах навіть незначні часові спотворення або завади можуть призводити до помилкового визначення положення інформаційно значущих моментів відтворення (ЗМВ) в приймачі, що збільшує ймовірність помилок приймання сигнально-кодових конструкцій. Крім того, зростання часової роздільної здатності імпульсів $t_c$ ускладнює вимоги до синхронізації передавальної та приймальної сторін системи зв'язку.

Для підвищення структурної прихованість розглянемо варіант збільшення інтервалу побудови сигнальних конструкцій $T_c$. Табл. 2.2 відображає залежність

кількості можливих реалізацій таймерних сигналів $N_p$ та показника структурної прихованості $S_{\text{ТСК}}$ при збільшенні інтервалу формування сигналу до $T_c = 8t_0$.

Аналіз результатів, наведених у табл. 2.2, показує, що збільшення інтервалу формування ТСК до $m = 8$ призводить до суттєвого зростання кількості можливих реалізацій ТСК $N_p$ у порівнянні з більш коротшими сигнальними конструкціями ($m = 4$). Навіть при мінімальному значенні параметра $s = 2$ кількість допустимих реалізацій становить $N_p = 91$, тоді як при $s = 10$ вона досягає $N_p = 1891$.

*Таблиця 2.2*

Показники $N_p$ та $S_{\text{тск}}$ на інтервалі часу $T_c = 8t_0$ в залежності від параметрів побудови ТСК *n*, *s* та *i*=2

| № | $m$ | *s* | *i* | $N_p$ | $S_{\text{тск}}$ |
|---|---|---|---|---|---|
| 1 | 8 | 2 | 2 | 91 | 6,51 |
| 2 | 8 | 3 | 2 | 190 | 7,57 |
| 3 | 8 | 4 | 2 | 325 | 8,34 |
| 4 | 8 | 5 | 2 | 496 | 8,95 |
| 5 | 8 | 6 | 2 | 703 | 9,46 |
| 6 | 8 | 7 | 2 | 946 | 9,89 |
| 7 | 8 | 8 | 2 | 1225 | 10,26 |
| 8 | 8 | 9 | 2 | 1540 | 10,59 |
| 9 | 8 | 10 | 2 | 1891 | 10,88 |

Отримані результати свідчать про значне розширення ансамблю комбінацій $N_p$ при збільшенні значень параметрів формування ТСК *n*, *s* та *i*. Це пояснюється тим, що збільшення тривалості інтервалу формування сигналу $T_c$ створює більшу кількість можливих часових комбінацій для розташування ЗММ. У результаті суттєво зростає варіативність структури сигналу та ускладняється процес його аналізу засобами радіоелектронної розвідки.

Показник структурної прихованості $S_{\text{ТСК}}$ також демонструє стале зростання при збільшенні параметра $s$. Для $s = 2$ значення прихованості становить $S_{\text{ТСК}} = 6{,}51$, а при $s = 10$ отримуємо $S_{\text{ТСК}} = 10{,}88$. Зростання структурної прихованості

$S_{\text{ТСК}}$ обумовлене збільшенням кількості можливих реалізацій ТСК, що приводить до розширення ансамблю сигналів, які необхідно проаналізувати при спробі несанкціонованого доступу або розкриття структури сигналу.

Порівняно з випадком формування ТСК на меншому часовому інтервалі $T_c = 4t_0$, збільшення параметра $n$ забезпечує значно ефективніше підвищення прихованості, ніж лише збільшення коефіцієнта часової дискретизації $s$. Це пов'язано з тим, що збільшення $s$ супроводжується зменшенням базового часового елемента $\Delta = t_0/s$, що може негативно впливати на завадостійкість системи через підвищення вимог до точності часової синхронізації та збільшення чутливості до шумів і часових флуктуацій.

Натомість збільшення інтервалу формування $T_c$ дозволяє підвищити структурну прихованість без критичного зменшення тривалості базових часових елементів $\Delta$, що є більш сприятливим з точки зору забезпечення завадостійкості системи передавання інформації. Це обґрунтовує необхідність вибору параметрів $n$, $s$ та $i$ з урахуванням компромісу між структурною прихованістю, завадостійкістю та пропускною здатністю каналу зв'язку.

Таким чином, результати, наведені у табл. 2.2, підтверджують, що збільшення інтервалу формування таймерних сигналів є ефективним способом підвищення структурної прихованості систем передавання інформації та забезпечення стійкості до засобів радіоелектронної розвідки й аналізу сигналів.

Розглянемо можливість підвищення структурної прихованості таймерних сигнальних конструкцій шляхом збільшення кількості ЗММ $i$. Результати розрахунків для випадку $i = 3$ при інтервалі формування сигналу $T_c = 8t_0$ наведені в табл. 2.3.

Аналіз отриманих результатів показує, що збільшення кількості ЗММ приводить до суттєвого зростання кількості можливих реалізацій таймерних сигналів $N_p$. Так, при $s = 2$ число допустимих реалізацій становить $N_p = 286$, тоді як при $s = 10$ воно збільшується до $N_p = 23426$.

*Таблиця 2.3*

Показники $N_p$ та $S_{\text{тск}}$ на інтервалі часу $T_c = 8t_0$ в залежності від параметрів побудови ТСК $m$, $s$ та $i$=3

| № | $m$ | $s$ | $i$ | $N_p$ | $S_{\text{тск}}$ |
|---|---|---|---|---|---|
| 1 | 8 | 2 | 3 | 286 | 8,16 |
| 2 | 8 | 3 | 3 | 816 | 9,67 |
| 3 | 8 | 4 | 3 | 1771 | 10,79 |
| 4 | 8 | 5 | 3 | 3276 | 11,68 |
| 5 | 8 | 6 | 3 | 5456 | 12,41 |
| 6 | 8 | 7 | 3 | 8436 | 13,04 |
| 7 | 8 | 8 | 3 | 12341 | 13,59 |
| 8 | 8 | 9 | 3 | 17296 | 14,08 |
| 9 | 8 | 10 | 3 | 23426 | 14,52 |

У порівнянні з ТСК з кількістю ЗММ $i = 2$ спостерігається багатократне збільшення ансамблю можливих сигнальних конструкцій. Це пояснюється тим, що збільшення кількості ЗММ призводить до зростання кількості можливих комбінацій розташування часових інтервалів у межах сигнальної конструкції. У результаті суттєво підвищується варіативність структури сигналу та ускладнюється процес його аналізу при несанкціонованому доступі. Показник структурної прихованості $S_{\text{ТСК}}$ також демонструє інтенсивне зростання. Для мінімального значення параметра $s = 2$ значення $S_{\text{ТСК}} = 8{,}16$, а при $s = 10$ отримаємо $S_{\text{ТСК}} = 14{,}52$.

Отримані значення $S_{\text{ТСК}}$ суттєво перевищують результати для ТСК з $i = 2$, що підтверджує високу ефективність збільшення кількості ЗММ як одного з основних способів підвищення структурної прихованості ТСК.

Зростання структурної прихованості $S_{\text{ТСК}}$ пояснюється розширенням ансамблю можливих сигнальних реалізацій, які необхідно проаналізувати для визначення структури сигналу. У цьому випадку противнику необхідно виконувати аналіз значно більшої кількості часових конфігурацій, що приводить до збільшення обчислювальної складності задачі розкриття структури ТСК.

Порівняльний аналіз табл. 2.2 та табл. 2.3 показує, що збільшення кількості ЗММ $i$ забезпечує більш інтенсивне зростання структурної прихованості, ніж лише збільшення параметра часової дискретизації $s$. Наприклад, при $s = 10$ та $i = 2$ структурна прихованість становила $S_{\text{ТСК}} = 10{,}88$, тоді як при $i = 3$ отримали $S_{\text{ТСК}} = 14{,}52$.

Таким чином, збільшення кількості ЗММ дозволяє значно підвищити рівень структурної невизначеності сигналу без необхідності надмірного зменшення базового часового елемента $\Delta$, що є важливим з точки зору забезпечення завадостійкості системи.

Разом із тим збільшення кількості інформаційно значущих моментів модуляції приводить до ускладнення процесів формування та синхронізації таймерних сигналів. Зростають вимоги до точності часової прив'язки, стабільності генераторів та швидкодії приймально-передавальної апаратури. Крім того, надмірне збільшення параметра $i$може призводити до зниження енергетичної ефективності системи та підвищення ймовірності помилок приймання сигналів у зашумлених каналах зв'язку.

Отже, результати, наведені у табл. 2.3, підтверджують, що збільшення кількості інформаційно значущих моментів модуляції є одним із найбільш ефективних способів підвищення структурної прихованості таймерних сигнальних конструкцій. Оптимальний вибір параметрів $n$, $s$ та $i$ дозволяє забезпечити необхідний баланс між прихованістю, завадостійкістю та складністю реалізації системи передавання інформації.

Доцільним також є дослідження граничні можливості збільшення показника ЗММ $i$. В табл. 2.4 наведено зміни показників $N_p$ та $S_{\text{ТСК}}$ в залежності від $i$.

Доцільним є дослідження граничних можливостей підвищення структурної прихованості таймерних сигналів шляхом зміни кількості ЗММ $i$. У табл. 2.4 наведено результати розрахунків показників кількості реалізацій $N_p$ та структурної прихованості $S_{\text{ТСК}}$ для інтервалу формування сигналу $T_c = 8t_0$ та різних значеннях параметра $s$.

Аналіз результатів табл. 2.4 свідчить, що збільшення ЗММ $i$ суттєво впливає на ансамбль можливих реалізацій ТСК $N_p$. При переході від $i = 4$ до $i = 5$ спостерігається найбільш інтенсивне зростання кількості можливих сигнальних реалізацій та показника структурної прихованості $S_{\text{ТСК}}$. Наприклад, при $s = 10$ для $i = 4$ кількість можливих реалізацій становить $N_p = 135751, S_{\text{ТСК}} = 17{,}05$, тоді як для $i = 5$: $N_p = 324632, S_{\text{ТСК}} = 18{,}31$.

*Таблиця 2.4*

Показники $N_p$ та $S_{\text{тск}}$ на інтервалі часу $T_c = 8t_0$ в залежності від параметрів побудови ТСК *n*=8, *s* та $i = 4, 5, 6, 7$

| № | *s* | $i = 4$ | | $i = 5$ | | $i = 6$ | | $i = 7$ | |
|---|---|---|---|---|---|---|---|---|---|
| | | $N_p$ | $S_{\text{тск}}$ | $N_p$ | $S_{\text{тск}}$ | $N_p$ | $S_{\text{тск}}$ | $N_p$ | $S_{\text{тск}}$ |
| 1 | 2 | 495 | 8,95 | 462 | 8,85 | 210 | 7,71 | 36 | 5,17 |
| 2 | 3 | 1820 | 10,83 | 2002 | 10,97 | 924 | 9,85 | 120 | 6,91 |
| 3 | 4 | 4845 | 12,24 | 6188 | 12,60 | 3003 | 11,55 | 330 | 8,37 |
| 4 | 5 | 10626 | 13,38 | 15504 | 13,92 | 8008 | 12,97 | 792 | 9,63 |
| 5 | 6 | 20475 | 14,32 | 33649 | 15,04 | 18564 | 14,18 | 1716 | 10,74 |
| 6 | 7 | 35960 | 15,13 | 65780 | 16,01 | 38760 | 15,24 | 3432 | 11,74 |
| 7 | 8 | 58905 | 15,85 | 118755 | 16,86 | 74613 | 16,19 | 6435 | 12,65 |
| 8 | 9 | 91390 | 16,48 | 201376 | 17,62 | 134596 | 17,04 | 11440 | 13,48 |
| 9 | 10 | 135751 | 17,05 | 324632 | 18,31 | 230230 | 17,81 | 19448 | 14,25 |

Отримані результати свідчать про значне розширення ансамблю сигнальних конструкцій $N_p$ при збільшенні кількості ЗММ $i$ до певного оптимального значення. Це пояснюється тим, що збільшення числа переходів $i$ між часовими інтервалами приводить до формування більшої кількості можливих часових конфігурацій сигналу, що підвищує рівень його структурної невизначеності.

Разом із тим подальше збільшення параметра $i$не приводить до необмеженого зростання структурної прихованості. Для випадку $i = 6$спостерігається зменшення кількості можливих реалізацій у порівнянні з $i = 5$. Наприклад, при $s = 10$ отримано $N_p = 230230, S_{\text{ТСК}} = 17{,}81$. Хоча значення структурної прихованості залишаються достатньо високими, вони вже менші, ніж при $i = 5$. Ще більш

помітне зменшення показників спостерігається для $i = 7$. У цьому випадку при $s = 10$: $N_p = 19448, S_{\text{ТСК}} = 14{,}25$. Таким чином, надмірне збільшення кількості ЗММ призводить до зменшення ансамблю допустимих сигнальних конструкцій $N_p$.

Причина такого ефекту полягає в особливостях формування таймерних сигналів. При надто великій кількості переходів між часовими інтервалами сигнальна конструкція стає надмірно структуровано насиченою, внаслідок чого зменшується кількість допустимих комбінацій розташування імпульсів на інтервалі формування сигналу. У результаті ансамбль реалізацій ТСК починає скорочуватися, а структурна прихованість – знижуватися.

Аналіз результатів також показує, що збільшення параметра $s$ для всіх значень $i$ приводить до монотонного зростання показників $N_p$ та $S_{\text{ТСК}}$. Наприклад, для $i = 5$ при збільшенні $s$ від 2 до 10 кількість можливих реалізацій зростає від $N_p = 462$ до $N_p = 324632$, а структурна прихованість збільшується від $S_{\text{ТСК}} = 8{,}85$ до $S_{\text{ТСК}} = 18{,}31$.

Це підтверджує, що параметр $s$ також має суттєвий вплив на рівень структурної прихованості сигналів, оскільки визначає кількість допустимих часових позицій усередині інтервалу формування ТСК.

Отримані результати свідчать про існування оптимального значення кількості ЗММ, при якому забезпечується максимальна структурна прихованість $S_{\text{ТСК}}$ таймерних сигналів. Для розглянутих умов найбільш ефективним є значення $i = 5$, при якому досягаються максимальні значення ансамблю реалізацій $N_p$ та показника структурної прихованості $S_{\text{ТСК}}$.

Отже, результати табл. 2.4 підтверджують, що підвищення структурної прихованості $S_{\text{ТСК}}$ таймерних сигналів досягається шляхом комплексного вибору параметрів $n$, $s$ та $i$. При цьому надлишкове збільшення кількості інформаційно значущих моментів модуляції може призводити до зворотного ефекту – зменшення ансамблю сигнальних конструкцій та погіршення характеристик прихованості.

На рис. 2.3 представлено залежності структурної прихованості $S_{\text{ТСК}}$ від параметра часової дискретизації $s$ та $i$=4, 5, 6 для інтервалу формування сигналу

$T_c = 8t_0$. Ці залежності демонструють вплив параметрів побудови таймерних сигналів на рівень їхньої структурної захищеності. Аналіз графіка показує, що для всіх значень кількості ЗММ $i$ спостерігається монотонне зростання структурної прихованості $S_{\text{ТСК}}$ при збільшенні параметра $s$. Це пояснюється тим, що збільшення часової дискретизації приводить до розширення множини допустимих часових позицій формування імпульсів, унаслідок чого суттєво збільшується ансамбль можливих реалізацій ТСК.

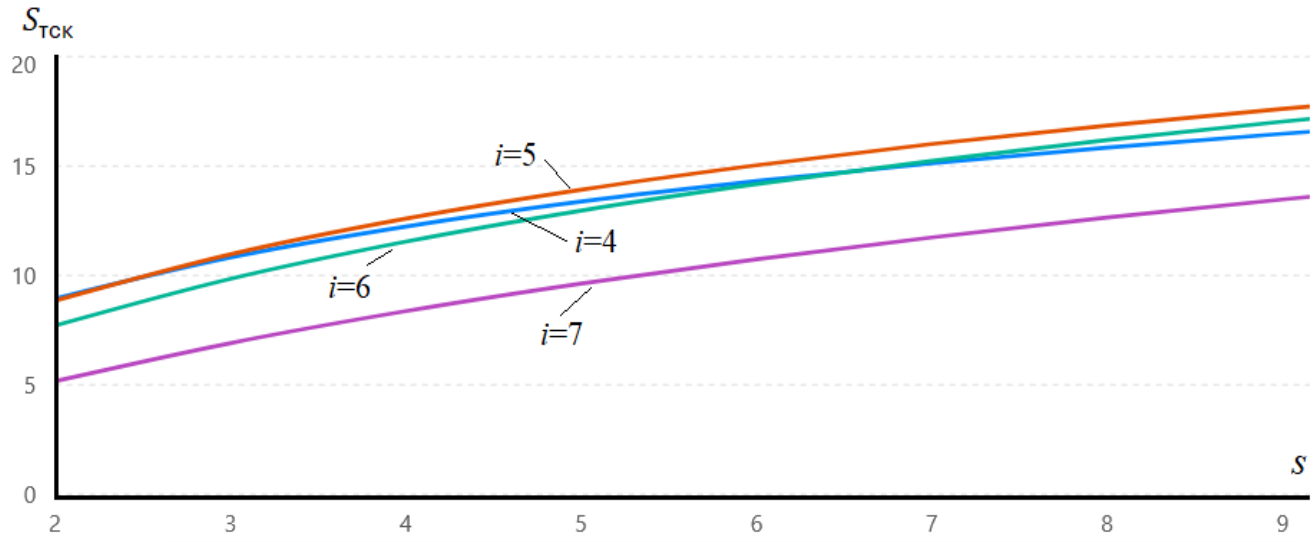



Рис. 2.3. Залежності структурної прихованості таймерних сигналів $S_{\text{ТСК}}$ на інтервалі $T_c = 8t_0$ в залежності від параметрів $s$ та $i$

Найбільш інтенсивне зростання показника структурної прихованості спостерігається для випадку $i = 5$. Саме при цьому значенні кількості ЗММ досягаються максимальні значення показника $S_{\text{ТСК}}$. Наприклад, при $s = 10$: $S_{\text{ТСК}} = 18{,}31$. Це свідчить про формування максимальної кількості допустимих сигнальних конструкцій та найвищий рівень структурної невизначеності сигналу.

Для випадку $i = 4$ також спостерігається значне зростання структурної прихованості $S_{\text{ТСК}}$ зі збільшенням параметра $s$, однак отримані значення є меншими порівняно з $i = 5$. Це пояснюється меншою кількістю можливих комбінацій розташування ЗММ.

При збільшенні кількості ЗММ до $i = 6$ показник структурної прихованості залишається достатньо високим, проте його значення вже менші, ніж для $i = 5$. Такий результат свідчить про наближення до граничного режиму насичення структури сигналу часовими переходами.

Для випадку $i = 7$ графік демонструє суттєве зниження структурної прихованості $S_{\text{ТСК}}$. Незважаючи на збільшення кількості ЗММ, ансамбль допустимих реалізацій сигналу скорочується через структурні обмеження побудови ТСК. У результаті зменшується рівень невизначеності сигналу та погіршуються характеристики прихованості.

Отримані результати підтверджують нелінійний характер залежності структурної прихованості від кількості інформаційно значущих моментів модуляції. Існує оптимальна область значень параметра $i$, при якій забезпечується максимальний рівень структурної прихованості $S_{\text{ТСК}}$ таймерних сигналів.

Таким чином, графік наочно підтверджує, що підвищення параметра часової дискретизації $s$ є ефективним способом збільшення структурної прихованості ТСК. Водночас надмірне збільшення кількості інформаційно значущих моментів модуляції може приводити до зменшення ансамблю сигнальних реалізацій та погіршення характеристик прихованості. Для досліджених умов найбільш раціональним є використання значень $i = 5$, при яких досягається максимальний рівень структурної прихованості системи передавання інформації.

На рис. 2.4 представлені залежності імовірності розкриття структури таймерних сигналів $p_{\text{стр}}$ від $s$ при різній кількості ЗММ $i$ та інтервалу формування комбінації $T_c = 8t_0$. Імовірність розкриття структури сигналу $p_{\text{стр}}$, представлена в логарифмічному масштабі, дозволяє наочно відобразити значне зменшення імовірності розкриття структури сигналу при збільшенні параметрів ТСК.

Аналіз графіка показує, що зі збільшенням параметра $s$ для всіх значень $i$ спостерігається монотонне зменшення ймовірності розкриття структури сигналу $p_{\text{стр}}$. Це пояснюється тим, що збільшення значення параметра $s$ призводить до

розширення ансамблю можливих реалізацій таймерних сигналів $N_p$, унаслідок чого ускладнюється процес аналізу сигналу засобами радіоелектронної розвідки.

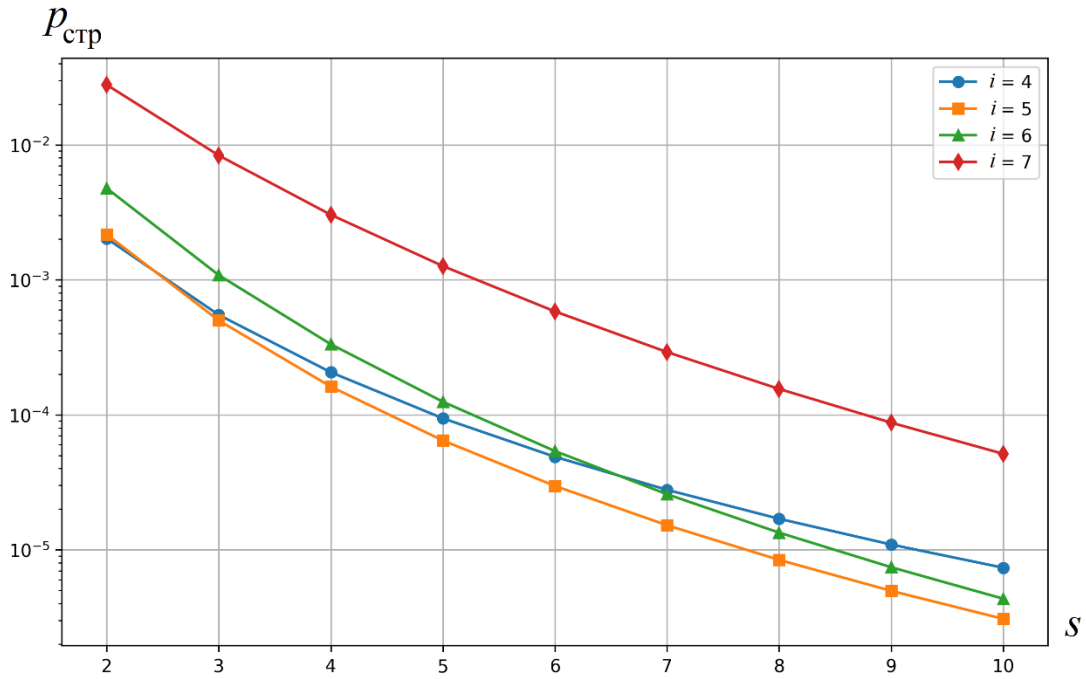



Рис. 2.4. Залежності імовірності розкриття структури таймерних сигналів $p_{\text{стр}}$

Найменші значення імовірності розкриття структури спостерігаються для випадку $i = 5$, що підтверджує результати попереднього аналізу табл. 2.4. Саме при цьому значенні кількості ЗММ забезпечується максимальний ансамбль реалізацій ТСК та найбільший рівень структурної прихованості $S_{\text{ТСК}}$.

Наприклад, при $s = 10$ для $i = 5$ імовірність розкриття структури сигналу становить приблизно $p_{\text{стр}} \approx 3 \cdot 10^{-6}$, що є найкращим показником серед досліджених варіантів. Для випадку $i = 4$ значення $p_{\text{стр}}$ також зменшується зі зростанням $s$, однак швидкість зменшення є меншою, ніж при $i = 5$. Це пов'язано з меншою кількістю можливих реалізацій ТСК.

При збільшенні кількості ЗММ до $i = 6$ спостерігається деяке погіршення характеристик прихованості порівняно з $i = 5$, хоча загальний рівень структурної захищеності залишається достатньо високим. Це свідчить про наявність

оптимального значення параметра $i$, після якого подальше збільшення кількості переходів уже не забезпечує ефективного приросту структурної прихованості.

Для випадку $i = 7$ графік демонструє найбільші значення ймовірності розкриття структури $p_{\text{стр}}$ серед усіх досліджених варіантів. Це пояснюється тим, що надмірне збільшення кількості ЗММ призводить до зменшення числа допустимих комбінацій формування сигналу, а отже – до скорочення ансамблю реалізацій ТСК.

Отримані результати підтверджують, що залежність структурної прихованості $S_{\text{ТСК}}$ від кількості ЗММ $i$ має нелінійний характер. Існує оптимальна область значень параметра $i$, при якій забезпечується мінімальна ймовірність розкриття структури сигналу та максимальна структурна прихованість.

Таким чином, графік наочно підтверджує ефективність використання таймерних сигналів для забезпечення структурної прихованості систем передавання інформації та дозволяє визначити раціональні параметри побудови комбіанцій з точки зору мінімізації ймовірності розкриття структури сигналу.

## 2.5 Метод захисту інформації на основі системи залишкових класів при формуванні таймерних сигнальних конструкцій

Одним із перспективних напрямів підвищення захищеності передавання інформації в умовах радіоелектронного протиборства є використання непозиційних методів подання даних та формування складних сигнальних конструкцій. Особливого значення такі методи набувають у військових та спеціальних інформаційно-комунікаційних системах, де поряд із забезпеченням завадостійкості необхідно реалізувати структурну прихованість та стійкість до несанкціонованого перехоплення сигналів.

Класичні методи захисту інформації [30, 65-67], що базуються виключно на криптографічному перетворенні або застосуванні класичних завадостійких кодів [14, 76], не завжди забезпечують необхідний рівень ефективності в умовах навмисних радіоелектронних впливів. Засоби радіоелектронної розвідки здатні

здійснювати виявлення характерних структурних ознак сигналів, визначати параметри їх формування та виконувати аналіз передаваних повідомлень [39, 40]. У зв’язку з цим актуальною є розробка методів, які поєднують властивості коригувального кодування та структурної прихованості сигнально-кодових конструкцій.

Одним із таких методів є застосування системи залишкових класів (СЗК) у поєднанні з таймерними сигналів. СЗК базується на китайській теоремі про залишки та передбачає представлення цілого числа у вигляді набору незалежних залишків за взаємно простими модулями [79]. Подібний спосіб подання інформації дозволяє розподілити інформаційний об’єкт між декількома незалежними каналами представлення та істотно ускладнити структуру сигнальної конструкції.

Нехай задано множину попарно взаємно простих модулів $\{p_1, p_2, \dots, p_l\}$, для яких виконується умова:

$$P = p_1 p_2 \dots p_l. \tag{2.23}$$

Тоді будь-яке число

$$A < P \tag{2.24}$$

може бути однозначно представлене у СЗК набором залишків

$$(A_1, A_2, \dots, A_l), \tag{2.25}$$

де

$$A_i = A mod p_i, i = 1,2, \dots, l. \tag{2.26}$$

Представлення числа у вигляді набору залишків має ряд важливих властивостей. По-перше, арифметичні операції виконуються незалежно в кожному модулі:

$$A \pm B \bmod P \leftrightarrow (A_1 \pm B_1 \bmod p_1, \dots, A_l \pm B_l \bmod p_l). \quad (2.27)$$

По-друге, забезпечується можливість паралельної обробки інформації та локалізації помилок при введенні надлишкових модулів. По-третє, залишкове представлення не містить прямого позиційного відображення інформації, що ускладнює її реконструкцію стороннім спостерігачем. Відновлення числа з набору залишків виконується за допомогою китайської теореми про залишки:

$$\begin{cases} A \equiv A_1 (\bmod p_1) \\ A \equiv A_2 (\bmod p_2) \\ \quad \vdots \\ A \equiv A_l (\bmod p_l) \end{cases}, \quad (2.28)$$

що гарантує існування єдиного розв'язку в межах інтервалу $0 \le A < P$.

Використання СЗК при формуванні таймерних сигналів передбачає інтерпретацію залишків не як цифрових символів, а як параметрів часової структури сигналу. Основою формування ТСК є базовий часовий елемент $\Delta$, тривалість якого менша за інтервал Найквіста $t_0$. Кількість часових елементів у межах інтервалу Найквіста визначається як $s = t_0/\Delta$. Формування ТСК здійснюється за наступних умов:

1) тривалість імпульсів $t_c$ повинна бути не менше $t_0$, тобто $t_c \ge t_0$;

2) тривалість окремого імпульсу задається співвідношенням $t_c = t_0 + \Delta k$, де $k = 0,1, \dots$ визначається кодовими словами СЗК;

3) обирається певна кількість ЗММ $= 1, 2, \dots, m-1$;

4) визначається інтервал побудови ТСК $T_c = t_0 m$, де $m$ – кількість інтервалів Найквіста.

На відміну від позиційних кодів, у яких інформація визначається положенням бітів у кодовому слові, у ТСК інформаційне навантаження переноситься часовими інтервалами між імпульсами. Це суттєво підвищує структурну складність сигналу та знижує можливість його класифікації засобами радіоелектронної розвідки. Кількість можливих таймерних сигнальних конструкцій визначається

як $N_{\text{р}} = [ns - i(s-1)]!/i!\,(ns - is)!$, де $n$ – кількість часових позицій, $s$ – число часових елементів, $i$ – кількість значущих моментів модуляції. Далі буде розглянуто практичний приклад формування ТСК на основі модулів $P_1 = 2$, $P_2 = 3$, $P_3 = 7$, побудову кодових слів, визначення інтервалів $T_c$та оцінку структурної прихованості таких сигнальних конструкцій.

Розглянемо практичну реалізацію методу формування таймерних сигнальних конструкцій із використанням системи залишкових класів. Для цього оберемо набір взаємно простих модулів: $P_1 = 2$, $P_2 = 3$, $P_3 = 7$. Загальна область представлення чисел у такій системі визначається добутком модулів:

$$N_{\text{тск}} = P_1 \times P_2 \times P_3 = 2 \times 3 \times 7 = 42.$$

Це означає, що в межах обраної системи можуть бути однозначно представлені всі числа: $A \in [0; 42)$. Кожне число перетворюється у залишковий вектор вигляду $(A_1, A_2, A_3)$, де:

$$A_1 = A \bmod 2,$$
$$A_2 = A \bmod 3,$$
$$A_3 = A \bmod 7.$$

Таким чином формується сукупність із $N_{\text{тск}} = 42$ кодових комбінацій. На відміну від класичного цифрового подання, залишкові вектори використовуються не як послідовності двійкових символів, а як параметри формування часової структури таймерного сигналу. Кожний залишок визначає тривалість окремого імпульсу або часовий інтервал між значущими моментами модуляції.

Нехай базовий інтервал Найквіста містить $s = 4$ часових елементи: $t_0 = 4\Delta$. Тоді тривалості імпульсів визначаються відповідно як $t_c = t_0 + \Delta k$. Розглянемо приклад формування ТСК для кодового слова з трьох імпульсів, які зазначені під номером 22 табл. 2.5, з мінімальною сумою залишків: (0,1,1).

Тривалості імпульсів становить:

$$t_{c1} = t_0 + \Delta \cdot 0 = t_0;$$
$$t_{c2} = t_0 + \Delta \cdot 1 = t_0 + \Delta;$$
$$t_{c3} = t_0 + \Delta \cdot 1 = t_0 + \Delta.$$

За умови $t_0 = 4\Delta$ отримуємо $T_c(0,1,1) = 4\Delta + 5\Delta + 5\Delta = 14\Delta$. Отже, $T_c(0,1,1) = 3t_0 + 2\Delta$. Розглянемо протилежний випадок – комбінацію з максимальною сумою залишків: $(1,2,6)$ (№ 41 табл. 2.6). Тоді:

$$t_{c1} = t_0 + \Delta,\ t_{c2} = t_0 + 2\Delta,\ t_{c3} = t_0 + 6\Delta.$$

Сумарний інтервал побудови становить:

$$T_c(1,2,6) = t_0 + \Delta + t_0 + 2\Delta + t_0 + 6\Delta.$$

З урахуванням $t_0 = 4\Delta$ одержимо:

$$T_c(1,2,6) = 4\Delta + \Delta + 4\Delta + 2\Delta + 4\Delta + 6\Delta = 21\Delta$$

Тобто:

$$T_c(1,2,6) = 5t_0 + \Delta.$$

Отримані результати свідчать, що часові інтервали різних ТСК є нерівномірними. Це створює проблему синхронізації та потребує нормалізації інтервалу формування сигналів. Для забезпечення виконання умови $t_c \geq t_0$ та уніфікації часової структури ТСК можуть бути використані декілька варіантів.

Перший варіант передбачає введення додаткового захисного інтервалу $t_0$ до максимальної комбінації. Тоді:

$$T_{cz1}(1,2,6) = 5t_0 + \Delta + t_0 = 6t_0 + \Delta.$$

За умови, що $t_0 = 4\Delta$ одержимо $T_{cz1} = 25\Delta$. У цьому випадку всі сигнальні конструкції формуються в межах єдиного інтервалу, однак виникає суперечність щодо цілочисельності параметра $m$ на інтервалі часу $T_c = mt_0$.

Другий варіант передбачає додаткове збільшення максимальної комбінації на $3\Delta$. Тоді:

$$T_{cz2} = 25\Delta + 3\Delta = 28\Delta.$$

В цьому випадку $T_{cz2} = 7t_0$, тобто забезпечуються $m = 7$, що задовольняє умову цілочисельності інтервалу побудови ТСК.

Третій варіант передбачає виключення максимальної комбінації $(1, 2, 6)$ та використання другої за тривалістю конструкції $(0,2,6)$. Після введення додаткового захисного інтервалу $t_0$ одержуємо

$T_{cz3} = t_0 + t_0 + 2\Delta + t_0 + 6\Delta + t_0$. Звідси $T_{cz3} = 24\Delta = 6t_0$.

У такому випадку $m = 6$, а кількість допустимих комбінацій зменшується: $N_{\text{тск}} = 41$.

Запропоновані варіанти демонструють можливість керування часовою структурою таймерних сигналів на основі СЗК та дозволяють забезпечити синхронізацію при збереженні структурної складності сигнальних конструкцій.

Таблиця 2.5

Кодові слова, що сформовані на основі модулів $P_1 = 2, P_2 = 3, P_3 = 7$ для № 1 … 10

| № | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 3 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 |
| 7 | 1 | 2 | 3 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| № | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 3 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 |
| 7 | 1 | 2 | 3 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |

Таблиця 2.6

Кодові слова, що сформовані на основі модулів $P_1 = 2, P_2 = 3, P_3 = 7$ для № 11 … 21

| № | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 3 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| 7 | 4 | 5 | 6 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| № | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 3 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 |
| 7 | 4 | 5 | 6 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |

Важливою особливістю сформованих ТСК є те, що інформація передається не значенням бітових символів, а часовими параметрами імпульсів. У результаті

навіть при перехопленні сигналу засобами радіоелектронної розвідки встановлення закону формування залишкових комбінацій є суттєво складнішим порівняно з класичними позиційними кодами.

Приклад синтезу таймерних сигналів, що сформовані на основі кодових слів (0, 2, 6), (1, 1, 5) та (1, 2, 5), надано на рис. 2.5. Всі імпульси $t_{с1}$, $t_{с2}$, $t_{с3}$ та $t_{с4}$ таймерних сигналів $X(0,2,6)$, $X(1,1,5)$ та $X(1,2,5)$ задовільнять умові (2.29), (2.20) і (2.31). В отриманих таймерних конструкціях кількість ЗММ $i = 3$.

Розглянемо для порівняльного аналізу завадостійкий код Хемінга з параметрами:

1) $n = 7$ – загальна кількість біт;

2) $k = 4$ –кількість інформаційних біт;

3) $r = 3$ – кількість перевірочних біт;

4) $d_0 = 3$ – мінімальна кодова відстань між дозволеними кодовими комбінаціями.

Код Хемінга має $N_{\text{доз рцк}} = 2^k = 16$ дозволених комбінацій та $N_{\text{ндоз рцк}} = 2^n - 2^k = 112$ недозволених комбінацій, кодову швидкість $\gamma_{\text{к}} = k/n = 4/7 = 0{,}57$ та виявляє до двох помилкових біт.

Розглянуті таймерні сигнали мають $N_{\text{доз тск}}(2,3,7) = 41$ дозволену комбінацію та не потребують додаткових перевірочних біт для виявлення помилок. Загальна кількість ТСК $N_{\text{заг тск}} = 455 \gg N_{\text{заг рцк}} = 2^n = 128$ та формуються на меншому інтервалі часу, тобто $m = 6 < n = 7$.

Для оцінки захищеності сигнальних конструкцій визначимо структурну прихованість ТСК і розрядно-цифрового коду, яка визначається з урахуванням загального числа $N_{\text{р}}$ можливих комбінацій, які використовуються для передавання інформаційних символів $S = \log_2 N_{\text{р}}$. Потенційну прихованість для ТСК оцінимо з урахуванням максимальної кількості комбінацій $S_{\text{п тск}} = \log_2 455 = 9$ дв. вим. Аналогічним чином оцінимо для коду Хемінга: $S_{\text{п рцк}} = \log_2 128 = 7$. Бачимо, що $S_{\text{п тск}} > S_{\text{п рцк}}$, що свідчить також про можливість таймерних сигналів забезпечувати функції захисту інформації від НСД.

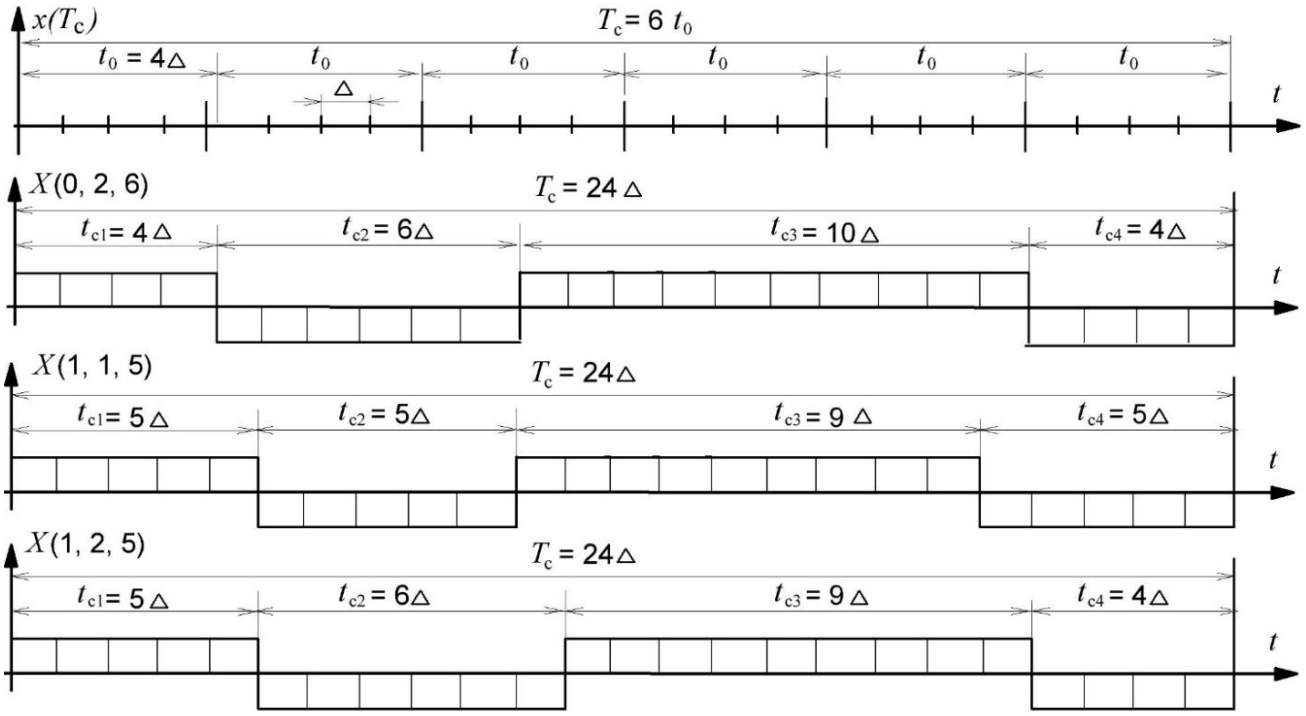



Рис. 2.5. Приклади формування ТСК за кодовими словами (0, 2, 6), (1, 1, 5) та (1, 2, 5)

Більшу кількість комбінацій можна сформувати з використанням інших простих модулів, наприклад {3, 5, 7} або {2, 3, 5, 7, 11}. За допомогою цих модулів загальна кількість ТСК $N_{\text{тск}} = 3 \times 5 \times 7 = 105$ та $N_{\text{тск}} = 2 \times 3 \times 5 \times 7 \times 11 = 2310$.

## 2.6 Висновки до розділу 2

1. У розділі проведено дослідження таймерних сигнальних конструкцій як основи побудови прихованих систем передавання інформації. Виконано аналіз основних інформаційних характеристик сигналів, що впливають на рівень структурної прихованості, завадостійкості та ефективності функціонування захищених каналів зв’язку.

2. Розглянуто ентропійні характеристики сигнальних конструкцій та показано, що збільшення кількості можливих сигнальних реалізацій приводить до

зростання інформаційної невизначеності сигналу й підвищення рівня його структурної прихованості. На основі формул Шеннона та Хартлі встановлено взаємозв'язок між інформаційною ємністю сигналу та параметрами побудови таймерних сигнальних конструкцій.

3. Проведено аналіз впливу параметрів побудови таймерних сигнальних конструкцій $n$, $s$ та $i$ на кількість реалізацій сигналів $N_p$, показник структурної прихованості $S_{\text{ТСК}}$ та ймовірність розкриття структури сигналу $p_{\text{стр}}$. Встановлено, що збільшення параметра часової дискретизації $s$приводить до розширення ансамблю сигнальних конструкцій і підвищення структурної прихованості.

4. Показано, що збільшення кількості інформаційно значущих моментів модуляції $i$ приводить до зростання структурної прихованості лише до певного оптимального значення. Для досліджених умов максимальні значення показників структурної прихованості досягаються при $i = 5$. Подальше збільшення кількості ЗММ призводить до зменшення кількості допустимих реалізацій сигналів та погіршення характеристик прихованості.

5. Дослідження формування ТСК на основі системи залишкових класів підтвердило можливість поєднання завадостійкого кодування та структурної прихованості в єдиній сигнально-кодовій конструкції. Для модулів $\{2, 3, 7\}$ було сформовано $N_{\text{тск}} = 42$ комбінації, з яких після нормалізації залишилося $N_{\text{доз}} = 41$допустима ТСК. При $s = 4$ часові інтервали змінювалися в межах $14\Delta \le T_c \le 21\Delta$, а після введення захисних інтервалів були отримані нормалізовані значення $T_{cz1} = 25\Delta$, $T_{cz2} = 28\Delta = 7t_0$та $T_{cz3} = 24\Delta = 6t_0$.

6. Порівняльний аналіз ТСК та класичного коду Хемінга $(7, 4)$ показав, що код Хемінга забезпечував лише $N_{\text{доз}} = 16$ дозволених комбінацій при кодовій швидкості $\gamma_k = 0{,}57$, тоді як ТСК на основі СЗК формували 41 дозволену комбінацію без введення додаткових перевірочних біт. Загальна кількість потенційних таймерних комбінацій становила $N_{\text{заг тск}} = 455$, що суттєво перевищувало можливості позиційного коду $N_{\text{заг рцк}} = 2^7 = 128$.

7. Отримані результати підтверджують ефективність використання таймерних сигнальних конструкцій для побудови захищених систем передавання інформації та створюють теоретичне підґрунтя для подальшого розроблення комбінованих методів забезпечення структурної прихованості та завадостійкості каналів зв’язку.

# РОЗДІЛ 3
# РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛІВ НА ОСНОВІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У третьому розділі досліджено методи прямого розширення спектра таймерних сигналів на основі псевдовипадкових послідовностей як засобу підвищення рівня захисту інформації в інформаційно-комунікаційних системах. Проаналізовано кореляційні, структурні та статистичні властивості класичних і хаотичних псевдовипадкових послідовностей, а також оцінено їх придатність для формування широкосмугових шумоподібних сигналів із підвищеним рівнем структурної та енергетичної прихованості. Досліджено вплив бази сигналу на показники прихованості, завадостійкості та ефективності передавання інформації. Обґрунтовано доцільність використання хаотичних псевдовипадкових послідовностей і системи залишкових класів для формування широкосмугових таймерних сигналів, що забезпечують підвищення стійкості інформаційно-комунікаційних систем до виявлення, перехоплення та інших кіберзагроз.

## 3.1 Основні принципи розширення спектра сигнальних конструкцій

Одним із найбільш ефективних методів підвищення прихованості та завадостійкості передавання інформації в інформаційно-комунікаційних системах є застосування методів розширення спектра позиційних сигналів [54, 75, 84,90]. До класичних методів розширення спектра належать: метод прямого розширення спектра за допомогою псевдовипадкових послідовностей (ПРС-ПВП; псевдовипадкове перелаштування робочих частот (ППРЧ, FHSS – Frequency Hopping Spread Spectrum); метод на основі лінійної частотної модуляції (ЛЧМ); комбіновані методи спектрального розширення. Основна ідея таких методів полягає у навмисному збільшенні ширини спектра передаваного сигналу порівняно з мінімально необхідною смугою частот для передавання інформації. У загальному

випадку база сигналу визначається як $B = \Delta f \cdot T$, де $\Delta f$ – ширина спектра сигналу; $T$ – тривалість сигналу. Одним із найбільш поширених методів широкосмугового передавання інформації є метод ПРС-ПВП [84,90], формування якого полягає у перемноженні інформаційного позиційного сигналу на високошвидкісну псевдовипадкову послідовність

$$s_{DSSS}(t) = m(t_0) \cdot c(\tau), \tag{3.1}$$

де $(t_0)$ – інформаційний сигнал; $c(\tau)$ – псевдовипадкова послідовність. При цьому тривалість ПВП

$$\tau \ll t_0. \tag{3.2}$$

У результаті такого перетворення спектр сигналу розширюється пропорційно швидкості зміни елементів ПВП $\tau$. Після приймання сигналу виконується кореляційне згортання з тією ж ПВП, що дозволяє відновити початковий сигнал та зменшити вплив вузькосмугових завад.

У результаті енергія сигналу розподіляється в широкому частотному діапазоні, що призводить до зменшення спектральної щільності потужності та ускладнює виявлення сигналу засобами радіоелектронної розвідки.

Зі збільшенням бази сигналу підвищується його енергетична прихованість, оскільки енергія сигналу розподіляється у ширшому спектральному діапазоні. Одночасно зростає завадостійкість системи завдяки можливості використання кореляційної обробки сигналу на приймальній стороні.

Для оцінювання коефіцієнта розширення спектра використовується співвідношення [90]:

$$K_s = \frac{\Delta f_s}{\Delta f_i}, \tag{3.3}$$

де $\Delta f_s$ – ширина спектра після розширення; $\Delta f_i$ – ширина спектра інформаційного сигналу. Збільшення коефіцієнта розширення спектра $K_s$ дозволяє зменшити спектральну щільність потужності:

$$G(f) = \frac{P_s}{\Delta f_s}, \tag{3.4}$$

де $P_s$ – потужність сигналу. Отже, при зростанні ширини спектра $\Delta f_s$ зменшується значення $G(f)$, що забезпечує підвищення енергетичної прихованості сигналу.

Як правило, класичні методи розширення спектра орієнтовані на використання з позиційними сигналами, у яких інформація передається зміною амплітуди, частоти або фази несучого коливання. Для таких сигналів розширення спектра реалізується шляхом безпосереднього накладання ПВП на інформаційний сигнал або шляхом зміни частоти передавання.

Однак таймерні сигнальні конструкції мають іншу структуру формування інформаційних ознак. У ТСК інформація передається не параметрами гармонічного коливання, а часовими інтервалами між імпульсами або їх тривалістю. Це означає, що класичні DSSS-методи не можуть бути безпосередньо застосовані до таймерних сигналів без зміни принципів формування сигнальної конструкції.

Особливість таймерних сигналів полягає в тому, що їх інформаційна структура формується в часовій області. Тому розширення спектра ТСК повинно враховувати: часову структуру сигналу; варіативність таймерних інтервалів; синхронізацію часових позицій; збереження інформаційної місткості; кореляційні властивості псевдовипадкових послідовностей.

У цьому випадку псевдовипадкові послідовності можуть використовуватись не лише для розширення спектра, а й для стохастичної зміни часової структури таймерного сигналу. Це дозволяє формувати шумоподібні широкосмугові сигнали зі складною часовою організацією та зниженими кореляційними ознаками.

Для широкосмугових таймерних сигналів особливого значення набуває оцінка автокореляційної функції (1.6) та взаємно-кореляційної функції [14, 27]:

$$R_{12}(\tau) = \int s_1(t)s_2(t-\tau)\,dt \qquad (3.5)$$

Низький рівень бічних пелюсток автокореляційної функції та малі значення взаємної кореляції між сигналами забезпечують зниження ймовірності виявлення та підвищення структурної прихованості.

Перспективним напрямом є використання псевдовипадкових послідовностей Уолша, а також хаотичних послідовностей, сформованих на основі динамічних систем. Такі сигнали характеризуються широким спектром, низькою кореляцією та високою складністю прогнозування їх структури.

Отже, класичні методи розширення спектра ефективно застосовуються для позиційних сигналів, однак для таймерних сигналів виникає потреба у розробленні нових алгоритмів спектрального розширення, які враховують часову структуру побудови ТСК та забезпечують підвищення енергетичної й структурної прихованості передавання інформації.

## 3.2 Обґрунтування та вибір псевдовипадкових послідовностей для розширення спектра позиційних сигналів

Ефективність практичної реалізації метод ПРС-ПВП значною мірою визначається кореляційними, структурними та ансамблевими властивостями використовуваних ПВП. У системах зв’язку з позиційними сигналами кодова послідовність $c(t)$, яка використовується для розширення спектра, повинна забезпечувати одночасне виконання декількох суперечливих вимог: високу завадостійкість, низький рівень взаємних завад, швидку синхронізацію та підвищену структурну прихованість сигналу.

Основними типами псевдовипадкових послідовностей [64, 74, 75, 84, 88], що використовуються в сучасних системах ПРС-ПВП, є: $M$-послідовності; послідовності Голда; послідовності Касамі; ортогональні коди Уолша; хаотичні псевдовипадкові послідовності.

$M$-послідовності формуються за допомогою лінійних регістрів зсуву зі зворотними зв'язками (LFSR) та мають максимальний можливий період:

$$N = 2^n - 1\,, \tag{3.6}$$

де $n$ – розрядність регістра. Основною перевагою $M$-послідовностей є їхні майже ідеальні автокореляційні властивості. Періодична автокореляційна функція має вигляд [26, 27]:

$$R_p(\tau) = \begin{cases} 1, & \tau = 0, \pm N, \pm 2N, \dots \\ -\frac{1}{N}, & \tau \neq 0. \end{cases}. \tag{3.7}$$

Наявність вузького центрального піка та малих бічних пелюсток забезпечує ефективну синхронізацію сигналів у приймачі та високу завадостійкість системи.

Разом із тим $M$-послідовності мають ряд суттєвих недоліків. Найбільш критичним є високий рівень взаємної кореляції між різними послідовностями ансамблю. Це призводить до збільшення міжканальних завад у багатокористувацьких системах зв'язку.

Крім того, *M*-послідовності характеризуються низькою лінійною складністю, що знижує рівень структурної прихованості. Завдяки лінійній структурі генерації така послідовність може бути відновлена за допомогою алгоритму Берлекемпа–Мессі після перехоплення фрагмента довжиною приблизно *2n* елементів. Це створює потенційну вразливість до засобів радіоелектронної розвідки.

Для покращення взаємно-кореляційних властивостей використовуються послідовності Голда, які формуються шляхом modulo-2 додавання двох спеціально підібраних $M$-послідовностей однакової довжини [26, 27]:

$$g_i = a_i \oplus b_i. \tag{3.8}$$

Головною перевагою кодів Голда є обмежений рівень бічних сплесків взаємно-кореляційної функції. Максимальне значення ВКФ визначається [26, 27]:

$$t(n) = \begin{cases} 1 + 2^{(n+1)/2}, & \text{для непарних } n, \\ 1 + 2^{(n+2)/2}, & \text{для парних } n. \end{cases} \quad (3.9)$$

Послідовності Голда дозволяють формувати великий ансамбль кодів:

$$N_G = N + 2, \quad (3.10)$$

де $N$ – період базової $M$-послідовності. Завдяки цьому вони широко використовуються в системах CDMA та інших багатокористувацьких системах зв'язку. Однак, незважаючи на покращені кореляційні характеристики, послідовності Голда також мають регулярну структуру, що може бути виявлена методами статистичного та кореляційного аналізу.

У випадках, коли необхідно мінімізувати рівень взаємних завад між сигналами, застосовуються послідовності Касамі. Вони формуються шляхом спеціальної вибірки елементів із $M$-послідовності. Максимальний рівень бічних сплесків взаємно-кореляційної функції для кодів Касамі становить:

$$R_{max} = 2^{n/2}. \quad (3.11)$$

Це забезпечує кращі взаємно-кореляційні властивості порівняно з кодами Голда. Перевагами кодів Касамі є: низький рівень взаємної кореляції; підвищена завадостійкість; ефективність у багатоканальних системах. Основним недоліком є обмежений обсяг ансамблю:

$$N_K = 2^{n/2}, \quad (3.12)$$

що знижує можливість використання великої кількості незалежних кодових каналів.

Окремий клас ортогональних ПВП становлять послідовності Уолша, які формуються на основі матриць Адамара [26, 27]:

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix}. \tag{3.13}$$

Основною властивістю кодів Уолша є взаємна ортогональність:

$$\sum_{i=1}^{N} w_k\,(i) w_l(i) = 0, k \neq l. \tag{3.14}$$

Це дозволяє повністю усунути міжканальні завади в ідеально синхронізованих системах. Разом із тим послідовності Уолша характеризуються: високою регулярністю структури; наявністю виражених спектральних компонент; передбачуваністю кодових комбінацій. У результаті рівень структурної прихованості таких сигналів є відносно низьким.

Для систем із підвищеними вимогами до прихованості перспективним є використання хаотичних псевдовипадкових послідовностей, сформованих на основі нелінійних динамічних систем. Одним із найпоширеніших прикладів є логістичне відображення:

$$x_{n+1} = r x_n (1 - x_n). \tag{3.15}$$

При значеннях параметра $r > 3{,}57$ система переходить у режим динамічного хаосу, а сформовані послідовності набувають властивостей псевдовипадковості. При $r = 3{,}9$ спостерігається стабільний хаотичний процес. Після квантування формується двійкова послідовність:

$$c_n = \begin{cases} 1, & x_n \geq 0.5, \\ -1, & x_n < 0.5. \end{cases} \tag{3.16}$$

Хаотичні послідовності [31, 64, 74] характеризуються: широким неперервним спектром; високою ентропією; низькою кореляційною помітністю; складністю прогнозування; високою структурною прихованістю. На відміну від класичних лінійних ПВП, хаотичні послідовності значно складніше піддаються відновленню засобами РЕР.

Аналіз властивостей класичних ПВП показує, що жоден тип послідовностей не є універсальним. $M$-послідовності забезпечують хорошу синхронізацію, коди Голда – компроміс між розміром ансамблю та взаємною кореляцією, коди Касамі – мінімальний рівень взаємних завад, а послідовності Уолша – ортогональність сигналів.

Однак усі класичні лінійні ПВП мають спільний недолік – передбачуваність структури та наявність регулярних кореляційних ознак. Це знижує рівень структурної прихованості сигналів та створює можливість їх ідентифікації засобами радіоелектронної розвідки.

У зв’язку з цим перспективним напрямом є використання комбінованих методів формування ПВП, які передбачають: нелінійне перетворення кодових послідовностей; динамічну зміну параметрів генерації; інтеграцію хаотичних процесів; адаптивне керування структурою сигналу. Такі методи дозволяють підвищити не лише завадостійкість, а й структурну приховання систем передавання інформації.

## 3.3 Кількісна оцінка та порівняльний аналіз структурної прихованості псевдовипадкових послідовностей

Для об’єктивного порівняльного аналізу розглянутих типів ПВП проведемо кількісну оцінку їхньої структурної прихованості $S_{\text{стр}}$. Під структурною прихованістю розумітимемо кількість інформації (у бітах), яку необхідно перехопити та аналізувати засобам РЕР для повного відновлення закону функціонування генератора ПВП.

У випадку лінійних послідовностей на основі регістрів, сформованих за допомогою LFSR, стійкість до розкриття визначається їхньою лінійною складністю $L$, що дорівнює мінімальній довжині регістра зсуву, здатного згенерувати дану послідовність. Згідно з алгоритмом Берлекемпа–Мессі, для повного зламу лінійної системи РЕР достатньо перехопити фрагмент послідовності довжиною $2L$ чипів. Отже, для таких ПВП структурна прихованість еквівалентна кількості біт, що однозначно задають початковий стан та коефіцієнти зворотного зв'язку регістра:

$$S_{\text{стр LFSR}} = 2L. \tag{3.17}$$

Для порівняння обчислимо значення $S_{\text{стр}}$ для базових ПВП однакового періоду $N = 2^n - 1$ (або близької довжини для кодів Уолша $N = 2^n$):

1) Оскільки *M*-послідовність формується одним лінійним регістром розрядності $n$, її лінійна складність є мінімальною і дорівнює $L = n$. Відповідно до (3.16), структурна прихованість становить:

$$S_{\text{стр } M} = 2n\,. \tag{3.18}$$

Наприклад, для регістра довжиною $n = 10$ ($N = 1023$ чипи), засіб РЕР розкриє структуру сигналу, перехопивши лише $2L = 20$ біт інформації.

2) Послідовності Голда формуються як сума за модулем 2 двох $M$-послідовностей. Лінійна складність результуючої послідовності дорівнює сумі лінійної складності базових регістрів: $L = n$. Таким чином, структурна прихованість зростає вдвічі порівняно з *M*-послідовностями:

$$S_{\text{стр Голд}} = 4n. \tag{3.19}$$

Для $n = 10$ значення структурної прихованості становитиме $S_{\text{стр Голд}} = 40$ дв. вим.

3) Послідовності Касамі формуються на основі проріджування базової *M*-послідовності. Їхня лінійна складність становить $L = \frac{3}{2}n$ (для парних $n$). Структурна прихованість визначається як:

$$S_{\text{стр Касамі}} = 3n. \tag{3.20}$$

При $n = 10$ значення прихованості дорівнює $S_{\text{стр Касамі}} = 30$ біт.

4) Ортогональні послідовності Уолша мають детермінований характер побудови завдяки використання матриць Адамара. Кожна послідовність довжиною $L = 2^n$ однозначно визначається своїм порядковим номером у матриці. Лінійна складність ряду функцій Уолша є вкрай низькою і для найгірших випадків (наприклад, функцій типу Rademacher) становить $L = \log_2 N = n$. Максимальна лінійна складність окремих функцій не перевищує $N$. Однак, зважаючи на високу регулярність структури та наявність фіксованих спектральних ліній, сторонній спостерігач здатний класифікувати ансамбль за допомогою швидкого перетворення Уолша–Адамара (FHT). Для розкриття конкретного каналу достатньо визначити його індекс серед $N$ можливих варіантів, що забезпечує ентропійну скритність на рівні:

$$S_{\text{стр Уолш}} = \log_2 N = n \quad . \tag{3.21}$$

5) Хаотичні псевдовипадкові послідовності на відміну від попередніх лінійних структур, сформовані за допомогою нелінійних відображень (наприклад, логістичного відображення (3.14)), мають теоретично нескінченну лінійну складність ($L \to \infty$). Спроби застосування алгоритму Берлекемпа–Мессі до таких послідовностей призводять до отримання значення $L \approx N/2$, що вимагає перехоплення майже всієї послідовності ($2L \approx N$). Структурна прихованість хаотичної системи визначається розрядністю представлення дійсних чисел у процесорі (floating-point precision) та чутливістю до початкових умов. Для

стандарту IEEE 754 (double precision) початковий стан $x_0$ та параметр керування $\lambda$ задаються 64-бітними числами (з яких 52 біти – мантиса). Таким чином, ентропійна прихованість генератора визначається сумарною невизначеністю ключових параметрів:

$$S_{\text{стр Хаос}} = b_{x0} + b_{\lambda}, \qquad . \tag{3.22}$$

де $b_{x0}$ та $b_{\lambda}$ – ефективна кількість біт інформації, що визначають точність завдання початкової точки та параметра відображення відповідно (практично досягається рівень $S_{\text{стр Хаос}} \geq 104 \ldots 128$ біт на один крок ініціалізації, незалежно від тривалості $N$).

Для узагальнення проведених розрахунків та наочного порівняння параметрів структурної прихованості при фіксованому періоді послідовності $N = 1023$ (для кодів Уолша $N = 1024$, розрядність регістрів $n = 10$) сформовано зведену табл. 3.1.

Аналіз даних табл. 3.1 наочно демонструє, що класичні лінійні ПВП (*M*-послідовності, коди Голда та Касамі), попри їхні високі кореляційні властивості, мають критично низькі показники структурної прихованості (20 … 40 біт). Це дозволяє сучасним комплексам радіоелектронної розвідки здійснювати автоматизоване перехоплення та розкриття структури таких сигналів у реальному часі.

Хаотичні послідовності забезпечують значне підвищення прихованості ($S_{\text{стр Хаос}} \geq 104$, проте їх впровадження обмежується складністю генерації ідентичних аналогових хаотичних траєкторій на передавальній та приймальній сторонах в умовах завад.

Отримані кількісні оцінки підтверджують наукову необхідність розробки нових комбінованих методів спектрального розширення, які б поєднували високу структурну прихованість нелінійних/хаотичних систем із математичною строгістю та надійною синхронізацією лінійних ПВП. Самим таким комбінованим рішенням

є інтеграція ПВП у часовий простір непозиційних таймерних сигнальних конструкцій (ТСК), що детально розглянуто у наступних розділах.

*Таблиця 3.1*

Порівняльні характеристики структурної прихованості різних типів ПВП

| Тип кодової послідовності | Математична основа формування | Лінійна складність $L$ (чипів) | Кількість чипів для розкриття РЕР ($2L$) | Структурна прихованість $S_{\text{стр}}$ (біт) |
|---|---|---|---|---|
| $M$-послідовність | Лінійний регістр зсуву (LFSR) | $n = 10$ | 20 | 20 |
| Послідовності Голда | Поелементна сума двох LFSR | $2n = 20$ | 40 | 40 |
| Послідовності Касамі | Вибірка (проріджування) LFSR | $1{,}5n = 15$ | 30 | 30 |
| Коди Уолша | Матриці Адамара (детерміновані) | $10 \ldots 1024$ | Залежить від індексу | $\approx 10$ |
| Хаотичні ПВП | Нелінійне логістичне відображення | $\approx N/2 = 512$ | $\approx N/2 = 1024$ | $\geq 104$ |

## 3.4 Методи підвищення прихованості псевдовипадкових послідовностей, що формуються на основі генераторів хаосу

Розвиток та інтенсифікація засобів РЕБ [5, 6, 7, 39, 40, 85] зумовлюють жорсткі вимоги до СКК, що використовуються у спеціальних ІКС. Такі конструкції повинні одночасно поєднувати високі показники завадостійкості, прихованості та криптографічної стійкості [20-21]. Одним із перспективних напрямів вирішення цієї задачі є застосування детермінованого хаосу [74, 82]. Хаотичні коливання, завдяки своїй структурі, мають унікальні властивості: високу чутливість до початкових умов; широкий і суцільний спектральний діапазон; статистичні

характеристики, що є близькими до білого шуму. Це дозволяє розглядати генератори хаосу як ефективну основу для формування ПВП із високим рівнем ентропії та низькими коефіцієнтами взаємної кореляції. Формування таких коливань може реалізовуватися як на апаратному рівні (на основі нелінійних електронних схем, зокрема схем Чуа чи ван дер Поля), так і програмно (на базі дискретних відображень та систем диференціальних рівнянь). У межах цього підрозділу досліджено методи підвищення криптостійкості ПВП, що синтезуються саме за допомогою програмних генераторів хаотичних процесів.

Розглянемо математичну модель генерації хаотичних послідовностей. Як базовий математичний апарат для генерації первинної послідовності чисел обрано одновимірне дискретне логістичне відображення [4], що описується рекурентним рівнянням [86, 88, 91]:

$$x_{i+1} = ax_i(1 - x_i), \tag{3.23}$$

При значенні $a = 3{,}9$ для системи (3.25) забезпечується стійкий хаотичний процес. При цьому забезпечується висока чутливість до початкових значень $x_0$, що є важливою властивістю для генерації ПВП.

Для формування збалансованої бінарної ПВП на основі континууму дійсних чисел $x_n$ виникає задача оптимізації порогу квантування. Побудова бітової послідовності без урахування реального розподілу щільності ймовірностей хаотичного процесу призводить до появи статистичного дисбалансу між кількістю нулів та одиниць. Для усунення цього недоліку запропоновано попередньо визначати динамічне середнє значення вибірки:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i. \tag{3.24}$$

У теоретичному ідеальному хаотичному режимі значення $\bar{x}$ прямує до 0,5. Проте в реальних цифрових реалізаціях через обмежену розрядну сітку ЕОМ

спостерігаються флуктуації та відхилення від цього значення, що знижує ентропію. З метою нормалізації та контролю статистичних параметрів запропоновано правило адаптивного порогового квантування:

$$b_i = \begin{cases} 0, & x_i < \bar{x}, \\ 1, & x_i > \bar{x}. \end{cases} \tag{3.25}$$

Врахування динамічного зсуву середнього значення за формулою дозволяє гарантувати необхідний баланс кількості символів «0» та «1» у вихідній послідовності $B = [b_1, b_2, \dots, b_L]$.

Для ускладнення процедури криптоаналізу (зокрема захисту від методів реконструкції фазового простору хаотичних систем) та покращення спектральних властивостей сформованого сигналу запропоновано метод додаткової просторово-часової модифікації шляхом циклічного зсуву бітів. Це дозволяє динамічно змінювати фазове положення кодової конструкції без втрати її ентропійних характеристик. Математично алгоритм лівого циклічного зсуву для блоку послідовності фіксованої довжини $L$:

$$B = [b_1, b_2, \dots, b_L] \tag{3.26}$$

реалізується за наступними етапами:

1. Спочатку визначається величина зсуву $k$, де $k < L$. Значення $k$ може виступати в ролі додаткового секретного ключа (або залежати від поточної ітерації іншого хаотичного відображення).

2. Реалізується перестановка елементів масиву, де новий індекс біта $b_i'$ визначається з урахуванням кільцевого переносу:

$$b_i' = b_{(i+k) \bmod N_j}. \tag{3.27}$$

Розглянемо чисельний приклад функціонування алгоритму для вектора $L = 8$. Нехай початковий вектор має вигляд:

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

Після застосування операції циклічного лівого зсуву на $k = 3$ позиції, модифікована послідовність набуває вигляду:

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

Дана трансформація суттєво ускладнює лінійне прогнозування послідовності, повністю зберігаючи її початкову щільність розподілу та вагу Геммінга.

Розглянемо автокореляційний аналіз та наддамо оцінку статистичних властивостей. Оцінку якості та придатності згенерованих ПВП для використання в криптографічних застосунках та системах зв'язку в умовах активної протидії засобів РЕБ проведено за допомогою автокореляційного аналізу. Критеріями оцінки визначимо наступні чинники:

1) виявлення прихованих періодичних залежностей;

2) оцінка шумоподібності для визначення спектральна щільності ПВП;

3) криптографічний захист.

На рис. 3.1 зображено результати розрахунку функції автокореляції $R_{\text{ВП}}(\tau)$ для базового випадкового шуму. Отримана крива характеризується наявністю ізольованого максимуму в точці $\tau = 0$ та стрімким спаданням до близьконульових значень при будь-яких просторово-часових зміщеннях. Така топологія графіка є властивою для некорельованих процесів типу «білого шуму». Відсутність стійких кореляційних зв'язків між відліками послідовності вказує на те, що кожен біт (або числове значення) генерується незалежно від решти компонентів потоку. Цей фактор нівелює можливість ретроспективного відновлення чи передбачення послідовності на основі її попередніх станів.

Розглянемо перший критерій. При виявленні прихованих періодичних залежностей зробимо розрахунок функції автокореляції $R(\tau)$ при кроках зсуву $\tau \neq 0$ (Рис. 2). Значення $R(\tau) \approx 0$ свідчить про відсутність внутрішніх статистичних зв'язків та унеможливлює упереджене перехоплення сигналу.

При другому критерії надається оцінка шумоподібності, тобто спектральної щільність сформованих ПВП. Наявність гострого піку автокореляції при $\tau = 0$ та її швидке спадання гарантує властивості білого шуму. Це забезпечує рівномірний розподіл енергії сигналу по частотному спектру (технології розширення спектра ПРС-ПВП), що ускладнює виявлення, пеленгацію та придушення сигналу засобами радіоелектронного придушення супротивника.

Третій критерій орієнтований на оцінці криптографічного захисту ПВП. Відсутність квазіперіодів підтверджує стійкість сформованого генератора до методів диференційного та лінійного криптоаналізу.

Практична цінність отриманих результатів кореляційного аналізу полягає у забезпеченні стеганографічної стійкості (невидимості контейнера), формуванні завадостійких кодових послідовностей для радіозв'язку та підвищенні стійкості шифротекстів до дешифрування.

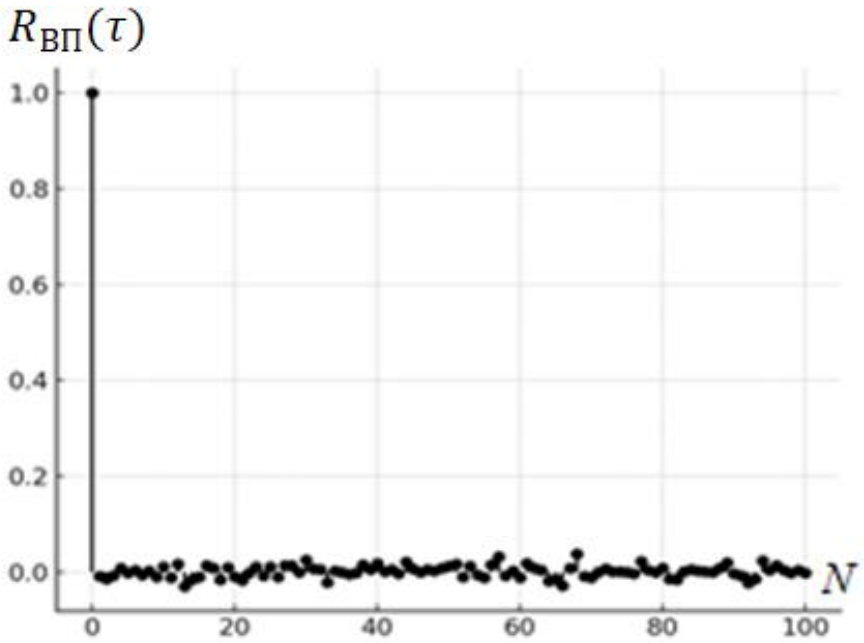



Рис. 3.1. Функція автокореляції ідеального випадкового процесу (білого шуму) $R_{ВП}(\tau)$

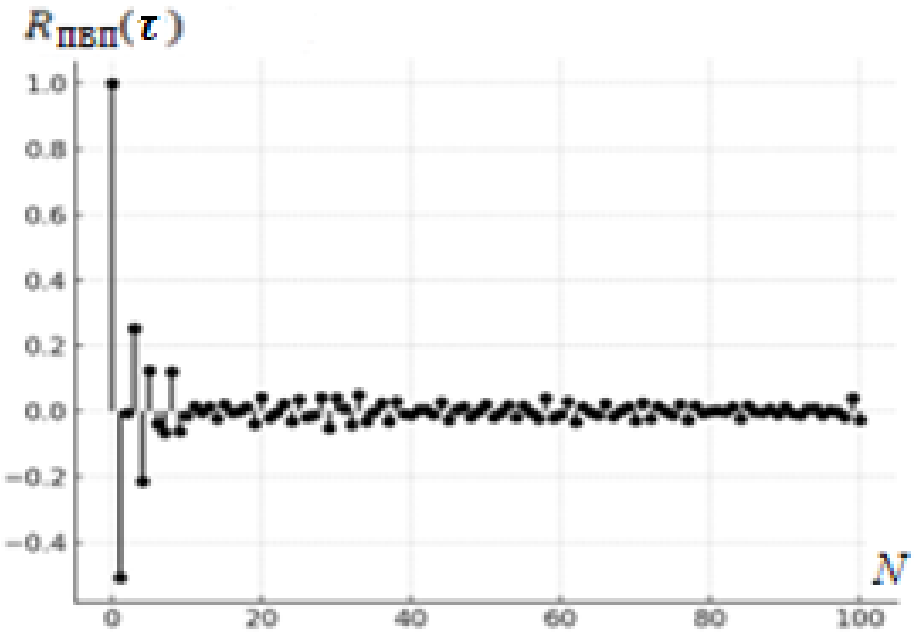



Рис. 3.2. Функція автокореляції згенерованої хаотичної послідовності $R_{\text{ПВП}}(\tau)$ на основі логістичного відображення

Аналіз отриманих графічних залежностей показує, що функція автокореляції хаотичної послідовності (рис. 3.2) ідентична за своїм характером функції автокореляції випадкового шуму (рис. 3.1). Вона має яскраво виражений дельта-подібний сплеск у точці $\tau = 0$ та миттєво спадає до значень, близьких до нуля, при будь-яких зміщеннях. Це математично доводить, що синтезована за допомогою логістичного відображення та циклічного зсуву ПВП володіє властивостями, тотожними білому шуму.

### 3.5 База сигналу та її вплив на прихованість і завадостійкість

Одним із ключових параметрів широкосмугових систем передавання інформації є база сигналу $B$, яка визначає співвідношення між часовими та спектральними характеристиками сигнальної конструкції. Значення бази сигналу $B$ безпосередньо впливає на рівень енергетичної прихованості, завадостійкість, частотну ефективність та ймовірність виявлення сигналу засобами радіоелектронної розвідки. У загальному випадку база сигналу визначається

як $B = \Delta f \times T$, де $\Delta f$ – ширина спектра сигналу; $T$ – тривалість сигналу. База сигналу є безрозмірною величиною та характеризує ступінь широкосмуговості сигналу. Якщо $B \gg 1$, сигнал вважається широкосмуговим. Для вузькосмугових сигналів значення бази наближається до одиниці.

Фізично база сигналу показує, наскільки енергія сигналу розподілена у часовій та частотній областях. Зі збільшенням бази сигналу енергія розсіюється в ширшому спектральному діапазоні, що призводить до зниження спектральної щільності потужності $G(f)$(3.31). Зменшення спектральної щільності потужності ускладнює виявлення сигналу засобами спектрального моніторингу та радіоелектронної розвідки, оскільки сигнал наближається до рівня шумового фону каналу зв'язку. Отже, збільшення бази сигналу забезпечує підвищення енергетичної прихованості. З наведеного виразу (1.12) бачимо, що збільшення ширини спектра дозволяє знизити помітність сигналу без необхідності значного зменшення його загальної потужності.

Крім прихованості, база сигналу суттєво впливає на завадостійкість системи зв'язку. У широкосмугових системах використовується кореляційне накопичення енергії сигналу на приймальній стороні. Після кореляційної обробки відбувається стискання спектра та концентрація енергії корисного сигналу, тоді як енергія вузькосмугових завад розподіляється по всьому спектру. Коефіцієнт виграшу від розширення спектра визначається як:

$$K_g = \frac{\Delta f_s}{\Delta f_i} = B, \tag{3.28}$$

де $\Delta f_s$ – ширина спектра широкосмугового сигналу; $\Delta f_i$ – ширина спектра інформаційного сигналу. Чим більша база сигналу, тим вищий коефіцієнт придушення вузькосмугових завад та більша завадостійкість системи. Разом з тим збільшення бази сигналу супроводжується зміною характеристик ефективності використання каналу зв'язку. Одним із основних показників є частотна ефективність:

$$\eta_f = \frac{R}{\Delta f}, \tag{3.29}$$

де $R$ – швидкість передавання інформації.

Із розширенням спектра значення $\Delta f$ зростає, тому частотна ефективність $\eta_f$ зменшується. Це означає, що підвищення прихованості та завадостійкості досягається ціною збільшення використання частотного ресурсу.

Іншим важливим показником є енергетична ефективність, яка оцінюється через відношення енергії біта до спектральної щільності шуму:

$$\eta_E = \frac{E_b}{N_0}, \tag{3.30}$$

де $E_b$ – енергія, що витрачається на передавання одного біта інформації.

Для широкосмугових систем характерним є те, що збільшення бази сигналу дозволяє знизити необхідне значення $E_b/N_0$ для забезпечення заданої ймовірності помилки. Це пояснюється виграшем від кореляційної обробки та накопичення енергії сигналу. Імовірність помилки при прийманні сигналу в каналі з адитивним білим гаусовим шумом визначається співвідношенням [14]:

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

де $Q(x)$ – функція помилки Гауса. Отже, збільшення бази сигналу дозволяє зменшити ймовірність помилки та підвищити достовірність передавання інформації.

Розглянемо ймовірність спотворення елементів систем зв’язку з ПРС-ПВП та фазовою модуляцією для шумоподібних таймерних сигналів [14]:

$$p^{\text{кг}}_{\text{ТСК ПВП}} = \frac{1}{2}e^{-\frac{B}{s}h^2_{\text{вх}}}. \tag{3.32}$$

На рис. 3.3 надано залежності ймовірності помилки $\lg p^{кг}_{ТСК\ ПВП}$ в системі зв'язку з ПРС-ПВП таймерних сигналів та фазовою модуляцією в залежності від $h$ та $B$. В табл. 3.2 надано порівняльний аналіз забезпечення ймовірності помилки для розрядно-цифрового коду та ТСК.

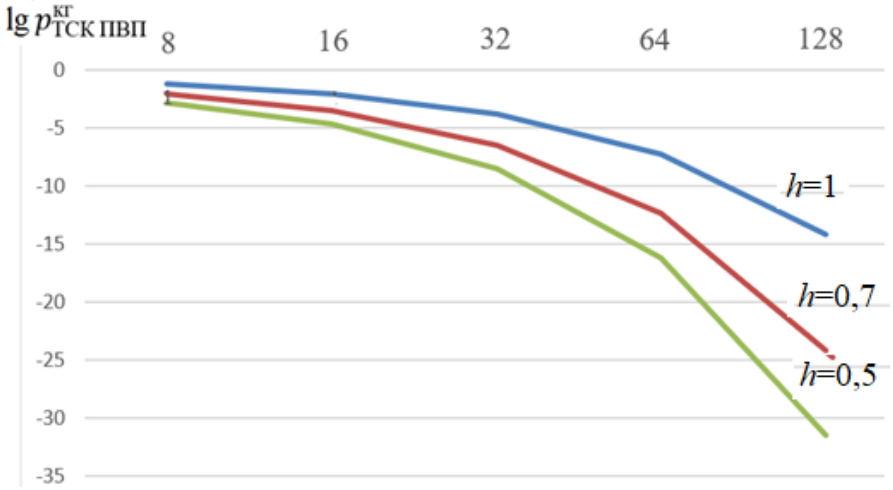



Рис. 3.3. Залежності ймовірності помилки $\lg p^{кг}_{ТСК\ ПВП}$ в системі зв'язку з ПРС-ПВП таймерних сигналів та фазовою модуляцією в залежності від $h$ та $B$

*Таблиця 3.2*

Порівняльний аналіз забезпечення ймовірності помилки для РЦК та ТСК при відношенні сигнал-шум $h$=0,7

| № | База сигналу | $p^{кг}_{РСК\ ПВП}$ | $p^{кг}_{ТСК\ ПВП}$ |
|---|---|---|---|
| 1 | 8 | 0,001848939 | 0,123298598 |
| 2 | 16 | 6,83715E-06 | 0,030405089 |
| 3 | 32 | 9,34932E-11 | 0,001848939 |
| 4 | 64 | 1,7482E-20 | 6,83715E-06 |
| 5 | 128 | 6,11238E-40 | 9,34932E-11 |

Аналіз даних табл. 3.2 показує, що використання шумоподібних таймерних сигналів для підвищення структурної прихованості супроводжується збільшенням імовірності структури таймерної комбінації ($p^{кг}_{ТСК\ ПВП}$), що зумовлює певне

погіршення енергетичних характеристик порівняно з позиційними методами розширення спектра. Разом із тим для великих значень бази сигналу $(B > 62)$ застосування таймерних сигналів є обґрунтованим, оскільки забезпечує додатковий рівень структурної прихованості при прийнятному рівні завадостійкості.

Для таймерних сигналів поняття бази сигналу має додаткові особливості. У ТСК інформація передається часовими параметрами сигналу, тому база визначається не лише шириною спектра та тривалістю сигналу, а й структурою часових інтервалів між імпульсами. У цьому випадку збільшення бази може досягатися: розширенням спектра за допомогою псевдовипадкових послідовностей; збільшенням кількості часових позицій; стохастичною зміною часових інтервалів; використанням хаотичних послідовностей. Це дозволяє одночасно підвищити енергетичну та структурну прихованість сигналів. Важливим є також взаємозв'язок між базою сигналу та структурною прихованістю. Зі збільшенням бази сигналу ускладняється спектральний та кореляційний аналіз, зменшується рівень взаємної кореляції між сигналами та підвищується ентропія сигнальної конструкції.

Отже, база сигналу є одним із основних параметрів широкосмугових систем зв'язку, який визначає компроміс між рівнем прихованості, завадостійкістю, енергетичною та частотною ефективністю. Збільшення бази сигналу забезпечує підвищення енергетичної та структурної прихованості, однак супроводжується зменшенням частотної ефективності системи. Для таймерних сигнальних конструкцій використання широкосмугових методів розширення спектра створює передумови для формування нового класу шумоподібних сигналів із покращеними характеристиками прихованості та завадостійкості.

### 3.6 Висновки до розділу 3

1. У розділі досліджено методи розширення спектра таймерних сигналів на основі псевдовипадкових послідовностей та визначено особливості їх застосування для формування широкосмугових таймерних сигнальних конструкцій. Показано,

що класичні методи DSSS, орієнтовані на позиційні сигнали, потребують адаптації до непозиційної часової структури ТСК.

2. Проведений аналіз псевдовипадкових послідовностей показав, що *M*-послідовності, коди Голда, Касамі та Уолша мають задовільні кореляційні властивості, однак характеризуються обмеженою структурною прихованістю через передбачуваність алгоритмів генерації та обмежений ансамбль можливих реалізацій.

3. Кількісне оцінювання структурної прихованості підтвердило переваги хаотичних псевдовипадкових послідовностей над класичними лінійними ПВП. Встановлено, що для М-послідовностей рівень структурної прихованості становив близько 20 дв. вим., для послідовностей Голда – 40 дв. вим., кодів Касамі – 30 дв. вим., тоді як хаотичні ПВП забезпечували рівень понад 100 дв. вим., що істотно ускладнювало їх відновлення засобами радіоелектронної розвідки.

4. Запропоновані методи підвищення криптостійкості хаотичних ПВП на основі адаптивного порогового квантування та циклічного зсуву забезпечили покращення статистичних характеристик сформованих послідовностей та наближення їх автокореляційних властивостей до характеристик білого шуму.

5. Дослідження впливу бази сигналу підтвердило її важливе значення у забезпеченні енергетичної прихованості та завадостійкості широкосмугових систем зв’язку. Показано, що зі збільшенням бази сигналу зменшується спектральна щільність потужності та підвищується коефіцієнт кореляційного виграшу. При збільшенні бази від $B$=8 до $B$=128 імовірність помилки для систем із прямим розширенням спектра суттєво зменшувалась як для позиційних, так і для таймерних сигналів.

6. Порівняльний аналіз розрядно-цифрових кодів і таймерних сигнальних конструкцій показав, що використання ТСК супроводжується деяким зростанням імовірності помилки порівняно з позиційними сигналами, однак при великих значеннях бази сигналу ($B$>64) застосування шумоподібних таймерних сигналів є доцільним завдяки суттєвому підвищенню структурної та енергетичної прихованості.

7. Дослідження формування таймерних сигнальних конструкцій на основі системи залишкових класів підтвердило можливість поєднання властивостей завадостійкого кодування та структурної прихованості в єдиній сигнально-кодовій конструкції. Встановлено, що кількість допустимих таймерних реалізацій суттєво перевищувала можливості класичних позиційних кодів, а структурна прихованість ТСК виявилась вищою порівняно з кодом Хемінга.

8. Сукупність отриманих результатів підтвердила перспективність використання широкосмугових методів розширення спектра, хаотичних псевдовипадкових послідовностей та таймерних сигнальних конструкцій для формування прихованих і завадостійких систем передавання інформації. Це створює теоретичне підґрунтя для подальшого розвитку комбінованих методів захисту інформації, що поєднують спектральне розширення, хаотичні процеси та таймерне кодування.

# РОЗДІЛ 4
# РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ МЕТОДУ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛЬНИХ КОНСТРУКЦІЙ ДЛЯ ПІДВИЩЕННЯ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

У четвертому розділі розроблено метод прямого розширення спектра таймерних сигналів для захисту інформації від несанкціонованого доступу. Метод спрямований на підвищення прихованості передачі інформації в інформаційно-комунікаційних системах. Досліджено процеси формування широкосмугових таймерних сигналів та проаналізовано їх кореляційні та спектральні характеристики. Запропоновано поняття інтерпретованої бази широкосмугового таймерного сигналу. Оцінено структурну та енергетичну прихованість сигналів з урахуванням параметрів таймерного кодування, псевдовипадкових послідовностей і системи модуляції. Доведено, що застосування методу забезпечує підвищення рівня захисту інформації від виявлення, перехоплення та несанкціонованого доступу в умовах радіоелектронного протиборства.

## 4.1 Інтерпретація бази широкосмугових таймерних сигналів

У сучасних системах радіозв’язку, що функціонують в умовах активної радіоелектронної протидії [5, 6–8], одним із ключових напрямів забезпечення прихованості та завадостійкості є використання широкосмугових сигналів [95–99]. Теоретичною основою їх застосування є методи розширення спектра, які дозволяють зменшувати спектральну щільність потужності сигналу, ускладнювати його виявлення та підвищувати стійкість до навмисних завад. Найбільш поширеним серед таких методів є пряме розширення спектра, яке базується на використанні псевдовипадкових послідовностей [94, 72, 75, 100].

У класичних системах передавання інформації із позиційним кодуванням розширення спектра здійснюється для сигналів з фіксованою тривалістю бітового

елемента $t_0$. Для таких систем поняття бази сигналу $B_{\text{ш}}$ є добре формалізованим і безпосередньо пов'язане з часовими та спектральними параметрами елементарного інформаційного символу. Однак використання непозиційних таймерних сигналів суттєво [101, 102] ускладнює застосування класичного способу до визначення бази сигналу $B_{\text{ш}}$. Це пов'язано з тим, що у ТСК інформація передається не положенням імпульсу в часі, а тривалістю часових інтервалів $t_c = t_0 + k\Delta$ між значущими моментами модуляції (ЗММ), що призводить до змінної структури сигналу в межах однієї сигнальної комбінації $T_c = nt_0$.

За таких умов класичне трактування бази сигналу $B_{\text{ш}}$, орієнтоване на фіксований часовий інтервал $t_0$, потребує перегляду та адаптації до особливостей таймерного кодування. Інтерпретація бази широкосмугових таймерних сигналів має важливе значення не лише для коректного синтезу шумоподібних сигналів, але й для оцінювання їх прихованості, завадостійкості та ефективності використання частотного ресурсу.

Теоретичним підґрунтям формування широкосмугових сигналів є теорема К. Шеннона щодо пропускної здатності каналу зв'язку [57]:

$$C = \Delta F \log_2 \left(1 + \frac{P_c}{P_{\text{ш}}}\right), \tag{4.1}$$

де $C$ – пропускна здатність каналу; $\Delta F$ – смуга частот сигналу; $P_c$– потужність сигналу; $P_{\text{ш}}$– потужність завади. З аналізу виразу (4.1) випливає, що забезпечення заданої швидкості передавання даних може досягатися різними комбінаціями енергетичних та частотних ресурсів каналу. Зокрема, при зменшенні відношення сигнал/шум

$$\frac{P_c}{P_{\text{ш}}} \to 1 \text{ або } \frac{P_c}{P_{\text{ш}}} \leq 1 \tag{4.2}$$

для збереження сталої пропускної здатності необхідним є збільшення смуги частот сигналу. Саме ця властивість лежить в основі методів широкосмугового

передавання інформації. Кількісною характеристикою широкосмугового сигналу є його база:

$$B_{\text{ш}} = T\Delta F, \tag{4.3}$$

де $B_{\text{ш}}$ – база сигналу; $T$ – тривалість сигналу; $\Delta F$ – ширина займаної смуги частот.

База сигналу характеризує ступінь розширення спектра та одночасно визначає потенційні можливості системи щодо забезпечення енергетичної прихованості та завадостійкості. При

$$B_{\text{ш}} \gg 1 \tag{4.4}$$

сигнал набуває властивостей шумоподібності, а його спектральна щільність потужності зменшується, що ускладнює виявлення засобами радіоелектронної розвідки.

У системах з позиційним кодуванням база сигналу визначається відносно окремого бітового інтервалу тривалістю $t_0$. У цьому випадку кожен інформаційний елемент має однакову часову структуру, а кількість імпульсів псевдовипадкової послідовності на інтервалі $t_0$ є сталою. База елементарного сигналу визначається як

$$B(t_0) = t_0\Delta F. \tag{4.5}$$

Це є характерним для класичних систем зв’язку з ПРС-ПВП (DSSS), у яких кожен біт повідомлення множиться на псевдовипадкову послідовність із фіксованою швидкістю чипів тривалістю $\tau$.

На відміну від позиційних сигналів, для таймерних сигналів характерним є непозиційний принцип кодування. У ТСК інформація передається тривалістю часових інтервалів між імпульсами, а не їх жорстко фіксованим положенням. Тривалість окремих елементів сигналу задовольняє умову $t_c \geq t_0$. Формування

часової структури ТСК виконується шляхом зміни тривалості інтервалів: $t_c = t_0 + k\Delta$ , де $k = 0,1, \dots, I$. Також потрібно відзначити, що тривалість базового елементу формування ТСК $\Delta$ залежить від параметру $s$, тобто $\Delta = t_0/s$, де $s$ характеризує кількість можливих градацій зміни тривалості імпульсу $t_c$.

Отже , на відміну від позиційних систем кодування, у межах однієї таймерної комбінації тривалості імпульсів $t_c$ можуть бути різними. Це означає, що база сигналу перестає бути сталою характеристикою окремого біта і не може визначатися виключно через параметри елементарного інтервалу $t_0$. Саме ця особливість створює принципову проблему для застосування класичних методів прямого розширення спектра до таймерних сигналів. Якщо у DSSS-системах для кожного біта використовується однакова кількість чипів псевдовипадкової послідовності, то для ТСК така процедура стає неоднозначною через змінну тривалість сигналів.

Отже, для непозиційних таймерних сигналів виникає необхідність нової інтерпретації бази сигналу, яка повинна враховувати не лише параметри окремого імпульсу, а весь часовий інтервал формування сигнальної конструкції. Це створює теоретичне підґрунтя для подальшого розгляду методів узгодження параметрів ТСК із псевдовипадковими послідовностями та формування широкосмугових шумоподібних таймерних сигналів

## 4.2 Формування широкосмугових таймерних сигналів із використанням псевдовипадкових послідовностей

Особливості побудови таймерних сигналів зумовлюють необхідність перегляду класичного методу реалізації прямого розширення спектра. У системах з позиційним кодуванням [101, 102] кожному бітовому елементу з фіксованою тривалістю $t_0$ відповідає певна кількість імпульсів ПВП $\tau$, що визначається базою сигналу $B_{\text{ш}}$. Для таймерних сигналів така схема не може бути використана безпосередньо через змінну тривалість часових інтервалів $t_c$, у межах яких передається інформація. Причиною цього є те, що на відміну від позиційних

сигналів, у ТСК інформація визначається не положенням окремого імпульсу, а сукупністю часових інтервалів $t_c = t_0 + k\Delta$ між значущими моментами модуляції. Це означає, що тривалість сигналу $t_c$ в межах комбінації не є сталою, а тому база сигналу повинна визначатися не для окремого імпульсу, а для всього інтервалу формування таймерної конструкції $T_c$. Інтерпретована база ТСК визначається кількістю імпульсів псевдовипадкової послідовності, що використовуються для розширення спектра на інтервалі передавання:

$$B_{\text{ТСК}} = N_{\tau\text{ТСК}}, \tag{4.6}$$

де $N_{\tau\text{ТСК}}$ – кількість елементів ПВП тривалістю $\tau$, що припадає на інтервал формування ТСК $T_c$. Для узгодження параметрів таймерного сигналу та псевдовипадкової послідовності необхідно виконання умови

$$N_{\tau\text{ТСК}} = B_{t_0} \cdot m, \tag{4.7}$$

де $B_{t_0}$ – база елементарного інтервалу $t_0$; $m$ – кількість інтервалів Найквіста в межах комбінації. Водночас число відліків, що характеризують часову структуру ТСК, визначається виразом

$$N_{\Delta\text{ТСК}} = s \cdot m, \tag{4.8}$$

де $s$ – кількість допустимих часових положень або значень тривалості імпульсів у межах одного інтервалу $t_0$. Для коректного розширення спектра необхідно забезпечити умову

$$B_{\text{ТСК}} \geq N_{\Delta\text{ТСК}}. \tag{4.9}$$

Нерівність (4.8) означає, що кількість імпульсів $B_{\text{ТСК}}$ розширення повинна бути не меншою за число можливих часових реалізацій таймерної конструкції

$N_{\Delta\text{ТСК}}$. Формування широкосмугового таймерного сигналу виконується шляхом перемноження ТСК, яка сформована на інтервалі часу $T_c$, із псевдовипадковою послідовністю:

$$x_{\text{тск}}(T_c, \tau) = c_{\text{ПВП}}(\tau) \cdot x(T_c, \Delta), \tag{4.10}$$

де $c_{\text{ПВП}}(\tau)$ – псевдовипадкова послідовність розширення спектра на інтервалі часу $T_c$; $x(T_c, \Delta)$ – таймерна сигнальна конструкція. У результаті кожен часовий сегмент ТСК замінюється відповідною групою елементів ПВП, що призводить до формування шумоподібного сигналу зі значно ширшим спектром. Подальше використання фазової маніпуляції дозволяє отримати широкосмуговий таймерний сигнал:

$$x_{\text{ШТСК}}(T_c, \tau) = g(\tau)\cos\left(2\pi f_0 \tau + x_{\text{тск}}(T_c, \tau)\right), \tag{4.11}$$

де $f_0$ – несуча частота; $g(\tau)$– огинаюча сигналу.

На рис. 4.1 представлено процес синтезу шумоподібного таймерного сигналу $x_{\text{штск фм}}(T_c, \tau)$ з використанням наступних параметрів:

1) $m = 4$ – кількість інтервалів Найквіста $t_0$ для формування ТСК на інтервалі часу $T_{\text{c}}$ (рис. 1(а));

2) $s = 4$ – кількість елементів $\Delta$ на інтервалі $t_0$;

3) $i = 2$ – кількість ЗММ в межах часового інтервалу $T_{\text{c}}$;

4) $B_{t_0} = 16$ – база сигналу для інтервалу часу $t_0$;

5) $B_{\text{ТСК}} = N_{\tau\text{ТСК}} = 54$ – інтерпретована база ТСК.

6) отриманий щумоподібний сигнал $x_{\text{ШТСК}}(T_c, \tau)$ характеризується одночасним поєднанням двох показників прихованості:

7) структурної прихованості, що забезпечується непозиційною структурою ТСК;

8) енергетичної прихованості, що досягається завдяки розширенню спектра та зменшенню спектральної щільності потужності.

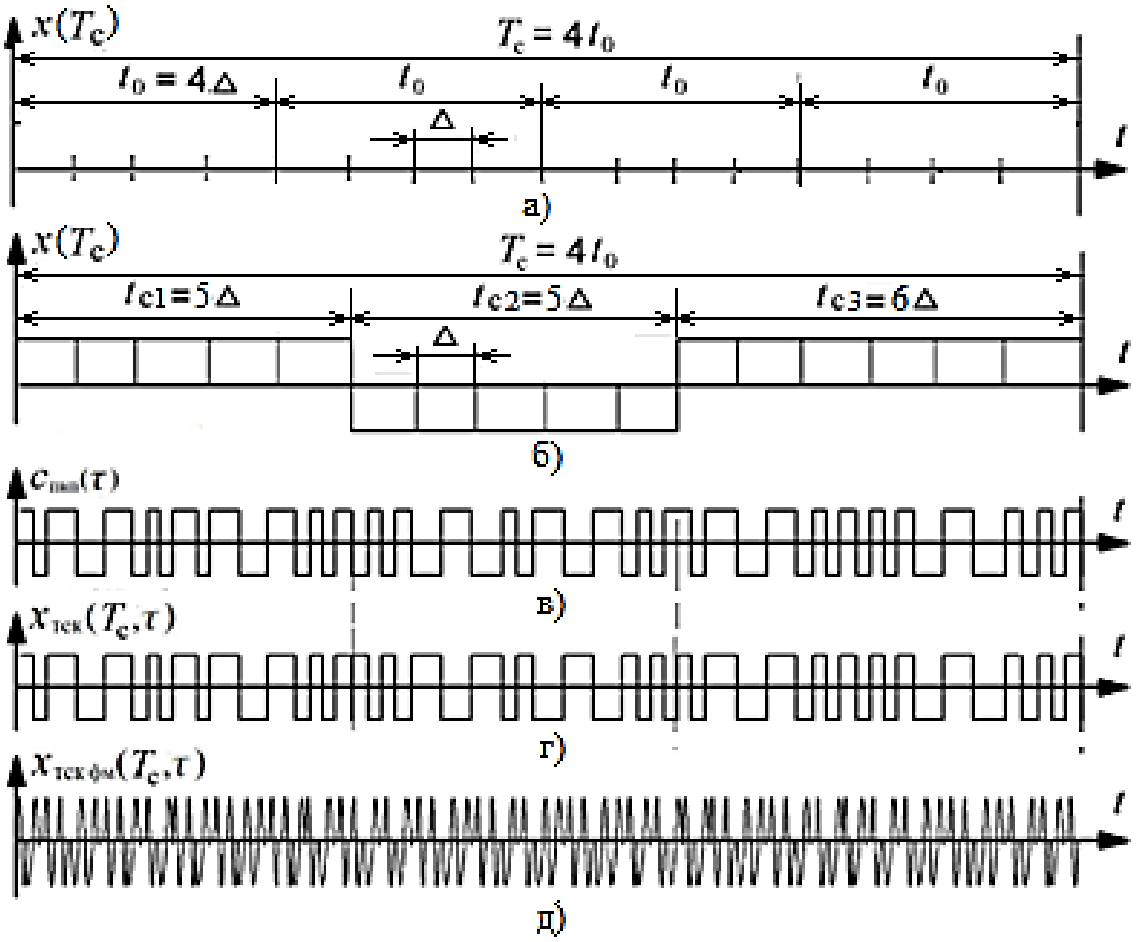



Рис. 4.1. Процес синтезу шумоподібного таймерного сигналу $x_{\text{штск фм}}(T_c, \tau)$

Зростання бази сигналу призводить до перерозподілу енергії сигналу у ширшій смузі частот. Спектральна щільність потужності при цьому визначається співвідношенням

$$G(f) = \frac{P_S}{\Delta F}, \tag{4.12}$$

де $P_s$ – потужність сигналу; $\Delta F$– ширина спектра. Зі збільшенням $\Delta F$величина $G(f)$зменшується, унаслідок чого сигнал стає менш помітним для засобів спектрального аналізу та радіомоніторингу. Отже, використання ПВП для розширення спектра таймерних сигнальних конструкцій забезпечує формування широкосмугових шумоподібних сигналів із керованими спектральними

характеристиками. На відміну від класичних DSSS-систем для позиційних кодів, розширення спектра ТСК виконується на інтервалі всієї сигнальної комбінації, що дозволяє узгодити змінну часову структуру сигналу з параметрами псевдовипадкової послідовності та створює додатковий резерв структурної прихованості.

### 4.3 Кореляційний прийом широкосмугових таймерних сигналів та відновлення їх структури

Однією з принципових особливостей систем передавання інформації на основі широкосмугових таймерних сигнальних конструкцій є необхідність відновлення не окремих позиційних символів, а часової структури всієї сигнальної комбінації. На відміну від класичних DSSS-систем, у яких процес демодуляції базується на визначенні стану окремого біта після кореляційного стискання спектра, у випадку ТСК необхідним є визначення значущих моментів відновлення та тривалостей часових інтервалів.

Приймання широкосмугового таймерного сигналу здійснюється за допомогою кореляційного приймача, структура якого передбачає синхронне перемноження прийнятого сигналу з локальною копією псевдовипадкової послідовності та подальше інтегрування результату. Прийнятий сигнал на вході приймача може бути представлений як

$$r(t) = s_{\text{штск}}(t) + n(t), \tag{4.13}$$

де $s_{\text{штск}}(t)$ – переданий широкосмуговий таймерний сигнал; $n(t)$ – адитивна шумова складова каналу. Після синхронного множення на локальну копію ПВП $c_{\text{л}}(t)$, отримуємо

$$z(t) = r(t)c_{\text{л}}(t). \tag{4.14}$$

За умови правильної синхронізації та збігу кодових послідовностей виконується умова

$$c_{\text{ПВП}}(t) \times c_{\text{л}}(t) \approx 1, \tag{4.15}$$

унаслідок чого енергія сигналу концентрується у вузькій смузі, а шумові складові залишаються розподіленими по спектру. Вихідна напруга інтегратора кореляційного приймача визначається виразом

$$U(t) = \int_0^{T_c} r(t)\, c_{\text{л}}(t) dt. \tag{4.16}$$

Інтегрування здійснюється на інтервалі формування таймерної комбінації $T_c$, а не окремого імпульсу, що є принциповою відмінністю приймання ТСК від класичних позиційних систем. У момент збігу локальної та прийнятої псевдовипадкових послідовностей на виході інтегратора формується максимум кореляційної функції

$$R_{xc}(\tau) = \int x(t) c(t - \tau) dt, \tag{4.17}$$

де $\tau$ – часовий зсув. Максимум кореляційної функції відповідає моменту правильної синхронізації та дозволяє здійснювати подальше визначення структури таймерної сигнальної конструкції.

На відміну від позиційних сигналів, у ТСК процес приймання передбачає визначення значущих моментів відновлення (ЗМВ), які відповідають екстремумам напруги інтегратора. Часові координати цих моментів визначаються в межах інтервалу $[-\Delta/2; \Delta/2]$, що забезпечує стійке відновлення структури сигналу навіть за наявності часових флуктуацій та завад.

Відновлення структури імпульсів ТСК з шумоподібного сигналу здійснюється за допомогою кореляційного прийому після демодуляції. На рис. 4.2 наведено часову залежність напруги $U_i$ на виході інтегратора кореляційного приймача в межах інтервалу формування ТСК $T_{\text{с}}$. По осі абсцис відкладено час $t$,

по осі ординат – рівень інтегрованої напруги $U_i$. Графік має ламану трикутну форму з чітко вираженими екстремумами, що відповідають значущим моментам відновлення (ЗМВ – передні і задні фронти) імпульсів ТСК. У межах інтервалу $T_c = 64\tau$ виділено три часові ділянки: $t_{c1}$, $t_{c2}$, та $t_{c3}$, які визначають тривалості окремих імпульсів комбінації ТСК-1.

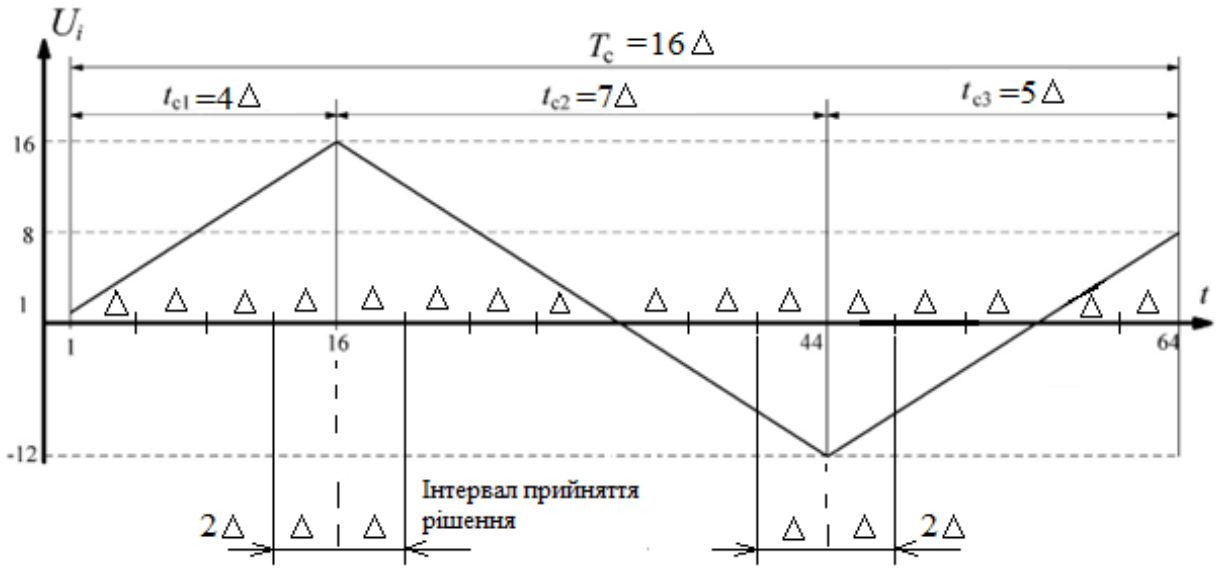



Рис. 4.2. Рівень напруги $U_i$ на виході інтегратора кореляційного приймача для визначення тривалостей $t_{c1} = 4\Delta, t_{c2} = 7\Delta, t_{c3} = 5\Delta$ комбінації ТСК-1 ($n = 4, s = 4, i = 2$)

На інтервалі $t_{c1} = 16\tau$ напруга зростає до локального максимуму, що відповідає накопиченню енергії корельованої ділянки сигналу. Далі, на інтервалі $t_{c2} = 28\tau$, спостерігається спад до мінімального значення, що відображає зміну полярності ЗМВ імпульсу ТСК. На завершальному інтервалі $t_{c3} = 20\tau$ напруга знову зростає, формуючи наступну ділянку інтегрування. Точки максимуму та мінімуму є ЗМВ (передні і задні фронти), оскільки саме за їх координатами визначаються тривалості імпульсів $t_{c1}$, $t_{c2}$, $t_{c3}$. У межах інтервалу

$$\Omega = [-\Delta, \Delta] \tag{4.18}$$

відносно кожного ЗМВ приймається рішення про положення переднього та заднього фронтів імпульсів ТСК. Значення δ визначається кодовою відстанню $d_0$ між дозволеними комбінаціями ТСК: при $d_0 = \Delta$ інтервал $\delta = \Delta/2$, а при $d_0 = 2\Delta$ отримуємо $\delta = \Delta$.

Точки екстремумів функції $U_i$ відповідають переходам між елементами ТСК, що дозволяє визначити тривалості імпульсів $t_{c1}$, $t_{c2}$, $t_{c3}$. В межах інтервалу $[-\Delta/2; \Delta/2]$ або $[-\Delta; \Delta]$ уточнюються положення передніх і задніх фронтів імпульсів, що забезпечує коректне відновлення структури сигналу навіть в умовах наявності завад.

Отже, інформаційний параметр ТСК відновлюється не шляхом оцінювання амплітуди чи фази сигналу, а через аналіз часової структури кореляційного відгуку. Ефективність кореляційного прийому широкосмугових сигналів оцінюється через коефіцієнт процесингового підсилення

$$G_p = \frac{\Delta F}{R_b} = B, \tag{4.19}$$

де $\Delta F$ – ширина спектра широкосмугового сигналу; $R_b$ – швидкість передавання інформації; $B$ – база сигналу. Процесингове підсилення характеризує виграш системи після кореляційного стискання спектра та визначає здатність приймача працювати за умов низького відношення сигнал/шум. Після кореляційного приймання відношення сигнал/шум збільшується приблизно у

$$G_p = B \tag{4.20}$$

разів, що дозволяє відновлювати сигнал навіть тоді, коли його спектральна щільність потужності перебуває нижче рівня шумового фону.

Для оцінювання ймовірності помилки приймання широкосмугових таймерних сигналів може використовуватися класичне співвідношення (3.31). Завдяки кореляційному стисканню спектра фактичне значення $E_b/N_0$ на виході

приймача збільшується, що забезпечує підвищення завадостійкості системи.

Отже, кореляційний прийом широкосмугових таймерних сигналів має суттєві відмінності від приймання класичних DSSS-сигналів. Якщо для позиційних систем основним завданням є відновлення окремих символів після деспреадингу, то у випадку ТСК виконується відновлення часової структури всієї сигнальної комбінації. Такий метод дозволяє одночасно реалізувати енергетичну прихованість за рахунок розширення спектра та структурну прихованість за рахунок непозиційної основи таймерного кодування, забезпечуючи підвищену стійкість до засобів радіоелектронної розвідки та активних завад.

## 4.4 Оцінка структурної прихованості широкосмугових таймерних сигналів

Одним із ключових показників ефективності широкосмугових таймерних сигнальних конструкцій є рівень їх структурної прихованості. На відміну від енергетичної прихованості, що визначається рівнем спектральної помітності сигналу та співвідношенням сигнал/шум, структурна прихованість характеризує складність розпізнавання внутрішньої організації сигнальної конструкції, встановлення закону її формування та визначення параметрів кодування стороннім спостерігачем.

У класичних системах передавання інформації структурна прихованість визначається кількістю можливих сигнальних реалізацій та ступенем невизначеності щодо їх структури. Для позиційних сигналів кількість можливих комбінацій обмежується позиційністю системи модуляції та довжиною кодової послідовності. У випадку таймерних сигнальних конструкцій ситуація істотно відрізняється, оскільки інформація передається за рахунок комбінації часових інтервалів між значущими моментами модуляції.

Потенційна структурна прихованість визначається як логарифмічна міра кількості допустимих сигнальних конструкцій

$$S_{\text{стр}} = \log_2 N, \tag{4.21}$$

де $S_{\text{стр}}$ – структурна прихованість, двійкових вимірів; $N$ – кількість можливих сигнальних конструкцій. Збільшення числа допустимих реалізацій безпосередньо ускладнює процедуру виявлення та класифікації сигналу засобами радіоелектронної розвідки. Для таймерних сигналів число можливих реалізацій визначається параметрами:

1) $m$ – кількість інтервалів Найквіста;
2) $s$ – кількість можливих часових положень;
3) $i$ – кількість значущих моментів модуляції.

Кількість реалізацій ТСК з фіксованою кількістю значущих моментів модуляції визначається співвідношенням

$$N_{\text{ТСК}} = \frac{[mS-i(S-1)]!}{i!\,[S(m-i)]!} \tag{4.22}$$

за умови

$$\tau_c \geq \Delta(s+i). \tag{4.23}$$

Якщо допускається використання кількох варіантів кількості значущих моментів модуляції, загальне число комбінацій визначається сумою

$$N_{\text{ТСК}} = \sum_{i=1}^{m} \frac{[mS-i(S-1)]!}{i!\,[S(m-i)]!}. \tag{4.24}$$

Кількість реалізацій $N_{\text{рт}}$ залежно від параметрів $m$, $s$ та ЗММ $i = 2$ надано в табл. 4.1. Ці співвідношення демонструють суттєву перевагу таймерних конструкцій над позиційними кодами. Для прикладу, при $m = 4$, $s = 5$, $i = 2$ одержуємо $N_{\text{ТСК}} = 66$. Для класичного розрядно-цифрового коду з тією ж кількістю елементів $N_{\text{РЦК}} = 2^4 = 16$. Отже, навіть без використання розширення спектра ТСК забезпечують у декілька разів більшу кількість сигнальних реалізацій.

*Таблиця 4.1*

Залежність кількості реалізацій $N_{\text{рт}}$ від параметрів $m$, $s$ та $i = 2$

| $s$ \ $m$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| 2 | 15 | 28 | 45 | 66 | 91 |
| 3 | 28 | 55 | 91 | 136 | 190 |
| 4 | 45 | 91 | 153 | 231 | 325 |
| 5 | 66 | 136 | 231 | 351 | 496 |
| 6 | 91 | 190 | 325 | 496 | 703 |
| 7 | 120 | 253 | 435 | 666 | 946 |

При $i = 3$ є можливість збільшити кількість реалізацій $N_{\text{рт}}$, але тільки для значень $m \geq 5$. В табл. 4.2 можна побачити, що при $m = 4$, $s = 5$, $i = 3$ кількість реалізацій $N_{\text{ТСК}} = 286$, що 4,3 рази більше ніж для $i = 2$. Ці приклади свідчать про достатню варіативність структури ТСК, яку можна обирати за допомогою параметрів побудови $m$, $s$ та $i$.

*Таблиця 4.2*

Залежність кількості реалізацій $N_{\text{рт}}$ від параметрів $m$, $s$ та $i = 3$

| $s$ \ $m$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| 2 | 10 | 35 | 84 | 286 | 91 |
| 3 | 20 | 84 | 220 | 455 | 816 |
| 4 | 35 | 165 | 455 | 969 | 1771 |
| 5 | 56 | 286 | 816 | 1771 | 3276 |
| 6 | 84 | 455 | 1330 | 2925 | 5456 |
| 7 | 120 | 680 | 2024 | 4495 | 9139 |

Послідовності Уолша при розширення спектра ТСК не забезпечують достатній захист передаваних сигнальних конструкцій. При параметрах таймерних сигналах $m = 10$, $s = 6$, $i = 4$, $B_{t_0} = 128$, ФМ-4 структурна прихованість $S_{\text{тск пвпУ}} = 25$ (строчка № 5, табл. 4.3). Для аналогічних параметрах ТСК при

використанні ПВП на основі генератора хаосу структурна прихованість $S_{\text{тск пвп}} = 146$. Це означає, що у випадку перехоплення такого шумоподібного сигналу засобами РЕР для розпізнання структури сигнальної конструкцій методом перебору потрібно зробити $2^{146}$ операцій.

Слід відзначити, що при формуванні широкосмугових таймерних сигналів загальна структурна прихованість визначається не лише параметрами ТСК, а й властивостями ПВП та системи модуляції. Інтегральний показник структурної прихованості широкосмугового таймерного сигналу може бути представлений як

$$S_{\text{ТСК–ПВП}} = \log_2 N_{\text{ТСК}} + \log_2 N_{\text{ПВП}} + \log_2 N_{\text{см}}, \qquad (4.25)$$

де $N_{\text{ТСК}}$ – кількість таймерних комбінацій; $N_{\text{ПВП}}$ – кількість імпульсів або станів псевдовипадкової послідовності; $N_{\text{см}}$ – позиційність системи модуляції.

Це співвідношення показує, що загальна структурна прихованість формується як сума внесків трьох незалежних механізмів:

1) непозиційної часової структури ТСК;

2) спектрального маскування за рахунок ПВП;

3) додаткової невизначеності, що створюється системою модуляції.

Слід зазначити, що внесок показника $S_{\text{тск}}$ у загальний рівень прихованості сигналу залишався відносно невеликим та визначався кількістю комбінацій, яка залежала від параметрів $m$, $s$ та $i$. Зокрема, при зміні параметрів ТСК від $(m = 8, s = 5, i = 3)$ до $(m = 12, s = 7, i = 5)$ значення $S_{\text{тск}}$ збільшувалося з 12 до 20 дв. вим., однак такий приріст становив менш як 10% від сумарної структурної прихованості.

На рис. 4.3 надано залежності $S_{\text{тск пвп}}$ від параметрів ТСК і кількості імпульсів розширення ПВП $N_{\text{пвп}}$. Забезпечення високого рівня структурної прихованості таймерного шумоподібного сигналу потребувало врахування таких положень:

1) збільшення бази $B_{t_0}$ виявилося найбільш ефективним способом підвищення $S_{\text{тск пвп}}$, однак його реалізація обмежувалася апаратними можливостями та ускладненням систем синхронізації передавача і приймача;

2) застосування систем модуляції з більшою позиційністю сприяло підвищенню швидкості передавання даних, проте супроводжувалося зниженням завадостійкості, що потребувало компромісу між пропускною здатністю та достовірністю зв'язку;

3) оптимізація параметрів ТСК $(m, s, i)$ здійснювалася з урахуванням вимог до достовірності передавання інформації та технічної реалізації системи для досягнення раціонального співвідношення між прихованістю, швидкістю та завадостійкістю.

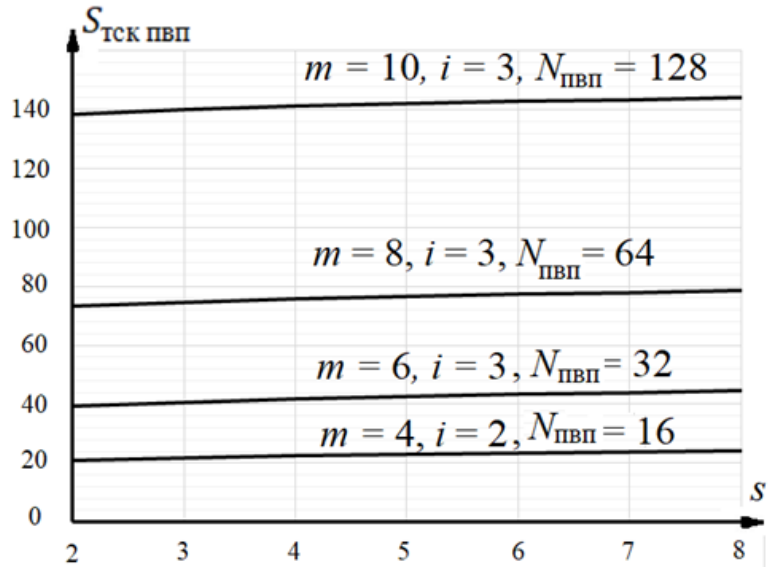



Рис. 4.3. Залежності $S_{\text{тск пвп}}$ від параметрів ТСК і кількості імпульсів розширення ПВП $N_{\text{пвп}}$

Отже, вибір параметрів системи зв'язку визначався результатами комплексного аналізу, який враховував переваги та обмеження різних методів формування сигнальних конструкцій. Найбільший вплив на значення $S_{\text{ТСК}-\text{ПВП}}$ має база розширення спектра, оскільки саме вона визначає число елементів псевдовипадкової послідовності $N_{\text{ПВП}} = B$. Наприклад, для параметрів $m = 8$, $s = 5$, $i = 3$ структурна прихованість власне ТСК становить приблизно $S_{\text{ТСК}} \approx 12$ двійкових вимірів.

*Таблиця 4.3*

Структурна прихованість таймерних шумоподібних сигналів на основі послідовностей Уолша і ПВП, що сформовані на основі логістичного генератора хаосу

| № | Параметри ТСК ($m$, $s$, $i$) | $S_{\text{тск}}$ | $B_{t_0}$, $N_{\text{пвп}}$ | $S_{\text{Уол}}$ , | Вид модуляції | $S_{\text{см}}$, | $S_{\text{тск пвпУ}}$ | $S_{\text{тск пвп}}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | $m$=8, $s$=5, $i$=3 | 12 | 64 | 6 | ФМ-2 | 1 | 19 | 77 |
| 2 | $m$=8, $s$=5, $i$=3 | 12 | 64 | 6 | ФМ-4 | 2 | 20 | 78 |
| 3 | $m$=8, $s$=5, $i$=3 | 12 | 64 | 6 | КАМ-8 | 3 | 21 | 79 |
| 4 | $m$=10, $s$=6, $i$=4 | 16 | 128 | 7 | ФМ-2 | 1 | 24 | 145 |
| 5 | $m$=10, $s$=6, $i$=4 | 16 | 128 | 7 | ФМ-4 | 2 | 25 | 146 |
| 6 | $m$=10, $s$=6, $i$=4 | 16 | 128 | 7 | КАМ-8 | 3 | 26 | 147 |
| 7 | $m$=12, $s$=7, $i$=5 | 22 | 256 | 8 | ФМ-2 | 1 | 21 | 279 |
| 8 | $m$=12, $s$=7, $i$=5 | 22 | 256 | 8 | ФМ-4 | 2 | 22 | 280 |
| 9 | $m$=12, $s$=7, $i$=5 | 22 | 256 | 8 | КАМ-8 | 3 | 23 | 281 |

При використанні бази розширення $B = 64$ та двійкової фазової маніпуляції $\log_2 N_{\text{см}} = 1$ одержуємо $S_{\text{ТСК}-\text{ПВП}} = 12 + 64 + 1 = 77$ двійкових вимірів.

За збільшення бази розширення до $B = 256$ структурна прихованість зростає до $S_{\text{ТСК}-\text{ПВП}} = 12 + 256 + 1 = 269$ двійкових вимірів.

Це означає, що збільшення бази розширення спектра від 64 до 256 забезпечує зростання структурної прихованості більш ніж утричі. Разом з тим, зростання бази сигналу супроводжується підвищенням вимог до систем синхронізації та апаратної реалізації. Зі збільшенням кількості імпульсів ПВП зростає тривалість процесу захоплення синхронізації, ускладняється робота кореляційного приймача та збільшується обчислювальна складність цифрової обробки сигналів.

Додатковий вплив на структурну прихованість має позиційність системи модуляції. Перехід від двійкової фазової маніпуляції до багатопозиційних методів (QPSK, QAM) збільшує кількість можливих станів сигналу $\log_2 N_{\text{см}}$, що підвищує загальний рівень структурної невизначеності. Проте таке рішення супроводжується зменшенням завадостійкості та зростанням вимог до відношення сигнал/шум.

Таким чином, структурна прихованість широкосмугових таймерних сигналів формується комплексною взаємодією трьох чинників: параметрів таймерної конструкції, бази розширення спектра та виду модуляції. На відміну від класичних DSSS-систем, де основний внесок у прихованість забезпечується лише псевдовипадковою послідовністю, у ТСК додатковий резерв прихованості створюється непозиційною часовою структурою сигналу. Це дозволяє реалізувати комбінований механізм захисту, який одночасно підвищує енергетичну та структурну прихованість передавання інформації в умовах радіоелектронного протиборства.

## 4.5. Аналіз кореляційних властивостей шумоподібних таймерних сигналів

Широкосмугові сигнали на основі прямого розширення спектра з використанням таймерних сигнальних конструкцій (ТСК) можуть бути представлені як розклад у базисі ортогональних функцій:

$$s(t) = \sum_{k=1}^{N_{\text{рп}}} a_k \, \varphi_k(\tau), \tag{4.26}$$

де $a_k$ – вагові коефіцієнти, що формуються псевдовипадковими або випадковими послідовностями; $\varphi_k(\tau)$ – ортогональні або квазіортогональні базисні функції; $N_{\text{рп}}$ – розмірність простору сигналу.

Використання класичних ортогональних базисів для розширення спектра позиційних сигналів не забезпечує достатнього рівня структурної прихованості. Це пов’язано з передбачуваністю структури сигналу, що робить його потенційно вразливим до відновлення методами кореляційного аналізу та спектрального моніторингу. У результаті знижується ефективність протидії засобам РЕР та НСД, що обґрунтовує необхідність використання більш складних шумоподібних структур.

Для оцінки впливу таймерних сигналів на структуру широкосмугового

сигналу розглянуто пряме розширення спектра з використанням послідовностей Уолша. Аналіз проводиться для трьох ТСК з параметрами $n = 4$, $s = 4$, $i = 2$ на інтервалі $T_c = m \cdot t_0$:

1) ТСК-1: $t_{c1} = 4\Delta$, $t_{c2} = 7\Delta$, $t_{c3} = 5\Delta$;

2) ТСК-2: $t_{c1} = 5\Delta$, $t_{c2} = 5\Delta$, $t_{c3} = 6\Delta$;

3) ТСК-3: $t_{c1} = 6\Delta$, $t_{c2} = 4\Delta$, $t_{c3} = 6\Delta$.

Для завдання розширення спектра використаємо різні ПВП Уолша з базою $B_{t_0} = 16$ наступної структурою:

1) $c_{17}$ = {1 –1 1 –1 1 –1 1 –1 1 –1 1 –1 1 –1 1 –1};

2) $c_{37}$ = {1 –1 1 –1 –1 1 –1 1 1 –1 1 –1 –1 1 –1 1};

3) $c_{47}$ = {1 –1 –1 1 –1 1 1 –1 –1 1 –1 1 1 –1 1 –1};

4) $c_{07}$ = {1 –1 –1 1 –1 1 1 –1 1 –1 –1 1 –1 1 1 –1};

5) $c_{55}$ = {1 –1 –1 1 –1 1 1 –1 1 –1 –1 1 –1 1 1 –1};

6) $c_{62}$ = {1 1 –1 –1 –1 –1 1 1 –1 1 1 –1 1 –1 –1 1}.

Визначимо кількість елементів розширення ТСК $\tau$ на інтервалі часу $T_c$ з урахуванням заданих параметрів ТСК:

$$N_{\tau\text{ТСК}} = B_{t_0} \times n = 16 \times 4 = 64.$$

Розрахуємо кількість елементів Δ на інтервалі побудові ТСК:

$$N_\Delta = n \times s = 4 \times 4 = 16.$$

Визначимо кількість елементів $\tau$ на інтервалі Δ:

$$N_\Delta = B_t / s = 16/4 = 4.$$

В табл. 4.4 за допомогою коефіцієнту кореляції $K_{cy}$ надана оцінка впливу ТСК на структуру широкосмугового сигналу. Отримані результати показують, що зміна структури ТСК суттєво впливає на кореляційні властивості сигналів навіть за фіксованого базису Уолша. Зокрема, збільшення варіативності тривалостей імпульсів призводить до зростання значень $K_{cy}$, що відображає зміну ступеня структурної подібності між реалізаціями сигналів.

*Таблиця 4.4*

Коефіцієнти кореляції $K_{cy}$ для різних ТСК ($n = 4$, $s = 4$, $i = 2$) та базисів Уолша

| $N$ | $K_{cy}$ | | | | | |
|---|---|---|---|---|---|---|
| | $c_{17}$ | $c_{37}$ | $c_{47}$ | $c_{07}$ | $c_{55}$ | $c_{62}$ |
| ТСК-1 | 0,125 | 0,135 | 0,126 | 0,125 | 0,135 | 0,126 |
| ТСК-2 | 0,375 | 0,387 | 0,387 | 0,375 | 0,387 | -0,250 |
| ТСК-3 | 0,500 | 0,516 | 0,516 | 0,500 | 0,516 | 0,516 |

Відновлення параметрів ТСК із шумоподібного сигналу здійснюється за допомогою кореляційного прийому після демодуляції. На виході інтегратора кореляційного приймача формується напруга $U_i$, яка відображає часову структуру сигналу на інтервалі $T_c$. Зсув тривалостей імпульсів $t_c = t_0 + k\Delta$ в межах інтервалу часу $T_c = t_0 \times n$ створює ансамбль сигналів зі змінною структурою. При розширенні спектра ТСК наявність зсувів $\Delta = t_0/s$ змінює часову структуру послідовності Уолша. Це означає, що противник, навіть знаючи базовий код Уолша, стикається з додатковою невизначеністю сигнальної конструкції. Аналіз кореляційних властивостей широкосмугових сигналів, сформованих на основі ТСК, показує, що коефіцієнт кореляції $K_{cy}$ між різними реалізаціями сигналів суттєво залежить від структури ТСК та вибраної ПВП Уолша. Наприклад, для трьох різних ТСК з параметрами $n = 4$, $s = 4$, $i = 2$ та різними тривалостями імпульсів $t_{c1}$, $t_{c2}$, $t_{c3}$ спостерігаються різні значення $K_{cy}$ для одних і тих самих ПВП Уолша (табл. 4.4). При використання ПВП $c_{17}$ для ТСК-1, ТСК-2, ТСК-3 отримуємо значення коефіцієнта кореляції 0,125, 0,375, 0,5 відповідно. Бачимо, що зміна структури ТСК призводить до значних відмінностей у кореляційних властивостях широкосмугових сигналів, що ускладнює передбачення точної тривалості імпульсів та їхню послідовність.

На рис. 4.4 наведено структурну схему формування шумоподібного таймерного сигналу в передавача, який складається з кодера завадостійкого коду,

формувача ТСК, пристрій перемножування ТСК $x_i^{\text{ТСК}}(t)$ з ПВП $s_1(t)$ та фазового модулятора.

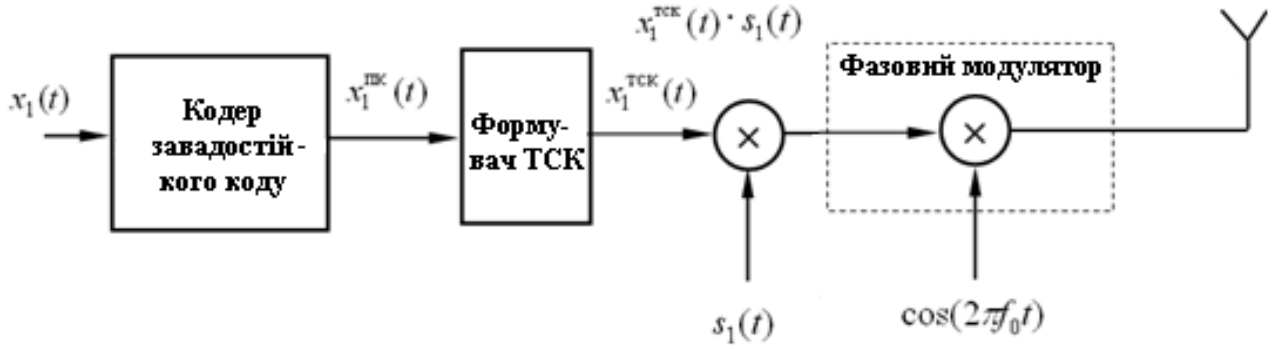



Рис. 4.4 – Формування шумоподібного таймерного сигналу в передавачі

На рис. 4.5 наведено структурну схему кореляційного приймача, у якому здійснювалося виділення таймерного сигналу із шумоподібного широкосмугового сигналу. Прийнятий сигнал з каналу зв'язку спочатку надходив до модему, де виконувалася демодуляція та підготовка сигналу до подальшої кореляційної обробки.

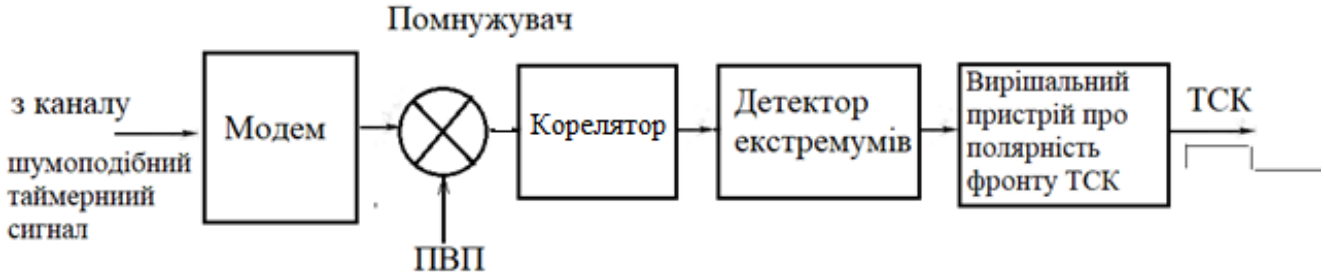



Рис. 4.5. Кореляційне виділення таймерного сигналу з шумоподібного сигналу в приймачі

Після демодуляції сигнал перемножувався з локально сформованою ПВП, синхронізованою з передавальною стороною. Така процедура забезпечувала кореляційне стискання спектра та концентрацію енергії корисного сигналу. Подальша обробка здійснювалася у кореляторі, на виході якого формувався

кореляційний відгук, що відображав часову структуру ТСК. Виділення значущих моментів відновлення виконувалося детектором екстремумів, після чого вирішальний пристрій визначав полярність фронтів та формував відновлену таймерну сигнальну конструкцію. Така структура приймача забезпечувала відновлення параметрів ТСК навіть за умов низького відношення сигнал/шум та наявності активних завад.

Таким чином, застосування таймерних сигналів у задачах прямого розширення спектра забезпечує формування шумоподібних сигналів із керованими кореляційними властивостями. Це дозволяє підвищити рівень прихованості та завадостійкості інформаційних систем, що функціонують в умовах радіоелектронного протиборства. Отримані результати можуть бути використані для подальшої розробки адаптивних методів синхронізації та оптимізації параметрів ТСК у захищених каналах зв'язку.

### 4.6 Висновки до розділу 4

1. Обґрунтовано необхідність нової інтерпретації бази широкосмугових таймерних сигналів, яка, на відміну від класичних DSSS-систем, визначалася не параметрами окремого бітового інтервалу $t_0$, а всім інтервалом формування таймерної сигнальної конструкції $T_c$. Показано, що база ТСК визначалась кількістю елементів псевдовипадкової послідовності $B_{\text{ТСК}} = N_{\tau\text{ТСК}}$, а для узгодження часової структури ТСК з параметрами ПВП виконувались умови $N_{\tau\text{ТСК}} = B(t_0) \cdot m$та $B_{\text{ТСК}} \geq N_{\Delta\text{ТСК}}$.

2. Дослідження процесу формування широкосмугових таймерних сигналів показало, що пряме розширення спектра виконувалося на інтервалі всієї сигнальної конструкції $T_c$, а не окремого імпульсу. Для параметрів $m = 4$, $s = 4$, $i = 2$та $B(t_0) = 16$ було отримано інтерпретовану базу $B_{\text{ТСК}} = 54$, що забезпечувало формування шумоподібного сигналу з одночасним поєднанням структурної та енергетичної прихованості.

3. Було встановлено, що кореляційний прийом широкосмугових ТСК

принципово відрізнявся від класичного приймання DSSS-сигналів, оскільки забезпечував відновлення часової структури всієї сигнальної комбінації. Показано, що інтегрування на інтервалі $T_c$ та аналіз екстремумів кореляційної функції дозволяли визначати значущі моменти відновлення та тривалості імпульсів $t_{ci}$. Процесингове підсилення визначалося співвідношенням $G_p = B$, що забезпечувало підвищення відношення сигнал/шум після кореляційного стискання спектра.

4. Проведене оцінювання структурної прихованості показало істотну перевагу ТСК над класичними позиційними кодами. Для параметрів $m = 4$, $s = 5$, $i = 2$кількість реалізацій становила $N_{\text{ТСК}} = 66$, тоді як для еквівалентного розрядно-цифрового коду – лише $N_{\text{РЦК}} = 16$. При $m = 4$, $s = 5$, $i = 3$ кількість реалізацій зростала до $N_{\text{ТСК}} = 286$, що підтвердило суттєвий вплив параметрів $m$, $s$та $i$на рівень структурної невизначеності.

5. Встановлено, що найбільший внесок у загальну структурну прихованість широкосмугового таймерного сигналу забезпечувала база розширення спектра та тип ПВП. Для параметрів $m = 10$, $s = 6$, $i = 4$, $B(t_0) = 128$і ФМ-4 при використанні послідовностей Уолша структурна прихованість становила $S_{\text{тск-пвпУ}} = 25$дв. вим., тоді як при використанні ПВП на основі логістичного генератора хаосу досягала $S_{\text{тск-пвп}} = 146$дв. вим. Це означало необхідність виконання приблизно $2^{146}$операцій для відновлення структури сигналу методом перебору.

6. Аналіз кореляційних властивостей шумоподібних таймерних сигналів підтвердив суттєвий вплив структури ТСК на характеристики широкосмугових сигналів. Для параметрів $n = 4$, $s = 4$, $i = 2$та бази $B(t_0) = 16$було визначено $N_{\tau\text{ТСК}} = 64$, $N_{\Delta} = 16$та $N_{\tau/\Delta} = 4$. Значення коефіцієнта кореляції $K_{cy}$змінювалися в межах від $0{,}125$до $0{,}516$ залежно від структури ТСК та вибраної ПВП Уолша. Зокрема, для послідовності $c_{17}$отримано $K_{cy} = 0{,}125$ для ТСК-1, $0{,}375$ – для ТСК-2 та $0{,}500$ – для ТСК-3, що підтвердило зростання структурної невизначеності при зміні часової організації сигналів.

7. Отримані результати підтвердили, що широкосмугові таймерні сигнальні конструкції забезпечували комбінований механізм захисту інформації за рахунок

одночасної реалізації енергетичної та структурної прихованості. Поєднання непозиційного таймерного кодування, прямого розширення спектра та кореляційного приймання створювало додатковий резерв стійкості до засобів радіоелектронної розвідки та активних завад, що свідчило про перспективність використання ТСК у захищених системах зв’язку.

# ВИСНОВКИ

У дисертаційній роботі вирішено актуальне наукове завдання підвищення прихованості передавання інформації в інформаційно-комунікаційних системах в умовах радіоелектронного протиборства шляхом розроблення методів формування широкосмугових таймерних сигналів із використанням псевдовипадкових, ортогональних та хаотичних послідовностей.

За результатами виконаних досліджень отримано такі основні результати:

**1.** Проведений аналіз сучасних методів прихованого передавання інформації показав, що класичні методи модуляції та DSSS мають обмеження щодо структурної прихованості через передбачуваність спектральних і кореляційних ознак, що обґрунтувало необхідність використання таймерних сигналів.

**2.** Отримано розвиток методу формування ТСК, у якому інформація задається часовими параметрами сигналу. Встановлено, що при $m = 4 \dots 10$, $s = 5$, $i = 3$ рівень структурної прихованості змінювався в межах $S_{\text{ТСК}} = 23 \dots 30$ дв. вим. Визначено оптимальні значення кількості значущих моментів модуляції: $i = m - 2$ для $m = 4 \dots 6$, $i = m - 3$ для $m = 7 \dots 9$ та $i = m - 6$ для $m = 10$.

**3.** Розроблено метод формування ТСК на основі системи залишкових класів, який поєднав завадостійке кодування та структурну приховання. Для модулів $\{2, 3, 7\}$ сформовано 42 таймерні комбінації, з яких 41 була допустимою після нормалізації. На відміну від коду Хемінга $(7, 4)$, що забезпечує 16 комбінацій при $\gamma_k = 0{,}57$, запропоновані ТСК формували 41 комбінацію без додаткових перевірочних біт.

**4.** Дослідження псевдовипадкових послідовностей показало, що класичні *M*-послідовності, коди Голда, Касамі та Уолша забезпечують добрі кореляційні характеристики, але характеризуються обмеженою структурною прихованістю. Для них отримано відповідно: $S_{\text{стр}} \approx 20, 40, 30$ та $n$ дв. вим., тоді як хаотичні ПВП забезпечували $S_{\text{стр}} > 100$ дв. вим., що суттєво перевищує можливості класичних лінійних послідовностей.

**5.** Запропоновано метод підвищення структурної прихованості хаотичних псевдовипадкових послідовностей на основі адаптивного порогового квантування та циклічного зсуву, які забезпечили статистичні та автокореляційні характеристики, близькі до білого шуму.

**6.** Удосконалено метод визначення бази широкосмугових таймерних сигналів через інтерпретовану базу $B_{\text{ТСК}} = B(t_0) \times m$, що враховує як базу окремого елемента, так і кількість інтервалів формування ТСК. На відміну від класичних DSSS-систем, спектральне розширення здійснюється з урахуванням часового інтервалу формування таймерної конструкції.

**7.** Встановлено визначальний вплив бази сигналу на приховання та завадостійкість. При збільшенні бази від $B = 8$ до $B = 128$ імовірність помилки суттєво зменшувалася як для позиційних, так і для таймерних сигналів. Показано, що хоча ТСК характеризуються дещо вищою ймовірністю помилки, при $B > 64$їх використання є доцільним завдяки виграшу у структурній прихованості та забезпеченню достатнього рівня енергетичної прихованості.

**8.** Проведене оцінювання широкосмугових ТСК підтвердило їх перевагу над позиційними кодами. Для $m = 4$, $s = 5$, $i = 2$кількість реалізацій становила 66, а при $i = 3$– 286, тоді як еквівалентний розрядно-цифровий код забезпечував лише 16реалізацій. Для параметрів $m = 10$, $s = 6$, $i = 4$, $B(t_0) = 128$ та ФМ-4 структурна прихованість при використанні кодів Уолша становила 25дв. вим., а при хаотичних ПВП досягала 146 дв. вим., що відповідало близько $2^{146}$ операцій перебору для відновлення структури сигналу.

**9.** Аналіз кореляційних властивостей підтвердив ефективність кореляційного приймання шумоподібних таймерних сигналів, для яких коефіцієнт кореляції змінювався в межах $K_{cy} = 0{,}125$–$0{,}516$, що свідчить про низьку передбачуваність сигналів і високу стійкість до кореляційного аналізу. Отримані результати підтверджують перспективність використання шумоподібних таймерних сигналів для побудови захищених систем зв'язку, які поєднують структурну та енергетичну прихованість і забезпечують підвищену стійкість до засобів радіоелектронної розвідки та завад.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Гнатюк С. О., Рябий М. О., & Лядовська В. М. (2014). Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. Зв'язок, (4), с. 3-7.

2. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення – 02.11.2023).

3. Боднар І. Р. "Інформаційна безпека як основа національної безпеки." Mechanism of Economic Regulation 1 (2014): с. 68-75.

4. 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.

5. Манько А. В. (2024) Метод адаптації системи радіозв'язку в умовах активного застосування засобів радіоелектронної боротьби. *Честь і закон*. № 2. 88–95. URL: nangu.edu.ua.

6. 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. https://repository.kpi.kharkov.ua/handle/KhPI-Press/93493.

7. 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

8. Shamanov D., Sorokin A. (2024) Аналіз сучасних методів радіоелектронної боротьби. *Системи управління, навігації та зв’язку* : Збірник наукових праць. – Полтава: ПНТУ, Т. 1 (75). 211–214.. https://doi.org/10.26906/SUNZ.2024.1.211

9. Пічугін М. Ф., Носова Г.Д. Збірник наукових праць ЖВІ НАУ. Випуск 3 – Аналіз тактики застосування підрозділів РЕБ у сучасних війнах та локальних збройних конфліктах. – К., 2010.

10. Семененко О. М., Бойко Р. В., Добровольський Ю. Б., Іванов В. Л., Кремешний О. І. Контррадіоелектронна боротьба як складова частина радіоелектронної боротьби в Збройних Силах України // Системи озброєння і військова техніка. – 2016. – Вип. 46. – С. 141-145.

11. Poisel, R. A. Modern Communications Jamming: Principles and Techniques. Boston: Artech House, 2011. 450 p.

12. Proakis, J. G., & Manolakis, D. K. Digital Signal Processing: Principles, Algorithms, and Applications. – 4th ed. – Upper Saddle River, NJ: Prentice Hall, 2007. – 1002 p.

13. Sklar, B. Digital Communications: Fundamentals and Applications.* – 2nd ed. – Upper Saddle River, NJ: Prentice Hall, 2001. – 1100 p.

14. Захарченко М.В. Системи передавання даних / М.В.Захарченко М.М. Гаджиєв, В.Є. Басов, О.М. Мартинова та ін. // – Т.1: Завадостійке кодування: підручник [для студ. вищ. техн. навч. закл.]. / – Одеса «Фенікс», 2009. – 406 с.

15. 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.

16. Горохов Ю.С. Метод кодового розділення каналів на основі таймерних сигнальних конструкцій / Ю.С. Горохов, Корчинский, Е.М. Рудий // Міжнародний науково-технічний журнал Вимірювальна та обчислювальна техніка в технологічних процесах. – 2016. – №1 – С.208-211.

17. 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.

18.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.

19. 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.

20.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.

21.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.

22.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.

23.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.

24.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 / Ін-т кібернетики ім. В. М. Глушкова НАН України. 2019. Вип. 19. С. 37–43.

25.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.

26.Adamy D. L. EW 101: A First Course in Electronic Warfare. Boston : Artech House, 2001. 320 p.

27.Knott, E. F., Shaeffer, J. F., Tuley, M. T. Radar Cross Section. 2nd ed. Boston: Artech House, 2004. 611 p.

28.Лунтовський А.О. Мультисервісні мобільні платформи / А.О. Лунтовський, М.В. Захарченко, А.І. Семенко – К.: ПВП «Задруга», 2014. – 214 с.

29.Лісовський П.М. Криптосистема військ радіоелектронної боротьби України / П.М. Лісовський, Ю.П. Лісовська // Навчальні посібники, Військове право, Ліра-К, 2024. – 130 с.

30.Голдвассер С., Мікалі С. Криптографія та теорія обчислень. – Київ : Наукова думка, 2016. – 320 с.

31.Політанський Р. Л., Політанський Л. Ф., Гресь О. В., Галюк С. Д. (2011) Система передавання даних з використанням генераторів хаосу. *Радиотехника*. № 164. 66–71.

32.Guan Z.-H., Huang F., Guan W. Chaos-based image encryption algorithm. *Physics Letters A*. 2005. Vol. 347, iss. 1–3. P. 116–123. https://doi.org/10.1016/j.physleta.2005.08.006

33.L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, Feb. 1990, doi: 10.1103/PhysRevLett.64.821.

34.Політанський Р. Л. Енергетична ефективність широкосмугової системи, що використовує фрактальні сигнали. *Новые технологии в телекоммуникациях* : материалы VI Междунар. научно-техн. симпозиума (Киев, январь 2013 г.). Киев, 2013. С. 60–63.

35.Голевич О. Б., Пивовар О. С. Застосування прямохаотичних надширокосмугових технологій у телекомунікаційних системах. *Информационные*

*процессы и технологии* : материалы Междунар. научно-практ. конф. (Севастополь, 22–26 апреля 2013 г.). Севастополь, 2013. С. 109.

36.Голевич О. Б., Пивовар О. С., Троцишин І. В. Результати порівняння деяких генераторів хаосу по кореляційним властивостям їх сигналів. Вимірювальна та обчислювальна техніка в технологічних процесах (ВОТТП-2015) : матеріали 14-ї Міжнародної науково-технічної конференції (Одеса, 5–9 червня 2015 р.). Одеса, 2015.

37.Голевич О. Б. Спосіб детектування хаотичних сигналів в умовах дії завад. Вимірювальна та обчислювальна техніка в технологічних процесах (ВОТТП-2015) : матеріали 14-ї Міжнародної науково-технічної конференції (Одеса, 5–9 червня 2015 р.). Одеса, 2015.

38.Голевич О. Б. Дослідження використання хаотичних коливань для телекомунікацій інформаційних сигналів. *Сучасні проблеми телекомунікацій (АПКТ-2013)* : матеріали 7-ї Міжнародної науково-технічної конференції (Хмельницький, 23 травня 2013 р.). Хмельницький : ХНУ, 2013. С. 71.

39.Зайцев Д. В., Яфонкін А. О., Ярема В. В. (2021). Основи зв'язку та радіоелектронна боротьба як вид бойового забезпечення : навчальний посібник : *Університет державної фіскальної служби України*. Ірпінь. 280 с. URI: https://ir.dpu.edu.ua/entities/publication/931c8879-4752-4096-a76d-6ab33b3b95e7/full

40.Шолохов С.М., Самборський І.І.,Вакуленко О.В., Ніколаєнко Б.А. (2021). Завадозахист радіоелектронних засобів. Частина 1. Основи завадозахисту систем зв'язку. – Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського. 210 с. URI: https://ela.kpi.ua/handle/123456789/63622

41.Горбатий І., Усатий О. (2025) Дослідження методів спектрального аналізу сигналів із розширеним спектром у сучасних комунікаційних системах : ICTEE. Т. 5, № 1. 125–135. https://doi.org/10.23939/ictee2025.01.125

42.Стасєв Ю. В., Нетренко К. Г., Хмельниченко К. В. (2022) Метод синтезу сигналів з псевдовипадковою перебудовою робочої частоти // Системи обробки інформації. № 3(170). DOI: https://doi.org/10.30748/soi.2022.170.07

43.Гриненко О. В., Кальченко В. В., Ободяк В. К., Пугач І. О., Савченко Т. Р. Адаптивне псевдовипадкове перелаштування робочої частоти для захищених мереж // CIT. 2025. DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-11

44.Maleki, A., Nguyen, H.H., Bedeer, E., & Barton, R. (2024). A Tutorial on Chirp Spread Spectrum Modulation for LoRaWAN : *Basics and Key Advances. IEEE Open Journal of the Communications Society*, 5, 4578–4612. URL: https://www.researchgate.net/publication/382580029_A_Tutorial_on_Chirp_Spread_Spectrum_Modulation_for_LoRaWAN_Basics_and_Key_Advances

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

46.Захарченко М. В., Горохов Ю. С., Кріль А. С., Ковальчук С. В. (2015). Кодове ущільнення при таймерних сигналах. *Сучасні інформаційні технології у сфері безпеки та оборони*. № 3 (24). С. 38–42. DOI: 10.33099/2311-7249/2015-24-3-38-42

47.Zaharchenko, M., Hadzhyiev, M., Salmanov, N., Golev, D., & Shvets, N. (2020). Information parameters of codes that are synthesized on the basis of one module. *Cybersecurity: Education, Science, Technique*, 3(7), 95–102. https://doi.org/10.28925/2663-4023.2020.7.95102.

48.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. C. 317. URI: https://ena.lpnu.ua/handle/ntb/14569

49.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.

50.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.

51.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. P. 41–44.

52.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.

53. 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.

54. 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.

55. 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.

56.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.

57. Shannon, C. E. A Mathematical Theory of Communication. – University of Illinois Press, 1948. – 144 pp.

58. 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.

59. Tian, H. Han, X. Niu, and X. Liu. Construction of Optimal Frequency Hopping Sequence Set with Low-Hit-Zone. Entropy, vol. 25, no. 7, p. 1044, July 2023 URI: https://www.mdpi.com/1099-4300/25/7/1044

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

61. Azim, A.W., Shubair, R., & Chafii, M. (2024). Chirp spread spectrum-based waveform design and detection mechanisms for LPWAN-based IoT: *a survey. IEEE Access,* vol. 12, pp. URI: https://www.researchgate.net/publication/377352793_Chirp_Spread_Spectrum-based_Waveform_Design_and_Detection_Mechanisms_for_LPWAN-based_IoT_-_A_Survey

62. Kaplan B. et al. (2021) Detection and direction of arrival estimation of drone FHSS signals // IEEE Access. Vol. 9. https://doi.org/10.1109/ACCESS.2021.3127199

63. Ristić, V.B., Todorović, B.M., & Stojanović, N.M. (2022). Frequency Hopping spread spectrum: history, principles and applications. Military Technical Courier, vol. 70(4), pp. 856–876. URL: https://www.researchgate.net/publication/364426596_Frequency_hopping_spread_spectrum_History_principles_and_applications

64. 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

65.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)* (Kyiv, October 26, 2021). CEUR Workshop Proceedings. 2022. Vol. 3187. P. 182–194. URL: https://ceur-ws.org/Vol-3187/paper17.pdf

66.Rudnytskyi V., Korchenko O., Lada N., Ziubina R., Wieclaw L., Hamera L. Cryptographic encoding in modern symmetric and asymmetric encryption. *Procedia Computer Science*. 2022. Vol. 207 : Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 26th International Conference KES-2022. P. 54–63.

67.Rudnytskyi, V., Lada, N., Pochebut, M., Melnyk, O., & Tarasenko, Ya. (2023). Increasing the cryptographic strength of CET-encryption by ensuring the transformation quality of the information block. 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 1–6.

68.Корчинський В.В. Оцінка структурної скритності сигнальних конструкцій на основі хаотичних сигналів в системах передачі конфіденційної інформації / В.В. Корчинський // Наукові праці ОНАЗ ім. О.С. Попова, 2012, No 1 - С 77-81.

69.Корчинський, В., Мар’ян, М., Богданюк, І., & Аль-Файюмі Халед. (2024). Метод захисту інформації від несанкціонованого доступу на основі динамічного хаосу. Scientific Collection «InterConf», (194), 448-453.

70.Корчинський В.В. Методи застосування динамічного хаосу в системах захисту інформації / В.В. Корчинський, Халед Аль-Файюмі // Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. – К.: НУОУ, 2023. – С 81-83.

71.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

72.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.

73.Корчинський, В., Рябуха, О., Бєлова, Ю., Степанов, В., & Гавель, С. (2024). Методи захисту інформації на основі розширення спектра сигналу. Scientific Collection «InterConf», (208), 216–220. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/6685

74.Політанський, Р.Л. Дослідження псевдовипадкових послідовностей, генерованих картами хаосу / Р.Л. Політанський, З.Ю. Готра // IV Міжнародна науково-технічна конференція і II студентська науково-технічна конфренція «Проблеми телекомунікацій». – Київ, Україна. – 2010. – С. 127-128.

75.Політанський, Л.Ф. Система передавання даних з використанням псевдовипадкових послідовностей в кодах Хемінга / Л.Ф. Політанський, Р.Л. Політанський, М.Г. Рождественська, О.В. Гресь // Труди XII-ї Міжнародної науково-практичної конференції «Сучасні інформаційні та електронні технології». – Одеса, Україна. – Травень. – 2011. – С. 156.

76.Основи теорії інформації та кодування : електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Майданюк В. П., Романюк О. Н., Тужанський С. Є. – Вінниця : ВНТУ, 2022. – 133 с.

77.Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : підручник. 2-ге вид., перероб. й допов. Харків : Форт, 2012. 878 с.

78.Горохов Ю.С. Зв’язок потужності таймерного коду з заданим числом інформаційних відрізків і значенням твірного елемента Δ / Ю.С. Горохов, Д.Н. Бектурсунов, М.В. Захарченко, В.В. Корчинський, Б.К. Радзімовський // Матеріали 14 міжнародної науково-технічної конференції Вимірювальна та

обчислювальна техніка в технологічних процесах: 5-10 червня 2015 р. в м.Одеса (Затока) – Одеса, 2015– С. 240-241.

79.Корчинський, В., Гавель, С., Сєдов, К., Севастєєв, Є., & Лімарь, І. (2025). Метод захисту інформації на основі системи залишкових класів при формуванні таймерних сигналів. Measuring and computing devices in technological processes, (3), 204–209. https://doi.org/10.31891/2219-9365-2025-83-37

80.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. https://doi.org/10.15587/2706-5448.2026.353067

81.Zaharchenko , M. ., Hadzhyiev , M. ., Salmanov , N. ., Shvets , N., & Havel , S. . (2021). Аналіз і оцінка якісних і кількісних показників інформації при вирішенні завдань побудови систем передачі і перетворення даних. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 3(11), 136–143. https://doi.org/10.28925/2663-4023.2021.11.136143

82.Корчинський, В., Рябуха, О., Халед, А.-Ф., Гавель, С., Міненко, В., & Криштафор, З. (2023). Дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей. *Measuring and computing devices in technological processes*, (1), 180–186. https://doi.org/10.31891/2219-9365-2023-73-1-24

83.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. Lviv Polytechnic National University, Vol. 11, No. 11, 50-55. https://doi.org/10.23939/acps2026.01.050

84.Гавель С.М., Славич В.О., Петровський Р.І., Комісар В.В. Методи формування шумоподібного сигналу на основі дискретних генераторів хаосу. 80-та ювілейна Міжнародна науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів і студентів. 26 листопада 2025 року. ДУТІЗ. С.308-311.

85.Гавель С. М., Беспятенко С. В. Захист інформації від несанкціонованого

доступу в умовах радіоелектронного конфлікту. Матеріали 78-ї Міжнародної науково-технічної конференції професорсько-викладацького складу, науковців, аспірантів та студентів (Одеса, 21–23 листопада 2023 р.). Одеса : ДУІТЗ, 2023. С. 111–113.

86.Гавель С.М., Мар'ян М.О., Перун І.П. Перспективи використання динамічного хаосу в системах захисту інформації Impact of Artificial Intelligence and Other Technologies on Sustainable Development: Proceedings of the 1st International Scientific and Practical Internet Conference, December 28-29, 2023. FOP Marenichenko V.V., Dnipro, Ukraine, p. 48-50. http://www.wayscience.com/wp-content/uploads/2024/01/Conference-Proceedings-December-28-29-2023.pdf

87.Корчинський В. В., Гавель С. М., Донкогло А. С., Галиця О. Т. Аналіз і дослідження методів підвищення захисту передаваної інформації на основі хаотичних коливань. Матеріали 79-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів (Одеса, 21–22 листопада 2024 р.). Одеса : ДУІТЗ, 2024. С. 94–96.

88.Гавель С.М., Славич В. О., Мар'ян М. О., Прилуцький А. О., Гавреш І.Р. Методи підвищення криптостійкості псевдовипадкових послідовностей, що формуються на основі генераторів хаосу. 1 Міжнародна науково-практична інтернет-конференція Reimagining the future: collaborative solutions for global problems 9-10 жовтня 2025 року. С. 66-68. http://www.wayscience.com/wp-content/uploads/2025/10/Conference-Proceedings-October-9-10-2025-1.pdf

89.Serhii Havel, Yevhen Vasiliu, Nikolaos Bardis, Sergii Staikutsa. Eavesdropping Attack of Two Eavesdroppers on the Ping-Pong Protocol with GHZ triplets. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 4-6 September, 2025, Gliwice, Poland P. 329-335 https://ieeexplore.ieee.org/xpl/conhome/11321922/proceeding

90.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.

91.Іванюк П. В., Політанський Р. Л. Оцінки чисельних характеристик систем детермінованого хаосу. *Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки* : матеріали І-ї Всеукр. наук.-практ. конф. (Чернівці, жовтень 2011 р.). Чернівці : ЧНУ, 2011. С. 107–110.

92. 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.

93. 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.

94.Політанський, Р.Л. Енергетична ефективність широкосмугової системи, що використовує фрактальні сигнали / Р.Л. Політанський // VI Международный научно-технический симпозиум «Новые технологии в телекоммуникациях». – Киев, Украина. – Січень, 2013. С. 60-63.

95. Кувшинов О. В., Шишацький А. В., Жук О. Г., Бєляков Р. О., Прокопенко Є. М., Леонтьєв 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.

96.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. URL: http://nbuv.gov.ua/UJRN/soivt_2017_2_34

97. 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 ВІТІ*. Вип. 1. 25-34.

98. 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. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2014_3_15

99.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. URL: http://nbuv.gov.ua/UJRN/soivt_2017_1_27

100. Сайко В. Г., Стеклов В. П. Проектування мереж радіозв'язку: Підручник для ВНЗ. –К.: Техніка, 2021. –320 с.

101. 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.

102. 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.

.

# ДОДАТКИ

## ДОДАТОК А

## ПЕРЕЛІК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

***Наукові праці, в яких опубліковано наукові результати дисертації:***

1. 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. https://doi.org/10.15587/2706-5448.2026.353067 **(Scopus)**

2. Zaharchenko , M. ., Hadzhyiev , M. ., Salmanov , N. ., Shvets , N., & Havel , S. . (2021). Аналіз і оцінка якісних і кількісних показників інформації при вирішенні завдань побудови систем передачі і перетворення даних. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 3(11), 136–143. https://doi.org/10.28925/2663-4023.2021.11.136143

3. Корчинський, В., Гавель, С., Сєдов, К., Севастєєв, Є., & Лімарь, І. (2025). Метод захисту інформації на основі системи залишкових класів при формуванні таймерних сигналів. Measuring and computing devices in technological processes, (3), 204–209. https://doi.org/10.31891/2219-9365-2025-83-37

4. Корчинський, В., Рябуха, О., Халед, А.-Ф., Гавель, С., Міненко, В., & Криштафор, З. (2023). Дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей. *Measuring and computing devices in technological processes*, (1), 180–186. https://doi.org/10.31891/2219-9365-2023-73-1-24

5. 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

6. 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. Lviv Polytechnic National University, Vol. 11, No. 11, 50-55. https://doi.org/10.23939/acps2026.01.050

***Наукові праці, які засвідчують апробацію матеріалів дисертації:***

7. Гавель С.М., Славич В.О., Петровський Р.І., Комісар В.В. Методи формування шумоподібного сигналу на основі дискретних генераторів хаосу. 80-та ювілейна Міжнародна науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів і студентів. 26 листопада 2025 року. ДУТІЗ. С.308-311.

8. Корчинський, В., Рябуха, О., Бєлова, Ю., Степанов, В., & Гавель, С. (2024). Методи захисту інформації на основі розширення спектра сигналу. Scientific Collection «InterConf», (208), 216–220. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/6685

9. Гавель С. М., Беспятенко С. В. Захист інформації від несанкціонованого доступу в умовах радіоелектронного конфлікту. Матеріали 78-ї Міжнародної науково-технічної конференції професорсько-викладацького складу, науковців, аспірантів та студентів (Одеса, 21–23 листопада 2023 р.). Одеса : ДУІТЗ, 2023. С. 111–113.

10. Гавель С.М., Мар’ян М.О., Перун І.П. Перспективи використання динамічного хаосу в системах захисту інформації Impact of Artificial Intelligence and Other Technologies on Sustainable Development: Proceedings of the 1st International Scientific and Practical Internet Conference, December 28-29, 2023. FOP Marenichenko V.V., Dnipro, Ukraine, p. 48-50. http://www.wayscience.com/wp-content/uploads/2024/01/Conference-Proceedings-December-28-29-2023.pdf

11. Корчинський В. В., Гавель С. М., Донкогло А. С., Галиця О. Т. Аналіз і дослідження методів підвищення захисту передаваної інформації на основі хаотичних коливань. Матеріали 79-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів (Одеса, 21–22 листопада 2024 р.). Одеса : ДУІТЗ, 2024. С. 94–96.

12. Гавель С.М., Славич В. О., Мар’ян М. О., Прилуцький А. О., Гавреш І.Р.

Методи підвищення криптостійкості псевдовипадкових послідовностей, що формуються на основі генераторів хаосу. 1 Міжнародна науково-практична інтернет-конференція Reimagining the future: collaborative solutions for global problems 9-10 жовтня 2025 року. С. 66-68.

http://www.wayscience.com/wp-content/uploads/2025/10/Conference-Proceedings-October-9-10-2025-1.pdf

13. Serhii Havel, Yevhen Vasiliu, Nikolaos Bardis, Sergii Staikutsa. Eavesdropping Attack of Two Eavesdroppers on the Ping-Pong Protocol with GHZ triplets. The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 4-6 September, 2025, Gliwice, Poland P. 329-335/ **(SCOPUS)** ISSN 1424-8220

https://ieeexplore.ieee.org/xpl/conhome/11321922/proceeding

14. 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.

# ДОДАТОК Б
# АКТИ ВПРОВАДЖЕННЯ

**ЗАТВЕРДЖУЮ**
Проректор з навчальної роботи
Державного університету інтелектуальних технологій і зв'язку
проф., д-р. наук з держ. управ.
_____ С. К. Хаджирадєва
«15» _____ 2026 року

**АКТ**
**впровадження результатів дисертаційної роботи**
**Гавеля Сергія Миколайовича**
**на тему: «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій»**

Комісія в складі:

Голова: декан факультету ІТК, д.т.н., проф. Василіу 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. склала цей акт про таке.

Результати дисертаційної роботи здобувача кафедри кібербезпеки та технічного захисту інформації Гавеля Сергія Миколайовича на тему «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій» впроваджено в навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку. Матеріали дослідження використовуються під час викладання дисциплін «Забезпечення кібербезпеки у ЗСУ» та «Теоретичні основи передавання та захисту інформації», зокрема в частині вивчення методів захисту інформації на фізичному рівні, підвищення структурної та енергетичної прихованості сигнально-кодових конструкцій, а також технологій прямого розширення спектра сигналів.

**Голова комісії:**
Декан факультету ІТК ДУІТЗ,
д.т.н., проф. Василіу Є.В.

**Члени комісії:**
д.т.н., проф., зав. 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.

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"КОБІ СС"
ЄДРПОУ 42507290,
Р/р IBAN UA963348510000000026006225980 АТ «ПУМБ» МФО 334851 ІПН 425072926541.

# АКТ ВПРОВАДЖЕННЯ

**результатів дисертаційної роботи**
**«Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій»**
**на здобуття наукового ступеня доктора філософії**
**за спеціальністю 125 Кібербезпека**

## ГАВЕЛЯ СЕРГІЯ МИКОЛАЙОВИЧА

Комісія у складі: директора Вихристюка Олексія Анатолійовича, начальника технічного відділу Гаврилея Сергія Анатолійовича.

Розглянувши результати дисертаційної роботи «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій», підтверджуємо, що основні наукові та практичні результати можуть застосовуватися в діяльності підприємства ТОВ «КОБІ СС».

Зокрема, практичну цінність становлять такі розробки:

– метод формування широкосмугових шумоподібних таймерних сигналів на основі прямого розширення спектра псевдовипадковими послідовностями, який може бути використаний для підвищення рівня захисту інформації в інформаційно-комунікаційних системах від несанкціонованого доступу та засобів радіоелектронної розвідки;

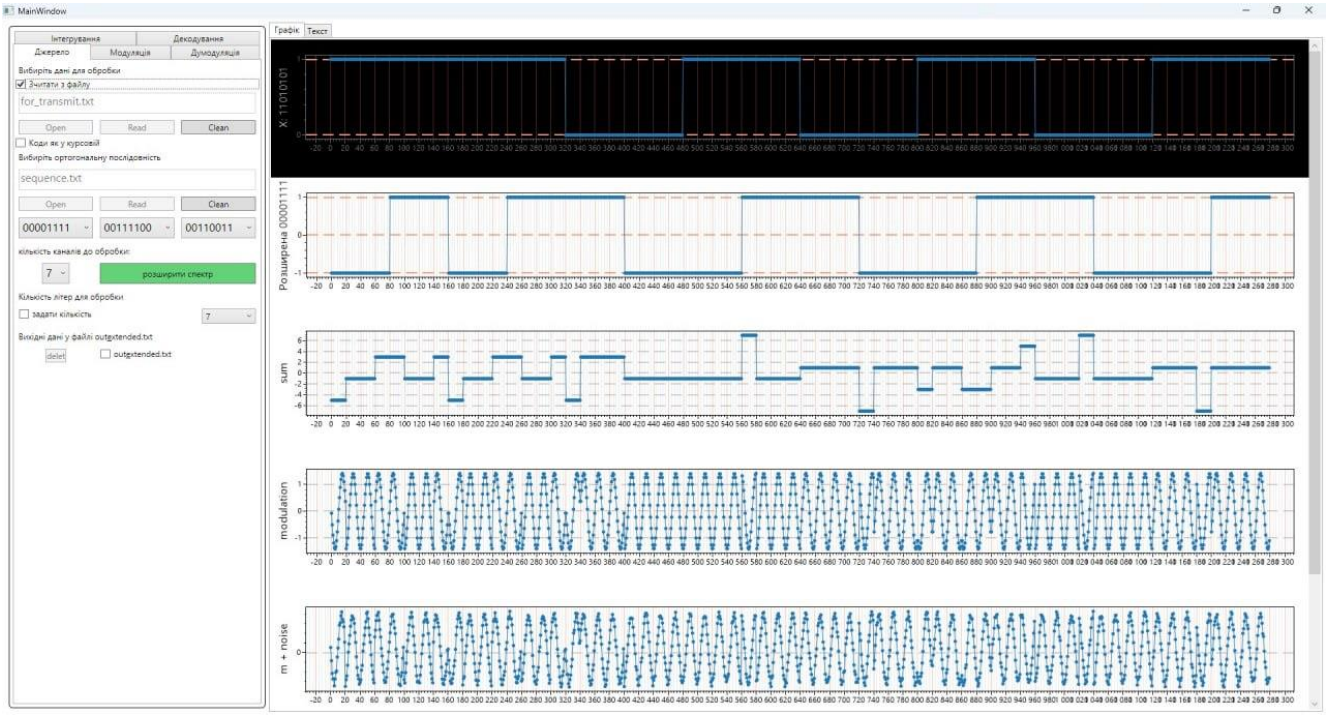
– методи розширення спектра таймерних сигнальних конструкцій із використанням послідовностей Уолша, хаотичних псевдовипадкових послідовностей та системи залишкових класів, що можуть застосовуватися під час проєктування захищених каналів передавання інформації та спеціалізованих систем зв'язку;

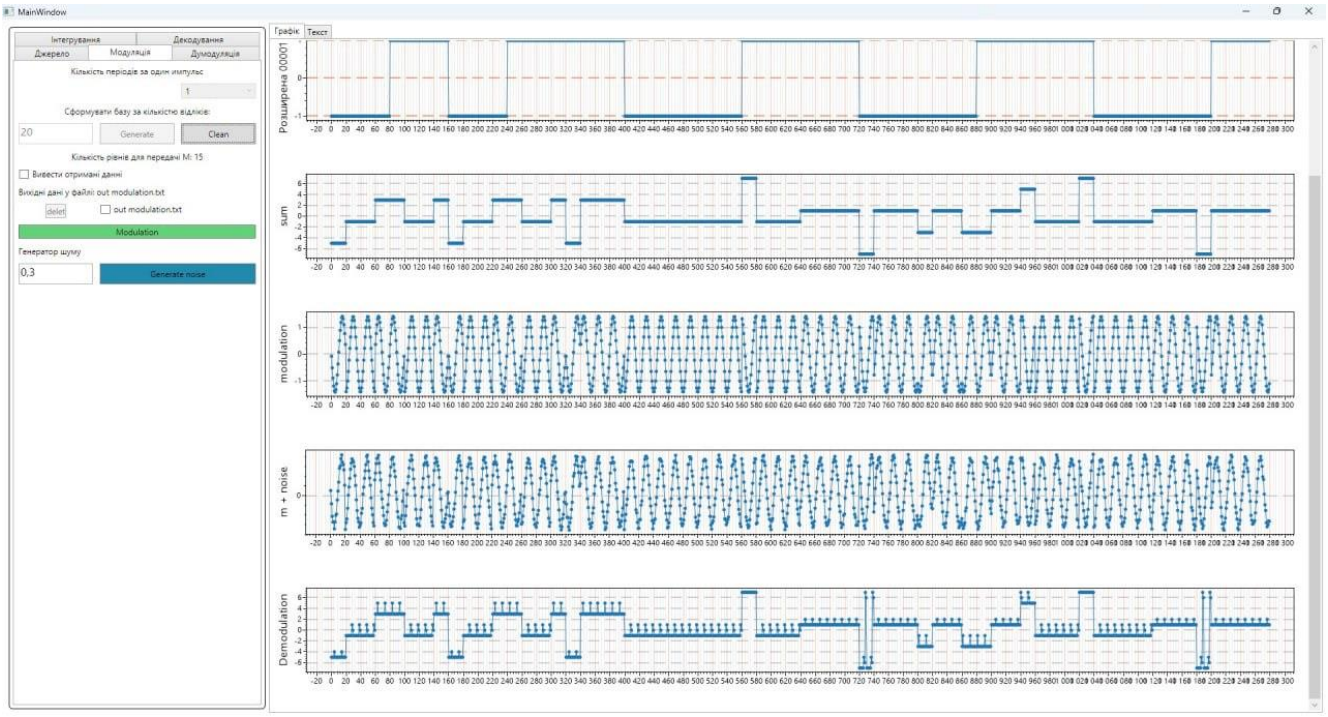
– результати дослідження спектральних і кореляційних властивостей широкосмугових таймерних сигналів, які можуть бути використані під час розроблення та модернізації захищених інформаційно-комунікаційних систем, що функціонують в умовах радіоелектронного протиборства.

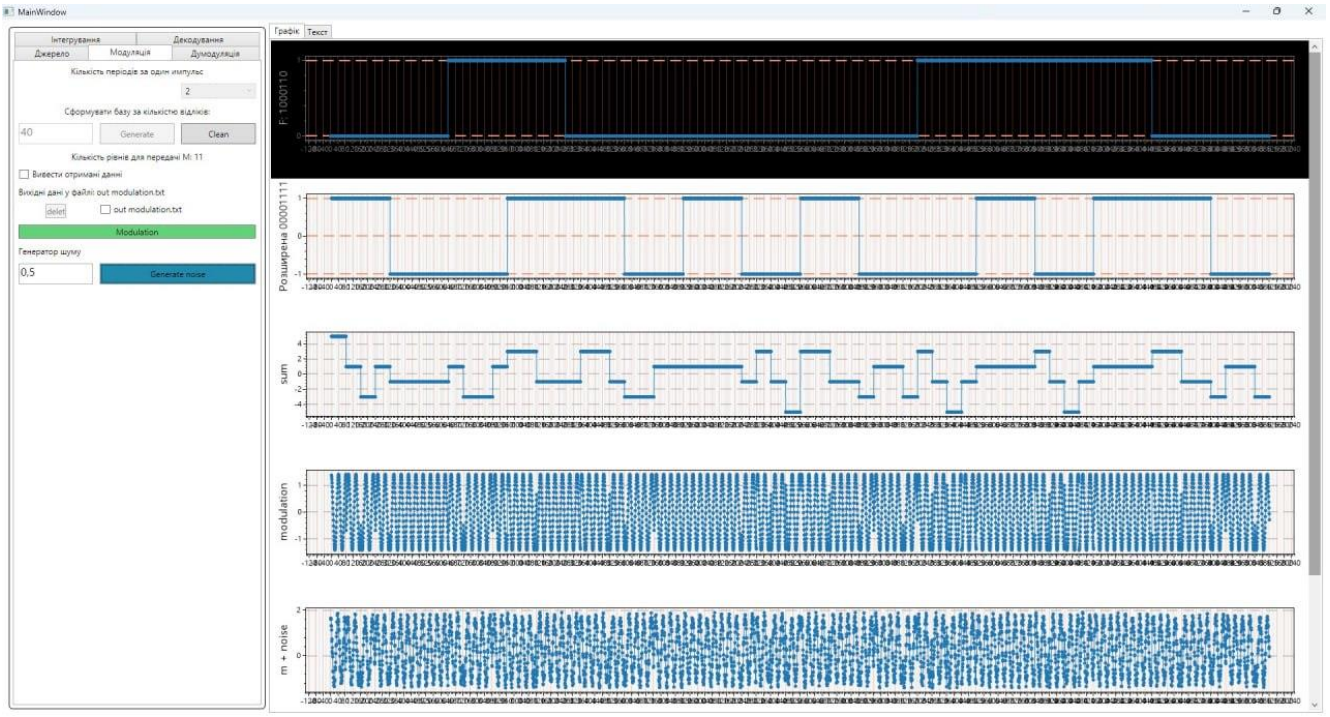
Директор ТОВ «КОБІ СС» _____ Олексій ВИХРИСТЮК
Начальник технічного відділу _____ Сергій ГАВРИЛЕЙ

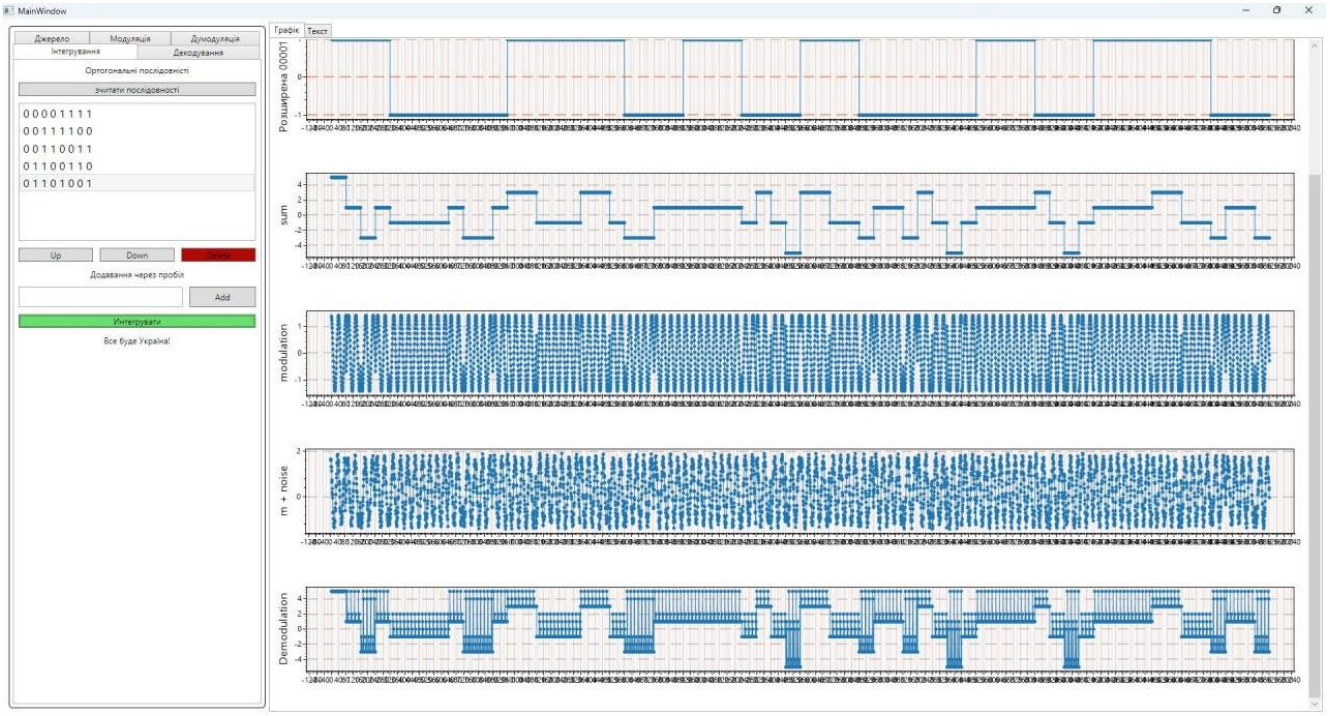
# ДОДАТОК В

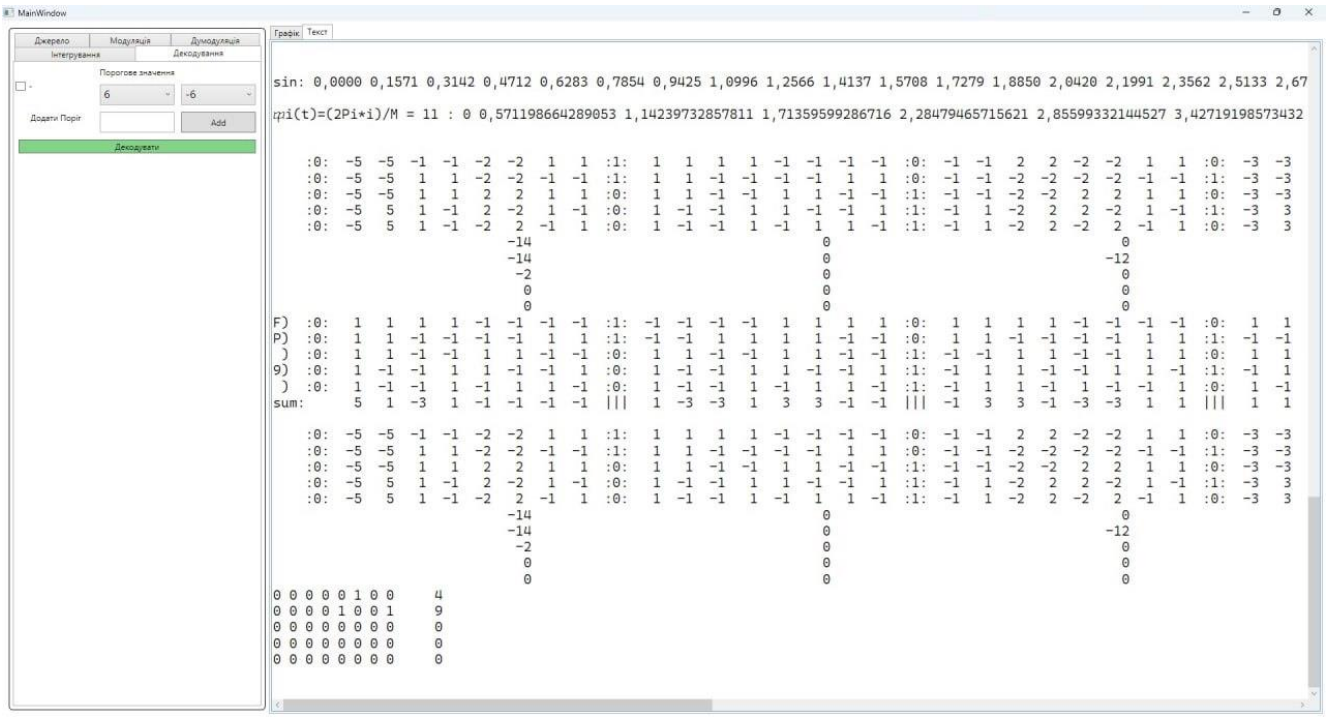
# ІНТЕРФЕЙС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МОДЕЛЮВАННЯ ШУМОПОДІБНИХ СИГНАЛІВ




MainWindow
Інтегрування
Декодування
Джерело
Модуляція
Демодуляція
Кількість періодів за один імпульс
2
Сформувати базу за кількістю відліків:
40
Generate
Clean
Кількість рівнів для передачі M: 11
Вивести отримані данні
Вихідні дані у файлі out modulation.txt
delet
out modulation.txt
Modulation
Генератор шуму
0,5
Generate noise
Графік
Текст
F: 1000110
Розширена 00001111
sum
modulation
m + noise


MainWindow
Джерело
Модуляція
Демодуляція
Інтегрування
Декодування
Ортогональні послідовності
зчитати послідовності
00001111
00111100
00110011
01100110
01101001
Up
Down
Delete
Додавання через пробіл
Add
Интегрувати
Все буде Україна!
Графік
Текст
Розширена 00001
sum
modulation
m + noise
Demodulation


MainWindow
Джерело
Модуляція
Демодуляція
Інтегрування
Декодування
Порогове значення
6
-6
Додати Поріг
Add
Декодувати
Графік
Текст
sin: 0,0000 0,1571 0,3142 0,4712 0,6283 0,7854 0,9425 1,0996 1,2566 1,4137 1,5708 1,7279 1,8850 2,0420 2,1991 2,3562 2,5133 2,67
exp i(t)=(2Pi*i)/M = 11 : 0 0,571198664289053 1,14239732857811 1,71359599286716 2,284794657156 21 2,855993321445 27 3,427191985734 32
sum: 5 1 -3 1 -1 -1 -1 -1 ||| 1 -3 -3 1 3 3 -1 -1 ||| -1 3 3 -1 -3 -3 1 1 ||| 1 1
0 0 0 0 0 1 0 0 4
0 0 0 0 1 0 0 1 9
0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0