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

Кваліфікаційна наукова праця
На правах рукопису

АЛЬ-ФАЙЮМІ ХАЛЕД

УДК 004.056.53:621.391.7

ДИСЕРТАЦІЯ

МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ НА ОСНОВІ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ СИГНАЛЬНО-КОДОВИХ 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
_____ Аль-Файюмі Халед
(*підпис*)

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

Одеса – 2024

АНОТАЦІЯ

Аль-Файюми Халед. Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. – Державний університет інтелектуальних технологій, Одеса, 2024.

У дисертаційній роботі наведено наукове обґрунтування та нове вирішення актуальної наукової проблеми, яке полягає у розробці та вдосконаленні методів підвищення завадозахищеності передавання інформації в інформаційно-комунікаційних системах на основі інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів.

Актуальність роботи полягає в необхідності розробки та дослідженні нових методів захисту інформації на основі сумісного використання позиційних, непозиційних та хаотичних сигналів, способів розширення спектра, що забезпечує підвищення прихованості передавання конфіденційних повідомлень.

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, а саме: фундаментальним науковим дослідженням теоретико-методологічних, науково-методичних та прикладних засад, а також проведення науково-дослідних робіт, пов’язаних з розробкою методів збільшення інформаційної місткості найквістового елементу та захищеності повідомлень з використанням таймерних сигнальних конструкцій, методів захисту інформації на основі динамічного хаосу, шумоподібних таймерних сигналів, інтеграції стохастичного шифрування, завадостійкого кодування, і декореляції помилок.

Забезпечення захисту інформації в сучасному інформаційному просторі є складною і постійно зростаючою проблемою. Можливості традиційних методів

захисту інформації часто виявляються недостатніми, оскільки зловмисники постійно створюють нові та вдосконалюють наявні технології атак. Застосування динамічного хаосу в різних галузях науки не оминає і такий важливий напрямок, як інформаційна безпека. Явище динамічного хаосу має певні особливості та переваги, які є перспективними з точки зору вдосконалення існуючих та створення нових систем захисту інформації. Динамічний хаос характеризується непередбачуваністю, чутливістю до початкових умов і параметрів, а також – складністю його динаміки. Такі властивості роблять його перспективним для підвищення основних показників завадозахищеності системи зв'язку, такі як прихованість та завадостійкість. Динамічний хаос може бути використаний для шифрування, маскування або змішування даних перед їх передачею. Синтез широкосмугових шумоподібних сигнальних конструкцій на основі хаотичних коливань дозволяє маскувати передаваний сигнал на фоні шумів та вирішувати завдання з підвищення енергетичної прихованості. Генерація псевдовипадкових чисел та ключів для криптографічних систем шифрування за допомогою генераторів хаосу збільшує інформаційну прихованість. Важливим для захисту інформації є підвищення структурної прихованості сигнальних конструкцій, що можливо шляхом ускладнення структури сигнальних конструкцій. Досягається це на основі сумісного використання хаотичних коливань з непозиційними сигналами, якими є таймерні сигнальні конструкції. Доцільність застосування таймерних сигналів для завдання захисту інформації обґрунтовується можливістю формування різних ансамблів комбінацій в залежності від параметрів їх побудови. Також, на основі таймерних сигналів можливо здійснювати контроль якості прийнятих сигнальних конструкцій без додаткових перевірочних елементів.

В цьому напряму працювали та зробили вагомий вклад різні зарубіжні та вітчизняні вчені, такі як: М. Захарченко, Л. Політанський, А. Семенко, А. Зюко, В. Банкет, Б. Радзімовський, К. Шеннон, А. Камінський, В. Гордійчук та інші.

В роботі запропоновано методи застосування динамічного хаосу в системах захисту інформації, що дозволяє реалізувати процеси передавання даних, їх

шифрування, маскування та змішування. Таким чином, використання динамічного хаосу для вирішення завдань захисту інформації є перспективним напрямком досліджень і розвитку. Це вимагає подальшої наукової роботи в цьому напрямку, розробки нових методів і алгоритмів, а також впровадження стандартів безпеки, що забезпечать ефективне застосування динамічного хаосу в реальних системах захисту інформації.

У зв'язку з цим існує необхідність вирішення актуального наукового завдання з розробки моделей, методів та алгоритмів інтегрованого захисту інформації на основі різних механізмів перетворення даних, що включає процеси розширення спектра непозиційних сигналів, статистичного шифрування з поєднанням додаткових функцій завадостійкого кодування та декореляції помилок.

Метою дисертаційної роботи є розв'язання науково-технічної проблеми підвищення прихованості передавання інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів.

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

1) дослідити та дати оцінку сучасним положенням та аспектам, що впливають на можливість підвищення завадостійкості та прихованості сигнальних конструкцій систем зв'язку, що забезпечують обмін конфіденційної інформації в умовах радіоелектронного конфлікту;

2) провести та дати оцінку варіаційним можливостям дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів;

3) розробити та дослідити методи підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних, які основані на сумісному використанні статистичного шифрування, завадостійкого кодування та декореляції помилок;

4) розробити та провести моделювання синтезованих шумоподібних сигналів на основі розширення таймерних сигналів за допомогою лінійної частотної модуляції, методи їх передавання та приймання;

5) дати кількісний і якісний аналіз синтезованим множинам таймерних сигнальних конструкцій для оцінки співвідношення між рівнями забезпечення показників енергетичної, структурної прихованості та коригувальної здатності коду.

Об'єкт дослідження: процеси перетворення позиційних та непозиційних сигнальних конструкцій для забезпечення підвищення прихованості передавання інформації в інформаційно-комунікаційних системах.

Предмет дослідження: ансамблі шумоподібних сигналів на основі методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів для збільшення прихованості сигнальних конструкцій.

Методи дослідження. Для вирішення поставлених задач в дисертації використано методи системного та порівняльного аналізу з метою визначення актуальності роботи та постановки наукового завдання. При аналізі та дослідженні варіаційних можливостей дискретних генераторів хаосу був використаний кореляційний аналіз та теорія ймовірнісного аналізу. При розробці методу захисту інформації на основі сумісного використання статистичного шифрування, завадостійкого кодування та декореляції було використано: теорія статистичного моделювання, теорії завадостійкого кодування, теорія прихованості та криптографії.

При розробці методу синтезу шумоподібних сигналів на основі розширення таймерних сигналів за допомогою лінійної частотної модуляції було використано: теорії захисту інформації, теорії сигналів та теорії завадостійкого кодування, а також методи статистичного й імітаційного моделювання.

Наукова новизна одержаних результатів полягає в наступному:

1. Отримала подальший розвиток теорія динамічного хаосу для систем захисту та передавання конфіденційної інформації, що дало змогу в результаті досліджень оцінити варіаційні можливості дискретних генераторів хаосу по

формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів, а також для систем маніпуляції, в яких для маскування процесу передавання непозиційних цифрових комбінацій використовуються хаотичні коливання.

2. Отримали подальший розвиток методи підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних: сумісного використання статистичного шифрування, завадостійкого кодування та декореляції помилок. Це дало змогу інтегрувати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі.

3. Отримала подальший розвиток теорія синтезу шумоподібних сигналів, яка спрямована на розширення спектра непозиційних сигнально-кодових конструкцій, за допомогою яких можна змінювати структуру таймерних комбінацій та коригувальну здатність по виявленню та виправленню помилок.

4. Вперше запропоновано метод синтезу шумоподібних сигналів на основі розширення спектра непозиційних таймерних сигналів за допомогою лінійної частотної модуляції, що дало змогу підвищити завадостійкість, енергетичну та структурну прихованості передавання сигнальних конструкцій.

Практичне значення одержаних в дисертації результатів полягає в збільшенні енергетичної та структурної прихованості сигнальних конструкцій шляхом застосування хаотичних коливань в системах модуляції для передавання непозиційних таймерних сигналів та в системах потокового шифрування. Встановлено, що незначні зміни параметрів дискретного генератора дають можливість створювати квазіортогональні послідовності чисел, взаємний коефіцієнт кореляції складає в межах $6{,}9\ 10^{-4}$ - $8{,}1\ 10^{-3}$.

Сумісне використання статистичного шифрування, завадостійкого кодування та декореляції помилок дало змогу поєднати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі зв’язку.

При цьому на кожному кроці перетворення інформації відбувається зростання інформаційної прихованості та підвищення завадостійкості.

Таким чином, застосування декореляції помилок дозволяють зменшити кратність помилок у кодових комбінаціях та використовувати режим виявлення помилок великої кратності $t_{\text{вияв}} = 2 \ldots 3$ в сполученні з виправленням помилок кратністю $t_{\text{вип}} = 1$.

Результати досліджень, виконаних в роботі, дозволяють встановити наступне: можливість синтезу шумоподібних непозиційних таймерних сигналів на основі лінійної частотної модуляції; застосування кореляційного прийому для виділення фронтів таймерних сигналів при відношенні сигнал-завада на вході приймача $h = P_c / P_i = 0{,}25$; забезпечення енергетичної прихованості, тобто можливість передавання за умови, що завада перевішує корисний передаваний сигнал в 2-4 рази. Застосування таймерних сигналів дало змогу підвищити структурну прихованість у порівнянні з розрядно-цифровим кодом.

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

Ключові слова: інформаційна безпека, енергетична та структурна прихованість, несанкціонований доступ, радіоелектронний конфлікт, перехоплення сигналу, випадкова та цілеспрямована завада, завадостійкість, криптостійкість, непозиційні таймерні сигнали, кібербезпека, шумоподібний сигнал, розширення спектра, кореляційний приймач, статистичне шифрування, декореляція помилок, завадостійке кодування.

ANOTATION

Khaled Alfaiomi. Methods for Improving Information Security Based on Concealed Transmission of Signal-Code Constructions – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the field of knowledge 12 − Information technologies in the specialty 125 − Cybersecurity. – State University of Intelligent Technologies and Telecommunications, Odesa, 2024.

This dissertation provides scientific substantiation and presents a novel solution to a pressing scientific problem, which involves the development and refinement of methods to enhance noise immunity in the transmission of information in information and communication systems. The solution is based on the integration of timer coding, statistical encryption, and noise-like signal synthesis.

The relevance of the work lies in the necessity to develop and study new methods of information protection based on the combined use of positional, non-positional, and chaotic signals, as well as spectrum expansion techniques to ensure enhanced concealment in the transmission of confidential messages.

The topic of the dissertation corresponds to the standards and professional competencies of the educational and scientific program for training Doctors of Philosophy in cybersecurity and technical information protection at the State University of Intellectual Technologies and Communications, Ministry of Education and Science of Ukraine. Specifically, it relates to fundamental research on theoretical, methodological, and applied principles for improving the efficiency of innovative and industrial enterprise activities. It also covers conducting research and design-development works related to developing methods for increasing the information capacity of Nyquist elements and ensuring the security of messages based on timer signal constructions, methods for protecting information using dynamic chaos, noise-like timer signal constructions, and the integration of information protection methods based on stochastic encryption, noise-immune coding, and error decorrelation.

Ensuring information security in the modern information space is a complex and continuously growing challenge. The capabilities of traditional information protection

methods are often insufficient as attackers constantly create new and improve existing attack technologies. The application of dynamic chaos in various scientific fields has also been extended to the critical area of information security. The phenomenon of dynamic chaos possesses specific features and advantages that are promising for improving existing and creating new information protection systems. Dynamic chaos is characterized by unpredictability, sensitivity to initial conditions and parameters, and the complexity of its dynamics. These properties make it promising for enhancing the primary indicators of communication system noise immunity, such as concealment and noise resistance. Dynamic chaos can be used for encrypting, masking, or mixing data before transmission. The synthesis of broadband noise-like signal constructions based on chaotic oscillations allows masking the transmitted signal against noise and solving tasks related to enhancing energy concealment. Generating pseudo-random numbers and keys for cryptographic encryption systems using chaos generators increases information concealment. Enhancing the structural concealment of signal constructions is essential for information protection, achievable by complicating the structure of signal constructions. This is realized through the combined use of chaotic oscillations with non-positional signals, such as timer signal constructions. The feasibility of using timer signals for information protection tasks is justified by the possibility of forming different sets of combinations depending on their construction parameters. Additionally, timer signals enable the control of signal quality without additional verification elements.

Significant contributions in this area were made by foreign and domestic scientists such as M. Zakharchenko, L. Polytansky, A. Semenko, A. Zyuko, V. Banket, B. Radzimovsky, K. Shannon, A. Kaminsky, V. Gordiychuk, and others.

The dissertation proposes methods for applying dynamic chaos in information protection systems, enabling the implementation of data transmission, encryption, masking, and mixing processes. Thus, using dynamic chaos for addressing information protection tasks represents a promising direction for research and development. This requires further scientific work in this area, developing new methods and algorithms, and implementing security standards that ensure the effective application of dynamic chaos in real information protection systems.

In this context, there is a need to solve an urgent scientific problem by developing models, methods, and algorithms for integrated information protection based on various data transformation mechanisms. These include spectrum expansion processes for non-positional signals, statistical encryption combined with additional functions of noise-resistant coding and error decorrelation.

The purpose of the dissertation is to solve the scientific and technical problem of enhancing the concealment of information transmission in information and communication systems by developing methods for integrating timer coding processes, statistical encryption, and noise-like signal synthesis.

To achieve this goal, the following scientific and technical tasks were addressed:

1. Investigate and assess modern positions and aspects influencing the possibility of enhancing the noise resistance and concealment of signal constructions in communication systems that ensure the exchange of confidential information under electronic warfare conditions.

2. Conduct and evaluate the variation capabilities of discrete chaos generators in forming a multitude of pseudo-random sequences with specified mutual correlation properties for stream encryption systems and direct spectrum expansion of timer signals.

3. Develop and study methods for enhancing the information concealment and noise resistance of information transmission based on integrated data transformation methods that combine statistical encryption, noise-resistant coding, and error decorrelation.

4. Develop and model synthesized noise-like signals based on timer signal expansion using linear frequency modulation, as well as methods for their transmission and reception.

5. Perform quantitative and qualitative analysis of synthesized sets of timer signal constructions to evaluate the relationship between energy, structural concealment, and code correction capabilities.

The object of the research: processes of transforming positional and non-positional signal constructions to ensure enhanced concealment in information transmission within information and communication systems.

The subject of research: sets of noise-like signals based on methods of integrating timer coding processes, statistical encryption, and noise-like signal synthesis to increase the concealment of signal constructions.

Research methods. To solve the tasks set in the dissertation, methods of systematic and comparative analysis were used to determine the relevance of the work and formulate the scientific problem. Correlation analysis and the theory of probabilistic analysis were applied when analyzing and studying the variation capabilities of discrete chaos generators. When developing the information protection method based on the combined use of statistical encryption, noise-resistant coding, and decorrelation, the theories of statistical modeling, noise-resistant coding, concealment, and cryptography were employed.

The scientific novelty of the obtained results is as follows:

1. The theory of dynamic chaos for information protection and confidential information transmission systems was further developed, allowing an assessment of the variation capabilities of discrete chaos generators for forming a multitude of pseudo-random sequences with specified mutual correlation properties. These sequences are applicable in stream encryption systems, direct spectrum expansion of timer signals, and manipulation systems where chaotic oscillations mask the transmission process of non-positional digital combinations.

2. The methods for enhancing information concealment and noise resistance in information transmission were further developed based on integrated data transformation methods: combining statistical encryption, noise-resistant coding, and error decorrelation. This allowed the integration of information protection processes against unauthorized access and accidental noise in communication channels.

3. The theory of noise-like signal synthesis was further developed to expand the spectrum of non-positional signal-code constructions, enabling modifications to timer combination structures and their error detection and correction capabilities.

4. A method for synthesizing noise-like signals based on spectrum expansion of non-positional timer signals using linear frequency modulation was proposed for the first

time. This method improved the noise resistance, energy, and structural concealment of transmitted signal constructions.

The practical significance of the dissertation results lies in increasing the energy and structural concealment of signal constructions through the application of chaotic oscillations in modulation systems for transmitting non-positional timer signals and in stream encryption systems. Minor parameter changes in the discrete generator enable the creation of quasi-orthogonal number sequences with mutual correlation coefficients ranging between $6{,}9 \times 10^{-4}$ and $8{,}1 \times 10^{-3}$.

The combined use of statistical encryption, noise-resistant coding and error correction made it possible to combine the protection of information from unauthorised access and accidental interference in the communication channel into a single process. At each step of information transformation, information concealment and noise immunity increase. Thus, the use of error correction made it possible to reduce the error rate in code combinations and use the high error rate detection mode $t_{\text{вияв}} = 2 \ldots 3$ in combination with error correction with a multiplicity of $t_{\text{вип}} = 1$.

The results of the research carried out in this work allowed us to establish the following: the possibility of synthesising noise-like non-positional timer signals based on the LFM; the use of correlation reception to isolate the TSC fronts at the signal-to-noise ratio at the input the receiver $h = P_c/P_i = 0{,}25$; ensuring energy concealment, i.e., the possibility of transmission provided that the noise outweighs the useful transmitted signal by a factor of 2-4. The use of timer signals made it possible to increase the structural concealment compared to the bit-digital code.

The results obtained in the dissertation have been implemented in the educational process of the Department of Cybersecurity and Technical Information Protection at the State University of Intellectual Technologies and Telecommunications, as evidenced by the relevant act of implementation. The practical value of the work lies in the applicability of the obtained results for the engineering design of radio and telecommunication systems, confirmed by the act of implementing the main research results at the enterprise LLC "AISYBERO".

Keywords: information security, energy and structural concealment, unauthorized access, electronic warfare, signal interception, random and targeted interference, noise resistance, cryptographic strength, non-positional timer signals, cybersecurity, noise-like signal, spectrum expansion, correlation receiver, statistical encryption, error decorrelation, noise-resistant coding.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у фахових виданнях, що входять до переліку, затвердженого МОН України

1. Volodymyr Korchynskyi, Valerii Hordiichuk, Vitalii Kildishev, Oleksandr Riabukha, Sergii Staikutsa, Khaled Alfaiomi. Method of information protection based on the integration of probabilistic encryption and noise immune coding. – *Radioelectronic and computer systems*, 2023.4.13, P.184-185. http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2023.4.13. (**SCOPUS**)

2. 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.

https://visn-icct.uu.edu.ua/index.php/icct/article/view/86/70

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

https://vottp.khmnu.edu.ua/index.php/vottp/article/view/118

4. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// *Наукові праці ОНАЗ*. – Одеса: ОНАЗ, 2020. – № 2, – P. – 65-69.

https://ojs.onat.edu.ua/index.php/sbornik_onat/issue/view/84.

5. Корчинський В.В. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційними системах веб-сервісів / В.В. Корчинський, В.Й.

Кільдішев, В.В. Онищук, Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». No 2 (02) 2021, – С. 195-201.

https://visn-icct.uu.edu.ua/index.php/icct/article/view/52.

6. Корчинський В.В. Ризики інсайдерських загроз у системах захисту інформації підприємств /В.В. Корчинський, Аль-Файюмі Х., Копитін Ю.В., Копитіна М.В.// *Наукові праці ОНАЗ ім. О. С. Попова* – Одеса: ОНАЗ, 2019, № 2. – С. 112-116.

https://ojs.suitt.edu.ua/index.php/sbornik_onat/article/view/1149

Наукові праці, які засвідчують апробацію матеріалів дисертації

7. Volodymyr Korchynskyi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services / Valentyn Onyshchuk, Vitalii Kildishev, Volodymyr Korchynskyi and Khaled Alfaiomi // Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – Lviv-Slavske, Ukraine February 22-26, 2022 P. 331-334 (**SCOPUS**).

https://ieeexplore.ieee.org/document/9766911

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

https://ieeexplore.ieee.org/document/10755658/

9. 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.
https://archive.interconf.center/index.php/conference-proceeding/article/view/5775

10. 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.

11. Корчинський В.В. Метод захисту інформації на основі ймовірнісного шифрування / В.В. Корчинський, О.М. Рябуха, Х.О. Аль-Файюмі, А.Ю. Василенко // 78-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів, Одесса, ДУІЗ, 21-22 листопада 2023 року. – С.154-156.

12. Корчинський В.В. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції /В.В. Корчинський Кільдішев В.И., Аль-Файюми Халед, Валігурський Ю.П // Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня – 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 31-33.

13. Корчинський В.В. Дослідження ефективності таймерних шумоподібних сигналів на основі лінійної частотної модуляції / Корчинський В.В., Рябуха О. М., Бердніков О.М., Аль-Файюми Халед, Поліщук К.В.// Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня – 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 27-30.

14. Корчинський В.В. Прогнозування та оцінки ризиків інсайдерських загроз / Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В., Валигурський Ю.П. //«Перспективні напрями захисту інформації: Матеріали шостої міжнародної всеукраїнської наук. пр. конф.», тези доповідей. – м. Одеса, 02-06 вересня 2020 р. – Одеса, Бондаренко М.О. ОНАЗ, 2020. – С.64-65.

15. Корчинський В.В. Мінімізація ризиків інсайдерських загроз в системах

захисту /В.В. Корчинський, Аль-Файюми Халед // Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів, ОНАЗ ім. О.С. Попова. Ч.І., Одеса, 12-14 грудня. – 2019. – С. 139.

Монографія

16. 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

ЗСЗ – завадозахищена система зв’язку;

СКК – сигнально-кодова конструкція

РЦК – розрядно-цифровий код;

ТСК – таймерна сигнальна конструкція

ШСЗ – широкосмугова система зв’язку;

ІКС – інфокомунікаційна система

ДП – джерело повідомлень;

ОІ – одержувач інформації;

ЕОМ – електронна обчислювальна машина;

ЗММ – значущий момент модуляції;

ЗМВ – значущий момент відтворення;

ПД – передавання даних;

ППС – пристрій перетворення сигналів;

СПД – система передавання даних;

ППРЧ – псевдовипадкова послідовність 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 теми. Забезпечення захисту інформації в сучасному інформаційному просторі є складною і постійно зростаючою проблемою. Можливості традиційних методів захисту інформації часто виявляються недостатніми, оскільки зловмисники постійно створюють нові та вдосконалюють наявні технології атак. Як правило, для завдання захисту інформації використовуються позиційні сигнали. Практично всі криптографічні методи, види модуляцій, алгоритми розширення спектра орієнтовані на сигнальні конструкції, в яких тривалість імпульсу має однаковий розмір у кодовому слові. Подальший розвиток методів захисту інформації може базуватися на синтезі більш складних сигнально-кодових конструкціях, в яких тривалість імпульсу змінюється за певними правилами та має можливість змінюватися за встановленими заздалегідь алгоритмами.

З цього приводу перспективним є застосування непозиційних сигнальних конструкцій, таких як таймерні та хаотичні сигнали.

Тривалий час теоретичний розвиток таймерного кодування орієнтувався на завдання підвищення завадостійкості та частотної ефективності застосування каналу зв’язку. В цьому напрямку працювали та зробили вагомий вклад різні зарубіжні та вітчизняні вчені, такі як: М. Захарченко, Л. Політанський, А. Семенко, А. Зюко, В. Банкет, Б. Радзімовський, К. Шеннон, А. Камінський, В. Гордійчук та інші.

Подальше дослідження таймерного кодування виявило унікальні їх можливості по захисту інформації від несанкціонованого доступу, що пов’язано з наявністю досить розвинутого механізму синтезу таймерних сигнальних конструкцій за допомогою їх початкових параметрів. Зміна цих параметрів дозволяє формувати різні ансамблі таймерних сигналів, що ускладнює їх структуру побудови та їх ідентифікацію у випадку перехоплення повідомлення при несанкціонованому доступі. Таким чином, таймерні сигнали мають властивість, яка

оцінюється показником структурної прихованості та можуть бути застосовані для захисту інформації на канальному рівні моделі OSI. Подальшим перспективним дослідженням є застосування таймерних сигналів з різними технологіями розширення спектра для завдань захисту інформації на фізичному рівні.

Явище динамічного хаосу має певні особливості та переваги, які є перспективними з точки зору вдосконалення існуючих та створення нових систем захисту інформації. Динамічний хаос характеризується непередбачуваністю, чутливістю до початкових умов і параметрів, а також – складністю його динаміки. Такі властивості роблять його перспективним для підвищення основних показників завадозахищеності систем зв'язку, таких як прихованість та завадостійкість. Динамічний хаос може бути використаний для шифрування, маскування або змішування даних перед їх передачею. Синтез широкосмугових шумоподібних сигнальних конструкцій на основі хаотичних коливань дозволяє маскувати передаваний сигнал на фоні шумів та вирішувати завдання з підвищення енергетичної прихованості. Генерація псевдовипадкових чисел та ключів для криптографічних систем шифрування за допомогою генераторів хаосу збільшує інформаційну прихованість. Важливим для захисту інформації є підвищення структурної прихованості сигнальних конструкцій, що можливо шляхом ускладнення структури сигнальних конструкцій. Досягається це на основі сумісного використання хаотичних коливань і таймерних сигнальних конструкцій.

В роботі запропоновано методи захисту інформації на основі позиційних та непозиційних сигналів, динамічного хаосу, що дозволяє реалізувати процеси передавання даних, їх шифрування, маскування та змішування. Розроблені методи розширення спектра таймерних сигналів на основі лінійної частотної модуляції. Використання динамічного хаосу для вирішення завдань захисту інформації є перспективним напрямком досліджень і розвитку. Це вимагає подальшої наукової роботи в цьому напрямку, розробки нових методів і алгоритмів, а також впровадження стандартів безпеки, що забезпечать ефективне застосування динамічного хаосу в реальних системах захисту інформації.

У зв’язку з цим існує необхідність вирішення актуального наукового завдання з розробки моделей, методів та алгоритмів інтегрованого захисту інформації на основі різних механізмів перетворення даних, що включає процеси розширення спектра непозиційних сигналів, статистичного шифрування з поєднанням додаткових функцій завадостійкого кодування та декореляцією помилок.

Зв'язок роботи з науковими програмами, планами, темами. Обрані напрями дисертаційного дослідження безпосередньо пов’язані із науково-технічними завданнями, сформульованими в Постанові Кабінету Міністрів України № 942 від 7.09.2011 р. із змінами, внесеними постановою КМ № 463 від 9.05.2023 р. «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року» (Розділ: «Інформаційні та комунікаційні технології», підрозділ: «Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека»). Тема роботи пов’язана з такими пріоритетними напрямами наукових досліджень Державного університету інтелектуальних технологій і зв’язку, як: інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони, системи захисту інформації від несанкціонованого доступу.

Метою дисертаційної роботи є розв’язання науково-технічної проблеми підвищення прихованості передавання інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів.

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

– дослідити та дати оцінку сучасним положенням та аспектам, що впливають на можливість підвищення завадостійкості та прихованості сигнальних конструкцій систем зв’язку, що забезпечують обмін конфіденційної інформації в умовах радіоелектронного конфлікту;

– провести та дати оцінку варіаційним можливостям дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів;

– розробити та дослідити методи підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних**,** які основані на сумісному використанні статистичного шифрування, завадостійкого кодування та декореляції помилок;

– розробити та провести моделювання синтезованих шумоподібних сигналів на основі розширення таймерних сигналів за допомогою лінійної частотної модуляції, методи їх передавання та приймання;

– дати кількісний і якісний аналіз синтезованим множинам таймерних сигнальних конструкцій для оцінки співвідношення між рівнями забезпечення показників енергетичної, структурної прихованості та коригувальної здатності коду.

Об’єкт дослідження: процеси перетворення позиційних та непозиційних сигнальних конструкцій для забезпечення підвищення прихованості передавання інформації в інформаційно-комунікаційних системах.

Предмет дослідження: ансамблі шумоподібних сигналів на основі методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів для збільшення прихованості сигнальних конструкцій.

Методи дослідження. Для вирішення поставлених задач, визначення актуальності роботи та наукового завдання в дисертаційній роботі використано методи системного та порівняльного аналізу. При дослідженні варіаційних можливостей дискретних генераторів хаосу був використаний кореляційний аналіз та теорія ймовірності. При розробці методу захисту інформації на основі інтегрування статистичного шифрування, завадостійкого кодування та декореляції помилок було використано: теорія ймовірності, теорія завадостійкого кодування, теорія прихованості та криптографії.

При розробці методу синтезу шумоподібних сигналів на основі розширення таймерних сигналів за допомогою лінійної частотної модуляції було використано: теорія захисту інформації, теорія сигналів та завадостійкого кодування, а також методи статистичного й імітаційного моделювання.

Наукова новизна одержаних результатів полягає в наступному:

1. Отримала подальший розвиток теорія динамічного хаосу для систем захисту та передавання конфіденційної інформації, що дало змогу в результаті досліджень оцінити варіаційні можливості дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів, а також для систем маніпуляцій, в яких для маскування процесу передавання непозиційних цифрових комбінацій використовуються хаотичні коливання.

2. Отримав подальший розвиток методи підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних: сумісного використання статистичного шифрування, завадостійкого кодування та декореляції помилок. Це дало змогу інтегрувати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі.

3. Отримала подальший розвиток теорія синтезу шумоподібних сигналів, яка спрямована на розширення спектра непозиційних сигнально-кодових конструкцій, за допомогою яких можна змінювати структуру таймерних комбінацій та коригувальну здатність по виявленню та виправленню помилок.

4. Вперше запропоновано метод синтезу шумоподібних сигналів на основі розширення спектра непозиційних таймерних сигналів за допомогою лінійної частотної модуляції, що дало змогу підвищити завадостійкість, енергетичну та структурну прихованості передавання сигнальних конструкцій.

Практичне значення одержаних в дисертації результатів полягає в збільшенні енергетичної та структурної прихованості сигнальних конструкцій шляхом застосування хаотичних коливань в системах модуляції для передавання

непозиційних таймерних сигналів та в системах потокового шифрування. Встановлено, що незначні зміни параметрів дискретного генератора дають можливість створювати квазіортогональні послідовності чисел, взаємний коефіцієнт кореляції складає в межах $6{,}9\ 10^{-4}$ - $8{,}1\ 10^{-3}$.

Сумісне використання статистичного шифрування, завадостійкого кодування та декореляції помилок дало змогу поєднати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі зв'язку. При цьому на кожному кроці перетворення інформації відбувається зростання інформаційної прихованості та підвищення завадостійкості. Так застосування декореляції помилок дозволяють зменшити кратність помилок у кодових комбінаціях та використовувати режим виявлення помилок великої кратності $t_{\text{вияв}} = 2 \ldots 3$ в сполученні з виправленням помилок з кратністю $t_{\text{вип}} = 1$.

Результати досліджень, виконаних в роботі, дозволили встановити наступне: можливість синтезу шумоподібних непозиційних таймерних сигналів на основі ЛЧМ; застосування кореляційного прийому для виділення фронтів ТСК при відношенні сигнал-завада на вході приймача $h = P_c / P_i = 0{,}25$; забезпечення енергетичної прихованості, тобто можливість передавання за умови, що шум перевішує корисний передаваний сигнал в 2-4 рази. Застосування таймерних сигналів дало змогу підвищити структурну приховання у порівнянні з розрядно-цифровим кодом.

Отримані в роботі результати впроваджені в навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку, що підтверджується відповідним актом впровадження. Практична цінність роботи в тому, що отримані результати придатні для застосування в діяльності ТОВ «АЙСАЙБЕРО», що підтверджено відповідним актом впровадження основних результатів дослідження.

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 об'єднання літер, що близькі за показниками ймовірності появи в текстах в групи для завдання статистичного шифрування та аналіз результатів дослідження; [2] – аналіз доцільності застосування непозиційних таймерних сигналів для підвищення структурної прихованості сигнальних конструкцій та аналіз результатів дослідження; [3] – розробка алгоритму дослідження для завдання аналізу варіаційних можливостей програмних генераторів хаосу для формування числових послідовностей; [4] – розробка алгоритму методу формування початкових параметрів програмних генераторів хаосу на основі перетворення геш-функції символів пароля користувача криптографічної системи; [5] – проведення експериментальної частини роботи, аналіз та обговорення результатів дослідження; [6] – проведення експериментальної частини роботи, аналіз та обговорення результатів дослідження.

Апробація результатів дисертації. Результати дослідження, представлені у дисертаційній роботі, доповідались на міжнародних та всеукраїнських конференціях: Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (Lviv-Slavske, Ukraine February 22-26, 2022 (**SCOPUS**); 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024 (**SCOPUS**); Scientific Collection «InterConf», (194): with the Proceedings of the 4th International Scientific and Practical Conference «Diversity and Inclusion in Scientific Area» Warsaw, Poland March 26-28, 2024; Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. – К.: НУОУ, 2023; 78-а науково-технічна конференція професорсько-викладацького складу,

науковців, аспірантів та студентів, Одесса, ДУІЗ, 21-22 листопада 2023 року; Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (30 серпня - 3 вересня 2021 р., м. Одеса); «Перспективні напрями захисту інформації: Матеріали шостої міжнародної всеукраїнської науково-практичної конференції» (02-06 вересня 2020 р., м. Одеса); Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів, ОНАЗ ім. О.С. Попова. (12-14 грудня, 2019, м. Одеса).

Публікації. За результатами досліджень по темі дисертаційної роботи опубліковано 16 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 [7-15] в матеріалах наукових конференцій, у тому числі 2 тези доповіді у журналах, які цитуються у наукометричних базах даних Scopus. Одна наукова праця включена до складу монографії [16].

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, двох додатків, списку використаних джерел і містить 150 сторінок основного тексту, 33 рисунків, 16 таблиць, 19 сторінок додатків. Список використаних джерел містить 113 найменувань і займає 14 сторінок. Загальний обсяг роботи складає 166 сторінку.

РОЗДІЛ 1
ОГЛЯД ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПРИХОВАНОСТІ ТА ЗАВАДОСТІЙКОСТІ ПЕРЕДАВАННЯ СИГНАЛЬНИХ КОНСТРУКЦІЙ

У розділі наведено загальну характеристику проблем захисту передаваної інформації в умовах радіоелектронного конфлікту. Розглянута модель завадозахищеної системи зв'язку, яка забезпечує захист інформації від несанкціонованого доступу та випадкових завад. Аналізуються можливості підвищення показників прихованості та завадостійкості на основі обраних критеріїв ефективності. Обґрунтовано напрямок подальших досліджень, сформульовано наукову проблему та задачі дослідження.

На основі наданого аналізу та отриманих результатів обґрунтовано вибір напрямів досліджень, запропоновано критерії й показники ефективності методів захисту інформації, що передається, математично формалізується постановка наукової проблеми.

1.1 Огляд проблем захисту передаваної інформації в умовах радіоелектронної боротьби

До інфокомунікаційних систем, зокрема, радіотехнічних систем, що працюють в умовах радіоелектронної боротьби (РЕБ), пред'являють особливі вимоги по забезпеченню захисту передаваної інформації [1-3]. Відомо, що оцінювати ефективність захисту інформації в таких умовах доцільно за допомогою комплексного показника завадозахищеності [4], який включає до свого складу такі важливі поняття як завадостійкість та прихованість. Цей показник має особливе значення при оцінюванні рівня забезпечення цілісності передаваних сигнально-кодових конструкцій та складності перехоплень повідомлень. Розглянемо поняття завадостійкість та прихованість з точки зору виконання завдань засобами РЕБ [5,

6]. Як правило, завдання РЕБ противника щодо перехоплення повідомлень можуть бути різноманітними, і вони зазвичай зорієнтовані на здійснення таких наступний дій: перехоплення передаваних радіосигналів; дешифрування перехоплених повідомлень; виявлення і локація джерела сигналу; аналіз метаданих.

Існують різні сценарії роботи РЕБ противника [7, 8]. Одним із таких сценаріїв є перехоплення радіосигналу за допомогою спеціальних радіотехнічних засобів, що призначені для прийому і аналізу електромагнітних хвиль, які передаються між різними об'єктами чи системами зв'язку. Після успішного виявлення передаваного сигналу засоби РЕБ противника можуть встановити відповідну цілеспрямовану заваду для його придушення [12,19].

Іншим сценарієм РЕБ [7,8] може бути запис перехопленого радіосигналу на інформаційний носій, його демодуляція та дешифрування з метою прослуховування. Також можливий інший варіант сценарію, коли противник має можливість змінювати частину вмісту повідомлення для подальшого його передавання своїми радіоелектронними засобами. Таким чином, відбувається перехоплення та модифікація перехопленого повідомлення, що використовується противником для певних оперативних завдань.

У випадку, коли перехоплені дані зашифровані, засоби радіотехнічної розвідки противника можуть намагатися дешифрувати їх, використовуючи методи криптоаналізу [9-11]. Це може вимагати великих обчислювальних ресурсів та часу, але успішне розшифрування може надати противнику доступ до важливої інформації. Також слід відзначити, що засоби РЕБ противника можуть використовувати спеціальні засоби радіозведення для виявлення та локації джерела радіосигналу. Це дозволяє їм визначити місцезнаходження важливих об'єктів чи військових підрозділів, які здійснюють радіозв'язок. Для отримання додаткової інформації про розташування сил протилежної сторони збираються та аналізуються метадані (наприклад, час, тривалість, напрямок передачі, тощо) радіосигналів. Застосування стеганографії дозволяє приховувати факт передавання секретних повідомлень всередині деякого інформаційного контейнера.

Перехоплення радіосигналів в умовах РЕБ [13,14] включає в себе застосування різних технічних та тактичних заходів. Основною метою такого перехоплення є отримання інформації про противника, його наміри та дії, а також порушення його комунікацій та управління. До основних складових перехоплення радіосигналів в умовах РЕБ можна віднести наступне [16]: розвідка та аналіз сигналів; засоби та технології перехоплення; протидія противнику; тактичні та стратегічні аспекти.

Розвідка радіочастот базується на виявленні та моніторингу радіочастотних спектрів [17-19], які використовуються супротивником. Аналіз сигналів включає дешифрування та аналіз перехоплених сигналів для визначення їхнього вмісту та джерела.

Засоби та технології перехоплення [19-21] основані на використанні спеціальних радіоприймачів, що здатні приймати широкі діапазони частот і виявляти слабкі сигнали. Також, характерним є використання різних типів антен для покращення прийому сигналів, включаючи направлені та широкодіапазонні антени. Цифрова обробка сигналів базується на застосуванні сучасних методів цифрової обробки сигналів для поліпшення якості перехоплених даних і їх подальшого аналізу [22-25].

Характерним для РЕБ є введення противника в оману шляхом передавання фальшивих сигналів [20, 21]. Тактичні та стратегічні аспекти обов’язково включають оптимальне розташування засобів перехоплення для забезпечення максимального покриття та ефективності. Також необхідним є вжиття заходів для захисту власних радіокомунікацій від перехоплення та глушіння противником [19, 26-29]. Важливість перехоплення радіосигналів в умовах РЕБ є критичним елементом сучасних військових операцій. Це дозволяє отримувати цінну розвідувальну інформацію [30-32], виявляти плани та наміри противника, а також ефективно керувати власними силами та засобами в умовах інтенсивної РЕБ [9-11].

Дешифрування перехоплених повідомлень в умовах РЕБ [5, 6] є складним процесом, що потребує спеціальних знань, технологій та методів. Основною метою дешифрування є отримання зрозумілої та корисної інформації з закодованих,

модульованих та зашифрованих перехоплених повідомлень. Для виконання цього завдання спочатку потрібна попередня обробка сигналів, яка включає видалення шумів та інших завад. Як правило, для цього використовуються цифрові методи обробки сигналів, такі як фільтрація, спектральний аналіз, демодуляція, декодування. Далі потрібно провести ідентифікацію типу шифру, який використовувався для захисту переданого повідомлення. Для цього задіється база даних відомих шифрів та методів їх дешифрування. Криптоаналіз використовується для зламу шифрів, якщо ключ шифру невідомий. Це може включати частотний аналіз, методи грубої сили, атаки за відомим текстом та інші техніки.

Аналіз та інтерпретація дешифрованих повідомлень включає перетворення даних у зрозумілий текстовий формат [5]. Потрібно зазначити, що навіть при успішному дешифруванні не завжди буде отриманий позитивний результат, що пов’язано з можливими додатковими методами перетворення даних та використання невідомих кодових таблиць. Прикладом такого додаткового перетворення може бути стиснення даних за певним алгоритмом, використання таймерних сигнальних конструкцій та інше.

Важливим є також аналіз метаданих, при якому відбувається процес їх вивчення та інтерпретації, які можуть включати інформацію про структуру, зміст, контекст і історію даних. Метою аналізу метаданих є отримання додаткової інформації, яка допоможе зрозуміти, як дані були створені, зібрані, зберігалися, використовувалися і керувалися. Аналіз метаданих включає: визначення джерел даних, їх типів та взаємозв'язків між ними; виявлення та виправлення помилок, визначення неповноти або невідповідностей у даних; підвищення ефективності зберігання, доступу та використання даних; аналіз відповідності стандартам та нормативам; надання корисної інформації для аналізу і прийняття рішень. Метадані можуть нести технічні властивості, що передбачає фіксацію, наприклад, розміру файлу, його формат та дату створення. Також вони можуть бути описовими, що включає, наприклад, ім’я автора, ключові слова та заголовок.

Наданий аналіз дає можливість встановити, які показники прихованості є важливими для забезпечення протидії реальним сценаріям РЕБ [13-15]. Доцільним

розглянути наступні показники прихованості: енергетична, структурна і інформаційна. Також існують і інші показники прихованості: часова, просторова та інші.

1.2 Аналіз демаскуючих характеристик сигнально-кодових конструкцій

В умовах РЕБ [10, 11] особливо важливо визначити характеристики сигналів, які можуть бути використані для їх виявлення та перехоплення. Проведемо аналіз основних характеристик сигналів, які враховуються при розробці та експлуатації систем зв'язку. Частотні характеристики сигналу включають несну частоту і смугу пропускання. Несна частота використовується для переносу інформаційного сигналу в область високочастотного спектра. Вибір несної частоти впливає на здатність сигналу до проникнення через різні перешкоди та на його вразливість до глушіння. Смуга пропускання характеризує діапазон частот, у якому розподіляється енергія сигналу. Збільшення спектрального ресурсу смуги пропускання дозволяє суттєво ускладнити виявлення та глушіння сигналу [4,12,13]. Амплітудні характеристики сигналу включають амплітуду та динамічний діапазон. Амплітуда сигналу характеризується максимальним значенням напруги або струму та може змінюватися в залежності від типу модуляції та умов передачі. Динамічний діапазон характеризується відношенням між максимальними та мінімальними значеннями сигналів, які можуть бути передані або прийняті системою без значної втрати якості [13,14].

Фазові характеристики розглядають фазу сигналу та фазовий шум. Фаза сигналу характеризує його положення у часі відносно деякої початкової точки. Фазові зміни можуть бути використані для модуляції інформації та можуть служити демаскуючою ознакою. Фазовий шум визначає випадкові зміни фази, що можуть впливати на якість сигналу та ускладнювати його виявлення.

Часові характеристики характеризують тривалість імпульсу та їх частоту. Тривалість імпульсу впливають на виявлення сигналів. Коротші імпульси можуть бути важчими для їх виявлення. Частота повторення імпульсів (ЧПІ) характеризує

кількість імпульсів, які передаються за одиницю часу. Зміна ЧПІ може використовуватися для ускладнення виявлення сигналу[13-15].

Модуляційні характеристики включають тип і індекс модуляції [23,24]. Тип модуляції описує спосіб, яким інформація накладається на несну частоту. Найбільш поширені типи модуляції включають амплітудну (АМ), частотну (ЧМ) та фазову (ФМ) модуляції. Індекс модуляції характеризує відношення величини зміни параметру носія (амплітуди, частоти або фази) до амплітуди інформаційного сигналу [23-25]. Високий індекс модуляції може ускладнювати виявлення та аналіз сигналу [14].

Розуміння та контроль над характеристиками сигналів є критичними для ефективної роботи систем зв'язку в умовах РЕБ [14,15]. Це включає як захист власних сигналів від виявлення та глушіння, так і можливість ефективного виявлення та аналізу сигналів протиборчої сторони.

На рис. 1.1 надана структурна схема моделі каналу передачі при впливі мультиплікативної та адитивної завад, яка може бути описана наступним чином. Джерело сигналу генерує вихідний сигнал $S(t)$. Мультиплікативна завада $M(t)$ впливає на передаваний сигнал $S(t)$:

$$S_m(t) = S(t) \times M(t), \tag{1.1}$$

де $S_m(t)$ – сигнал після впливу мультиплікативної завади.

При дії адитивної завади $N(t)$ сигнал змінюється наступним чином:

$$S_a(t) = S(t) + N(t), \tag{1.2}$$

де $S_a(t)$ – сигнал після впливу адитивної завади.

Загальний вплив адитивної $N(t)$ та мультиплікативної завади $M(t)$ на передаваний сигнал $S(t)$ в системі зв’язку має наступний вид:

$$S_{tot}(t) = S(t) \times M(t) + N(t). \tag{1.3}$$

На рис. 1.1 надана структурна схема моделі каналу передавання даних при впливі мультиплікативної $\mu(t)$ та адитивної $\xi(t)$ завад. Цей канал додатково вносить спотворення або затримку передаваного сигналу. Завданням приймача (ПРМ) є прийняти сигнал $S_{tot}(t)$ і максимально можливо відновити форму сигналу $S(t)$ з урахуванням впливу завад.

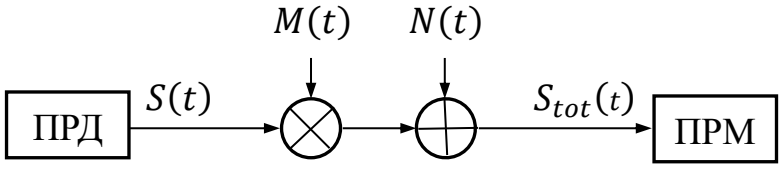


Рис. 1.1. Модель каналу зв'язку при впливі мультиплікативної та адитивної завад

В умовах РЕБ станція радіоелектронної розвідки (РЕР) виявляє та аналізує сигнал $S_{tot}(t)$, який вже знаходиться під впливом адитивної $N(t)$ та мультиплікативної завади $M(t)$. Як бачимо з рис. 1.2 основною проблемою для передавання конфіденційного повідомлення в умовах РЕБ є наявність каналу виявлення та перехоплення сигналу. При цьому, можливі різні сценарії станції РЕР [9-11]. Використовується канал придушення, тобто станція постановки завад генерує навмисні адитивні та мультиплікативні завади $M_{reb}(t)$ та $N_{reb}(t)$, які додаються до сигналу:

$$S_{tot\ reb}(t) = S_{tot}(t) \times M_{reb}(t) + N_{reb}(t). \quad (1.4)$$

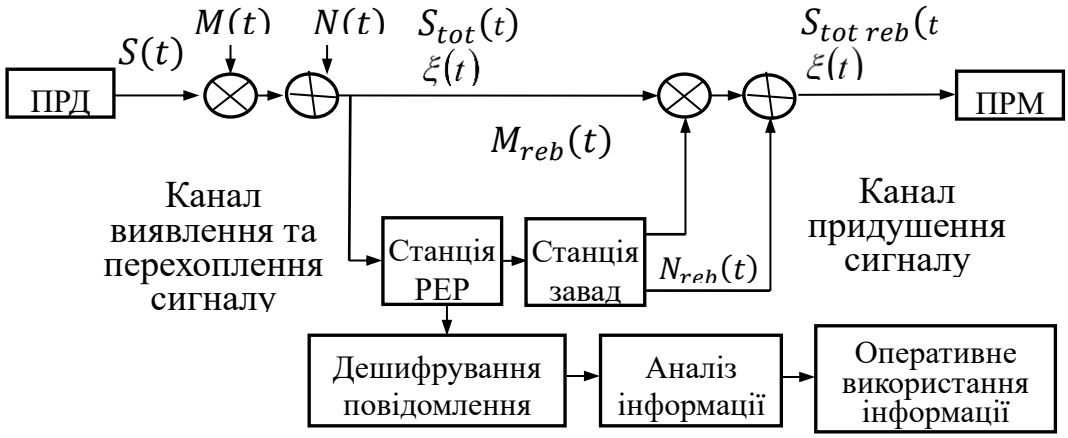


Рис. 1.2. Модель каналу зв'язку в умовах РЕБ

Також можливий варіант розпізнавання перехоплених сигналів та дешифрування повідомлення для подальшого його оперативного використання. Успішна робота РЕР основана на виявленні демаскуючих характеристик радіосигналів [13,14], що передаються по каналу зв'язку. Як правило, для систем модуляції використовується гармонійний сигнал в якості несної частоти. Зміна одного або декількох параметрів несної частоти відповідно до низькочастотного інформаційного сигналу дозволяє реалізувати певний вид модуляції. Процес розпізнавання сигналу засобами РЕР зводиться до ідентифікації типу модуляції. Найпростішим є розпізнавання таких видів модуляції, в яких відбувається зміна невеликої кількості параметрів несної частоти. Так передаваний сигнал, в якому використовується амплітудна модуляція (АМ), частотна модуляція (ЧМ) і фазова модуляція (ФМ) не має ніяких механізмів захисту і може розпізнаватися засобами РЕР. Кожен вид модуляції має свої демаскуючі ознаки, які можуть бути використані для виявлення та аналізу сигналів в умовах РЕБ. До таких ознак сигналу потрібно віднести [14,15]: спектральні характеристики; фазові зміни; амплітудні коливання; частотні відхилення. Спектральні характеристики характеризують сигнал з певним видом модуляції і унікальним розподілом енергії у частотному спектрі. Спектральний аналіз дозволяє визначити такі характеристики сигналу [16,17].

З урахуванням зазначених демаскуючих характеристик сигнальних конструкцій доцільно розглянути методи протидії засобам РЕР. Для зменшення ризику виявлення та аналізу доцільно використовувати розсіювання енергії сигналу у досить великому діапазоні частот та шифрування інформаційного повідомлення [4].

1.3 Забезпечення завадозахищеності передавання інформації на основі позиційних кодів

Властивості сигнально-кодових конструкцій доцільно оцінювати за допомогою комплексного показника завадозахищеності [4, 76, 94], який

характеризує спроможність системи зв'язку забезпечувати завадостійкість та прихованість передавання інформації в умовах РЕБ.

Завадостійкість спрямована на забезпечення відповідних вимог до ймовірнісно-часових характеристик передавання інформації та характеризується різними показниками [78-80]:

$$P(\geq 1, n) = f\left(P_{\text{ВП}}, P_{\text{НП}}, P_{\text{СТ}}, q_{\text{п}}, q_{\text{л}}\right), \tag{1.5}$$

де $P(\geq 1, n)$ – ймовірність спотворення кодового блоку, що складається з n біт; $P_{\text{ВП}}$, $P_{\text{НП}}$ – ймовірності появи виявлених і невиявлених помилок у прямому каналі; $P_{\text{СТ}}(n)$ – імовірність стирання кодового блоку n; $q_{\text{п}}$, $q_{\text{л}}$ – ймовірності придушення та утворення помилкового сигналу запиту у зворотному каналі.

Мінімізація часу передавання інформації в умовах РЕБ важлива для зменшення ймовірністі втручання противника та позитивного впливу на процес захисту повідомлень від НСД. З цього приводу обґрунтованим є обмеження затримки пакетів на основі критерію підвищення відносної ефективної швидкості передавання інформації R за умови збереження допустимої ймовірності невиявлених помилок $P_{\text{НП}}(n)$, тобто [79, 87, 88]:

$$R > R_{\text{пр}}, \; P_{\text{НП}}(n) \leq P_{\text{НП}}^{\text{доп}}(n), \tag{1.6}$$

де $R_{\text{пр}}$ – коефіцієнт відносної ефективної швидкості системи зв'язку; $P_{\text{НП}}^{\text{доп}}(n)$ – допустима ймовірність невиявлених помилок в кодовому блоку n.

Для забезпечення завадостійкості передавання даних використовуються завадостійкі коди [79, 80]. При цьому режим використання цих кодів залежить від типу системи зв'язку. В системах, в яких відсутній зворотній зв'язок використовується, як правило, коригувальний код в режимі виправлення помилок. В системах із зворотнім зв'язком використовується режим виявлення помилок з перезапитом пакету на повторну передачу [79, 87]. Також, можлива комбінація

режиму виправлення та виявлення помилок. Слід відзначити, що використання коригувального коду вимагає додаткових часових або частотних ресурсів для передачі перевірочних біт *r*. В цьому випадку довжина інформаційної кодової комбінації *k* збільшиться і загальна довжина блоку становить:

$$n=k+r. \tag{1.7}$$

Як бачимо з (1.7) використання завадостійкого коду збільшує час передавання сеансу зв'язку, що збільшує ймовірність виявлення $P_{\text{ен}}$ такого сигналу в радіоканалі. Величина надлишковості залежить від якості каналу зв'язку, по якому відбувається передавання інформації. Статистичні дослідження реальних каналів довели, що найбільша нестабільність характерна для радіоканалів [88, 92]. Це пояснюється тим, що цей канал відкритий і для нього існує велика кількість джерел ненавмисних завад. Важливим параметром завадостійкого коду є кодова швидкість [79]:

$$\gamma_{\text{к}} = \frac{k}{n}. \tag{1.8}$$

Кодова швидкість визначає долю корисної передаваної інформації. При цьому Шеннон довів [104,], що для будь-якого каналу з пропускною здатністю C існують коди, які можуть забезпечити надійне передавання інформації з ймовірністю помилки, яка прагне до нуля, якщо кодова швидкість $\gamma_к$ не перевищує пропускну здатність каналу C:

$$\gamma_к \leq C. \tag{1.9}$$

Якщо використовувати довші коди (тобто збільшувати загальну довжину коду *n*), можна досягти надзвичайно малої ймовірності помилки, і кодова швидкість $\gamma_к$ може наближатися до одиниці за умови, що рівень шуму в каналі дозволяє

передавати інформацію на швидкості близькій до пропускної здатності каналу. Важливим параметром, який впливає на кодову швидкість є мінімальна кодова відстань d_0, яка визначає мінімальну кількість біт, що відрізняються між будь-якими двома дозволеними кодовими комбінаціями. Цей показник визначає коригувальну здатність кодів. Здатність коду по виявленню помилок дорівнює [79]:

$$t_{\text{вияв}} = d_0 - 1. \tag{1.10}$$

Виправляча здатність коду дорівнює:

$$t_{\text{випр}} = \frac{d_0 - 1(2)}{2}. \tag{1.11}$$

Оцінити можливість існування коду з певними параметрами можливо за допомогою критерію Варшамова-Гільберта, який дозволяє визначити верхню межу числа надлишкових символів у кодовому слові[79]:

$$2^k \geq \frac{2^n}{\sum_{i=0}^{d_0-1}\left(\frac{n}{i}\right)}, \tag{1.12}$$

де $\left(\frac{n}{i}\right)$ – біноміальний коефіцієнт, що визначає кількість комбінацій вибору i елементів з n. Цей критерій використовується для побудови блокових кодів, що мають задану мінімальну кодову відстань d_0. Якщо нерівність (1.12) виконується, то існує код з параметрами n, k і d_0, який буде мати необхідну здатність до виправлення помилок.

Циклічні коди [79, 80], як і інші коди з корекцією помилок, мають властивість, що зі збільшенням довжини коду n, можна досягти вищої надійності передачі (табл. 1.1). Однак кількість перевірочних символів зростає повільніше порівняно з кількістю інформаційних символів, тому кодова швидкість $\gamma_к$ збільшується і може прагнути до 1 при дуже великих n. З цього можна зробити висновок, що «короткі» коди мають більше перевірочних символів відносно кількості інформаційних, тому

їх кодова швидкість нижча. «Довгі» коди дозволяють зменшити частку перевірочних символів, оскільки з більшою кількістю символів можна коригувати більше помилок, не жертвуючи значною кількістю інформаційних символів.

З табл. 1.1 бачимо, що при фіксованому значенні $d_0 = 3$ та збільшенні довжини кодового блоку кодова швидкість $\gamma_к$ наближається до 1, тобто зберігається коригувальна здатність коду. Проте, з практичної точки зору збільшення довжини кодової комбінації можливе лише до певної межі, яка визначається рівнем шуму та пропускною здатністю каналу. При великих значеннях *n* збільшуються ймовірності спотворення кодового блоку $P(n)$, а також підвищується кратність помилок $t_{\text{пом}}$. Це означає, що використовувати такі кодові блоки доцільно лише для «хороших» станів каналу, тобто з ймовірністю бітової помилки $p_0 \to 0$.

Таблиця 1.1

Основні показники завадостійкого коду при $d_0 = 3$

№	*n*	*k*	*r*	$\gamma_к$	d_0
1	7	4	3	0.571	3
2	15	11	4	0.733	3
3	31	26	5	0.839	3
4	63	57	6	0.905	3
5	127	120	7	0.945	3
6	255	247	8	0.969	3
7	511	502	9	0.982	3
8	1023	1013	10	0.990	3
9	2047	2036	11	0.995	3

В табл. 1.2 наведено приклад збільшення довжини кодових блоків *n* =127 … 4095, при яких забезпечується кратність виправлення помилок $t_{\text{пом}} = 7 \ldots 31$. При цьому, для всіх цих завадостійких кодів забезпечується $\gamma_{\text{к}} \approx 0{,}5$.

Таким чином, існує певне протиріччя між завданням мінімізації часу передавання інформації та забезпеченням умови $\gamma_к \to 1$, що потрібно враховувати при побудові систем зв’язку, які працюють в умовах РЕБ.

Із загальної точки зору, прихованість характеризує ступінь ускладнення перехоплення сигналу, розпізнавання його структури та вмісту повідомлення. Цей

показник доцільно визначати ймовірністю розвідки наявності сигналу в каналі засобами РЕБ [4]:

$$P_{\text{розв}} = P_{\text{ен}} P_{\text{стр}} P_{\text{інф}} \tag{1.13}$$

де $P_{\text{ен}}$ – ймовірність визначення процесу передавання сигналу; $P_{\text{стр}}$ – ймовірність розкриття структури перехопленого сигналу; $P_{\text{інф}}$ – ймовірність розкриття вмісту перехопленого повідомлення за умови, що структура сигналу визначена.

Таблиця 1.2

Основні показники завадостійкого коду при різних значеннях d_0

№	n	k	r	$\gamma_к$	d_0
1	7	4	3	0.571	3
2	15	7	8	0.467	5
3	31	16	15	0.516	7
4	63	36	27	0.571	11
5	127	64	63	0.504	15
6	255	139	116	0.545	21
7	511	265	246	0.518	31
8	1023	520	503	0.508	41
9	2047	1032	1015	0.504	51
10	4095	2056	2039	0.502	63

Енергетична прихованість спрямована на ускладнення виявлення передаваного сигналу засобами радіоелектронної розвідки. Досягається це за рахунок різних методів розширення спектра сигналу. Енергетична прихованість в цьому випадку залежить від бази широкосмугового сигналу:

$$B >> 1. \tag{1.14}$$

Як правило, база сигналу B співпадає з кількістю елементів $N_{\text{пвп}}$ розширення початкового інформаційного сигналу тобто:

$$B = N_{\text{пвп}}. \tag{1.15}$$

Наприклад, для методу передавання даних на основі псевдовипадкового перескоку робочої частоти (ППРЧ) значення $N_{\text{пвп}}$ співпадає з кількістю використовуваних несних частот. При методі ППРЧ несна частота змінюється за певним законом у достатньо великому діапазоні. Як правило, такий сигнал складно перехопити з причини непередбачливості зміни за часом значення несної частоти, яка відома тільки приймачу системи зв'язку з ППРЧ. Принцип розширення спектра методом ППРЧ надано на рис. 1.3.

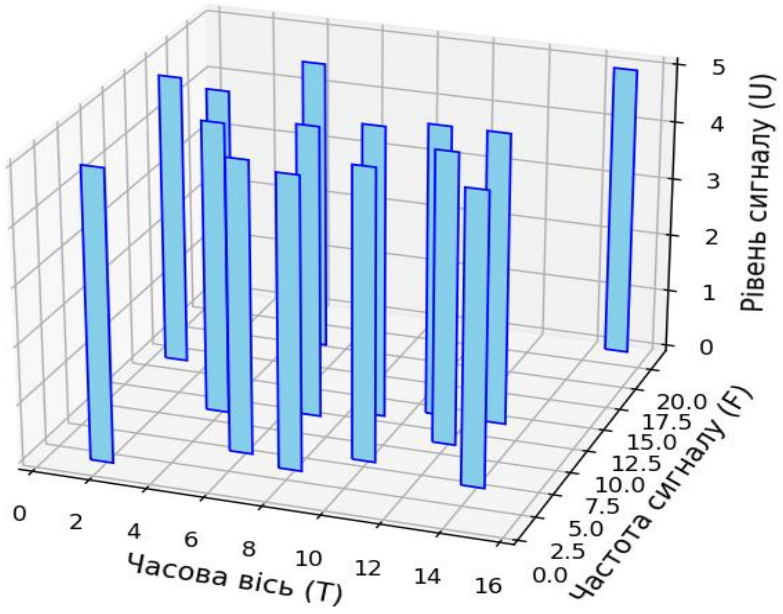


Рис. 1.3. Принцип розширення спектра методом ППРЧ

Також можливий метод підвищення енергетичної прихованості за рахунок прямого розширення спектра сигналу псевдовипадковими послідовностями (ПВП) $N_{\text{пвп}}$ (рис. 1.4).

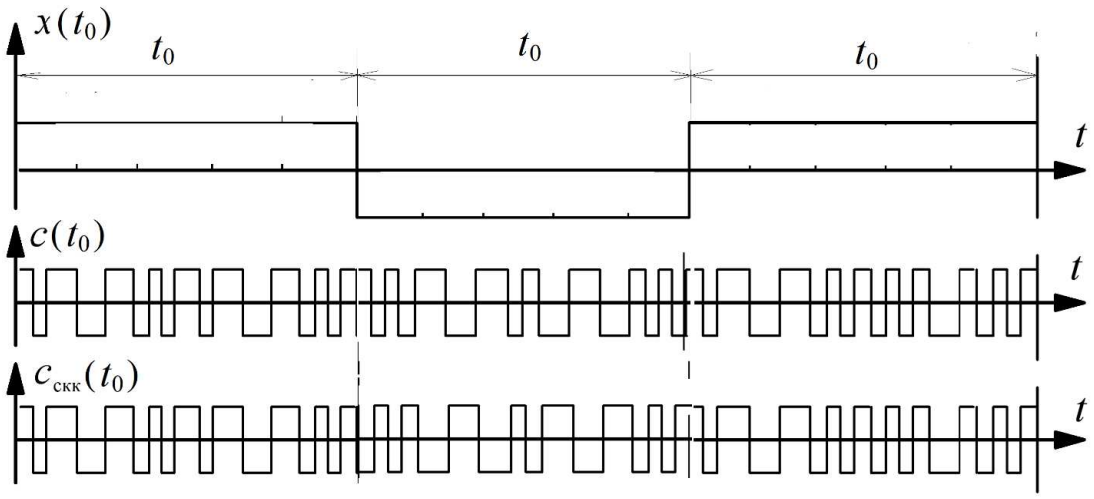


Рис. 1.4. Принцип прямого розширення спектра ПВП

При цьому методі бітовий елемент t_0 замінюється на певні структури ПВП $c(t_0)$:

$$x_{\text{скк}}(T_c) = c_i(t_0) \times x(t_0). \tag{1.16}$$

Це дозволяє розподілити енергію біта у великому діапазоні частот. В сучасних технологіях ПРС значення $N_{\text{пвп}} \geq 128$, що суттєво може ускладнити виявлення такого широкосмугового сигналу засобами РТР.

Наступним методом підвищення енергетичної прихованості є метод розширення спектра за допомогою лінійно-частотної модуляції (ЛЧМ – LFM). При ЛЧМ [102,103] частота сигналу змінюється лінійно (рис. 1.5) протягом заданого часового інтервалу t_0:

$$f(t_0) = f_c + k \cdot x(t_0), \tag{1.17}$$

де f_c – початкова несна частота; k – коефіцієнт модуляції; $x(t_0)$ – значення зміни напруги сигналу в залежності від t_0. Модуляцію позиційного сигналу на інтервалі t_0 можна представити за допомогою виразу:

$$s_{\text{ЛЧМ}}(t) = U_0 \cos(\varphi_0 + \varphi(t)) = U_0 \cos\left(\varphi_0 + 2\pi\left(f_0 t + \frac{b}{2}t^2\right)\right), \tag{1.18}$$

де U_0 – амплітуда сигналу; φ_0 – початкова фаза; b – коефіцієнт, який визначає швидкість зміни частоти, $t = t_0$ – тривалість сигналу.

Енергетична прихованість методу ЛЧМ досягається шляхом збільшення або зменшення частоти рівномірно в залежності від логічного значення бітового елемента, що призводить до утворення ефекту "частотного сканування". Це дозволяє розподілити енергію сигналу по ширшому частотному діапазону, що знижує його потужність на кожній окремій частоті. Як результат, це значно ускладнює перехоплення сигналу засобами РЕР і зменшує ймовірність визначення місця передавання. Розподіл сигналу в широкому спектрі частот ускладнює створення ефективних радіозавад. Щоб протидіяти такому сигналу, засоби РЕР змушені генерувати широкосмугові завади, що вимагає великих ресурсів і енерговитрат.

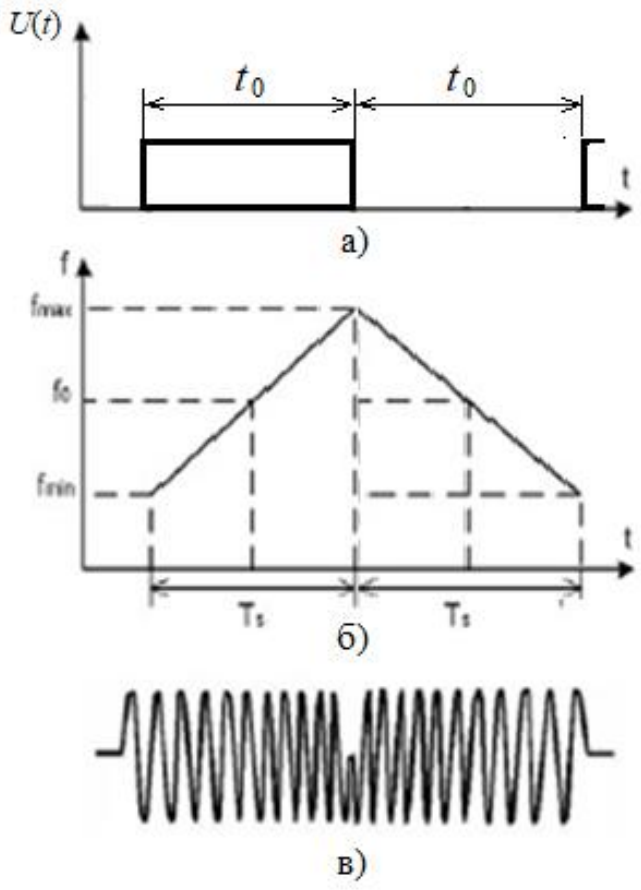


Рис. 1.5. Принцип прямого розширення спектра за допомогою ЛЧМ

Структурна прихованість методу ЛЧМ [102, 103] полягає в підвищеній складності аналізу та ідентифікації параметрів складного сигналу. Використання

адаптивної ЛЧМ дозволяє динамічно змінювати параметри сигналу в реальному часі. Це додатково ускладнює спроби аналізу сигналу засобами РЕР, роблячи комунікацію більш стійкою до перехоплення та заглушення.

Енергетична прихованість на основі методу розширення спектра хаотичними коливаннями [39-41] в умовах РЕБ може бути досягнена завдяки унікальним характеристикам таких сигналів, що пояснюється їх значною непередбачуваністю та випадковістю. Такі властивості хаотичних сигналів є особливо перспективними для розробки на їх основі методів модуляції цифрових послідовностей. Можна спрогнозувати, що методи передавання на основі хаотичних коливань можуть бути достатньо ефективними для захисту сигнальних конструкцій від перехоплення, аналізу та дій радіозавад. Хаотичні коливання створюються за допомогою апаратних або програмних генераторів хаосу. Апаратні датчики [43, 44] реалізуються за допомогою схемотехнічних рішень. Програмні генератори хаосу [53-55] використовують певні алгоритми для створення числового ряду. Наприклад, логістичний генератор хаосу реалізується на основі математичного виразу [71, 74, 75]:

$$x_{n+1} = ax_n(1 - x_n), \tag{1.19}$$

де a – параметр управління. Характерним для цього виразу є те, що незначні зміни параметрів початкових значень генератора призводять до формування нової послідовності числових значень в інтервалі від 0 до 1. Це дозволяє створювати достатньо велику кількість варіантів хаотичного процесу $x(t)$. Для генератора (1.6) на рис. 1.6 (а) наведено приклад центрованої восьмирівневої дискретної реалізації сигналу $x_{\text{д}}(t)$ при начальному значенні $x_{n=0}$= 0,5 і a = 3,9. На рис. 1.6 (б) надано хаотичні коливання $x_{\text{хк}}(t)$, що сформовані на основі дискретного сигналу $x_{\text{д}}(t)$.

Для синтезу шумоподібного сигналу на основі хаотичних коливань необхідно замінити цифрову послідовність $a(t)$ на хаотичні коливання $x_{\text{хк}}(t)$ з урахування знаку біту «1» і «−1», тобто

$$x_{\text{шхс}}(t) = a(t) \times x_{\text{хк}}(t). \qquad (1.20)$$

Хаотичні сигнали мають ширший спектр [68-70] і здатні краще пристосовуватися до змінних умов навколишнього середовища, що підвищує їх стійкість до впливу різного роду радіоелектронних атак. Завдяки своїй динамічній природі, хаотичні сигнали забезпечують не лише енергетичну, але й структурну прихованість, ускладнюючи процеси виявлення і демодуляції, що робить їх важливим інструментом для захисту інформації в умовах інтенсивного радіоелектронного протистояння.

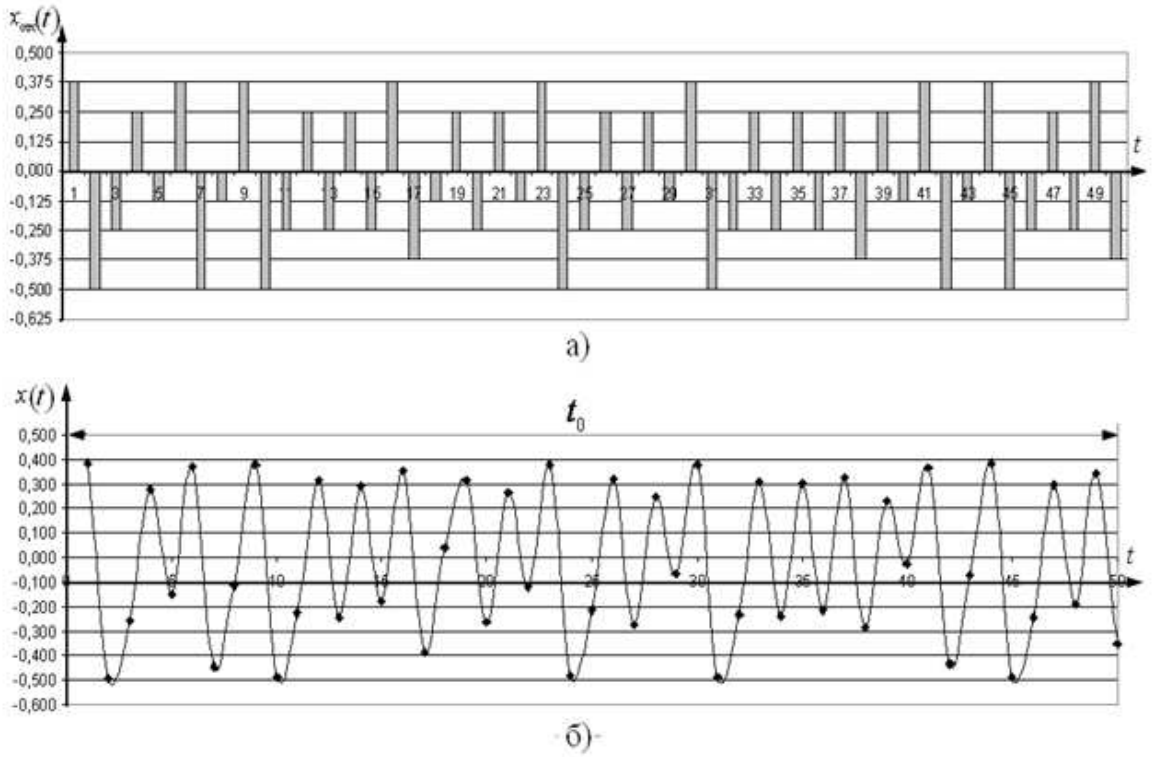


Рис. 1.6. Центрована реалізація дискретної послідовності відліків $x_{\text{д}}(t)$ (а) і хаотичних коливань $x_{\text{д}}(t)$

Структурна прихованість хаотичних сигналів [74] досягається завдяки їхній складній та нестабільній структурі коливань, що значно ускладнює ідентифікацію параметрів сигналу засобами РЕР. За допомогою хаотичних сигналів [33-35] можливо більш ефективно використовувати радіочастотний спектр, оскільки їх спектральна щільність зазвичай є вищою в порівнянні з традиційними методами

модуляції. Це дозволяє не лише збільшити енергетичну прихованість, але й оптимізувати використання частотного ресурсу [4].

Характерним є те, що хаотичні коливання забезпечують підвищену стійкість [36-38] до різного роду зовнішніх перешкод та загроз, характерних для радіоелектронної боротьби. Висока варіативність таких сигналів унеможливлює їх просте перехоплення або блокування, що робить їх ідеальними для надійної та безпечної передачі даних в умовах інтенсивного електромагнітного впливу. Завдяки цьому хаотичні сигнали не тільки підвищують стійкість комунікаційних систем, але й сприяють адаптивності у динамічно змінних умовах бойових дій.

1.4 Забезпечення енергетичної прихованості сигнальних конструкцій

На стадії розробки методів забезпечення енергетичної прихованості розглядаються такі алгоритми синтезу сигнальних конструкцій, на основі яких є можливість приховувати реальний факт передавання енергії сигналу в каналі. Енергетична прихованость [4, 99] роботи системи зв'язку характеризує спроможність суттєвого ускладнення роботи засобів РЕР по виявленню факту передавання сигналу в ефірі за рахунок їх демаскуючих показників. Тобто, для того, щоб забезпечити енергетичну прихованість передавання, потрібно використовувати такі сигнальні конструкції, які складніше виявляються засобами РЕР. Оцінка енергетичної прихованості полягає у визначенні ймовірності правильного виявлення факту передавання сигналу $P_{\text{вияв}}$ засобами РЕБ. При цьому, важливо враховувати вплив співвідношення сигнал-завада у каналі та способів виявлення сигналу. Енергетичну прихованість доцільно характеризувати здібністю системи зв'язку забезпечити задану ймовірність прийому бітового елемента p_0 повідомлення при мінімальному співвідношенні сигнал-шум. Це можливо при застосуванні широкосмугових сигналів з базою [94, 99, 103]:

$$B = \Delta f T >> 1. \qquad (1.21)$$

де Δf – смуга частот сигналу; T – тривалість цифрового елементу. Такі сигнали характеризуються низькою спектральною щільністю потужності, що ускладнює їх виявлення некогерентною обробкою в приймачі засобами РЕР. Як правило, при розширенні спектра сигналу спостерігається погіршення показника частотної ефективності використання каналу по смузі частот

$$\gamma = R/\Delta f_{\text{еф}}, \tag{1.22}$$

де R – швидкість передавання інформації; $\Delta f_{\text{еф}}$ – ефективна ширина спектра сигналу (смуга пропускання каналу). Проте покращується ефективність використання каналу по потужності

$$\beta = R/h_0^2, \tag{1.23}$$

де $h_0^2 = P_s/N_0$ – відношення середньої потужності сигналу P_s на вході приймача до енергетичного спектра АБГШ N_0. Протиріччя між показниками ефективності використання каналу γ і β дозволяє вирішувати завдання підвищення енергетичної прихованості. Наведемо доказ такого ствердження.

Доведення. Хай $\Delta f_{\text{еф}} \to \infty$, $P_s \to 0$. З урахуванням того факту, що швидкість передачі $R = I/T_s$, де I – кількість передаваної інформації за інтервал часу T_s. Враховуємо, що $E_s/I = E_b$, тоді для коефіцієнта β (1.23) визначимо наступні вирази:

$$\beta = RN_0/P_s = N_0/(P_sT_s/I) = N_0/E_b = 1/\beta_E, \tag{1.24}$$

де β_E – коефіцієнт, який є зворотним для β. Можна зробити наступний висновок, що чим менша кількість енергії E_b витрачується на передавання одного біта інформації при заданих рівнях шуму N_0, тим вища енергетична ефективність β, що і потрібно було довести.

Методи забезпечення енергетичної прихованості сигналу на основі частотного ресурсу надано на рис. 1.7.

Існують різні методи реалізації енергетичної прихованості за рахунок розширення спектра передаваного сигналу $\Delta f_{\text{еф}}$ [4, 99, 105]:

1) псевдовипадковий перескок робочої частоти (ППРЧ – FHSS – Frequency Hopping Spread Spectrum);

2) пряме розширення спектра псевдовипадковими послідовностями (ПВП – DSSS – Direct Sequence Spread Spectrum);

3) лінійна частотна модуляція (ЛЧМ – LFM – Linear Frequency Modulation);

4) комбіноване розширення спектра на основі ППРЧ та ПВП;

5) модуляція на основі хаотичних коливань.

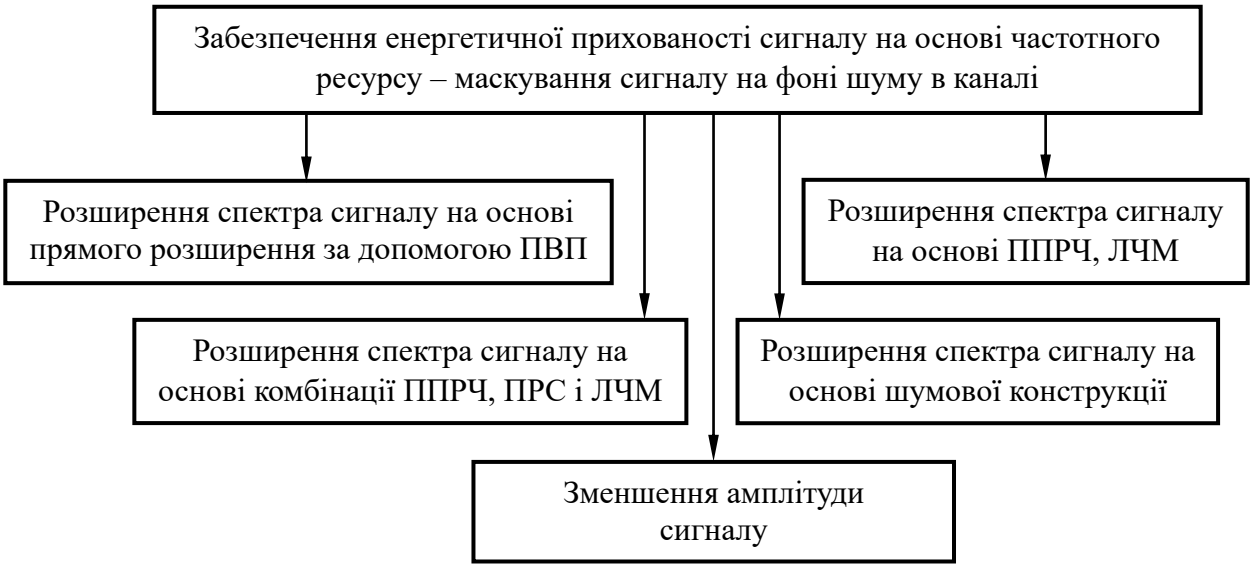


Рис. 1.7. Методи забезпечення енергетичної прихованості сигналу на основі частотного ресурсу

Метод розширення спектра на основі ППРЧ застосовується в різних стандартах передавання даних, таких як: WiFi (IEEE 802.11), Bluetooth та інше. Слід відзначити, що практично всі країни, які входять до складу НАТО використовують у військових операціях радіостанції з ППРЧ, що пояснюється можливістю забезпечення прихованості передавання конфіденційних даних шляхом розширення спектра за допомогою застосування великої кількості несних частот,

які змінюються за певним законом. Прийняти такий сигнал може тільки радіоприймач, якому цей закон зміни несною частоти відомий.

Фактично, можна стверджувати, що вже на першому фізичному рівні моделі OSI на основі методу ППРЧ [4, 102, 105] реалізовано криптографічний доступ, який полягає у складності розпізнавання закону слідкування несних частот з причини великої кількості можливих комбінацій:

$$N_{\text{нч}} = C_{N_{\text{загнч}}}^{K_{\text{нч}}} = \frac{N_{\text{загнч}}!}{K_{\text{нч}}!(N_{\text{загнч}} - K_{\text{нч}})!}, \quad (1.25)$$

де $N_{\text{загнч}}$ – загальна кількість несних частот; $K_{\text{нч}}$ – кількість несних частот, яке використовується із загальної кількості $N_{\text{загнч}}$.

З формули (1.25) можна зробити висновок, що при достатній кількості $N_{\text{загнч}}$ і $K_{\text{нч}}$ можна забезпечити достатню високу структурну прихованість або криптостійкість даного методу передавання.

Метод ППРЧ можна представити, як метод частотної модуляції з багатьма несних частот К (ЧМ-$К_{нс}$). Існують різні варіанти переносу цифрової інформації за допомогою ППРЧ. Це може бути варіант методу ППРЧ, коли одна несна частота переносить один біт інформації. В цьому випадку згідно (1.23) не буде зменшення кількості енергії E_b, яке витрачається на передавання одного біта інформації при заданому рівні шуму N_0. Тобто, такий процес передавання можна побачити за допомогою сучасних сканерів та аналізаторів радіочастотного спектра. З цього можна зробити висновок, що метод ППРЧ є достатньо ефективним з точки зору забезпечення криптографічної стійкості сигнальних конструкцій вже на першому рівні моделі OSI, що пояснюється складністю перехоплення такого сигналу в умовах великої кількості сторонніх сигналів в бойових умовах.

Таким чином, метод ППРЧ може забезпечувати енергетичну прихованість тільки за допомогою розширення спектра передаваного сигналу з використанням великої кількості несних частот, які змінюються в процесі передавання за певним

законом. Збільшення смуги частот $\Delta f_{\text{еф}}$ передаваного сигналу призводить до погіршення частотної ефективності γ цього методу, що особливо не впливає на його переваги по забезпеченню прихованості зв'язку. Енергетична ефективність β при цьому залишається незмінною, тобто як і при ЧМ-К.

Перевагою методу ППРЧ є те, що розширення спектра $\Delta f_{\text{еф}}$ дає можливість в процесі передавання даних вирішити проблему електромагнітної сумісності і працювати з іншими пристроями радіозв'язку. На рис. 1.8 надано приклад передавання сигналу ППРЧ на фоні роботи інших систем радіозв'язку, що зроблено за допомогою аналізатора спектра TinySA Ultra (SDR приймач) в польових умовах. Спектр сигналу ППРЧ розподіляється в досить великому діапазоні частот (верхня частина рис. 1.8).

При цьому можна побачити спектри вузькосмугових радіопередавачів – це амплітудні викиди несних частот, які суттєво не впливають на процес передавання методом ППРЧ. У нижній частині рис. 1.8 відображено модуляційний ефект від передавання несних частот методу ППРЧ, які фіксуються на екрані SDR приймача у вигляді коротких горизонтальних ліній на фоні чотирьох несних частот вузькосмугових радіопередавачів. Це доводить той факт, що при заданому рівні шуму N_0 рівень енергії E_b, який витрачається на один біт, є достатнім для виявлення факту передавання сигналів методом ППРЧ. Підвищення енергетичної прихованості методу ППРЧ може бути за рахунок зменшення тривалості часу випромінювання несної частоти $T_{\text{б}}$.

Реалізувати це можливо при застосуванні кількох несних частот $K_{\text{нч б}}$ для передавання одного біту на інтервалі часу T, тобто час випромінювання становить:

$$T_{\text{б}} = T / K_{\text{нч б}} . \qquad (1.26)$$

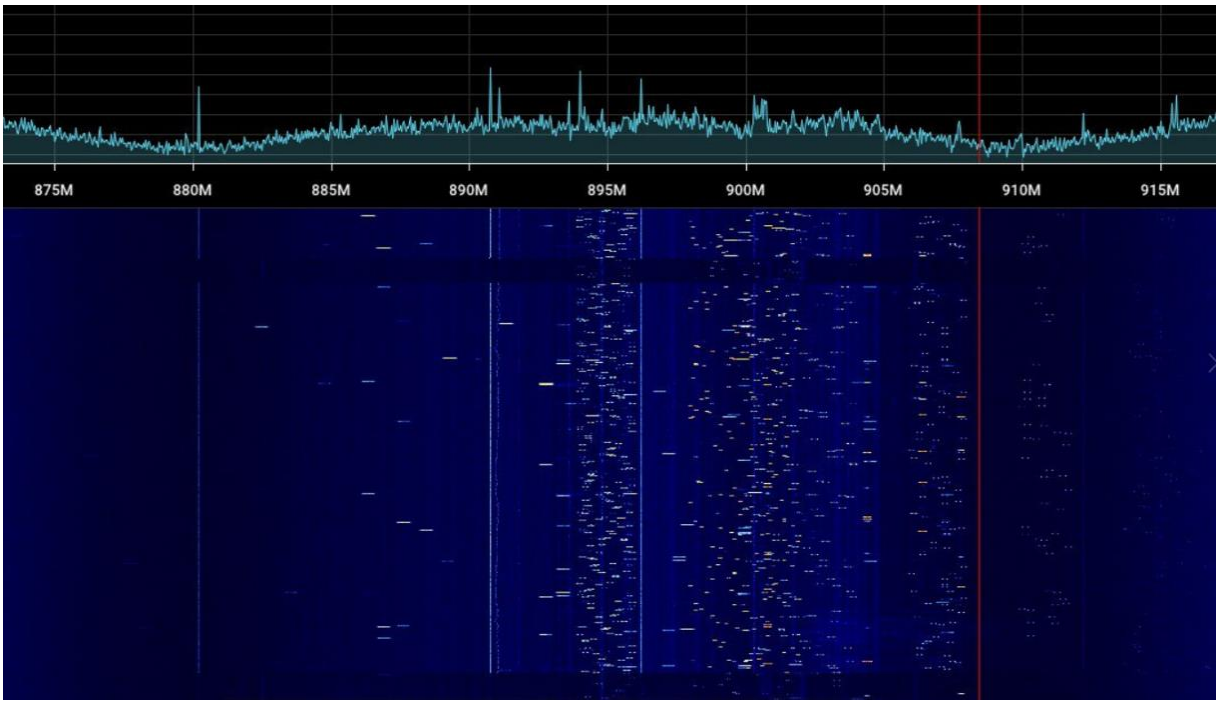


Рис. 1.8. Приклад сканування вузькосмугових
та широкосмугових сигналів

Вочевидь, що перерозподіл енергії для передавання одного біту можливо за рахунок збільшення значення $K_{\text{нч б}}$, що є перспективою підвищення енергетичної прихованості при ускладненні реалізації цього методу.

1.5 Аналіз можливостей підвищення структурної прихованості сигнальних конструкцій

Необхідність забезпечення сигнальних конструкцій, які призначені для передавання конфіденційної інформації, відповідним рівнем структурної прихованості [4, 100, 101] пояснюється як певний внесок в загальну складову механізмів захисту інформації для систем зв’язку, що працюють в умовах радіоелектронного конфлікту. На стадії розробки методів забезпечення структурної прихованості розглядаються такі алгоритми синтезу сигнальних конструкцій, на основі яких є можливість приховувати факт наявної їх структури. На рис. 1.9 надано варіанти забезпечення структурної прихованості. З розвитком глобальної мережі Інтернет метод забезпечення структурної прихованості на основі стеганографії

набуває поширений інтерес, що пояснюється великою кількістю наукових публікацій і досліджень в цьому напрямку.

Стеганографія базується на вбудовуванні даних конфіденційної інформації за певним алгоритмом в певні формати файлів, такі як зображення, аудіофайли чи текстові документи. Цей метод приховування інформації орієнтується на те, що невеликий об’єм даних, вкрапляється в інший об’єкт, який значно більшого розміру. Бачимо, що цей метод захисту інформації має достатньо велику надлишковість, проте, це не вважається його основним недоліком, тому що основним критерієм його ефективності є забезпечення високої прихованості передавання конфіденційних даних. Отже, цей метод має достатньо високу властивість по маскуванню, ефективність якого залежить від розміру даних, що вбудуються в інший інформаційний об’єкт.

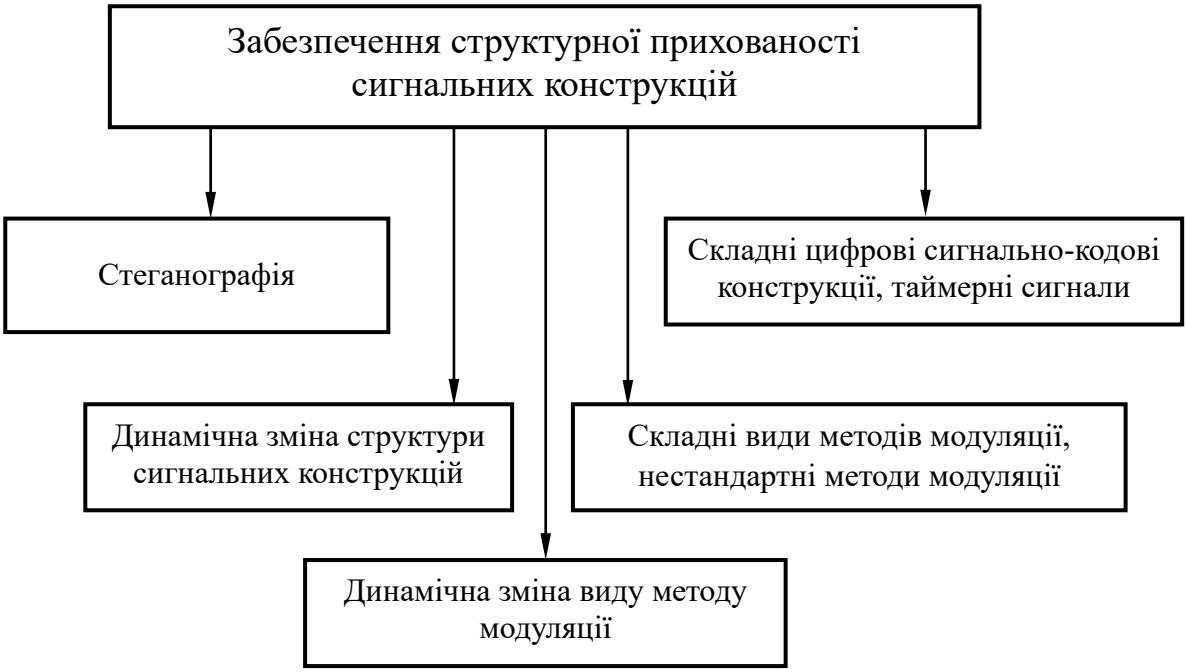


Рис. 1.9. Методи забезпечення структурної прихованості сигнальних конструкцій

Перспективним для підвищення структурної прихованості є використання складних цифрових сигнально-кодових конструкцій:

1) складні види методів модуляції;

2) нестандартні методи модуляції;

3) динамічна зміна виду методу модуляції;

4) динамічна зміна структури сигнальних конструкцій (непозиційні таймерні сигнали);

5) використання складних сигнально-кодових конструкцій (непозиційні таймерні сигнали).

Структурна прихованість [4, 100, 101] спрямована на ускладнення розпізнавання структури сигнально-кодових конструкцій (СКК) засобами РЕБ. Як правило, структурна прихованість залежить від кількості СКК $A_{\text{СКК}}$, які може використати система зв'язку при організації процесу передавання інформації. З ймовірнісної точки зору потенційна структурна прихованість визначається:

$$p_{\text{стр}} = \frac{1}{A_{\text{СКК}}}. \tag{1.27}$$

Також структурну прихованість можна оцінювати :

$$S_{\text{стр}} = log_2 A_{\text{СКК}}.. \tag{1.28}$$

Потенційну структурну прихованість можна оцінювати на різних моделях OSI. На першому фізичному рівні моделі OSI структурна прихованість залежить від багатопозиційності системи маніпуляції, а на другому канальному рівні – від структури коду.

У сучасних цифрових інфокомунікаційних системах (ІКС) все ширше використовуються ефективні методи модуляції [52, 53, 60-63] та завадостійкого кодування [79, 80]. Перехід до ансамблів багатопозиційних сигналів у ІКС збільшує інформаційну швидкість і забезпечує передачу великих обсягів інформації. Сучасна елементна база дозволяє застосовувати в ІКС досить складні методи завадостійкого кодування, забезпечуючи високу достовірність передавання інформації. В багатьох

наукових роботах [60-63] наведено дослідження різних методів модуляції та кодування в ІКС, що відображає як досягнення теорії, так і практичні застосування. Проте, на жаль, зараз обмаль наукових досліджень, в яких відображається структурна прихованість в залежності від побудови сигнально-кодових конструкцій та вибору системи модуляції, що вкрай важливо для захисту інформації, яка передається.

Можна зазначити кілька етапів розвитку сигнально-кодових конструкцій у напрямку поєднання методів маніпуляції, завадостійкого кодування та завдань підвищення структурної прихованості для захисту передаваної інформації від випадкових завад та НСД.

Як відомо, теорія сигналів та теорія кодування [79, 80] протягом тривалого часу розвивалися незалежно одна від одної. Далі для підвищення завадостійкості та швидкості передавання інформації виникла необхідність в розвитку перспективного напрямку на перетині цих теорій. В роботах вітчизняних та зарубіжних авторів [23, 24, 60] надано дослідження, щодо можливостей ІКС, у яких для передавання інформації використовуються ансамблі багатопозиційних сигналів у поєднанні з завадостійкими кодами, причому процедури маніпуляції/кодування (деманіпуляції/декодування) здійснюються спільно. Раціональні методи побудови таких сигнально-кодових конструкцій поєднують у собі позитивні якості як багатопозиційних ансамблів, так і завадостійких кодів, достатньо прості в реалізації на практиці алгоритми декодування та при їх використанні в ІКС дозволяють суттєво наблизитися до теоретичних меж ефективності. Питання синтезу таких систем маніпуляції/кодування, аналізу їх структури, завадостійкості та ефективності, деманіпуляції/декодування складають основний зміст перспективного напрямку в теорії зв'язку. Іншим етапом розвитку цього напрямку є питання захисту інформації, що передається, та охоплює перші два рівні моделі OSI. Для цього необхідно оцінити структурну прихованість існуючих систем модуляції та перспективність їх для захисту інформації від НСД.

Принцип побудови багатопозиційних ансамблів систем модуляції засновано на зміні одного або кількох параметрів сигналу несійного коливання: амплітуди,

фази і частоти. Тобто можливі різні комбінації, наприклад: амплітуди і фази; частоти і фази; амплітуди, фази і частоти; амплітуди і частоти та інше. Процедура оптимізації багатопозиційних ансамблів сигналів полягає в тому [23, 24, 60], що коли розглядається деякий фіксований обсяг дискретних сигналів M в сигнальному просторі, їх вектори повинні бути розташовані на максимально можливій взаємномій відстані. Як правило, такі задачі оптимізації розташувань сигнальних конструкцій в системах модуляції вирішуються в багатовимірній геометрії на основі теорії просторових точкових решіток. За умови, що координати векторів сигналів ансамблю збігаються з центрами просторової точкової решітки можна забезпечити максимальну кількість сигнальних точок M та максимальну питому швидкість:

$$\gamma_N = \frac{\log M}{N} \ , \tag{1.29}$$

N – визначає мірність простору сигналів.

Слід відзначити, що мінімальна відстань у такому ансамблі, яка визначає завадостійкість, буде визначена радіусами сфер, центри яких утворюють решітку. Можливі різновиди ансамблів багатопозиційних сигналів на основі КАМ (QAM – Quadrature Amplitude Modulation). У цих системах амплітуда і фаза носія змінюються для кодування бітів даних, і кожна сигнальна конструкція може представляти певну кількість бітів. Наприклад, КАМ-4 має 4 різних сигнальних конструкцій, кожна з яких представлена комбінацією з 2 біт. Сузір'я такого виду модуляції може бути зображено на діаграмі І-К (ін-квадрат) як 4 точки, розташовані на різних відстанях та кутах. КАМ-128 має 128 різних сигнальних конструкцій, кожна з яких переносе 7 біт.

Приклади використання процедури оптимізації для деяких видів модуляції наведені на рис 1.10.

З точки зору теорії прихованості розглянемо можливості існуючих методів модуляції для забезпечення структурної прихованості. Для системи маніпуляції

ФМ-2 структурна прихованість $S_{\text{стрФМ-2}} = log_2 2 = 1$, а для системи маніпуляції КАМ-512 бачимо збільшення цього показника $S_{\text{стрКАМ-512}} = log_2 5\,12 = 9$. З точки зору криптографії значення показників структурної прихованості, що подано в табл. 1.3 невеликі.

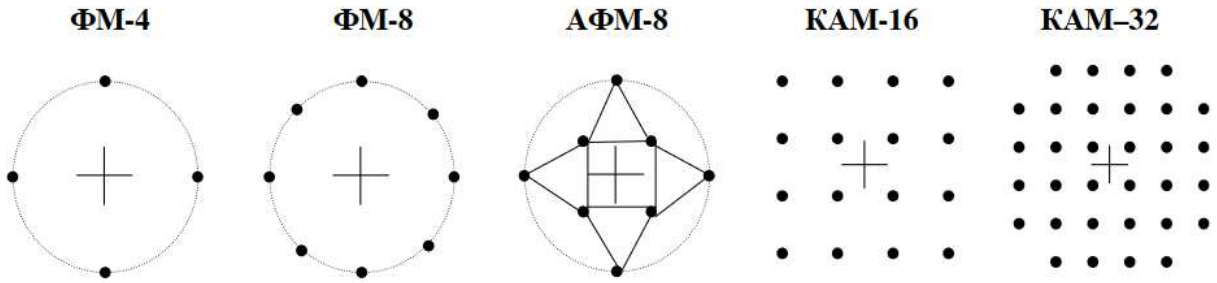


Рис. 1.10. Багатопозиційні ансамблі двовимірних сигналів

Наприклад, для системи маніпуляції КАМ-128 криптостійкість дорівнює усього $K_{r\text{КАМ}-128} = 128$, що у порівнянні з криптографічними протоколами шифрування DES та AES $K_{r\text{DES}} = 2^{56}$ та $K_{r\text{AES}} = 2^{128}$, відповідно, це занадто замало. Також можна стверджувати, що коли мова йде про стандартизовані методи модуляції [23, 60] з питомою швидкістю модуляцій $\lambda_{\text{мод}} \geq 3$. При цьому, засоби РЕР мають відповідні технічні можливості для розпізнавання сигнальних конструкцій з такими видами модуляції. Також в табл. 1.3 наведено можливість забезпечення ймовірності бітової помилки $p_0 = 10^{-5}$ для різних видів модуляцій за рахунок збільшення потужності багатопозиційного сигналу. За умови, що потужність сигналів однакова, збільшення швидкості передавання інформації та структурної прихованості, супроводжується зменшенням ймовірності p_0 .

Як правило, засоби РЕБ проводять радіомоніторинг в умовах параметричної невизначеності, що потребує використання методів "сліпого" оцінювання радіосигналів для ідентифікації типу маніпуляцій на фоні шумів. Велика кількість наукових праць [15-17] присвячена методам ідентифікації типів модуляцій на основі: аналізу спектра; оцінювання параметрів сигналу; штучного інтелекту; статистичного аналізу; теорії розпізнавання образів та інші.

Ці методи можуть застосовуватися окремо або в комбінації для досягнення більш точної та надійної ідентифікації системи модуляції.

Таблиця 1.3

Значення структурної прихованості для різних видів маніпуляцій

№	Вид модуляції та криптографічний протокол	Значення структурної прихованості $S_{\text{стр}}$	Структурна прихованість (криптостійкість)	Відношення сигнал/шум E_0/N_0, дБ ($p_0 = 10^{-5}$)
1	ФМ-2, АМ-2, ЧМ-2	1	2	-
2	ФМ-4	2	4	9,6
3	КАМ-4	2	4	-
4	ФМ-8	3	8	13,5
5	АФМ-8	3	8	12,0
6	КАМ-16	4	16	14,0
7	КАМ-32	5	32	16,1
8	КАМ-64	6	64	18,5
9	КАМ-128	7	128	20,9
10	КАМ-256	8	256	23,5
11	КАМ-512	9	512	-
12	DES	54	2^{54}	-
13	AES	128 (256)	2^{128} (2^{256})	-

Метод аналізу спектра полягає у вивченні спектра сигналу для визначення характерних особливостей, що вказують на тип модуляції. Різні модуляційні схеми мають відмінні спектральні характеристики, такі як положення бічних смуг, особливості амплітудного чи фазового спектра.

Методи оцінювання сигналу використовують математичні алгоритми для аналізу вхідного сигналу і визначення його параметрів, таких як амплітуда, частота чи фаза. Зазвичай це включає кореляційні методи, методи адаптивної фільтрації та інші.

Застосування методів машинного навчання та штучного інтелекту для розпізнавання модуляційних сигналів стає в наш час все більш поширеним. Ці методи можуть використовувати нейронні мережі, класифікатори та інші алгоритми для автоматичного визначення типу модуляції.

Методи статистичного аналізу базуються на аналізі статистичних параметрів сигналу, таких як моменти, кореляції та інші статистичні характеристики, що можуть бути використані для визначення типу модуляції.

Методи ідентифікації системи модуляції, що ґрунтуються на теорії розпізнавання образів [16] з використанням величин статистики вищих порядків, стали широко використовуваними. Ці методи основуються на порівняльному аналізу теоретичних та розрахованих значень кумулянтів вищих порядків і не залежать від величини адитивного гауссівського шуму. Перевага цього методу полягає в тому, що використання кумулянтів дозволяє ефективно розпізнавати різноманітні типи цифрової модуляції.

Слід відзначити, що навіть при наявності на теперішній час різноманітних та удосконалених засобів ідентифікації систем модуляції, вони не уникнули певних недоліків:

1) кількісті розпізнаваних типів модуляції обмежено;

2) малі ймовірності правильного розпізнавання типу модуляції з подібними фазовими сузір'ями;

3) вплив помилок синхронізації на правильність розпізнавання сузір'я в залежності від складності в реалізації;

4) необхідність задіяння великих обчислювальних ресурсів.

Наданий аналіз дозволяє зробити висновок, що для ускладнення процедури ідентифікації виду маніпуляції доцільно використовувати нестандартні системи маніпуляції, в яких відбувається зміна параметрів у часі. Це може бути зміна розташування векторів у сузір’ї системи модуляції. Наприклад, КАМ-16 з певним видом сузір’я чергується в КАМ-16 з іншим сузір’ям. Приклад такої зміни значень фази та амплітуди надано на рис. 1.11.

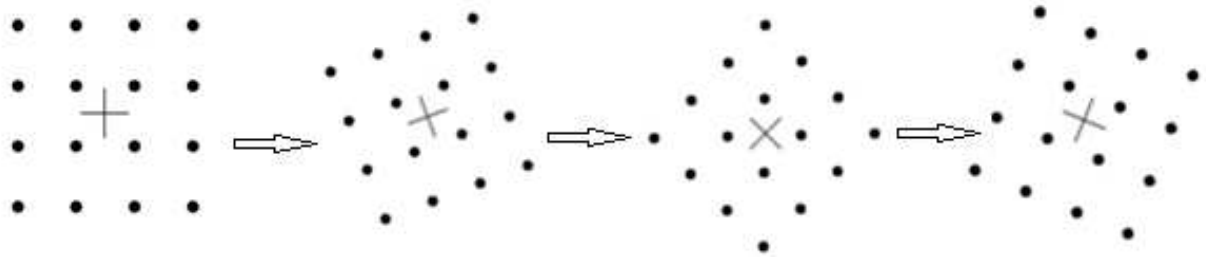


Рис. 1.11. Приклад зміни розташування векторів у сузір’ї системи модуляції КАМ-16

Вочевидь, що це значно ускладнить ідентифікацію системи модуляції та дозволить суттєво підвищити структурну прихованість сигнальних конструкцій.

1.6 Перспектива підвищення прихованості передавання сигнальних конструкцій

Як свідчить проведений аналіз забезпечення захисту інформації в сучасному інформаційному просторі є складною і постійно зростаючою проблемою. Практично всі сучасні методи забезпечення прихованості передавання інформації – шифрування, модуляція, алгоритми розширення спектра – орієнтовані на позиційні сигнали, в яких тривалість імпульсу має однаковий розмір у кодовому слові. Проте можливості традиційних методів захисту інформації часто виявляються недостатніми, оскільки постійно створюються нові та вдосконалюються наявні технології атак, НСД, засоби виявлення та перехоплення сигналу.

Подальший розвиток методів захисту інформації може базуватися на синтезі більш складних сигнально-кодових конструкціях, в яких тривалість імпульсу змінюється за певними правилами та має можливість змінюватися за встановленими заздалегідь алгоритмами. З цього приводу перспективним є застосування непозиційних сигнальних конструкцій, в якості яких пропонуються таймерні та хаотичні сигнали.

Обґрунтовується це тим, що таймерне кодування має унікальні можливості по інтегруванню методів захисту інформації від несанкціонованого доступу та

завадостійкого кодування. Наявність розвинутого механізму синтезу таймерних сигнальних конструкцій за допомогою початкових параметрів дозволяє створювати різні ансамблі сигналів. Це ускладнює структуру їх побудови та ідентифікацію у випадку перехоплення повідомлення при НСД. Таймерні сигнали мають властивість, яка оцінюється показником структурної прихованості та можуть бути застосовані для захисту інформації на канальному рівні моделі OSI. Подальшим перспективним дослідженням є застосування таймерних сигналів з різними технологіями розширення спектра для завдань захисту інформації на фізичному рівні.

Явище динамічного хаосу має певні особливості та переваги, які є перспективними з точки зору вдосконалення існуючих та створення нових систем захисту інформації. Динамічний хаос характеризується непередбачуваністю, чутливістю до початкових умов і параметрів, а також - складністю його динаміки. Такі властивості роблять його перспективним для підвищення основних показників завадозахищеності системи зв’язку, таких як прихованість та завадостійкість. Застосування динамічного хаосу в системах захисту інформації дозволить реалізувати процеси прихованої передачі даних та їх шифрування. Синтез широкосмугових шумоподібних сигнальних конструкцій на основі хаотичних коливань дозволяє маскувати передаваний сигнал на фоні шумів та вирішувати завдання з підвищення енергетичної прихованості. Генерація псевдовипадкових випадкових чисел та ключів для криптографічних систем шифрування за допомогою генераторів хаосу збільшує інформаційну прихованість. Важливим для захисту інформації є підвищення структурної прихованості сигнальних конструкцій, що можливо шляхом ускладнення структури сигнальних конструкцій. Досягається це на основі сумісного використання хаотичних коливань і таймерних сигнальних конструкцій.

Доцільним є подальший розвиток методів підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних, при якому сумісно використовується статистичне шифрування, завадостійке кодування та декореляція помилок. Це дає змогу

інтегрувати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі.

Розвиток теорії синтезу шумоподібних сигналів на основі розширення спектра непозиційних сигнально-кодових конструкцій дозволить змінювати структуру таймерних комбінацій та коригувальну здатність по виявленню та виправленню помилок, що забезпечить підвищення структурної прихованості та завадостійкості передавання сигнально-кодових конструкцій.

Перспективним також є адаптивний метод синтезу шумоподібних сигналів на основі розширення спектра непозиційних таймерних сигналів за допомогою лінійної частотної модуляції. Це дасть змогу підвищити завадостійкість, енергетичну та структурну прихованості передавання сигнальних конструкцій.

Метою дисертаційної роботи є розв’язання науково-технічної проблеми підвищення завадозахищеності передавання інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів для збільшення прихованості сигнальних конструкцій.

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

– дослідити та дати оцінку сучасним положенням та аспектам, що впливають на можливість підвищення завадостійкості та прихованості сигнальних конструкцій систем зв’язку, що забезпечують обмін конфіденційної інформації в умовах радіоелектронного конфлікту;

– провести та дати оцінку варіаційним можливостям дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів;

– розробити та дослідити методи підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних, які основані на сумісному використанні статистичного шифрування, завадостійкого кодування та декореляції помилок;

– розробити та провести моделювання синтезованих шумоподібних сигналів на основі розширення таймерних сигналів за допомогою лінейної частотної модуляції, методи їх передавання та приймання;

– дати кількісний і якісний аналіз синтезованим множинам таймерних сигнальних конструкцій для оцінки співвідношення між рівнями забезпечення показників енергетичної, структурної прихованості та коригувальної здатності коду.

Висновки до розділу 1

1. В результаті аналізу встановлено, що для забезпечення захисту інформації, що передається, використовуються різні методи розширення позиційного сигналу. Розвиток сучасних засобів РЕР дозволяє за допомогою вже малогабаритних SDR сканерів радіочастотного спектра виявляти не тільки вузькосмугові, так і широкосмугові сигналі. Тривалий період вважалося, що метод ППРЧ є достатньо надійним з точки зору забезпечення енергетичної прихованості, за якою сигнал практично не виявляється в радіоефірі. Проте технологічний провив в галузі створення високошвидкісних мікроконтролерів дозволяє створювати достатньо ефективні засоби виявляння таких сигналів. Тривалість часу передавання на одній несній частоті при заданому рівні шуму N_0 рівень енергії E_b, який витрачається на один біт, є достатнім для виявлення факту передавання сигналів методом ППРЧ.

Це вимагає пошуку та розробки більш ефективних методів синтезу широкосмугових сигналів для підвищення їх енергетичної та структурної прихованості.

2. Аналіз показав, що перспективний метод підвищення енергетичної прихованості можливий за рахунок прямого розширення спектра сигналу ПВП, структура яких може змінюватися за певним алгоритмом. Умовою для підвищення енергетичної прихованості є використання шумоподібних сигналів з великою базою, що дозволяє розподілити енергію біта у більшому діапазоні частот. Умовою забезпечення структурної прихованості є використання для розширення спектра

сигналів ПВП з невідомою структурою. Такі умови розширення спектра дозволяють суттєво ускладнити виявлення такого широкосмугового сигналу засобами РЕР.

3. Енергетична прихованість методу ЛЧМ досягається шляхом збільшення або зменшення частоти рівномірно в залежності від логічного значення бітового елемента, що дозволяє розподілити енергію сигналу по ширшому частотному діапазону. Для подальшого підвищення прихованості передавання шумоподібних сигналів доцільно розробити метод розширення спектра непозиційних сигналів за допомогою ЛЧМ.

4. Енергетична прихованість на основі методу розширення спектра хаотичними коливаннями в умовах РЕБ може бути досягнена завдяки унікальним характеристикам таких сигналів, що пояснюється їх значною непередбачуваністю та випадковістю. Такі властивості хаотичних сигналів є особливо перспективними для розробки на їх основі методів модуляції цифрових послідовностей. Таким чином, можна спрогнозувати, що методи передавання на основі хаотичних коливань можуть бути достатньо ефективними для захисту сигнальних конструкцій від перехоплення, аналізу та дій радіозавад.

5. Слід відзначити перспективність розробки методу захисту інформації, який інтегрує різні ступені перетворення даних в єдину задачу. Кожна ступінь перетворення при цьому забезпечує покращення прихованості показників передавання та завадостійкості. Для цієї мети пропонується дослідити сумісне використання статистичного шифрування, завадостійкого кодування та декореляцію помилок.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ВАРІАЦІЙНИХ МОЖЛИВОСТЕЙ ГЕНЕРАТОРІВ ХАОСУ

Досліджуються статистичні характеристики та варіаційні можливості генераторів хаосу по формуванню псевдовипадкових послідовностей для використання їх в різних системах захисту інформації. Доцільність даного дослідження обґрунтовується властивостями динамічного хаосу, для якого характерним є деякий нерегулярний та аперіодичний процес, що призводить до зміни нелінійної динамічної системи.

2.1 Застосування динамічного хаосу для захисту інформації

Ідея використання динамічного хаосу в системах захисту та передачі інформації [36-38] почала розвиватися з другої половини XX століття, після відкриття явища динамічного хаосу в математичних та фізичних системах. Ранні наукові дослідження зосереджувалися на нелінійних динамічних системах, зокрема в роботах Лоренца у 1960-х роках [34, 51], що показали, як невеликі зміни у початкових умовах можуть призводити до великих і непередбачуваних результатів – основної характеристики хаотичних систем.

У восьмидесятих роках минулого століття було досліджено властивості динамічного хаосу [64-67] в таких областях науки, як фізика, біологія та математика. Були виявлені явища чутливості до початкових умов і нелінійності, що лягло в основу теоретичної бази для подальших застосувань хаосу в технологіях передачі і захисту інформації.

Властивості динамічного хаосу стало основою для появи наукових праць щодо застосування хаотичних систем для криптографії та захисту інформації [48-50]. Було запропоновано використовувати динамічний хаос для генерації

випадкових послідовностей, які могли б служити ключами для шифрування [40-43].

Перші практичні спроби реалізації хаотичного шифрування були пов'язані з використанням генераторів Лоренца та інших хаотичних схем [45, 46]. Результати досліджень показали [48-50], що хаотичні сигнали можуть бути використані для маскування інформаційних сигналів, тим самим забезпечуючи високий рівень захисту.

На початку 21-го століття було запропоновано велику кількість методів для застосування хаосу в передачі інформації [54-56]. Одним із найбільш перспективних напрямків стало використання хаотичних осциляторів у радіозв'язку та системах оптичної передачі даних. Також, було запропоновано численні алгоритми, які використовували хаотичні системи для шифрування та приховування інформації [57-59].

Подальше застосування динамічного хаосу пов’язано з сучасними криптографічними системами. Характерним також є те, що хаотичні системи почали використовуватися в технологіях стеганографії, тобто прихованого передавання інформації в електронних повідомленнях або зображеннях. Крім того, хаотичні методи знаходять застосування у фізичній реалізації генераторів випадкових чисел [53-55], що є важливим для криптографічних систем.

Застосування динамічного хаосу залишається важливим напрямком досліджень у галузі захисту інформації. Особлива увага приділяється використанню хаотичних систем у безпроводових комунікаціях [50-51] та квантових криптографічних протоколах. Хаос також знаходить застосування у захисті інформаційних систем від кібератак, адже хаотичні сигнали складно відтворити або зламати.

2.2 Порівняльний аналіз апаратних та програмних генераторів хаосу

У сучасній науці та техніці генератори хаосу широко використовуються через їх здатність створювати непередбачувані й складні сигнали, що робить їх

незамінними в таких сферах, як криптографія, безпека інформаційних систем, системи модуляції та інше [50-52]. Для цих задач можуть бути використані як апаратні, так програмні генератори хаосу, за допомогою яких створюються випадкові або псевдовипадкові сигнали на основі хаотичних процесів [53-54].

Особливість апаратних генераторів хаосу полягає в тому, що вони працюють на основі фізичних процесів, таких як турбулентність рідин, тепловий шум або інші хаотичні явища. Такі генератори відображають природну хаотичність, яку важко передбачити. Це означає, що перевагами апаратних генераторів хаосу є більш високий рівень випадковості через використання фізичних хаотичних процесів. При цьому високий рівень безпеки забезпечується за рахунок того, що важко змоделювати або передбачити поведінку такої системи, що робить їх доцільним для використання в криптографії. Вочевидь, що висока швидкість генерації апаратних генераторів забезпечується за рахунок, наприклад, схемотехнічних рішень певної елементної бази. Це означає, що апаратні генератори можуть працювати швидше за програмних.

Проте до недоліків апаратних генераторів слід віднести складність їх реалізації, тобто вони потребують спеціального обладнання, що збільшує вартість і ускладнює обслуговування. Крім того, для них характерна нестабільність генерації випадкових процесів, що пов’язано із залежністю від зовнішніх фізичних факторів, наприклад, температури, вологості, радіації та інше.

Програмні генератори хаосу [53-55] базуються на алгоритмах, що імітують хаотичні процеси. Такі генератори використовуються у тих системах, де апаратні рішення недоцільні або надто дорогі. Перевагою програмних генераторів хаосу є проста їх інтеграція, яка не потребує додаткового обладнання та може працювати на стандартних процесорах. Такі генератори мають властивість масштабованості, тобто їх можна легко модифікувати для різних потреб, адаптуючи під певні задачі. Висока гнучкість генераторів пояснюється тим, що алгоритми можуть бути налаштовані для досягнення необхідного рівня хаотичності. До недоліків програмних генераторів слід віднести менший рівень випадковості у зв’язку з використанням математичних алгоритмів для отримання результатів, які завжди

будуть псевдовипадковими, що може призвести до певних вразливостей. Іншою проблемою використання програмних генераторів є низька їх швидкість у порівнянні з апаратними генераторами. При цьому ефективність програмних генераторів залежить від продуктивності та архітектури обладнання на якому реалізується процес.

Таким чином, апаратні генератори хаосу краще підходять для задач, що потребують максимальної випадковості та високого рівня безпеки, тоді як програмні генератори є більш доступними та гнучкими для інтеграції в різні системи, але можуть бути менш надійними в критичних застосуваннях.

Апаратно-програмні генератори хаосу поєднують переваги як апаратних, так і програмних генераторів, забезпечуючи високу продуктивність та гнучкість для різних застосувань, зокрема в криптографії, захисті інформації, моделюванні та електронній війні. В основі таких генераторів лежить апаратна частина, що виконує обробку сигналів або генерацію хаотичних процесів на фізичному рівні. Програмна частина забезпечує алгоритмічний контроль, конфігурацію та подальшу обробку даних, зокрема їх адаптацію для специфічних завдань. Програмні алгоритми дозволяють адаптувати хаотичні процеси до різних умов, що робить цей тип генераторів більш універсальним. Апаратна частина забезпечує високу стабільність, оскільки зменшується залежність від обчислювальних ресурсів центрального процесу, а програмна частина дозволяє автоматично коригувати параметри генерації для збереження необхідного рівня хаотичності та непередбачуваності. Таким чином, апаратно-програмні генератори здатні забезпечити оптимальний баланс між високою швидкістю і мінімальними витратами обчислювальних ресурсів, що дозволяє використовувати їх у реальному часі без значного навантаження на систему. В табл. 2.1 надано порівняльний аналіз генераторів хаосу.

Таблиця 2.1

Порівняльний аналіз генераторів хаосу

Тип генератора	Швидкість формування послідовностей	Особливості
Апаратні генератори	1–10 Гбіт/с	Швидкість залежить від фізичних процесів і часто перевищує інші типи, особливо у випадку високочастотних схем.
Програмні генератори	100 Мбіт/с – 1 Гбіт/с	Швидкість обмежена обчислювальною потужністю ЦП та складністю алгоритму, може суттєво варіюватися.
Апаратно-програмні генератори	500 Мбіт/с – 5 Гбіт/с	Швидкість значно вища за програмні аналоги завдяки спеціалізованим апаратним компонентам, при цьому зберігається гнучкість.

Бачимо, що програмні генераторі здатні виробляти псевдовипадкову послідовність зі швидкістю в межах 100 Мбіт/с - 1 Гбіт/с, що пояснюється обмеженою обчислювальною потужністю центрального процесу та ступенем складності алгоритму. Апаратні генератори можуть досягати найвищої швидкості до 10 Гбіт/с завдяки використанню фізичних процесів. Апаратно-програмні генератори здатні працювати зі швидкістю формування послідовностей в межах 500 Мбіт/с до 5 Гбіт/с, що робить їх швидшими за програмні рішення та наближатися за продуктивністю до рівня апаратних.

У сучасній науці і техніці генератори хаосу знаходять широке застосування завдяки своїй здатності генерувати непередбачувані та складні сигнали. Доцільним є дослідження аналізу варіаційних можливостей генераторів хаосу, зокрема їх здатності формувати вибірки з заданими статистичними властивостями.

2.3 Аналіз алгоритмів генерації випадкових та псевдовипадкових чисел

Генератори чисел відіграють важливу роль у системах шифрування [35-36, 58], оскільки від їх якості залежить стійкість криптографічних алгоритмів. У системах шифрування використовуються два основних типи генераторів чисел. Для аналізу алгоритмів роботи генераторів псевдовипадкових послідовностей (ПВП) розглянемо математичні вирази і формули, що описують їх функціонування. Робота генераторів ПВП ґрунтується на детермінованих алгоритмах, які за допомогою початкового значення генерують послідовність чисел, що виглядають випадковими.

Одним з найпростіших способів формування ПВП є лінійний конгруентний генератор (ЛКГ), який описується наступним математичним виразом:

$$X_{n+1} = (aX_n + c) \bmod m \tag{2.1}$$

де X_n – поточне число ПВП; a і c – параметри генератора; m – модуль (константа, зазвичай велике просте число); X_0 – початкове значення.

Генератор Mersenne Twister (MT) забезпечує великий період формування ПВП, але його математичний опис більш складніший [34]. Основою є рекурентна формула, яка використовує бітові операції:

$$X_{n+k} = X_{n+k} \oplus \langle (X_n \& u) | (X_n \& l) \rangle \gg r \tag{2.2}$$

де X_n – поточне число ПВП; u, l – параметри, що використовуються для побітових операцій; >> – операція побітового зміщення вправо; $\oplus$ — операція XOR.

Генератор псевдовипадкових чисел CSPRNG (Cryptographically Secure Pseudorandom Number Generator) [34-37] забезпечує високий рівень безпеки та використовується в криптографічних додатках. CSPRNG гарантує, що його вихід важко передбачити або відтворити без знання початкових умов або секретних

ключів. CSPRNG часто використовують криптографічні алгоритми, наприклад, блочні шифри в режимі лічильника. Математично це можна описати так:

$$X_n = \text{Encrypt}(K, \text{Counter}) \tag{2.3}$$

де K – секретний ключ; Counter – лічильник, який збільшується з кожною ітерацією; Encrypt – блочний шифр (наприклад, AES), що застосовується до лічильника. Криптографічна стійкість цього генератора пояснюється тим, що кожен новий блок залежить від секретного ключа та змінного лічильника.

Генератор істинно випадкових чисел TRNG (True Random Number Generator) [34-35] використовує фізичні явища (наприклад, термічний шум, квантові процеси або інші природні процеси) для генерації дійсно випадкових чисел, на відміну від псевдовипадкових, які генеруються за алгоритмами. TRNG застосовуються в ситуаціях, де потрібна висока непередбачуваність, наприклад, у криптографії для генерації ключів або інших критично важливих даних. У зв'язку з тим, що TRNG використовують фізичні явища, і тому їх не можна повністю описати детермінованими математичними формулами. Однак базовий процес TRNG можна представити як функцію збору ентропії з випадкових фізичних процесів. TRNG можна описати наступною формулою:

$$X_n = f(E_n) \tag{2.4}$$

де E_n – ентропія, зібрана з фізичного процесу (наприклад, термічного шуму); $f(E_n)$ – функція, яка перетворює фізичні дані в цифрові значення. Таким чином, процес отримання ентропії є нелінійним і непередбачуваним, тому TRNG вважаються дійсно випадковими.

Якщо для формування чисел використовується шум у напівпровідниках, випадкові коливання напруги (або струму) можна математично виразити через випадковий процес:

$$V(t) = A \cdot \sin(2\pi f t + \phi) \tag{2.5}$$

де A – амплітуда сигналу; f – частота коливань; ϕ – випадкова фаза. Далі цей шум перетворюється в цифрові дані через аналого-цифровий перетворювач.

HMAC_DRBG [37, 38] є одним з типів CSPRNG (Cryptographically Secure Pseudorandom Number Generator), який використовує HMAC (Hash-based Message Authentication Code) для генерації криптографічно стійкої послідовності випадкових чисел. На основі геш-функцій цей генератор здатний забезпечити високий рівень безпеки. Формула його роботи наступна:

$$X_n = \text{HMAC}(K, V) \tag{2.6}$$

де K – ключ HMAC, який оновлюється після кожного виклику генератора; V - внутрішній стан генератора, який також постійно змінюється; HMAC - криптографічна функція на основі гешування.

HMAC_DRBG базується на HMAC, що використовує криптографічно стійку геш-функцію, таку як SHA-256 або SHA-512, для генерування випадкових чисел. Його основна задача – генерувати послідовності чисел, які виглядають випадковими та є криптографічно захищеними, тобто їх важко передбачити або відтворити. Щоб оцінити трудомісткість алгоритму розглянемо основні кроки генерації чисел в HMAC_DRBG. Ініціалізація полягає в тому, що генератор ініціалізується з використанням початкового значення та випадкових даних. Далі внутрішній стан генератора оновлюється після кожної операції. Це дозволяє підтримувати криптографічну стійкість, навіть якщо частина стану стає відомою атакуючому. Після ініціалізації генератор використовує функцію HMAC для створення випадкових чисел з використанням внутрішнього стану. Використання HMAC забезпечує високу стійкість до атак на генератор випадкових чисел. Високий рівень безпеки забезпечується завдяки оновленню внутрішнього стану генератора після кожного запиту на генерацію нового випадкового числа. Використання геш-функції гарантує мінімізацію ймовірності колізій (двох однакових результатів при різних вхідних значеннях).

Порівняльний аналіз генераторів випадкових та псевдовипадкових чисел надано в табл. 2.2. З таблиці бачимо, що PRNG (наприклад, Mersenne Twister, LCG) демонструють дуже високу швидкість, але вони не підходять для криптографії через низький рівень безпеки. CSPRNG (AES-CTR DRBG, HMAC_DRBG) забезпечують високу криптографічну стійкість, але працюють значно повільніше через додаткові обчислювальні операції (AES, HMAC, гешування). TRNG (Intel RDRAND, QRNG) мають відносно повільну швидкодію через використання фізичних процесів, але забезпечують найвищий рівень випадковості.

Також слід відзначити, що швидкодія генераторів залежить від багатьох факторів, таких як оптимізація програмного забезпечення, апаратні можливості та конкретні алгоритми. Генератори псевдовипадкових чисел мають детерміновані математичні моделі, такі як лінійний конгруентний метод або Mersenne Twister, а також криптографічно стійкі генератори на основі блочних шифрів та геш-функцій. Генератори істинно випадкових чисел (TRNG), що використовують фізичні явища, не мають такої ж математичної визначеності, але базуються на зборі ентропії.

Таблиця 2.2

Порівняльний аналіз генераторів випадкових та псевдовипадкових чисел

Генератор	Тип	Швидкодія (Мб/с)	Безпека	Примітки
Mersenne Twister	Псевдовипадковий	~ 2000 – 4000 Мб/с	Низька	Швидкий, але не підходить для криптографії.
Linear Congruential Generator	Псевдовипадковий	~ 4000 – 6000 Мб/с	Низька	Простий та швидкий, але небезпечний для криптографії.
AES-CTR DRBG	Криптографічно стійкий (	~ 200 – 500 Мб/с	Висока	Використовує AES у режимі лічильника (CTR), оптимальний для криптографії.
HMAC_DRBG (SHA-256)	Криптографічно стійкий (	~ 50 – 150 Мб/с	Висока	Повільніший через використання SHA-256, але надійний і стійкий до атак.
Hash_DRBG (SHA-256)	Криптографічно стійкий (CSPRNG)	~ 50 – 200 Мб/с	Висока	Швидкість залежить від геш-функції, наприклад, SHA-256.

2.4 Дослідження граничних параметрів генераторів хаотичних процесів

Генератори хаосу використовуються для створення послідовностей, які мають властивості, подібні до випадкових, але є детермінованими. Їх застосовують у різних областях, зокрема в криптографії, системах модуляції та моделюванні складних систем. В основі таких генераторів лежать динамічні системи, що демонструють чутливість до початкових умов, тобто малі зміни в початкових параметрах призводять до великих змін у результатах. Ця властивість називається детермінованим хаосом. Генератори хаосу, як і лінійно-конгруентні генератори, можуть бути реалізовані апаратним, програмним та апаратно-програмним способом. Для кожного програмного генератору хаосу характерним є свій вид функції відображення x_i та допустиме значеннями керуючих параметрів [71, 72]:

$$x_{i+1} = f(x_0; x_i; a), \tag{2.7}$$

де $f(\cdot)$− нелінійна функція відображення; a − керуючий параметр; x_0, x_i, x_{i+1} − початкові значення хаотичного процесу.

Для генераторів хаосу характерним є рівномірний закон розподілу числової послідовності в інтервалі]0…1[, яке отримується за відповідним алгоритмом. Можна визначити наступні переваги детермінованого способу генерування числової послідовності:

а) при застосуванні числової вибірки є можливість попередньої її вибору із заздалегідь перевіреними статистичними властивостями. Такий підхід забезпечить необхідну стабільність формування числової послідовності і не потребує її регулярного тестування;

б) можливість відтворення послідовності з потрібного значення числової позиції;

в) незначна кількість операцій, яка потрібна для генерування кожного значення числової послідовності;

г) обчислювальний процес формування числової послідовності не займає великий обсяг пам'яті;

д) період послідовності повинен бути не менше, ніж заданий процес.

Проведемо аналіз найбільш відомих алгоритмів хаотичних генераторів.

Логістичне відображення (Logistic Map) [71, 72, 75, 76] є один з найпростіших і найбільш відомих прикладів динамічної системи, яка може демонструвати як регулярну, так і хаотичну поведінку залежно від параметрів. Логістичне відображення такого генератора визначається наступною рекурентною формулою:

$$x_{i+1} = ax_i(1 - x_i), \tag{2.8}$$

де x_i – поточне значення в межах $0 \leq x_i \leq 1$; a – параметр зростання, який відповідає за характер динаміки хаотичного процесу, зазвичай $0 \leq r \leq 4$, проте $a = 3{,}9$ забезпечує стабільний процес коливань.

В залежності від значення параметра a, логістичне відображення може демонструвати різні режими поведінки:

1) $0 < a < 1$ – популяція швидко вмирає (стабілізується на нулі);

2) $1 < a < 3$ – система стабілізується на одному фіксованому значенні. Наприклад, для значення a = 2.5 система стабілізується на значенні a = 0.6 незалежно від початкового значення x_0;

3) $3 < a < 3.57$ – система починає демонструвати періодичну поведінку, переходячи між кількома значеннями;

4) $3{,}57 < a < 4$ – система стає хаотичною, при цьому будь-яка зміна початкового значення x_0 може призвести до кардинально різних результатів, що є прикладом «ефекту метелика».

При значенні параметра a близько до 4 система стає детермінованою хаотичною. Це означає, що хоча система повністю визначена і відтворювана, її поведінка виглядає випадковою, і важко передбачити результат після багатьох ітерацій без точного знання початкових умов.

На рис. 2.1 наведені діаграми, з яких можна побачити зміну траєкторій хаотичного коливання для різних значень $a = 2{,}6; 2{,}9; 3{,}2, 3{,}5; 3{,}7; 3{,}86; 3{,}9$.

При $a = 2{,}6$ логічне відображення вироджується на самому початку свого існування. Аналогічний результат буде отриманий при $a = 2{,}9$. При значенні $a = 3{,}2$ отримуємо гармонійне коливання. Регулярне коливання з двома різними амплітудами отримуємо при $a = 3{,}5$.

Коливання «дивного» процесу будуть отримані при $a = 3{,}86$, при якому виникає чергування різних станів сигналу: загасання, зростання та стабілізація. Дійсне хаотичне коливання отримуємо при $a = 3{,}9$.

Наведені на рис. 2.1 приклади дозволяють зробити наступні висновки:

- для малих значень a, траєкторія x_i швидко сходиться до фіксованого значення.

- для значень a в діапазоні від 3 до 4 можна спостерігати біфуркації – коли система починає періодично змінюватися між двома і більше значеннями;

- при значеннях a близьких до 4, графік хаотичний, і жодна чітка періодичність не спостерігається.

Таким чином, логістичне відображення добре ілюструє, як прості нелінійні системи можуть мати дуже складну і навіть хаотичну поведінку, що робить його корисним для багатьох галузей науки.

Розглянемо більш складну дискретну динамічну систему генерації числової послідовності на основі Хенона (Hénon Map) [68], яка була вперше запропонована Мішелем Хеноном в 1976 році для моделювання динаміки в двовимірних системах. Система Хенона є прикладом простого нелінійного відображення, яке генерує хаотичні траєкторії і використовується для дослідження теорії хаосу та атракторів. Математичний вираз системи Хенона визначається як система двох рекурентних рівнянь:

$$\begin{cases} x_{n+1} = 1 + a \cdot x_n^2 + y_n \\ y_{n+1} = b \cdot x_n. \end{cases} \tag{2.9}$$

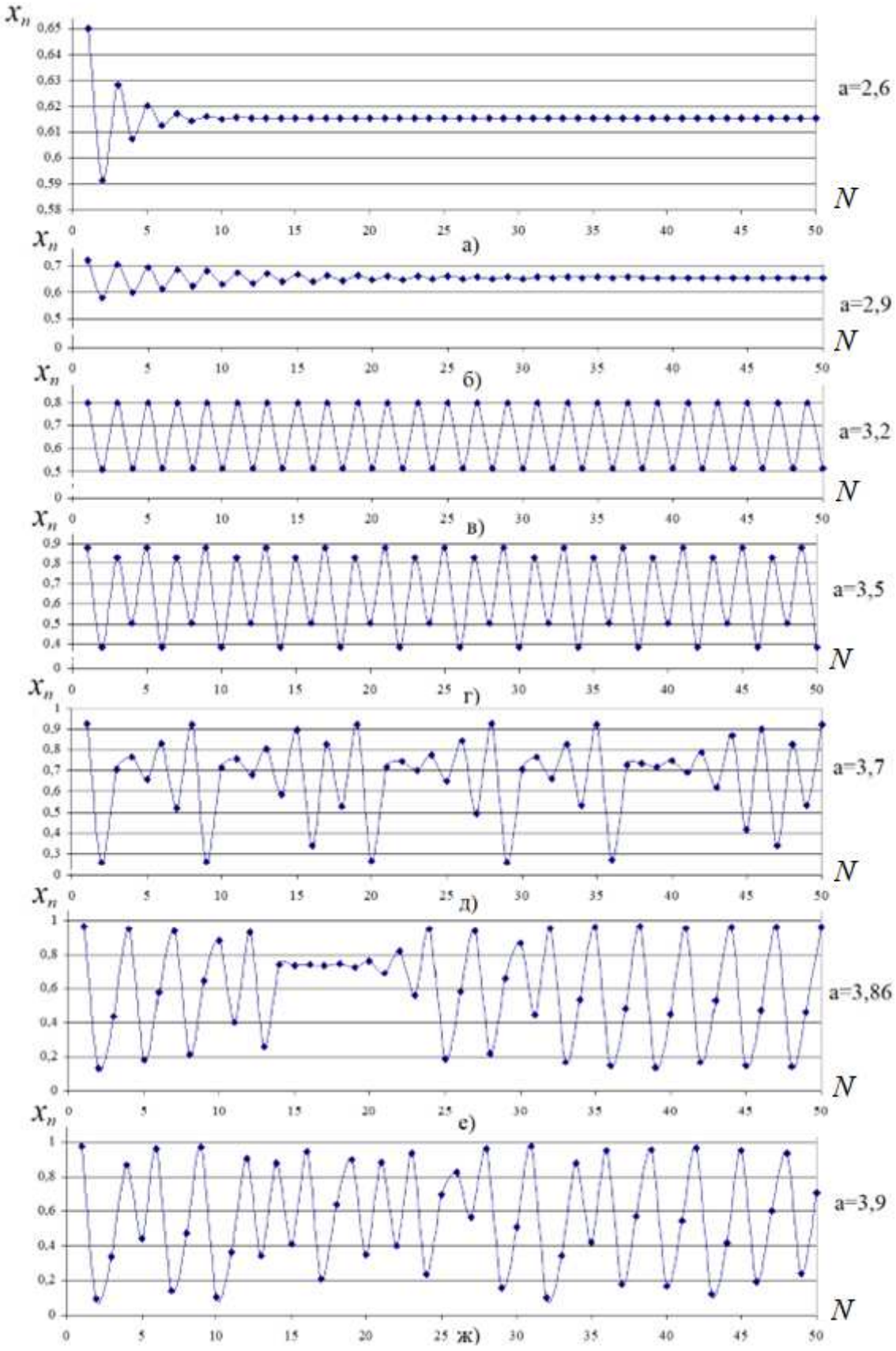


Рис 2.1. Діаграми хаотичного процесу логістичного відображення при різних значеннях параметру a

На рис. 2.2 надано графік, побудований на основі математичних виразів системи Хенона. Він ілюструє траєкторії хаотичної поведінки системи в двовимірному просторі для стандартних значень параметрів a = 1,4 та b = 0,3. Бачимо, що точки на графіку формують характерний фрактальний атрактор Хенона.

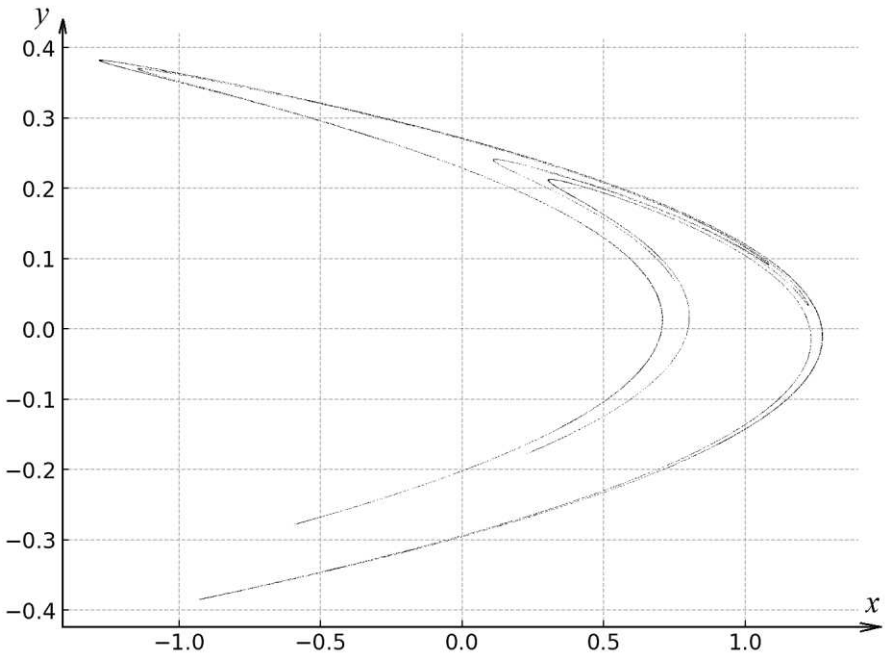


Рис 2.2. Траєкторії хаотичної поведінки системи Хенона для стандартних значень параметрів a = 1,4 та b = 0,3

Система Хенона працює у двовимірному просторі і на кожній ітерації значення x_n і y_n оновлюються відповідно до вищевказаних рівнянь, утворюючи траєкторію точки на площині. Нелінійність системи забезпечується квадратичним членом x_n^2 в першому рівнянні, що робить систему придатною для моделювання хаотичних явищ. Для певних значень параметрів система Хенона демонструє чутливість до початкових умов і хаотичну поведінку – навіть невелика зміна початкових умов призводить до зовсім різних траєкторій.

На рис. 2.2 надано графіки хаотичних процесів для x_n і y_n, що побудовані на основі математичних виразів системи Хенона (2.9).

При стандартних значеннях параметрів система формує відомий хаотичний атрактор. Атрактор Хенона є фракталом, що означає, що він має подібні структури

на різних масштабах, що можна побачити на рис. 2.3. Характерним є те, що невелика зміна початкових значень x_n і y_n може призвести до радикально різних траєкторій, що є типовою ознакою хаотичних систем. При певних значеннях параметрів система Хенона може демонструвати періодичну поведінку, але за стандартних значень a і b її поведінка хаотична. Хаотична поведінка системи Хенона може використовуватися для генерації псевдовипадкових чисел для завдання шифрування даних.

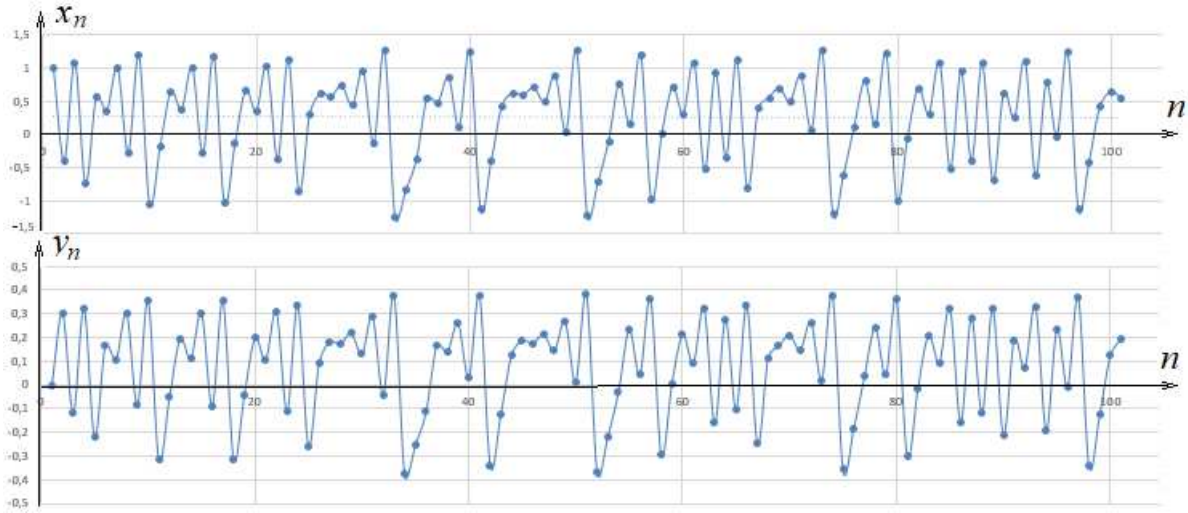


Рис. 2.3. Графіки хаотичних процесів для x_n і y_n системи Хенона

Відображення Тенту (Tent Map) є прикладом динамічної системи, яка демонструє хаотичну поведінку при певних значеннях параметрів. Ця система є однією з класичних моделей у теорії хаосу і використовується для вивчення дискретних динамічних систем. Відображення Тенту описується за допомогою наступного математичного виразу:

$$x_{n+1} = \begin{cases} r \cdot x_n, & \text{якщо } x_n < 0{,}5 \\ r \cdot (1 - x_n), & \text{якщо } x_n \geq 0{,}5 \end{cases} \tag{2.10}$$

де x_n – стан системи на n-й ітерації; r – параметр, що визначає форму "намету" (tent).

Для відображення Тенту на рис. 2.4 надано графіки хаотичних процесів для x_n для різних значень r. Можна відзначити наступну динаміку зміни процесу поведінки відображення Тенту. Так, при малих значеннях параметру $r \leq 1$ система сходиться до стаціонарного значення.

При збільшенні значення r система починає проявляти періодичну поведінку. В межах значень $1 \leq r \leq 1{,}19$ спостерігаються періодичні коливання. При значенні параметру в межах $1{,}2 \leq r \leq 1{,}5$ система може переходити в хаотичний режим. Проте в цих межах є такі значення параметру r, коли також можуть спостерігатися періодичні коливання.

Генератор хаосу на основі статечного відображення є прикладом динамічної системи, яка демонструє хаотичну поведінку. Цей тип генератору також називають поліноміальним відображенням або відображенням ступені і є однією з варіацій хаотичних генераторів, які використовують нелінійні функції для створення хаотичних послідовностей.

Генератор статечного відображення описується наступним математичним виразом:

$$x_{n+1} = r \cdot x_n^d (1 - x_n). \tag{2.11}$$

де x_n – значення системи на n-ій ітерації; r – параметр хаотичності, за допомогою якого відбувається контроль зміни швидкості хаотичного процесу; d – значення ступеня, що визначає нелінійність системи; n – номер ітерації. Відображення має просту структуру, але демонструє хаотичну поведінку при невеликих значеннях параметрів $r \approx 1 \ldots 1{,}1$. При великих значеннях система демонструє стабільну поведінку і може сходитися до стаціонарної точки.

Генератор на основі відображення зі зсувом (Shift Map) є класичним прикладом динамічної хаотичної системи. Цей генератор використовує за принципом зсуву чисел у певному діапазоні між 0 і 1 із застосуванням модуля.

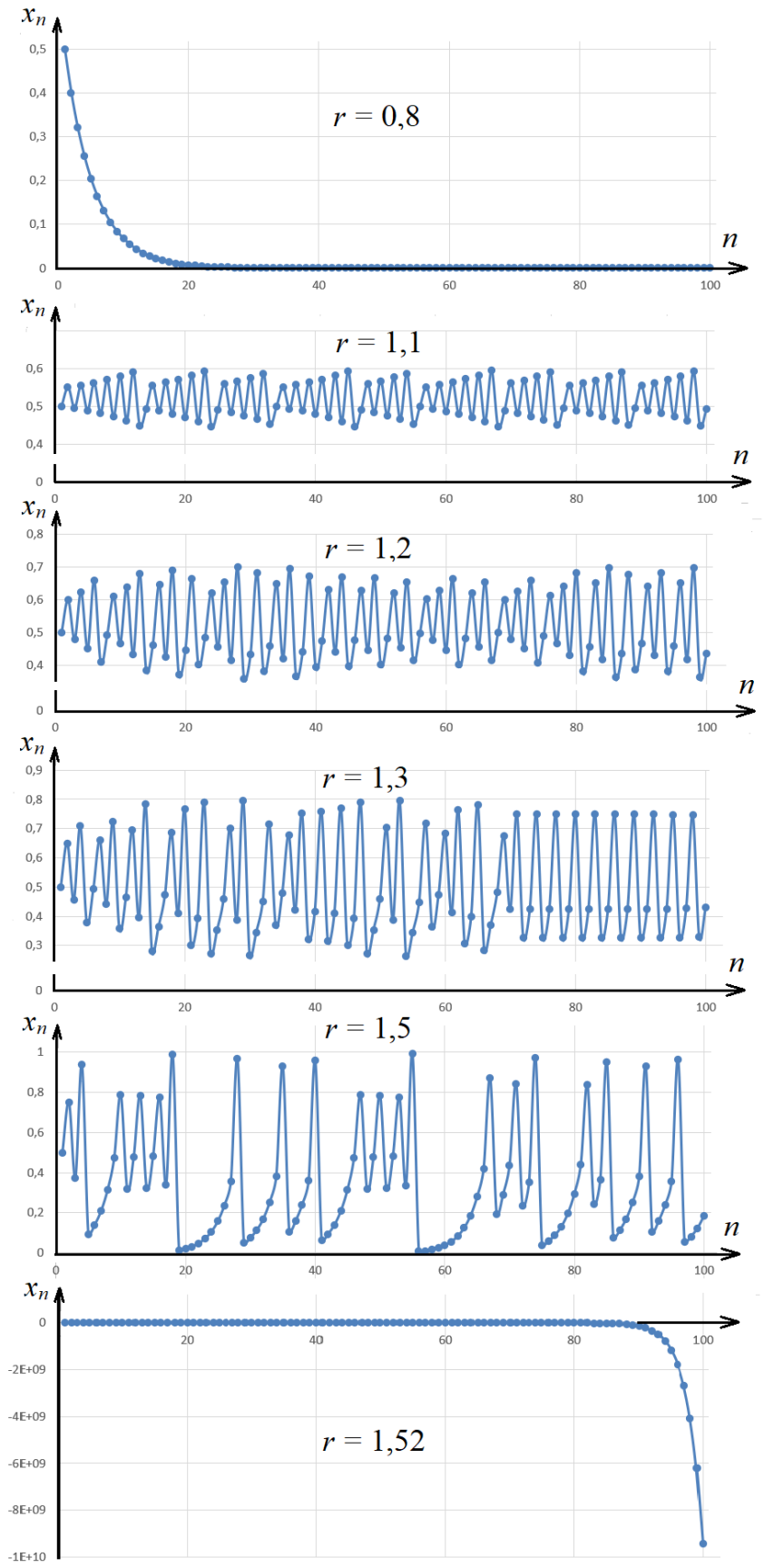


Рис. 2.4. Графіки хаотичних процесів для відображення Тенту для різних значень r

Відображення зі зсувом описується за наступним виразом:

$$x_{n+1} = (a \cdot x_n) \bmod 1, \tag{2.12}$$

де x_n – поточне значення послідовності; a – параметр, що визначає рівень зсуву; $\bmod 1$ – операція модуля, яка обмежує значення x_n в межах інтервалу]0, 1[.

Графіки хаотичних процесів для відображення зі зсувом для різних значень r надано на рис. 2.5. Параметр a вибирається більшим за 1, проте, як бачимо з діаграм, не завжди буде забезпечена стабільність хаотичних коливань. Це вимагає додаткових досліджень з пошуку відповідних значень параметру a, при якому забезпечується стабільність хаотичних коливань.

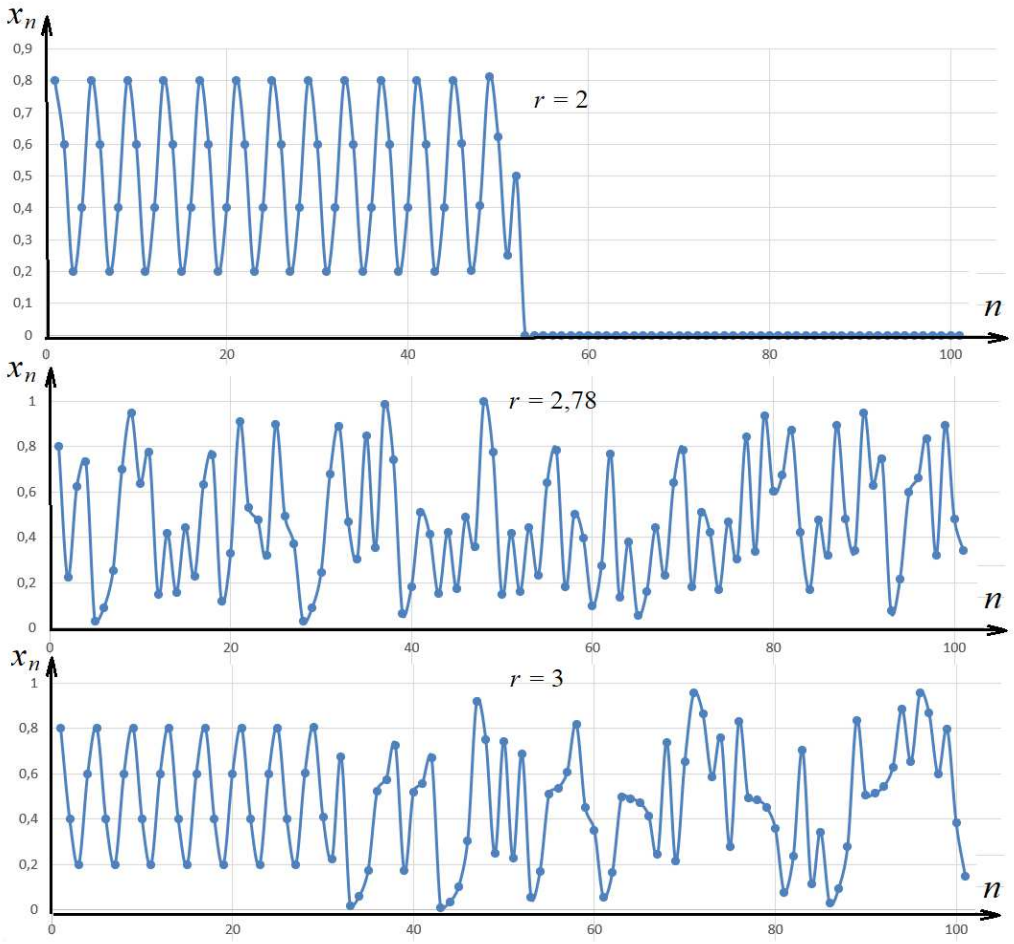


Рис. 2.5. Графіки хаотичних процесів для відображення зі зсувом для різних значень r

2.5 Кореляційний аналіз варіаційних можливостей генераторів хаосу

Для оцінки варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей проведемо дослідження на основі кореляційного аналізу [71]. Відомо, що в криптографічних системах використовуються лінійно-конгруентні генератори або апаратні генератори зі зворотним зв'язком. Однак, такі генератори мають недоліки, зокрема, короткий період генерації псевдовипадкових послідовностей та обмежену кількість можливих комбінацій. З огляду на це, доцільно дослідити властивості хаотичних генераторів, період генерації яких залежить від розрядної сітки обчислювальної системи. Важливо зазначити, що якість таких генераторів необхідно оцінювати за допомогою тестів NIST. Таким чином, для практичного використання хаотичних генераторів у криптографії потрібен ретельний аналіз їхніх статистичних характеристик.

На основі хаотичних послідовностей також розробляються різноманітні методи модуляції, які забезпечують структурне та енергетичне маскування сигнальних конструкцій. Це стало можливим завдяки властивостям динамічного хаосу: рух детермінованої динамічної системи за певних умов має характеристики шумового сигналу, а процес відзначається нелінійністю і неперіодичністю. Важливою особливістю генераторів хаосу є те, що навіть незначні зміни початкових параметрів хаотичного процесу спричиняють значні зміни в генерованих коливаннях. Це дозволяє формувати різноманітні траєкторії хаотичних процесів, що відкриває можливість створення практично необмеженої кількості комбінацій псевдовипадкових послідовностей (ПВП) заданої довжини.

Однак, для практичного застосування динамічного хаосу в системах шифрування та модуляції необхідно розробити методи, що дозволяють формувати початкові параметри генератора, наприклад, на основі введеного пароля. У зв'язку з цим, важливо оцінити варіаційні можливості хаотичних генераторів щодо формування псевдовипадкових послідовностей з необхідними кореляційними властивостями. На жаль, це питання отримало недостатню увагу в існуючих

наукових дослідженнях, що підкреслює важливість подальших досліджень у цьому напрямку. Основною метою цієї роботи є вивчення варіаційних можливостей хаотичних генераторів для створення псевдовипадкових послідовностей із заданими кореляційними характеристиками.

Оцінка варіаційних можливостей хаотичних генераторів при формуванні псевдовипадкових послідовностей на основі кореляційного аналізу полягає в дослідженні рівня залежності між елементами послідовності, яку генерує система. Кореляційний аналіз дозволяє визначити ступінь зв'язку між значеннями в різних ітераціях, що дає змогу оцінити випадковість та ефективність генератора. Низька кореляція між елементами послідовності вказує на високу ентропію та, відповідно, кращі криптографічні властивості. Такий підхід є ключовим для оцінки придатності хаотичних генераторів у криптографічних системах.

Для завдання дослідження розглянемо генератор хаосу логістичного відображення (2.8), який забезпечує найкращу стабільність хаотичних коливань. Вхідними параметрами для такого генератора є початкове число послідовності x_0 і $a = 3{,}9$. Зазначимо [71], що зміна параметра a може бути в дуже обмеженому діапазоні значень.

Проведемо дослідження впливу параметра a на процес хаотичного коливання. Розглянемо та оцінимо відмінність за допомогою коефіцієнту кореляції двійкових ПВП, що сформовані на основі хаотичних коливань з різними параметрами a. Для формування послідовності виконаємо наступну послідовність дій:

1) на інтервалі від нуля до одиниці сформуємо $N = 10^6$ чисел:

$$x_1,\ x_2,\ x_3, \ldots, x_N; \tag{2.13}$$

2) визначається математичне очікування вибірки x_c;

3) числовий інтервал від нуля до одиниці ділиться на дві частини з урахуванням значення x_c: один інтервал $]0; x_c]$; другий – $[x_c; 1[$;

4) логічне значення нуль «0» обирається за умови, що поточне значення послідовності $0 < x_j \leq x_c$, якщо $x_c < x_j < 1$, тоді «1»;

5) далі перевіряється коефіцієнт кореляції k_{ji} між двійковими послідовностями з різними значеннями параметра a або x_j.

Знайдемо коефіцієнти кореляції k_{ji} між хаотичними двійковими послідовностями логістичного відображення, що сформовані для різних початкових значень a і x. Дослідження були проведені для кількості двійкових чисел $N = 50000$ та значень послідовностей a_1 і x_1 та a_2 і x_2.

Результати кореляційного аналізу двійкових послідовностей $X_j(a_j, x_j)$ і $X_i(a_i, x_i)$ для числової вибірки $N = 50000$ зведено в табл. 2.3. Отримані результати свідчать, що за допомогою невеликих змін початкових значень x_j -=0,2 та 0,95 та параметру a= 3,90001 та 3,9 є можливість генерувати двійкові ПВП, коефіцієнт кореляції між якими прагне до нуля, тобто . $k_{ji} \to 0$. Невеликі значення отриманих коефіцієнтів кореляції 0,00176, 0,00213, 0,0081, 0,00069, 0,00377 свідчить про незначний зв'язок між двійковими послідовностями. Таким чином, можна зробити висновок, що на основі генератору хаосу можна сформувати значну кількість послідовностей за рахунок зміни початкових значень x_j та a. Наявність зв'язку між послідовностями можна пояснити значним коефіцієнтом кореляції на початку їх формування. Для перевірки цього ствердження на рис. 2.6 … 2.10 надано залежності коефіцієнтів кореляції між хаотичними процесами логістичного відображення, в яких використовуються різні початкові значення. Можна побачити, що коефіцієнти кореляції мають достатньо великі значення при формуванні перших $N = 300 - 500$ чисел. Потім можна побачити стабілізацію коефіцієнта кореляції, який прагне до нуля.

На рис. 2.6 для значень послідовностей з початковими параметрами $a_1 = 3{,}9,\ x_1 = 0{,}5$ та $a_2 = 3{,}90001,\ x_2 = 0{,}5$ надана залежність коефіцієнта кореляції. Бачимо, що при незначній зміні параметра $a_1 = 3{,}9$ і $a_2 = 3{,}90001$ спочатку спостерігається суттєва залежність між числами, про що свідчить високе

значення коефіцієнту кореляції $k_{ji} = 0{,}08\ldots0{,}8$. Однак при значенні вибірок $N > 300$ коефіцієнт кореляції прагне до нуля, тобто $k_{ji} \to 0$.

Таблиця 2.3

Коефіцієнти кореляції двох хаотичних процесів логістичного відображення при кількості двійкових чисел $N = 50000$

x_1	0,50	0,50	0,50	0,20	0,20
x_2	0,5	0,5001	0,75	0,95	0,35
a_1	3,90001	3,90	3,90	3,90	3,90
a_2	3,90	3,90	3,90	3,90	3,90
k_{ji}	-0,00176	-0,00213	-0,0081	-0,00069	-0,00377

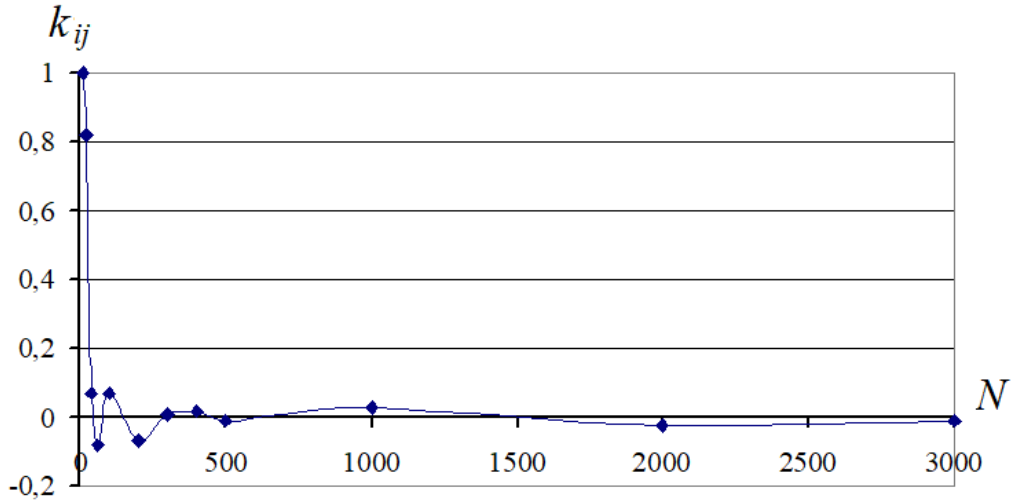


Рис 2.6. Залежність коефіцієнту кореляції для двійкових ПВП від N при значеннях $a_1 = 3{,}9$, $x_1 = 0{,}5$ та $a_2 = 3{,}90001$, $x_2 = 0{,}5$

Для двох послідовностей хаотичних процесів з параметрами $a_1 = 3{,}9$, $x_1 = 0{,}5$ та $a_2 = 3{,}9$ і $x_2 = 0{,}5001$ на рис. 2.7 надана залежність коефіцієнта кореляції для $N = 3000$. Бачимо, що при невеликій зміні початкових значень $x_1 = 0{,}5$ і $x_2 = 0{,}5001$, спочатку спостерігається суттєва залежність між послідовностями ($k_{ji} = 0{,}08\ldots0{,}7$), проте при вибірки $N > 750$ коефіцієнт кореляції $k_{ji} \to 0$.

Для двійкових послідовностей $a_1 = 3{,}9$, $x_1 = 0{,}5$ та $a_2 = 3{,}9$, $x_2 = 0{,}75$ на рис. 2.8 надана залежність коефіцієнта кореляції. Бачимо, що для цих процесів

спочатку також спостерігається деяка залежність послідовностей, проте при $N > 400$ коефіцієнт кореляції k_{ji} зменшується та повільно прагне до нуля.

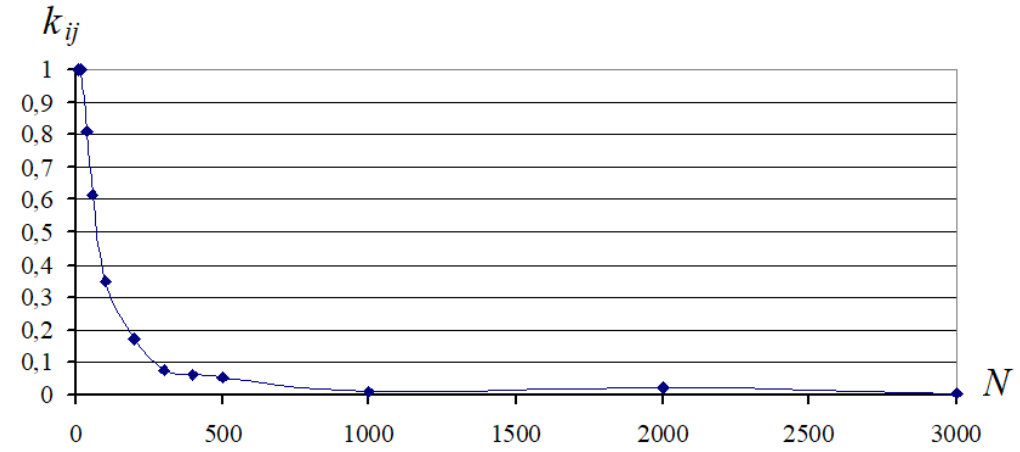


Рис. 2.7. Залежність коефіцієнту кореляції для двійкових ПВП від N при значеннях $a_1 = 3{,}9$, $x_1 = 0{,}5$ та $a_2 = 3{,}9$, $x_2 = 0{,}5001$

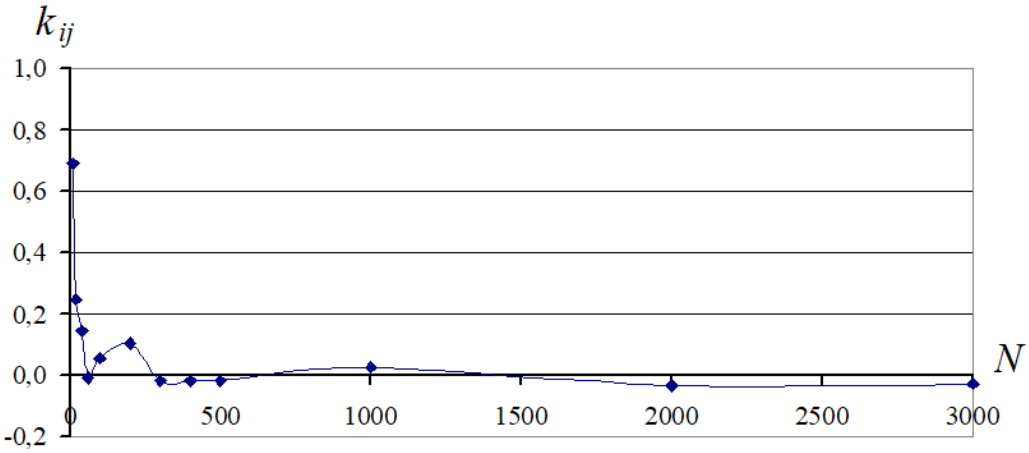


Рис. 2.8. Залежність коефіцієнту кореляції для двійкових ПВП від N при значеннях $a_1 = 3{,}9$, $x_1 = 0{,}5$ та $a_2 = 3{,}90001$, $x_2 = 0{,}75$

На рис. 2.9 надана залежність коефіцієнта кореляції від довжини двійкової послідовності при значеннях: $a_1 = 3{,}9$, $x_1 = 0{,}2$ та $a_2 = 3{,}9$, $x_2 = 0{,}95$. З діаграми бачимо, що спочатку спостерігається деяка залежність між числами ПВП з коефіцієнтом кореляції $k_{12} \approx 0{,}1$. При значенні вибірки $N > 500$ коефіцієнт кореляції зменшується і складає $k_{12} \approx 0{,}05$, що свідчить про наявність деякої залежності цих процесів.

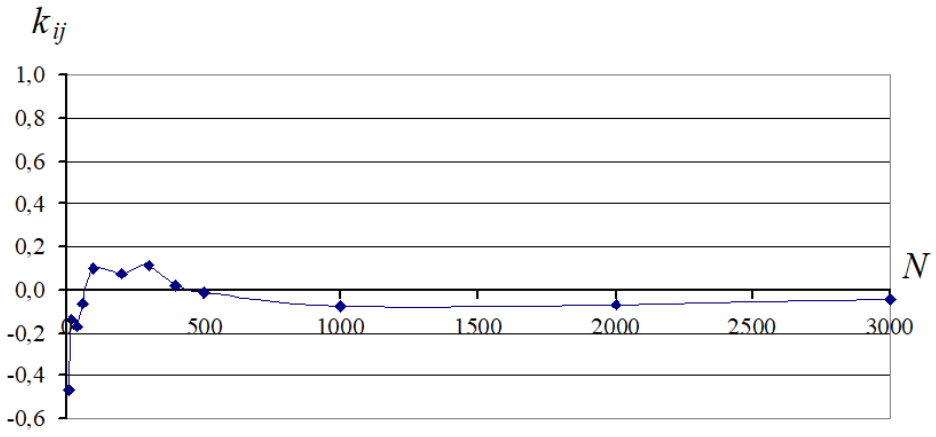


Рис. 2.9. Залежність коефіцієнту кореляції для двійкових ПВП від N при значеннях $a_1 = 3{,}9$, $x_1 = 0{,}2$ та $a_2 = 3{,}9$, $x_2 = 0{,}95$

На рис. 2.10 надана залежність кореляції двох хаотичних процесів для значень: $a_1 = 3{,}9$ і $x_1 = 0{,}2$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}35$ – друга ПВП. Бачимо, що при значеннях вибірок $N > 500$ коефіцієнт кореляції k_{ji} зменшується та практично дорівнює нулю.

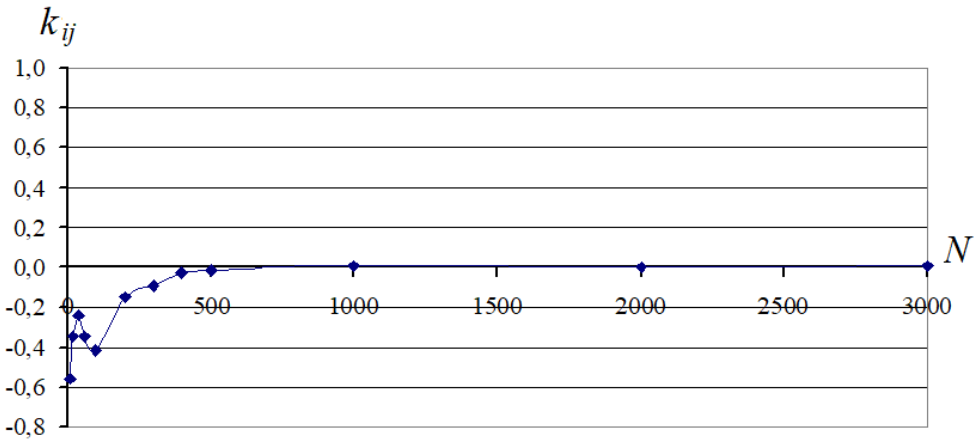


Рис. 2.10. Залежність коефіцієнту кореляції для двійкових ПВП від N при значеннях $a_1 = 3{,}9$, $x_1 = 0{,}2$ та $a_2 = 3{,}9$, $x_2 = 0{,}35$

2.6 Метод формування параметрів для генераторів хаосу на основі геш-функцій

Використання генераторів хаосу в криптографічних системах потребує певних алгоритмічних перетворень початкових параметрів по формуванню ПВП з

символами пароля користувача [72]. Відомо, що незначні зміни початкових параметрів генераторів хаосу призводять до утворення нових значень їх траєкторій коливань. Це означає, що при незначних змінах символів паролю користувача, навіть одного, запропонований алгоритм повинен формувати різні параметри генератору хаосу. Метою роботи є розробка алгоритму формування початкових параметрів програмних генераторів хаосу на основі перетворення символів введеного пароля користувача геш-функцією.

Розглянемо алгоритм ініціалізації початкових параметрів для одного або кількох генераторів хаосу на основі геш-функції. Початкові параметри генераторів при цьому повинні залишатися у секреті. Обрана геш-функція для формування початкових параметрів повинна задовольняти властивостям, які визначають її криптографічну стійкість [72]: складність до відновлення прообразу; стійкість до колізій першого та другого родів.

Нехай для криптографічної системи потокового шифрування [28] використовується один або кілька програмних генераторів хаосу логістичного відображення [72], за допомогою яких необхідно сформувати кілька гама-послідовностей: $x_{i+1} = ax_i(1 - x_i)$, де $a = 3{,}9$ – керуючий параметр, $x_i =]0\ldots1[$ – початкове значення хаотичної послідовності. Також можна використовувати і інші генератори хаосу [68-70]. Для формування початкових параметрів (ключів) генераторів хаосу запропоновано застосовувати перетворення символів пароля за допомогою геш-функції. Це дозволяє виконувати гешування масиву символів довільної довжини в бітову послідовність встановленої довжини (геш-код).

В якості прикладу розглянемо пароль, який складається з наступних символів: ^B69PvH*F7UcHv$3. В табл. 2.4 наведено результати гешування символів цього пароля за допомогою різних геш-функцій: CRC32; Haval; SHA-1; SHA-256; SHA-384; SHA-512. Розглянемо на прикладі функції SHA-512 метод формування початкових параметрів для п'яти послідовностей генератора хаосу (2.1). Як було зазначено в пункті 2.4 значення параметра a впливає на якість генеруємої послідовності, тому межі його зміни є строго обмеженими.

Тому, для спрощення даного дослідження, приймемо той факт, що значення керуючого параметра є константою, тобто a = 3,9.

Таблиця 2.4

Результати гешування символів пароля ^B69PvH*F7UcHv$3

CRC32	45b8fa89
Haval	3347217c69a19aee3468e10da3a9d585
SHA-1	8fe552437292690894e8f2a23a705413c3e72f24
SHA-256	d8b4966f7267943e74c1a4e1697af81460f8a80448b29785b5cf9c12287c3bde
SHA-384	6a28c21ba8eafe3532c950ff9f3e6894aaef016824991537f883794d80cc1342d63666bcffaa935cc38414203488bd8e
SHA-512	a66d3ea958ba9438956dae1bc6bfe74e624edb0c2034980694575e412f3ab1a4d981027e8ae79eb55f65ffff39bd3e29b5469c73bded51833abd274848b916e3

У табл. 2.5 представлено результати перетворення отриманого геш-коду a66d3ea958ba943895 в початкові параметри генератора хаосу (2.5), алгоритм якого полягає в наступному:

1) послідовність геш-коду розбивається на сегменти чисел певної довжини, наприклад, три (рядок №1, табл. 2.5);

2) в рядку № 2 – результати перетворення сегментів геш-коду в десяткові числа;

3) в рядку № 3 – десяткові числа перетворюються в дійсні числа y_i;

4) в рядку № 4 використовується операція перетворення за наступним алгоритмом:

$$x_1 = y_1; x_2 = 1 - y_2; x_3 = y_3; x_4 = 1 - y_4; x_5 = 1 - y_5; x_6 = 1 - y_6. \quad (2)$$

Дана операція необхідна для поліпшення статистичних властивостей формованої вибірки. В результаті перетворення будуть отримані наступні початкові параметри генератора хаосу: $x_1 = 0{,}2662_1$; $x_2 = 0{,}661$; $x_3 = 2709$; $x_4 = 0{,}7766$; $x_5 = 0{,}2371$; $x_6 = 0{,}7803$.

Таблиця 2.5

Перетворення геш-коду в початкові параметри генератору хаосу

№ дії	1	2	3	4	5	…	43	M_x
1	a66	d3e	a95	8ba	943	…	e3	
2	2662	3390	2709	2234	2371	…	227	
3	0,2662	0,339	0,2709	0,2234	0,2371	…	0,023	0,237
4	0,2662	0,661	0,2709	0,7766	0,2371	…	0,023	0,481

Як бачимо з табл. 2.5 в рядку №3 отримані значення числової послідовності в інтервалі від 0 до 1 з кількістю членів $N = 43$ мають середнє значення $S_x = 0{,}237$. Це є суттєвим відхиленням від теоретичного значення математичного очікування рівномірного закону $M_x = 0{,}5$. З цієї причини була запропонована операція перетворення №3 табл. 2.5. Результати, що представлені в рядку №4 табл. 2.5 показали поліпшення статистичних властивостей послідовності, тобто значення $S_x = 0{,}481$.

Таким чином, запропонований метод формування початкових параметрів (ключів) генератора хаосу на основі символів пароля користувача дозволяє використовувати для цього різний набір геш-функцій. Отриманий геш-код в результаті гешування можна використовувати для перетворення його в потрібний діапазон чисел початкових параметрів використовуваного генератора хаосу.

Висновки до розділу 2

1. Проведено аналіз апаратних та програмних генераторів для завдання використання їх в криптографії та системах модуляції. Найбільш ефективними з точки зору забезпечення високого рівня випадковості хаотичних процесів є апаратні генератори хаосу, робота яких побудована на основі фізичних процесів. Проте, до недоліків апаратних генераторів слід віднести складність їх реалізації та нестабільність генерації випадкових процесів, що пов’язано із залежністю від зовнішніх фізичних факторів, наприклад, температури, вологості, радіації та інше. Програмні генератори хаосу дозволяють адаптувати хаотичні процеси до різних

умов, що робить цей тип генераторів більш універсальним. До недоліків програмних генераторів слід віднести менший рівень випадковості у зв'язку з використанням математичних алгоритмів для отримання псевдовипадкових послідовностей, що може призвести до певних вразливостей. Іншою проблемою використання програмних генераторів є низька їх швидкість у порівнянні з апаратними генераторами. Апаратно-програмні генератори хаосу здатні забезпечити оптимальний баланс між високою швидкістю і мінімальними витратами обчислювальних ресурсів, що дозволяє використовувати їх у реальному часі без значного навантаження на обчислювальну систему.

2. Виконано дослідження граничних параметрів різних генераторів хаосу: логістичного відображення; системи Хенона; відображення Тенту; статечного відображення; відображення зі зсувом. Генератор логістичного відображення має певний діапазон значень параметру $3.57 < a < 4$, коли система стає хаотичною. При цьому встановлено, що будь-яка зміна початкового значення x_0 може призвести до кардинально різних результатів. При значенні параметра a близько до 4 система стає детермінованою і хаотичною. Стабільність хаотичного процесу на основі логістичного відображення обґрунтовує доцільність його використання в різних системах шифрування та системах модуляції.

Генератор хаосу на основі Хенона працює у двовимірному просторі і на кожній ітерації значення x_n і y_n оновлюються, утворюючи траєкторію точки на площині. Для певних значень параметрів система Хенона демонструє чутливість до початкових умов і хаотичну поведінку – навіть невелика зміна початкових умов призводить до зовсім різних траєкторій, що може бути використано для генерації псевдовипадкових чисел систем шифрування даних і методах модуляції.

Генератор хаосу на основі статечного відображення має просту структуру, але демонструє хаотичну поведінку при невеликих значеннях параметрів $r \approx 1 \ldots 1{,}1$. Даний генератор показав нестабільність процесу формування хаотичних послідовностей, що робить його недоцільним для застосування в системах шифрування і методах модуляції.

Генератор хаосу на основі відображення зі зсувом не завжди забезпечує стабільність хаотичних коливань при значенні параметру $a \geq 1$. Це вимагає додаткових зусиль з пошуку відповідних значень параметру a, при якому забезпечується стабільність хаотичних коливань. Це робить недоцільним його для використання в системах шифрування і методах модуляції.

3. Запропоновано використовувати кореляційний аналіз для дослідження варіаційних можливостей генераторів хаосу. Кореляційний аналіз дозволяє визначити ступінь зв'язку між значеннями в різних ітераціях, що дає змогу оцінити випадковість та ефективність генератора. Виконано аналіз для генератора хаосу логістичного відображення. Отримані результати кореляційного аналізу двійкових послідовностей $X_j(a_j, x_j)$ і $X_i(a_i, x_i)$ для числової вибірки $N = 50000$ показали, що за допомогою невеликих змін початкових значень генератора є можливість отримувати двійкові послідовності з взаємним коефіцієнтом кореляції, який прагне до

нуля ($k_{ji} \to 0$). Невеликі значення отриманих коефіцієнтів кореляції 0,00176, 0,00213, 0,0081, 0,00069, 0,00377 свідчить про незначний зв'язок між двійковими послідовностями при формуванні перших $N = 300 - 500$ чисел.

4. Запропонований метод формування початкових параметрів генератора хаосу на основі символів пароля користувача дозволяє використовувати для цього різний набір геш-функцій. Отриманий геш-код в результаті гешування можна використовувати для перетворення його в потрібний діапазон чисел початкових параметрів використовуваного генератора хаосу.

РОЗДІЛ 3
ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ІНТЕГРОВАНИХ МЕТОДІВ ПЕРЕТВОРЕННЯ ДАНИХ З ВИКОРИСТАННЯМ СТАТИСТИЧНОГО ШИФРУВАННЯ

Дана оцінка запропонованому методу підвищення інформаційної прихованості та завадостійкості на основі спільного використання статистичного шифрування, завадостійкого кодування та декореляції помилок. Обґрунтовано, що метод комбінованого статистичного шифрування може бути застосований для розробки реальних завадозахищених систем зв'язку, в яких вирішується задача підвищення прихованості і завадостійкості передавання конфіденційної інформації.

3.1 Огляд проблеми інтегрованих методів захисту інформації та постановка завдання дослідження

Підвищення завадозахищеності [4] сучасних телекомунікаційних систем вимагає ефективних і водночас простих методів захисту інформації, як від НСД, так і від випадкових завад у каналі зв'язку. Завадозахищеність дозволяє оцінити ефективність системи зв'язку, що працює в умовах радіоелектронної боротьби. Основними показниками завадозахищеності є завадостійкість і прихованість. Завадостійкість [79, 80, 87] оцінює здатність системи зв'язку забезпечувати задану точність передавання інформації при наявності випадкових завад. Прихованість [4] характеризує спроможність системи зв'язку забезпечувати захист передаваної інформації в умовах РЕБ.

Залежно від рівня моделі OSI, на якому здійснюється захист інформації від НСД, виділяють різні види прихованості [4]: інформаційна, структурна, енергетична та інші. Для забезпечення інформаційної прихованості, як правило, використовуються криптографічні протоколи [26, 82-84]. Структурна прихованість [74] спрямована на ускладнення розпізнавання структури сигнально-кодових конструкцій і реалізована на другому рівні моделі OSI. Енергетична прихованість

[4, 103] характеризує здатність системи зв’язку маскувати переданий сигнал під рівень завад з метою ускладнення його виявлення та перехоплення засобами радіоелектронної розвідки противника. Цей тип прихованості реалізується на першому рівні моделі OSI за допомогою різних методів розширення спектру [103] вихідного вузькосмугового сигналу. Слід враховувати той факт, що, як правило, завдання, пов’язані із забезпеченням завадостійкості та прихованості, дослідники розглядали окремо і незалежно один від одного. В результаті, в системах зв'язку, в яких необхідно забезпечити мінімальну швидкість обробки повідомлення в передавачі і приймачі, ця вимога не виконується. Для мінімізації часу обробки виправданим є використання простих методів перетворення даних, на основі яких можуть бути реалізовані інтегровані методи захисту від НСД та випадкових завад, в яких алгоритми забезпечення шифрування і завадостійкості об’єднані в єдину задачу.

Для виконання поставлених вимог доцільно використовувати підхід, при якому для захисту конфіденційної інформації використовуються різні методи перетворення даних, які доповнюють один одного, забезпечуючи підвищення криптографічної стійкості і завадостійкості. Для вирішення даної проблеми пропонується використовувати статистичне шифрування [81, 85], при якому для підвищення інформаційної прихованості (кріптостійкості) слід враховувати ентропію появи символів у повідомленні.

Особливість статистичного шифрування [81, 85] полягає у можливості формування різних кодових комбінацій зашифрованого тексту для одного і того ж відкритого тексту. Результати дослідження показали, що нерівномірний розподіл ймовірності появи символів у відкритому тексті є причиною їх кореляції з випадковими комбінаціями зашифрованого тексту на виході ймовірнісного кодера. Це означає, що цей метод захисту інформації від НСД може бути вразливим до частотного аналізу. Для вирішення цієї задачі пропонується використовувати алгоритм перерозподілу випадкових комбінацій, у якому ймовірність їх появи на виході статистичного кодера прагне до рівномірного закону.

З урахуванням цього потрібно виконати наступні дослідження:

1) провести статистичний аналіз розподілу символів у текстах різної довжини та тематики;

2) визначити граничні значення відхилення ймовірності появи символів у текстах від середнього значення;

3) на основі результатів дослідження запропоновати принципи формування простору випадкових кодових комбінацій для статистичного кодера.

Для підвищення інформаційної прихованості та завадостійкості кодових шифрограм шифртекстів пропонується використовувати статистичне шифрування разом з ітераційним кодом і декореляцією помилок.

Слід відзначити, що відомі методи статистичного шифрування, як правило, не враховують ентропію дискретного джерела інформації і не забезпечують контроль за правильністю передавання інформації. Також, цей метод шифрування розглядався окремо від завадостійкого кодування. Для вирішення цієї проблеми пропонується:

1) при формуванні простору випадкових кодових комбінацій враховувати середню ймовірність появи символів у відкритому тексті;

2) збільшення простору випадкових комбінацій здійснювати за рахунок додаткових перевірочних біт ітераційного кодування;

3) використовувати декореляцію помилок для зменшення кратності помилок у прийнятих комбінаціях та реалізувати при цьому змішування біт у шифрограмах за певним законом.

Таким чином, метою даного розділу є розробка інтегрованого методу захисту інформації на основі статистичного шифрування та завадостійкого кодування з декореляцією помилок.

3.2 Аналіз досліджень систем статистичного шифрування

Як правило, при передаванні даних по каналах зв'язку потрібно вирішити дві різні задачі: забезпечити захист даних від випадкових завад у каналу [79, 92, 93] та забезпечити захист інформації [26, 28, 73] від НСД.

Перше розв'язання задачі, засноване на теорії завадостійкого кодування, не стосується питань захисту інформації від НСД. Рішення другої проблеми базується на теорії криптографії, яка призвела до створення великої кількості різноманітних систем шифрування. Роботи К. Шеннона [103, 104] з кодування та шифрування послужили відправною точкою для розвитку цих двох напрямків незалежно один від одного. Пізніше намітилася тенденція поєднання процесів завадостійкого кодування і шифрування. З'являється низка робіт, зокрема [81, 85], у яких дослідники пропонують комплексний підхід до захисту інформації.

У 1984 році С. Голдвассер і С. Мікалі [106, 107] вперше запропонували принцип статистичного шифрування для криптосистеми з відкритим ключем. Недоліком такої криптосистеми є її вразливість до атак відкритого тексту. З цього випливає, що криптоаналітик може зашифрувати будь-яке повідомлення за допомогою відкритого ключа, а потім порівняти його з перехопленим зашифрованим текстом.

У 2002 році А. Молдован запропонував гомофонний шифр [73, 86, 108, 109] на основі імовірнісного шифрування, який забезпечив механізм збалансування статистичних характеристик зашифрованих знаків повідомлення до рівноймовірних. Основним недоліком такої системи шифрування є складність практичної реалізації.

У 2015 році Г. Мальцев запропонував комбіноване випадкове кодування (шифрування), яке реалізовано одночасно із завадостійким кодуванням та псевдовипадковою зміною ансамблю [110]. Можна підсумувати, що при такому способі захисту інформації від випадкових завад і НСД поточна якість каналу буде впливати на довжину кодових комбінацій шифрограми. З цієї причини для забезпечення необхідної надійності передавання інформації надлишковість коригувального коду повинна вибиратися з урахуванням найгіршої якості каналу. Недоліком такої системи є висока надлишковість комбінацій шифрограм, необхідна для забезпечення необхідної надійності передавання та захисту інформації від НСД.

Відмічені недоліки розглянутих методів статистичного шифрування дозволили зробити висновок про доцільність використання багатоступеневої схеми

перетворення даних [81]. При цьому на кожному етапі необхідно вирішувати завдання підвищення завадостійкості та інформаційної прихованості без суттєвого збільшення надлишковості випадкових кодових комбінацій. Таким чином, пропонується схема перетворення даних за допомогою трьох ступенів [81]:

1) перший ступінь захисту інформації реалізується за допомогою статистичного шифрування, при якому при формуванні простору випадкових комбінацій враховується ентропія дискретного джерела інформації;

2) на другому етапі використовується ітераційне кодування з контролем випадкових комбінацій на парність. Це вирішує проблему контролю цілісності даних і збільшує простір випадкових комбінацій за рахунок формування матриці зі змінними параметрами. Такий завадостійкий алгоритм кодування також дозволить підвищити показник інформаційної прихованості;

3) на третьому етапі реалізується декореляція помилок для зменшення кратності групування помилок у прийнятих кодових комбінаціях. Таке перетворення дозволяє підвищити завадостійкість каналу і не висуває високих вимог до коригуючої здатності коду. Підвищення інформаційної прихованості на цьому етапі здійснюється на основі заданого алгоритму зчитування розрядів кодових комбінацій ітераційної кодової матриці.

Таким чином, кожен етап перетворення даних забезпечує підвищення інформаційної прихованості зашифрованого тексту. На другому і третьому етапах також вирішуються завдання підвищення завадостійкості.

3.3 Інтеграція функцій шифрування і завадостійкого кодування

У роботах [81, 85] відзначено доцільність об’єднання в єдиний процес перетворення даних, що пов’язані з функціями шифрування та завадостійкого кодування. У криптографічних протоколах використовуються певні алгоритми перетворення даних, які дозволяють конвертувати відкритий текст у закритий. Криптографічна стійкість алгоритму залежить від довжини ключа. Можна звернути увагу на те, що як при завадостійкому кодуванні, так і при шифруванні

здійснюється перетворення даних. Проте в теорії кодування [79] і криптографії [26] вирішуються дві протилежні проблеми. Цим пояснюється наявність у телекомунікаційних системах двох різних блоків шифрування та завадостійкого кодування.

Для завдання захисту інформації від НСД завадостійке кодування не може бути застосовано, оскільки дозволена комбінація є розділеною, тобто розташування інформаційних і контрольних бітів заздалегідь відомо. Як правило, завадостійке кодування [79, 80] реалізується шляхом додавання до інформаційної частини k комбінації контрольних біт r, які формуються за певним алгоритмом. Завадостійкий код характеризується коригувальною здатністю, яка визначає кратність виявлення $t_{\text{вияв}}$ та виправлення помилок $t_{\text{випр}}$.

У роботах [79, 80] запропоновано різні варіанти використання завадостійкого кодування для захисту передаваної інформації від випадкових завад і НСД. Як правило, це забезпечується таким алгоритмом кодування, при якому сформовані дозволені кодові комбінації є нероздільними, тобто втрачається зв'язок між інформаційними і перевірочними розрядами. Фактично при цьому відбувається перетворення відкритої інформації в закриту. Наприклад, для криптосистеми McEliece, яка побудована на основі завадостійкого коду визначено мінімальні значення параметрів n=1024, $t_{\text{випр}}$=50 і k=524, при яких досягається висока криптографічна стійкість шифру і коригувальна здатність. Забезпечується це за рахунок зменшення кодової швидкості $\gamma_{\text{к}} = 0{,}51$ та використання достатньо великого простору можливих кодових блоків $N_{\text{ш}} = 2^{1024}$ для шифрування $k = 2^{524}$ інформаційних комбінацій. Проте продуктивність такої системи шифрування і завадостійкого кодування на два-три порядки вище, ніж у криптосистеми з відкритим ключем RSA. Однак головним недоліком криптосистеми McEliece є висока надлишковість шифрування.

У роботах [81, 85] запропоновано різні варіанти інтеграції статистичного шифрування (випадкового кодування) з різними варіантами завадостійкого

кодування. У деяких роботах [85] випадкове кодування розуміється як статистичне шифрування, оскільки вони мають схожі принципи генерації зашифрованих текстів на основі випадкових комбінацій.

Інтеграція статистичного шифрування з завадостійким кодом [81] забезпечує: захист від випадкових завад; криптостійкість шифрограми; контроль цілісності передаваної інформації. Можна виділити основні особливості такої інтеграції [81]:

1) забезпечення необхідної завадостійкості системи передачі з урахуванням ймовірності помилок та особливостей їх розподілу в дискретному каналі;

2) на стороні передавача здійснюється пряме стохастичне перетворення кодового блоку повідомлення, в якому поєднуються функції шифрування та завадостійкого кодування, а також враховуються статистичні характеристики каналу;

3) на приймальній стороні виконується зворотне перетворення кодового блоку, при якому аналізується цілісність отриманого блоку, при необхідності він коригується і перетворюється у відкриті дані конфіденційного повідомлення.

Слід зазначити, що реалізація даного методу захисту інформації як від випадкових завад, так і від НСД забезпечується за рахунок використання ансамблю випадкових кодових комбінацій, збільшення якого зможе забезпечити необхідний рівень криптографічного захисту. Водночас слід відзначити певні недоліки стохастичного шифрування:

1) при виборі ансамблю випадкових кодових комбінацій не враховується ентропія дискретного джерела інформації, що підвищує вразливість даного способу захисту інформації від НСД;

2) криптографічна стійкість методу безпосередньо залежить від ступеню надлишковості випадкових комбінацій, яка виникає внаслідок операції заміни комбінації символу відкритого текстового.

Для усунення цих недоліків пропонуємо підвищити криптографічну стійкість методу шляхом перерозподілу вибірки випадкових кодових комбінацій з урахуванням ймовірності появи символів на виході джерела повідомлення. Це дозволить на виході ймовірнісного перетворювача отримати потік випадкових

кодових комбінацій з рівномірним законом розподілу. Для зменшення надлишковості випадкових кодових комбінацій пропонується інтегрувати завадостійке кодування таким чином, щоб деякі з надлишкових бітів одночасно використовувалися як для виявлення або корекції помилок, так і для збільшення розміру ансамблю випадкових кодових комбінацій.

3.4 Алгоритм статистичного шифрування Гольдвассера і Микалі

Застосування невизначеності в системах шифрування інформації дозволяє суттєво підвищити їх криптографічну стійкість. Вперше схему статистичного шифрування запропонували Ш. Гольдвассер і С. Микалі [111, 112], в якій криптографічна стійкість досягається за рахунок використання безліч випадкових кодових комбінацій. При шифруванні ці комбінації обираються випадковим чином за допомогою генераторів випадкових чисел з деякого ймовірнісного простору L з метою відображення кодових послідовностей символів відкритого тексту [112]:

$$E_K: M \times R_{add} \to C, \tag{3.1}$$

де E_K – функції шифрування; K – секретний ключ; M – простір відкритих текстів; R_{add} – блок конкатенації; C – простір шифротекстів. При такому криптографічному перетворенні багаторазове шифрування одного і того ж самого відкритого тексту призведе до отримання зовсім різних шифрограм, що є певною перевагою. Проте при цьому використовуються надлишкові випадкові комбінації, тобто кількість біт у випадкових комбінаціях перевищує ніж у коді відкритого тексту m. При цьому від довжини випадкових комбінацій залежить криптографічна стійкість шифрограми, що є основним його недоліком цього методу шифрування.

На рис. 3.1 зображена одна з можливих структурних схем статистичного шифрування з використанням електронної кодової книги (ECB), в якій реалізовано режим простої заміни.

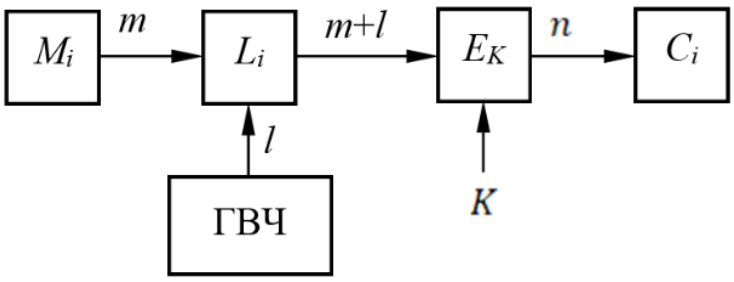


Рис. 3.1. Схема статистичного шифрування в режимі використання електронної кодової книги

Кодові комбінації довжиною m з вихідного простору символів відкритих текстів M_i надходять до блоку конкатенації L_i. За допомогою генератора випадкових чисел (ГВЧ) обираються комбінації довжини $m + l$, які також надходять до блоку L_i, де відбувається конкатенація послідовностей m.

З виходу блоку L_i розширена кодова комбінація $m + l$ надходить на вхід блоку шифрування E_i. На виході блоку E_i буде отримана зашифрована комбінація з розрядністю n, яка буде більше комбінації m символів відкритого тексту на l біт. При використанні однакового ключа при шифруванні будуть отримані різні шифрограми для однакового відкритого інформаційного тексту.

Таким чином, можна визначити наступні переваги статистичного шифрування: збільшення часу життя ключів; збільшення швидкості перетворення за рахунок зменшення раундів; можливість регулювання криптографічної стійкості шляхом збільшення надлишковості випадкових комбінацій. Проте, у випадку перехоплення зашифрованих повідомлень, криптограф зловмисника лишається в змозі обчислити функцію шифрування. Недоліком статистичного шифрування є те, що зберігається можливість використання частотного аналізу зашифрованого повідомлення для завдання його дешифрування.

3.5 Аналіз загроз і атак на шифрограми статистичного шифрування

Аналіз вимог до методу формування простору випадкових комбінацій виконаємо з урахуванням можливих атак на шифрограми системи статистичного

шифрування. Відомо [81, 85], що криптоаналіз шифрограм, отриманих за допомогою статистичного шифрування, може здійснюватися кількома методами. Основні види криптоаналізу, які можуть бути застосовані, включають: частотний аналіз; аналіз за відомим відкритим текстом (Known-plaintext attack); аналіз за обраним відкритим текстом (Chosen-plaintext attack); аналіз за обраною шифрограмою (Chosen-ciphertext attack); атака на базі адаптивного обраного відкритого тексту (Adaptive-chosen plaintext attack); математичний криптоаналіз; диференціальний і лінійний криптоаналіз.

Частотний аналіз побудований на особливостях статистичного шифрування, в якому може існувати зв’язок між відкритим текстом і закритим. Це означає, що для любого тексту характерні певні особливості: частотний розподіл символів або груп символів. Якщо шифрограма не достатньо приховує ці зв’язки, криптоаналітик може провести успішний частотний аналіз, зіставляючи частоти символів у шифрограмі з частотами символів у вихідному тексті.

Також криптоаналітик може використати аналіз шифрограми за відомим відкритим текстом [113]. У тому випадку, якщо криптоаналітик має доступ до частини відкритого тексту та відповідної шифрограми, він може використати цю інформацію для встановлення закономірностей у шифруванні або навіть для відновлення ключа.

Аналіз за обраним відкритим текстом дає можливість криптоаналітику самостійно вибирати відкритий текст для шифрування і отримувати відповідні шифрограми. Отже, у криптоаналітика з’являється можливість вивчати зміни у структурі шифрограми в залежності від різних вхідних даних, і виявити вразливості в алгоритмі статистичного шифрування.

Криптоаналітик також може використати аналіз за обраною шифрограмою з метою отримувати відповідний відкритий текст [113]. Це може бути особливо небезпечним для систем, де можлива така взаємодія, і дозволяє шукати кореляції між шифрованими і розшифрованими даними.

При використанні атаки на базі адаптивного обраного відкритого тексту криптоаналітик адаптує свої запити до шифрування на основі відповідей системи.

Це дозволяє поступово вивчати внутрішню структуру шифру і використовувати слабкі місця для зламування системи.

Математичний криптоаналіз може використовуватися в тому випадку, якщо алгоритм статистичного шифрування має математичну основу, наприклад, використовує відомі статистичні моделі або перетворення. В цьому випадку криптоаналітик може застосувати методи алгебраїчного аналізу для пошуку вразливостей.

Диференціальний і лінійний криптоаналіз використовують відмінності між відкритими текстами і відповідними шифрограмами для аналізу динаміки змін, які відбуваються під час шифрування. Якщо статистичне шифрування піддається певним закономірностям, цей тип криптоаналізу може бути ефективним.

Таким чином, шифрограми, створені за допомогою статистичного шифрування, можуть бути вразливими до широкого спектра криптоаналітичних методів, особливо якщо існує певний статистичний зв'язок між вхідними та вихідними комбінаціями шифратора. Тому, при розробці алгоритму системи статистичного шифрування потрібно це враховувати, особливо при формуванні випадкових комбінацій.

3.6 Розробка методу формування простору випадкових комбінацій для системи статистичного шифрування

Для підвищення ефективності статистичного шифрування розглянемо можливість зменшення надлишковості випадкових комбінацій при збереженні або збільшенні криптографічної стійкості за умови, що при формуванні простору випадкових комбінацій E_i враховується ентропія дискретного джерела інформації [81, 85]. Ентропія для випадку, коли символи на виході джерела інформації не підпорядковуються рівномірному закону розподілу, визначається наступним чином:

$$H_{NOL}(M) = -\sum_{j=1}^{L} p_j(m_j) \times log_2\, p_j\,(m_j), \qquad (3.2)$$

де $p_j(m_j)$ – ймовірність появи символу m_j у повідомленні. Ентропія для алфавіту російської мови с урахуванням ймовірності появи символів в тексті складає $H_{NUL}(M)$=4,42. У випадку рівноімовірного закону розподілу символів, що з'являються в тексті повідомлення ентропія $H_{UL}(M)$=5.

Таким чином, можна визначити головну умову підвищення криптографічної стійкості статистичного шифрування, коли комбінації, які застосовуються у просторі E_i для шифрування, з'являються в шифрограмі з рівноімовірним законом розподілу, тобто:

$$H_{NUL}(C) \to H_{UL}(C). \tag{3.3}$$

Ще однією умовою підвищення криптографічної стійкості є збільшення розрядності комбінацій шифрування l, тобто

$$n = m + l \to \infty. \tag{3.4}$$

Потрібно відзначити, що з практичної точки зору збільшувати n до нескінченності неможливо, що означає про необхідність обмеження цього показника. З урахуванням наявності частотного аналізу можна припустити про існування статистичного зв'язку між окремими комбінаціями відкритого тексту і комбінаціями шифрограм. Отже, в результаті шифрування будуть зберігатися деякі закономірності заміни комбінацій символу відкритого тексту комбінаціями шифрограм. Для тексту любої мови характерно наступне:

– повторюваність букв, пар букв, тобто *m* (*m*-грам);

– сполучуваність букв один з одним;

– чергування голосних і приголосних, а також деякі інші особливості.

Як правило, ці характеристики є досить стійкими, проте з деякими відхиленнями в залежності від особливості тематики тексту. Слід відзначити, що частотний аналіз є один із ефективних методів криптоаналізу, який застосовується

для розкриття шифрів шляхом аналізу частоти появи символів у зашифрованому тексті. Основна ідея цього методу полягає в тому, що у багатьох мовах деякі літери з'являються частіше за інші. Наприклад, у англійській мові літера "е" є найчастіше вживаною, а у українській – "о". Частотний аналіз базується на припущенні, що в зашифрованому тексті зберігається частотний розподіл символів оригінального тексту. Для кожної мови існує своя частотна таблиця символів, що дозволяє порівнювати частоти символів у зашифрованому тексті із статистичними даними для конкретної мови. Найбільш ефективний частотний аналіз для шифрів заміни, таких як шифр Цезаря або моноалфавітні шифри, де кожна літера тексту замінюється іншою літерою. У таких шифрах зберігається частотний розподіл літер, що дозволяє проводити аналіз. Проте частотний аналіз стає менш ефективним у випадку, коли частотний розподіл комбінацій у шифрограмі носить рівномірний характер. Також слід відзначити, що крім аналізу окремих літер, частотний аналіз може включати дослідження частоти появи біграм, триграм та інших комбінацій символів. Це дозволяє виявити типові слова чи фрази, які можуть бути використані для розкриття ключа. Також, чим більше тексту доступно для аналізу, тим точнішими є результати частотного аналізу. Проте невеликі шифрограми можуть не відображати типовий розподіл частот комбінацій шифрограм, що знижує ефективність цього методу.

Таким чином, частотний аналіз передбачає, що шифрограма з великим об’ємом комбінацій дасть можливість виявити ймовірність появи заданої літери алфавіту у відкритому тексті.

Проведемо аналіз появи символів в російськомовних текстах з різною довжиною: N_1 =1424, N_2 =3382 і N_3 = 22336. В табл. 3.1 представлені результати досліджень, які свідчать, що відхилення ймовірності появи символів від середньої ймовірності $p_j(c_j)$ в текстах залежить від їх розміру та тематики.

Наприклад, літера «е» для текстів розміром N_1 і N_2 має відхилення відповідно Δ_1=30,45% і Δ_2=27,15%, що майже у два рази більше (Δ =12,41), ніж для тексту з більшим обсягом символів N_3. Також можна побачити певну статистичну закономірність на прикладі літери «е» наближення її

ймовірності появи ($p(\text{е})_1$=0,0590 при N_1=1424, $p(\text{е})_2$=0,0618 при N_2=3382, $p(\text{е})_3$=0,0743 при N_3=22336) до середнього значення $p(\text{е})$=0,08483 при збільшенні N_i зберігається. Також виявлені аномальні відхилення ймовірності появи деяких символів від середньої ймовірності $p_j(c_j)$, що не пов'язано із збільшенням обсягу тексту. Наприклад, для літери «т» в залежності від розміру тексту отримані наступні значення імовірностей її появи $p(\text{т})_1$=0,0625, $p(\text{т})_2$=0,0574 і $p(\text{т})_3$=0,0536 з відхиленням від середньої імовірності $p_j(\text{т}_j)$=0,06318, відповідно, $\Delta(\text{т})_1$=1,08%, $\Delta(m)_2$ =9,15% і $\Delta(m)_3$ = 15,16%.

Як бачимо, що для літери «т» мінімальне відхилення імовірності її появи отримано для тексту меншого розміру, що свідчить про можливі певні статистичні аномалії. З урахуванням зазначеного в табл. 3.2 запропоновано варіанти розподілу комбінацій шифрування символів при надлишковості l =1, 2, 3 та ймовірності появи символів у відкритому тексті за умови, що кількість символів в алфавіті відкритого тексту M_i=33. У стовпчиках 4, 6, 8 табл. 3.2 для текстів різного розміру (N_1=1424; N_2 = 3382; N_3=22336) надано кількість випадкових комбінацій для кожного символу з урахуванням середньої імовірності його появи в тексті:

$$N_i(c_j) = p_j(c_j) \times N_l, \tag{3.5}$$

де N_l – кількість символів в тексті.

З теоретичної точки зору в результаті використання для кожного символу своєї множини випадкових кодових комбінацій $N_i(c_j)$ на виході статистичного шифратора отримаємо рівноімовірний їх розподіл. Таким чином, буде втрачено зв'язок між вхідними даними та шифрограмами при статистичному шифруванні. Для зменшення трудомісткості даного алгоритму розподілу випадкових комбінацій розглянемо інші варіанти.

Таблиця 3.1

Статистичні показники появи символів в текстах різного розміру

№	Символ	Середня ймовірність $p_j(c_j)$ появи символів в тексті	Відхилення імовірності появи символів в текстах з різною довжиною від середньої імовірності					
			N_1=1424		N_2 =3382		N_3 =22336	
			1424	$\Delta(c_j)_1$,%	3382	$\Delta(c_j)_2$,%	22336	$\Delta(c_j)_3$,%
1	2	3	4	5	6	7	8	9
1	о	0,10983	0,0955	13,05	0,095	13,50	0,0927	15,60
2	е	0,08483	0,0590	30,45	0,0618	27,15	0,0743	12,41
3	а	0,07998	0,0723	9,60	0,0671	16,10	0,0642	19,73
4	и	0,07367	0,0674	8,51	0,078	-5,88	0,0600	18,56
5	н	0,06700	0,0632	5,67	0,0529	21,04	0,0561	16,27
6	т	0,06318	0,0625	1,08	0,0574	9,15	0,0536	15,16
7	с	0,05473	0,0442	19,24	0,0426	22,16	0,0409	25,27
8	р	0,04746	0,0358	24,57	0,0464	2,23	0,0385	18,88
9	в	0,04533	0,0435	4,04	0,0331	26,98	0,0431	4,92
10	л	0,04343	0,0358	17,57	0,0302	30,46	0,0331	23,79
11	к	0,03486	0,0239	31,44	0,0237	32,01	0,0242	30,58
12	м	0,03203	0,0253	21,01	0,0378	-18,01	0,0272	15,08
13	д	0,02977	0,0225	24,42	0,0216	27,44	0,0237	20,39
14	п	0,02804	0,0225	19,76	0,0287	-2,35	0,0239	14,76
15	у	0,02615	0,0190	27,34	0,0180	31,17	0,0216	17,40
16	я	0,02001	0,0267	-33,43	0,0163	18,54	0,0160	20,04
17	ы	0,01898	0,0154	18,86	0,0186	2,00	0,0190	-0,11
18	ь	0,01735	0,0091	47,55	0,0139	19,88	0,0169	2,59
19	г	0,01687	0,0126	25,31	0,0121	28,28	0,0148	12,27
20	з	0,01641	0,0154	6,15	0,0136	17,12	0,0137	16,51
21	б	0,01592	0,0091	42,84	0,0133	16,46	0,0098	38,44
22	ч	0,0145	0,0147	-1,38	0,0103	28,97	0,0133	8,28
23	й	0,01208	0,0105	13,08	0,0109	9,77	0,0105	13,08
24	х	0,00966	0,0084	13,04	0,0121	-25,26	0,0107	-10,77
25	ж	0,0094	0,0084	10,64	0,0062	34,04	0,0093	1,06
26	ш	0,00718	0,0084	-16,99	0,0053	26,18	0,0075	-4,46
27	ю	0,00639	0,0049	23,32	0,0053	17,06	0,0048	24,88
28	ц	0,00486	0,0014	71,19	0,005	-2,88	0,0028	42,39
29	щ	0,00361	0,0035	3,05	0,0047	-30,19	0,0018	50,14
30	э	0,00331	0,003	9,37	0,0024	27,49	0,0026	21,45
31	ф	0,00267	0,00205	23,22	0,0035	-31,09	0,00207	22,47
32	ъ	0,00037	0,00033	10,81	0,00031	16,22	0,00031	16,22
33	ё	0,00013	0,00014	-7,69	0,00011	15,38	0,00014	-7,69

Таблиця 3.2

Статистичне шифрування з використанням чотирьох груп випадкових комбінацій

№	Символ	Середня імовірність появи символів в тексті $p_j(c_j)$	Розподіл кількості випадкових комбінацій з урахуванням ймовірності появи символів $p_j(c_j)$ в текстах з різною довжиною та загальної кількості випадкових кодових комбінацій $N_{заг}$					
			$l=1$		$l=2$		$l=3$	
			$N_{l=1}$=512, $\gamma_{Ш}$=0,889		$N_{l=2}$=1024, $\gamma_{Ш}$=0,8		$N_{l=3}$=2048, $\gamma_{Ш}$=0,727	
1	2	3	4	5	6	7	8	10
1	о	0,10983	56	$N_{гр\ 1}$=297 $N_{1\text{-}8}$=37	112	$N_{гр\ 1}$=595 $N_{1\text{-}8}$=74	225	$N_{гр\ 1}$=297 $N_{1\text{-}8}$=149
2	е	0,08483	43		87		174	
3	а	0,07998	41		82		164	
4	и	0,07367	38		75		151	
5	н	0,06700	34		69		137	
6	т	0,06318	32		65		129	
7	с	0,05473	28		56		112	
8	р	0,04746	24		49		97	
9	в	0,04533	23	$N_{гр\ 2}$=133 $N_{9\text{-}16}$=17	46	$N_{гр\ 2}$=266 $N_{9\text{-}16}$=33	93	$N_{гр\ 2}$=133 $N_{9\text{-}16}$=66
10	л	0,04343	22		44		89	
11	к	0,03486	18		36		71	
12	м	0,03203	16		33		66	
13	д	0,02977	15		30		61	
14	п	0,02804	14		29		57	
15	у	0,02615	13		27		54	
16	я	0,02001	10		20		41	
17	ы	0,01898	10	$N_{гр\ 3}$=62 $N_{17\text{-}24}$=8	19	$N_{гр\ 3}$=125 $N_{17\text{-}24}$=16	39	$N_{гр\ 3}$=62 $N_{17\text{-}24}$=31
18	ь	0,01735	9		18		36	
19	г	0,01687	9		17		35	
20	з	0,01641	8		17		34	
21	б	0,01592	8		16		33	
22	ч	0,0145	7		15		30	
23	й	0,01208	6		12		25	
24	х	0,00966	5		10		20	
25	ж	0,0094	5	$N_{гр\ 4}$=19 $N_{26\text{-}33}$=2	10	$N_{гр\ 4}$=39 $N_{26\text{-}33}$=5	19	$N_{гр\ 4}$=19 $N_{26\text{-}33}$=10
26	ш	0,00718	4		7		15	
27	ю	0,00639	3		7		13	
28	ц	0,00486	2		5		10	
29	щ	0,00361	2		4		7	
30	э	0,00331	2		3		7	
31	ф	0,00267	1		3		5	
32	ъ	0,00037	0,19		0,38		0,76	
33	ё	0,00013	0,07		0,13		0,27	

З урахуванням зробленого статистичного аналізу появи символів в текстах різного розміру згідно табл. 3.1 розглянемо варіант ділення випадкових комбінацій на чотири групи. Як було зазначено раніше ймовірність появи символів в текстах може суттєво відрізнятися від значення середньої ймовірності $p_j(c_j)$, як в більшу сторону, так і меншу. Це означає, що для спрощення формування вибірки випадкових комбінацій можливо їх об'єднання в певні групи для символів, ймовірності появи яких несуттєво відрізняються.

Для прикладу, в стовпчику 5 табл. 3.2 представлено ділення алфавіту на чотири групи. В першу групу увійшли літери від «о» до «р», в межах яких ймовірність появи змінюється від 0,10983 до 0,04746, тобто перше і останнє значення відрізняється приблизно у два рази.

В другу групу увійшли літери від «в» до «я», в межах яких ймовірність появи змінюється від 0,04533 до 0,02001, тобто перше і останнє значення відрізняється приблизно у 2,265 рази.

В третю групу увійшли літери від «ы» до «х», в межах яких ймовірність появи змінюється від 0,01898 до 0,00966, тобто перше і останнє значення відрізняється приблизно у 19,648 рази.

В четверту групу увійшли літери від «в» до «я», в межах яких ймовірність появи змінюється від 0,0094 до 0,000013, тобто перше і останнє значення відрізняється приблизно у 723 рази.

Для значення надлишковості шифрування $l = 1$ довжина випадкових комбінацій складає $k = m + l = 8 + 1 = 9$, де $m = 8$ – це кількість біт для кодування символів алфавіту. Тоді загальна кількість випадкових комбінацій становить:

$$N_l = 2^k. \tag{3.6}$$

Тобто для нашого випадку $N_{l=1} = 512$. Кодова швидкість статистичного шифрування оцінюється за формулою:

$$\gamma_{\text{ш}} = \frac{k}{n}. \tag{3.7}$$

Для $l = 1$ кодова швидкість шифрування $\gamma_{\text{ш}}$=0,889. Вочевидь, що збільшення надлишкових елементів l зменшує кодову швидкість статистичного шифрування, проте криптостійкість шифрування підвищується. Так, для $l = 2$ кількість випадкових комбінацій $N_{l=2} = 1024$, для $l = 3$ отримаємо $N_{l=3} = 2048$. Це призводить до зменшення долі конфіденційного повідомлення в шифрограмі, тобто $\gamma_{\text{ш}}$=0,8 та 0,787.

З табл. 3.2 бачимо, що для першої групи для $l = 1$ використовується $N_{\text{гр }1}$=297 комбінацій. На кожний символ першої групи витрачається:

$$N_{1\text{-}8}=N_{\text{гр }1}/N_c, \tag{3.8}$$

де N_c – кількість символів у групі.

Таким чином, в першій групі для шифрування кожного символу отримаємо $N_{1\text{-}8}$=37 випадкових комбінацій. Для другої групи $N_{\text{гр }2}$=133 і $N_{9\text{-}16}$=17. Також можна побачити, що для третьої та четвертої груп спостерігається зменшення кількості випадкових комбінацій: $N_{\text{гр }3}$=63, $N_{17\text{-}24}$=8 і $N_{\text{гр }4}$=19, $N_{25\text{-}33}$=2. Тобто, для групи символів з меншою ймовірністю їх появи використовується менша кількість комбінацій. Такий підхід у виборі кількості випадкових комбінацій сприяє виконанню умові (3.3), коли комбінації шифрограми прагнуть до рівномірного закону їх розподілу.

В стовпчиках 7, 9 табл. 3.2 аналогічним чином надано розподіл випадкових комбінацій $N_{l=2} = 1024$ і $N_{l=3} = 2048$ для символів алфавіту з урахуванням кількості додаткових біт $l = 2$ та $l = 3$.

Звісно, що чим більша буде кількість груп, тим кращі матимемо статистичні характеристики на виході шифратора. Вибір кількості груп може використовуватися для адаптивного підходу до управління криптографічної стійкості системи статистичного шифрування. В табл. 3.3 надано варіант розподілу випадкових

комбінацій, в якому використовується 15 груп. При цьому в кожній групі об'єднані символи з близькими значеннями середньої ймовірності їх появи. Зміна в процесі статистичного шифрування множин випадкових комбінацій для символів алфавіту дозволить суттєво зменшити загрози і атаки на шифрограми статистичного шифрування.

3.7 Метод інтеграції статистичного шифрування, завадостійкого кодування з декореляцією помилок

Розглянемо метод інтеграції ймовірнісного шифрування та завадостійкого кодування. Для ефективного використання пропускної спроможності каналу необхідне його узгодження із джерелом інформації на вході. Відповідно до основної теореми Шеннона про кодування [8, 9] ймовірність помилкового елемента передачі даних по каналу з завадами прагне нулю за умови $n \to \infty$. Це означає, що кодова швидкість

$$\gamma_{\text{к}} = k/(k+r) = k/n \to 1, \tag{3.9}$$

а кількість перевірочних елементів r зростає несуттєво, порівняно з інформаційною частиною k. В табл. 3.4 надана динаміка зміни показників $\gamma_{\text{к}}$, k і r для циклічного коду з мінімальною кодовою відстанню $d_0 = 4$.

Як було зазначено раніше, основним недоліком статистичного шифрування є надлишковість. Вочевидь, що зі збільшенням надлишковості статистичного шифрування зростає криптостійкість, а кодова швидкість падає. Аналогічна динаміка характерна і для завадостійкого коду. Як правило, чим більша надлишковість коду, тим вища завадостійкість. Розглянемо наступний варіант інтеграції, коли спочатку виконується ймовірнісне шифрування, а потім завадостійке кодування. В цьому випадку довжина кодового блоку:

$$n = m + l + r, \tag{3.10}$$

Таблиця 3.3

Статистичне шифрування з використанням п’ятнадцяти груп випадкових комбінацій

№	Символ	Середня ймовірність появи символів в тексті $p_j(c_j)$	Розподіл кількості випадкових комбінацій з урахуванням ймовірності появи символів $p_j(c_j)$ в текстах з різною довжиною та загальної кількості випадкових кодових комбінацій $N_{заг}$					
			$l=1$		$l=2$		$l=3$	
			$N_{l=1}$=512		$N_{l=2}$=1024		$N_{l=3}$=2048	
1	2	3	4	5	6	7	8	10
1	о	0,10983	56	$N_{гр\ 1}$=56	112	$N_{гр\ 1}$=112	225	$N_{гр\ 1}$=225
2	е	0,08483	43	$N_{гр\ 2}$=123	87	$N_{гр\ 2}$=243	174	$N_{гр\ 2}$=486
3	а	0,07998	41	$N_{2\text{-}4}$=41	82	$N_{2\text{-}4}$=81	164	$N_{2\text{-}4}$=162
4	и	0,07367	38		75		151	
5	н	0,06700	34	$N_{гр\ 3}$=96	69	$N_{гр\ 3}$=189	137	$N_{гр\ 3}$=378
6	т	0,06318	32	$N_{5\text{-}7}$=32	65	$N_{5\text{-}7}$=63	129	$N_{5\text{-}7}$=126
7	с	0,05473	28		56		112	
8	р	0,04746	24	$N_{гр\ 4}$=69	49	$N_{гр\ 4}$=138	97	$N_{гр\ 4}$=279
9	в	0,04533	23	$N_{8\text{-}10}$=23	46	$N_{8\text{-}10}$=46	93	$N_{8\text{-}10}$=93
10	л	0,04343	22		44		89	
11	к	0,03486	18	$N_{гр\ 5}$=34	36	$N_{гр\ 5}$=68	71	$N_{гр\ 5}$=136
12	м	0,03203	16	$N_{11\text{-}12}$=17	33	$N_{11\text{-}12}$=34	66	$N_{11\text{-}12}$=68
13	д	0,02977	15		30		61	
14	п	0,02804	14	$N_{гр\ 6}$=42	29	$N_{гр\ 6}$=86	57	$N_{гр\ 6}$=172
15	у	0,02615	13	$N_{13\text{-}15}$=14	27	$N_{11\text{-}12}$=43	54	$N_{11\text{-}12}$=86
16	я	0,02001	10	$N_{гр\ 7}$=20	20	$N_{гр\ 7}$=40	41	$N_{гр\ 7}$=80
17	ы	0,01898	10	$N_{16\text{-}17}$=10	19	$N_{16\text{-}17}$=20	39	$N_{16\text{-}17}$=40
18	ь	0,01735	9		18		36	
19	г	0,01687	9	$N_{гр\ 8}$=26	17	$N_{гр\ 8}$=52	35	$N_{гр\ 8}$=104
20	з	0,01641	8	$N_{18\text{-}20}$=	17	$N_{18\text{-}20}$=26	34	$N_{18\text{-}20}$=52
21	б	0,01592	8	$N_{гр\ 9}$=16	16	$N_{гр\ 9}$=30	33	$N_{гр\ 9}$=62
22	ч	0,0145	7	$N_{21\text{-}22}$=8	15	$N_{21\text{-}22}$=15	30	$N_{21\text{-}22}$=31
23	й	0,01208	6	$N_{гр\ 10}$=6	12	$N_{гр\ 10}$=12	25	$N_{гр\ 10}$=25
23	й	0,01208	6	$N_{гр\ 10}$=6	12	$N_{гр\ 10}$=12	25	$N_{гр\ 10}$=25
24	х	0,00966	5	$N_{гр\ 11}$=10	10	$N_{гр\ 11}$=20	20	$N_{гр\ 11}$=38
25	ж	0,0094	5	$N_{24\text{-}25}$=5	10	$N_{24\text{-}25}$=10	19	$N_{24\text{-}25}$=19
26	ш	0,00718	4	$N_{гр\ 12}$=6	7	$N_{гр\ 12}$=14	15	$N_{гр\ 12}$=28
27	ю	0,00639	3	$N_{26\text{-}27}$=3	7	$N_{26\text{-}27}$=7	13	$N_{26\text{-}27}$=14
28	ц	0,00486	2	$N_{гр\ 13}$=2	5	$N_{гр\ 13}$=5	10	$N_{гр\ 13}$=10
29	щ	0,00361	2	$N_{гр\ 14}$=4	4	$N_{гр\ 14}$=6	7	$N_{гр\ 14}$=14
30	э	0,00331	2	$N_{29\text{-}30}$=2	3	$N_{29\text{-}30}$=3	7	$N_{29\text{-}30}$=7
31	ф	0,00267	1		3		5	
32	ъ	0,00037	0,19	$N_{гр\ 15}$=3	0,38	$N_{гр\ 15}$=6	0,76	$N_{гр\ 15}$=9
33	ё	0,00013	0,07	$N_{31\text{-}33}$=1	0,13	$N_{31\text{-}33}$=2	0,27	$N_{31\text{-}33}$=3

де r – кількість перевірочних елементів. При спільному використанні статистичного шифрування та завадостійкого кодування кодова швидкість визначається на основі наступного виразу:

$$\gamma_{\text{шк}} = \frac{m}{m+l+r}. \tag{3.11}$$

Таблиця 3.4

Залежність кодової швидкості m від при $d_0 = 4$

№	n	k	r	$\gamma_{\text{к}}$
1	31	19	12	0,612
2	63	51	12	0,809
3	127	114	13	0,897
4	255	242	13	0,949
5	511	497	14	0,972
6	1023	1009	14	0,986
7	2047	2002	15	0,978
8	4095	4080	15	0,996

Згідно з табл. 3.4 покращити коефіцієнт $\gamma_{\text{шк}}$ можна за рахунок збільшення довжини кодового блоку n. Відповідно до (3.9) доцільно вибирати кодові блоки більшої довжини. Однак в реальних системах передавання даних (ПД) зі зворотним зв'язком (ЗЗ) максимальну довжину пакета обмежують. Це пов’язано з тим, що на пакети великої довжини в більшій мірі впливають випадкові завади, що може суттєво збільшити кількість перезапитів. Ефективна швидкість системи ПД зі ЗЗ оцінюється за допомогою коефіцієнтів $\gamma_{\text{к}}$ і $\gamma_{\text{е}}$ [9]:

$$R_{\text{е}} = \gamma_{\text{к}} \cdot \gamma_{\text{е}} = \frac{1-P_{\text{ст}}(n)}{1+(M-1)\cdot P_{\text{ст}}(n)}, \tag{3.12}$$

де M – кількість кодових блоків, що повторюються; $\gamma_{\text{е}}$ – коефіцієнт, який враховує ймовірність запитів пакета; $P_{\text{ст}}$ – ймовірність стирання пакета.

Отже, зі збільшенням довжини пакета n можливість його спотворення збільшується, тобто $\gamma_{\text{к}} \to 1$, $\gamma_{\text{е}} \to 0$ і $R_{\text{е}} \to 0$. На рис. 3.2 представлені залежності і від довжини пакета. З діаграми бачимо, що умова [79, 88]:

$$\gamma_{\text{к}} = \gamma_{\text{е}} \tag{3.13}$$

визначає оптимальну довжину пакета $n_{\text{опт}}$, при якому забезпечується максимальне значення ефективної швидкості $R_{\text{е}} = R_{max}$.

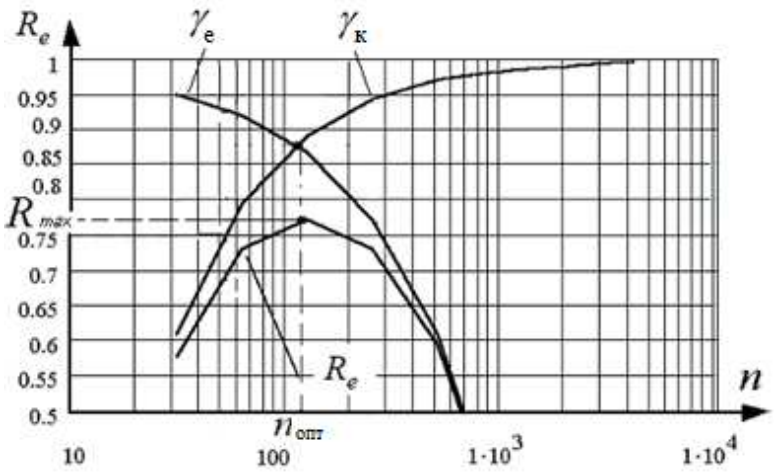


Рис. 3.2. Залежність $R_{\text{е}}$, $\gamma_{\text{к}}$ і $\gamma_{\text{е}}$ від довжини пакету n

Розглянемо інтеграцію ймовірнісного шифрування та завадостійкого кодування на основі ітеративного коду, в якому використовуються перевірочні елементи на основі біту перевірки на парність.

Загальний алгоритм такого завадостійкого коду полягає в створенні перевірочної матриці (Н-матриця), в якій кожне кодове слово представляється як вектор, який містить як інформаційні, так і перевірочні біти. Для створення коду використовується перевірочна двовимірна матриця

$$H = n \times v, \tag{3.14}$$

де $n = m + l + r$ – загальна кількість біт у рядку; v – кількість комбінацій у матриці. Матриця Н має наступний вид:

$$H=\begin{bmatrix} x_{11} & x_{12} & x_{1j} & p_{1m} \\ x_{21} & x_{22} & \cdots x_{2j} & p_{2m} \\ & \vdots & & \vdots \\ x_{g1} & x_{gv} & x_{gj} & p_{gm} \\ p_{v1} & p_{v2} & \cdots p_{vj} & p_{vm} \end{bmatrix} \quad (3.15)$$

де $x_{11}, x_{12}, \dots, x_{1j}$ – випадкова комбінація, що отримана в результаті статистичного шифрування; $p_{1m}, p_{2m}, \dots, p_{gm}, p_{vm}$ – перевірочні елементи рядків; $p_{v1}, p_{v2}, \dots, p_{vj}$ – перевірочні елементи стовбців.

При кодуванні ітеративним кодом відбувається додавання до випадкових комбінацій контрольних бітів, які визначаються через перевірки парності:

$$\begin{aligned} p_{1m} &= x_{11} \oplus x_{12} \oplus \dots \oplus x_{1j} \\ p_{2m} &= x_{21} \oplus x_{22} \oplus \dots \oplus x_{2j} \\ &\dots \\ p_{gm} &= x_{g1} \oplus x_{g2} \oplus \dots \oplus x_{gj} \\ p_{vm} &= x_{v1} \oplus x_{v2} \oplus \dots \oplus x_{vj} \end{aligned} \quad (3.16)$$

Кожен рядок матриці Н відповідає одному рівнянню парності, яке містить біти випадкових комбінацій. Аналогічним чином знаходяться перевірочні біти $p_{v1}, p_{v2}, \dots, p_{vj}$ для бітів стовпчиків. Кодове слово буде при цьому виглядати наступним чином:

$$x_{11}x_{12} \dots x_{1j}p_{1m}x_{21}x_{22} \dots x_{2j}p_{2m} \dots x_{g1}x_{gv} \dots x_{gj}p_{gm}p_{v1}p_{v2} \dots p_{vj}p_{vm}.$$

Для підвищення криптографічної стійкості доцільним є можливість змінювати розмір матриці Н. Це означає, що в одному рядку можуть бути біти інших випадкових комбінацій. Вкраплення перевірочних елементів в кодове слово та зміна розміру матриці Н додатково ускладнює його структуру. Періодична зміна параметрів матриці Н дозволяє суттєво зменшити загрози і атаки на шифрограми статистичного шифрування.

Ітеративний код с перевіркою на парність має мінімальну кодову відстань між дозволеними кодовими комбінаціями $d_0 = 4$. При цьому здатність коду по виявленню помилок $t_{\text{вияв}} = d_0 - 1 = 4 - 1 = 3$. Виправляюча здатність коду $t_{\text{випр}} = 1$. Даний код здатний виправляти однократну помилку або фіксувати помилки за допомогою синдромів по строкам та стовпчикам.

Розглянемо наступний рівень інтеграції статистичного шифрування і завадостійкого коду з декореляцією помилок. Як правило, декореляція помилок не використовувалася для завдання захисту інформації від НСД. Основна ідея декореляції помилок спрямована на зниження ймовірності виникнення групових помилок, які можуть виникати через випадкові завади у каналі зв'язку. Декореляція виконується шляхом перестановки певної послідовності біт кодових блоків на певну відстань, щоб вони не йшли один за одним в каналі передавання. Такий спосіб передавання біт кодових блоків дозволяє уникати випадків, коли, наприклад, імпульсна завада, спричиняє групову помилку, що збільшує кратність помилок. Велика кратність помилок у кодових блоках не дозволяє виправляти помилки завадостійким кодом з малою корегувальною здатністю. Таким чином, щоб не збільшувати надлишковість завадостійкого коду доцільним є використання декореляції помилок.

В приймачі після прийому сигналу порядок біт у кодових блоках відновлюється, а помилки розподіляються по іншим комбінаціям повідомлення. Це призводить до зменшення кратності помилок у кодових блоках та дозволяє ефективніше їх виправляти за допомогою коригуючих кодів. На рис. 3.3 надано принцип декореляції помилок із збереженням порядку розміщення біт у кодових блоках.

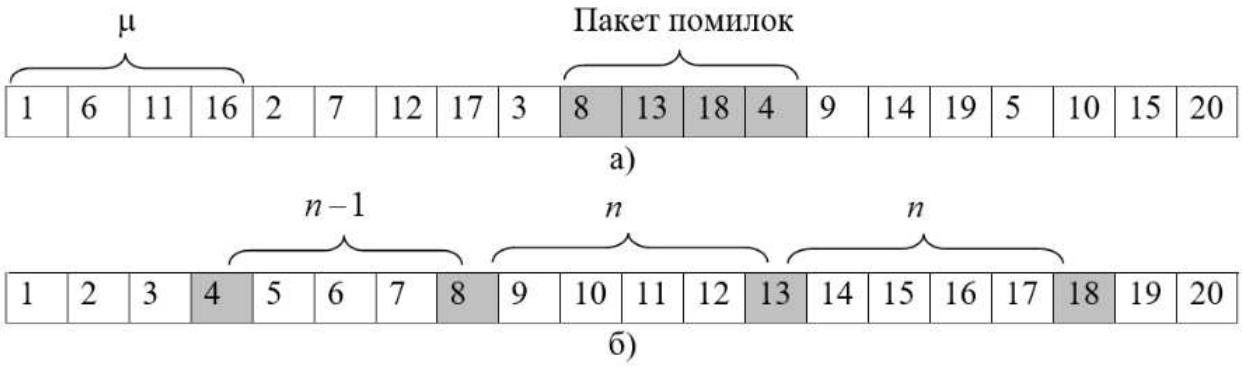


Рис. 3.3. Принцип декореляції помилок із збереженням порядку розміщення біт у кодових блоках

З рис. 3.3 бачимо, що при цьому методі декореляції помилок відбувається найпростіший перерозподіл біт по кодовим блокам. Для підвищення загальної криптостійкості методу статистичного шифрування пропонується перед початком декореляції виконати в межах кодових блоках перестановку біт за певними правилами $П_1$, $П_2$ … $П_N$, а потім робити їх перенесення по кодовим блокам, як це представлено на рис. 3.4. З урахування цього можна запропоновувати декореляцію помилок з вбудованою функцією шифрування.

Рис. 3.4. Метод декореляції помилок з функцією шифрування

Таким чином, інтеграцію статистичного шифрування, завадостійкого кодування та декореляцію помилок можна представити як систему захисту від НСД та випадкових завад, яка складається з трьох ступенів. При цьому на кожній ступені використовується певна надлишковість і завдання по захисту інформації. Характеристика рівнів інтегрованого захисту інформації від НСД та випадкових

завад надана в табл. 3.5. Бачимо, що на кожній ступені використовується певна надлишковість додаткових біт та забезпечується завдання по захисту інформації. На першій ступені статистичне шифрування забезпечує захист тільки від НСД та потребує для цього використання додаткових біт l, щоб згенерувати випадкові комбінації. При цьому від кількості l залежить криптостійкість методу шифрування. На другій ступені завадостійке кодування на основі ітеративного коду забезпечує захист від випадкових завад та за рахунок вкраплення перевірочних біт в структуру випадкових кодових блоків підвищує криптостійкість методу статистичного шифрування. На третій ступені декореляція помилок забезпечує підвищення завадостійкості за рахунок зменшення групування помилок у кодових блоках. Також на цій ступені забезпечується підвищення криптостійкості шляхом перемішування біт в межах кодових блоках за певними правилами $П_1$, $П_2$ … $П_N$.

Таблиця 3.5

Характеристика рівнів інтегрованого захисту інформації

№	Ступені захисту інформації	Склад кодового блоку		
		Кількість біт у комбінації	Додаткові біти	Характеристика
1	Статистичне шифрування	m	l	Захист від НСД
2	Завадостійке кодування випадкових комбінацій на основі ітеративного коду	$m + l$	r	Забезпечується завадостійкість та підвищується криптостійкість кодових блоків
3	Декореляція помилок	$m + l + r$	-	Сприяє підвищенню криптостійкості та завадостійкості

На рис. 3.5 надана схема інтеграції статистичного шифрування, завадостійкого кодування та декореляції помилок з наступними параметрами:

1) k – кількість біт у рядку після статистичного шифрування;

2) s – кількість кодових блоків у матриці;

3) $r_{\text{заг}} = r_{\text{ряд}} + r_{\text{ст}}$ – загальна кількість перевірочних біт в рядках та стовпчиках ітеративного коду;

4) $k_{\text{заг}} = m \times s$ – загальна кількість біт для завдань завадостійкого кодування;

5) $n_{\text{заг}} = s(m + l) + r_{\text{заг}}$ – загальна кількість біт в ітеративному коді; – кількість перевірочних біт для кожного рядка та стовпця; – загальна кількість перевірочних елементів.

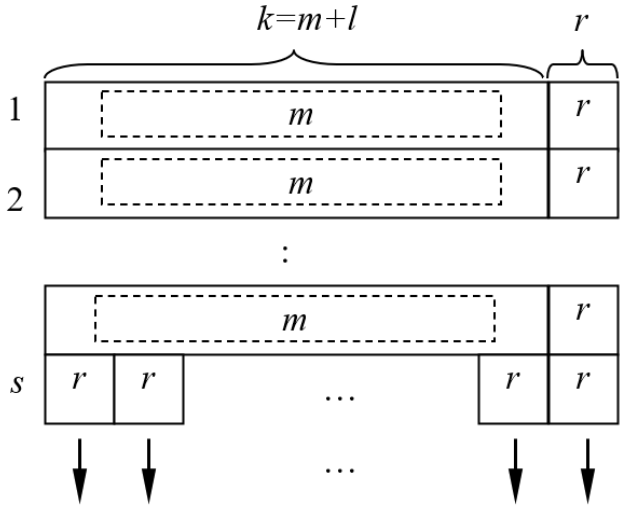


Рис. 3.5. Інтеграція статистичного шифрування, завадостійкого кодування та декореляції помилок

На рис. 3.6 надано структурну схему статистичного шифрування з інтеграцією завадостійкого кодування та декореляцією помилок, в якій параметри перетворення даних змінюються на кожній ступені за певними параметрами.

Джерело інформації (ДІ) видає пристрою кодування (ПК) символи b_i , які перетворюються в кодові комбінації m. Далі кодові комбінації символів b_i перетворюються блоком випадкових комбінацій (БВК) у випадкові комбінації $k = m + l$. Ймовірнісний аналізатор (ІА) використовується для визначення ймовірнісних параметрів $p_j(u_j)$ символів b_i повідомлення використовуваного алфавіту ДІ. З урахуванням значень $p_j(u_j)$ для кожного символу b_i визначається кількість випадкових кодових комбінацій для БВК за допомогою кодової книги (КГ1). Загальна кількість випадкових комбінацій $N_{\text{заг}} = 2^k$ визначається з урахуванням надлишкових елементів l. Далі кожної інформаційної комбінації Q_i ставиться у

відповідність випадкова комбінація c_j, яка обирається за допомогою генератора випадкових чисел (ГВЧ) з сформованого ансамблю $C(c_j \in C)$. Пристрій завадостійкого кодування (ПЗК) формує матрицю з урахуванням параметрів, які надходять від кодової книги КГ2, поточний стан якої встановлюється за допомогою генератора псевдовипадкових чисел (ГПВЧ-1). Далі виконується завадостійке кодування з вкрапленням у послідовність значень перевірочних елементів. Матриця може змінювати свої розміри з урахуванням надаваних параметрів від КГ2. Пристрій перестановки (ПП) виконує зміну розташування біт в межах кодових блоків шляхом їх перемішування з урахуванням даних, які надходять від КГ3, поточний стан якої визначається ГПВЧ-2. Далі кодові блоки надходять на пристрій декореляції, в якому відбувається рознесення бітів кодових блоків на певний інтервал часу, що забезпечує зменшення групування помилок. За допомогою КГ3 та ГПВЧ-3 встановлюються поточні параметри пристрою декореляції.

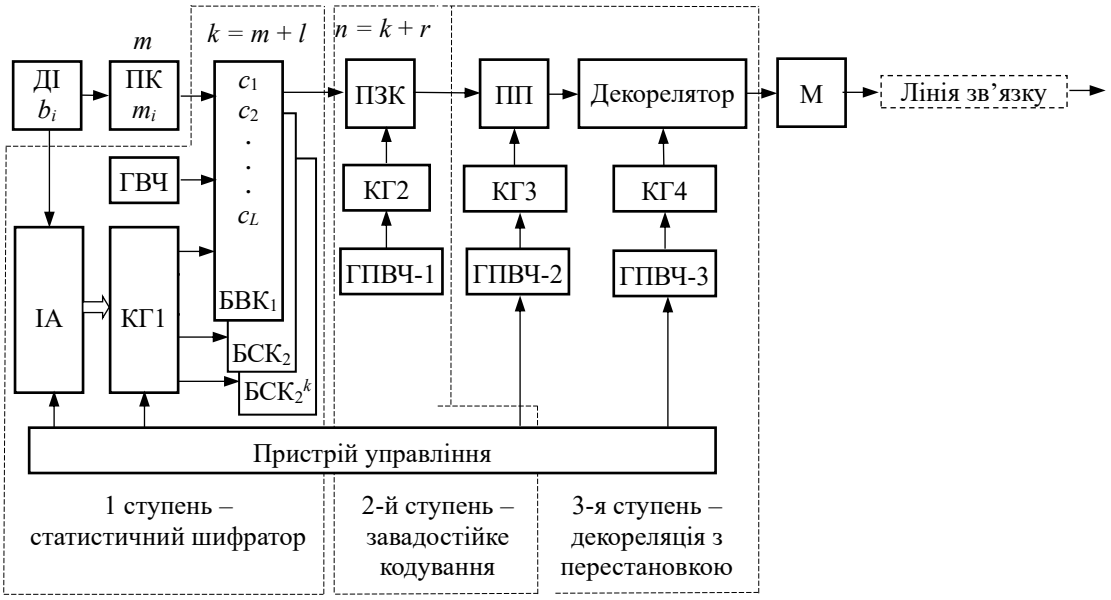


Рис. 3.6. Структурна схема системи статистичного шифрування з інтеграцією завадостійкого кодування з декореляцією помилок

Висновки до розділу 3

1. Проведено аналіз існуючих систем статистичного шифрування та визначені загальні їх недоліки, для яких характерна: висока надлишковість комбінацій шифрограм з метою забезпечення необхідної надійності передавання та захисту інформації від НСД; не в повній мірі враховується ентропія дискретного джерела інформації для формування випадкових комбінацій, що збільшує ймовірність успішних атак на шифрограми.

2. Визначено, що основною проблемою при застосуванні криптографічного захисту на основі статистичного шифрування є нерівномірність розподілу ймовірності появи символів в повідомленні, що вимагає враховувати ентропію дискретного джерела інформації при формуванні випадкових комбінацій.

3. Розглянуті можливі загрози і атаки на шифрограми статистичного шифрування. Для підвищення ефективності протидії частотному аналізу та іншим загрозам запропоновано алгоритм зменшення надлишковості випадкових комбінацій при збереженні або збільшенні криптографічної стійкості статистичного шифрування за умови, що при формуванні простору випадкових комбінацій E_i враховується ентропія дискретного джерела інформації. Для усунення недоліків статистичного шифрування та для підвищення його криптографічної стійкості запропоновано:

– використовувати перерозподіл випадкових кодових комбінацій з урахуванням ймовірності появи символів на виході джерела повідомлення. Це дозволить отримати на виході статистичного перетворювача шифрограми з рівномірним законом розподілу випадкових комбінацій;

– для зменшення надлишковості випадкових кодових комбінацій запропоновано інтегрувати завадостійке кодування таким чином, щоб надлишкові перевірочні біти одночасно використовувалися як для виявлення або корекції помилок, так і для збільшення розміру ансамблю випадкових кодових комбінацій.

4. Запропоновано використовувати декореляцію помилок не тільки для зменшення групування помилок у дискретному каналі, а також для завдання

захисту інформації від НСД. Для цього потрібно використовувати зміну розташування біт в межах кодових блоків шляхом їх перемішування по певному алгоритму.

5. Отримано подальший розвиток методів підвищення інформаційної прихованості та завадостійкості передавання інформації на основі інтегрованих методів перетворення даних: сумісного використання статистичного шифрування, завадостійкого кодування та декореляції помилок. Це дало змогу інтегрувати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі.

РОЗДІЛ 4
МЕТОДИ ФОРМУВАННЯ ШУМОПОДІБНИХ ТАЙМЕРНИХ СИГНАЛІВ

На основі таймерних сигнальних конструкцій досліджено методи формування шумоподібних сигналів. Обґрунтована доцільність використання непозиційних сигналів в системах радіозв'язку для забезпечення підвищення структурної та енергетичної прихованості. Такі системи спроможні ефективно працювати в умовах радіоелектронного конфлікту. Проаналізовано властивості таймерних сигнальних конструкцій для з’ясування переваг непозиційних сигналів перед позиційними по забезпеченню структурної прихованості. Розроблено методи розширення спектра на основі таймерних сигнальних конструкцій з можливістю зміни їх структури та параметрів.

4.1 Обґрунтованість розширення спектра таймерних сигналів

Забезпечення високого рівня завадозахищеності систем радіозв'язку [4, 103, 105] є одним із ключових напрямів захисту передаваних сигнальних конструкцій від перехоплення та НСД повідомлень. Поняття завадозахищеності охоплює сукупність показників, за якими оцінюється ефективність систем радіозв'язку. Основними характеристиками завадозахищеності є стійкість до радіозавад та високий рівень прихованості. Існують наступні типи прихованості: енергетична, структурна, інформаційна, просторова, тощо.

Ускладнення структури передаваного сигналу [4, 103] дозволяє розв'язати низку завдань щодо підвищення енергетичної та структурної прихованості сигнальних конструкцій. Це особливо важливо при перехопленні сеансу радіозв'язку засобами радіоелектронної розвідки супротивника. В завадозахищених системах радіозв'язку енергетична та структурна прихованість сигналів досягається шляхом використання шумоподібних сигналів (ШПС) [103, 105]. Для цього

застосовуються різні методи розширення спектра сигналу [102, 103, 105], такі як ППРЧ, пряме розширення спектра з використанням ПВП, ЛЧМ та інші. Відомо [99, 101], що основою для генерації ШПС є процес розширення спектра двійкової послідовності.

Сучасний розвиток теорії шумоподібних сигналів зараз спрямований на використання ТСК [79, 80, 87, 88, 97], які є непозиційними. Формування таких шумоподібних ТСК вимагає нових алгоритмів. Це пояснюється тим, що існуючі методи формування ШПС орієнтовані на позиційні сигнали. Впровадження таймерних шумоподібних сигналів є виправданим з огляду на необхідність використання більш складної структури сигналу для підвищення основних показників прихованості [93-96].

Таким чином, дослідження в галузі застосування таймерних шумоподібних сигналів є обґрунтованим для підвищення завадозахищеності каналу радіозв'язку [101]. Таймерні сигнали за особливістю їх побудови належать до класу непозиційних сигнальних конструкцій. Непозиційні сигнали забезпечують низку переваг порівняно з позиційними, але також вони мають певні недоліки. На основі ТСК є можливість реалізувати завадостійке кодування. За рахунок особливої структури ТСК не потрібно використовувати перевірочні біти. При формуванні сигнальних конструкцій за рахунок певних параметрів є можливість створювати різні ансамблі таймерних сигналів [97]. Такі можливості таймерних сигналів сприяють вирішенню завдань щодо забезпечення високого рівня основних показників прихованості сигнальних конструкцій [100, 101]. Таким чином, основною метою цього дослідження є синтез шумоподібних сигналів з урахуванням параметрів побудови ТСК.

4.2 Методи розширення спектра таймерних сигналів на основі псевдовипадкового перескоку робочої частоти

ППРЧ є один із методів розширення спектра сигналу, який використовується для підвищення завадозахищеності радіозв'язку [99, 105]. При цьому методі

розширення спектра робоча частота передаваного сигналу змінюється за псевдовипадковим законом у достатньо великому діапазоні частот. Зміна несних частот досягається за допомогою певного алгоритму псевдовипадкового закону. Достатня висока завадостійкість методу ППРЧ забезпечується за рахунок постійної зміни несної частоти, що ускладнює створення цілеспрямованих завад для придушення передаваних сигналів. Енергетична прихованість методу ППРЧ забезпечується завдяки зміні несної частоти, що ускладнює виявлення та перехоплення такого сигналу. Для успішного перехоплення такого сигналу необхідно синхронізуватися з частотними змінами сигналу, що майже неможливо без доступу до псевдовипадкового закону несної частоти. Метод ППРЧ широко використовується у військових системах радіозв'язку, супутникових і мобільних мережах, де потрібна підвищена безпека і стійкість до завад.

Існує кілька методів ППРЧ [99], які відрізняються за способом зміни частоти та алгоритмами генерації псевдовипадкового закону. Основні методи ППРЧ можуть бути наступними [99]:

1) повільний метод ППРЧ, при якому частота змінюється рідше, ніж відбувається передача символів даних. При такому алгоритмі кілька символів передаються на одній частоті, перш ніж вона зміниться. Цей метод ППРЧ використовується в умовах, коли потрібно більше часу для передавання кожного символу і де швидкі зміни частоти можуть бути небажаними. Він простіший в реалізації, але менш ефективний у протидії завадам порівняно з швидким ППРЧ;

2) швидкий метод ППРЧ, при якому частота змінюється швидше, ніж передаються символи даних. При цьому кожен символ може передаватися на різних частотах. Також можливий варіант, коли одна частота може використовуватися для передавання частини символу. Цей метод забезпечує достатньо високу завадостійкість і прихованість сигналу, оскільки складніше створити ефективну цілеспрямовану заваду чи виявити сигнал через постійні зміни несної частоти;

3) адаптивний метод ППРЧ, при якому зміна несної частоти залежить від умов середовища. Система може «пропускати» частоти, які зазнають сильних завад або зайняті іншими передавачами. Цей метод використовується для підвищення

ефективності передавання в складних умовах РЕБ, де необхідним є уникнення від дії інтенсивних радіозавад;

4) комбінований метод ППРЧ, якій поєднує повільний і швидкий ППРЧ для забезпечення більш гнучкого управління несною частотою в залежності від ситуації. Такий метод ППРЧ використовується для досягнення оптимального балансу між завадостійкістю та ефективністю передачі;

5) синхронний метод ППРЧ, в якому передавач і приймач змінюють несну частоту синхронно, використовуючи одну й ту саму псевдовипадкову послідовність для перемикання. Такий метод використовується в умовах, де важлива висока точність синхронізації в радіоканалі;

6) в асинхронному методі ППРЧ передавач і приймач частота змінюється незалежно, що ускладнює перехоплення і підвищує завадозахищеність. Цей метод використовується в системах, де потрібна додаткова стійкість до радіоелектронного придушення.

Розглянуті методи ППРЧ можуть бути використані для певних завдань в залежності від вимог до завадостійкості, прихованості та ефективності передавання сигналу. Розглянемо можливість адаптації методу ППРЧ к розширенню спектра ТСК.

При використанні швидкого методу ППРЧ час передачі одного біту t_0 позиційного коду на одній несній частоті може бути [99]:

$$t_{\text{пер}} \leq t_0. \tag{4.1}$$

Для повільного методу ППРЧ на одній несній частоті $\Delta f_{\text{ппрч}}$ передається кілька біт позиційного коду:

$$t_{\text{пер}} > t_0. \tag{4.2}$$

Враховуючи особливість побудови таймерного сигналу [79] виконаємо розширення його спектра з використанням ППРЧ. У таймерного сигналу базовим

елементом побудови його сигнальної конструкції є інтервал часу Δ. Для визначення тривалості імпульсів таймерного сигналу задається деякий часовий інтервал побудови [79]:

$$T_c = nt_0, \tag{4.3}$$

де n – кількість бітових елементів Найквіста з тривалістю t_0. Тривалість імпульсів в межах інтервалу T_c складає:

$$t_c = t_0 + \Delta \times l\ , \tag{4.4}$$

де $l \in 0, 1, 2, 3, \ldots$ і парне $\Delta = t_0/s$ ($s \in 2, 3, \ldots k$).

Тривалість імпульсів таймерних сигналів, тобто відстань між ЗММ ($t_c \geq t_0$) не менша за інтервал Найквіста ($t_0 = 1/\Delta F_c$) і парна значенню Δ. Виконання такої умови формування імпульсів усуває міжсимвольні спотворення в таймерних сигналах. Значення s показує кількість Δ на інтервалі часу t_0. Значення i відображає кількість ЗММ в межах таймерного сигналу, яке може змінюватися $i = 1,2,\ldots,n-1$. На рис. 4.1 (а) представлена часова діаграма ТСК на інтервалі часу $T_c = 4t_0$.

З рис. 4.1. можна побачити, що тривалість імпульсу t_c в межах ТСК може бути більше значення t_0. Це означає, що застосувати умову (4.1) або (4.2) для розширення спектра ТСК методом швидкої або повільної ППРЧ не представляється можливим. Проблемою використання цих методів є непозиційність ЗММ в таймерному сигналі по відношенню до інтервалу Найквіста t_0.

4.3 Розширення спектра таймерних сигналів за допомогою швидкого методу псевдовипадкового перескоку робочої частоти

Розглянемо варіант розширення спектра ТСК [99] тривалістю передачі несної частоти $t_{\text{пер}} < t_0$ та $t_{\text{пер}} \leq \Delta$. Це забезпечить реалізацію швидкого методу ППРЧ з використанням інтервалу Δ для передавання кількох несних частот. Для цього методу спочатку використовується пряме розширення спектра таймерного сигналу за допомогою ПВП $c(T_c)$ (рис. 4.1 б) з інтервалом часу імпульсу τ. Спектр таймерного сигналу $x_{\text{тск}}(t_c)$ розширюється за допомогою елементів:

$$\tau = \Delta / j, \tag{4.5}$$

де j =1, 2, 3, … – кількість елементів з тривалістю τ на інтервалі часу Δ.

Таймерний сигнал за допомогою ПВП $c(T_c)$ (рис. 4.1 (б)) перетворюється в широкосмуговий сигнал (рис. 4.1 (в)) за наступною формулою:

$$x_{\text{скк}}(T_c) = x_{\text{тск}}(t_c) \times c(T_c). \tag{4.6}$$

Після цього виконується додаткове розширення спектра вже широкосмугового таймерного сигналу $x_{\text{скк}}(T_c)$ за допомогою швидкого методу ППРЧ (рис. 4.1 (г)):

$$u'(t) = x_{\text{скк}}(T_c) U_0 \, cos(\omega(g(t)t)), \tag{4.7}$$

де $cos(\omega(g(t)t))$ – ансамбль частот, що є функцією кодового сигналу $g(t)$.

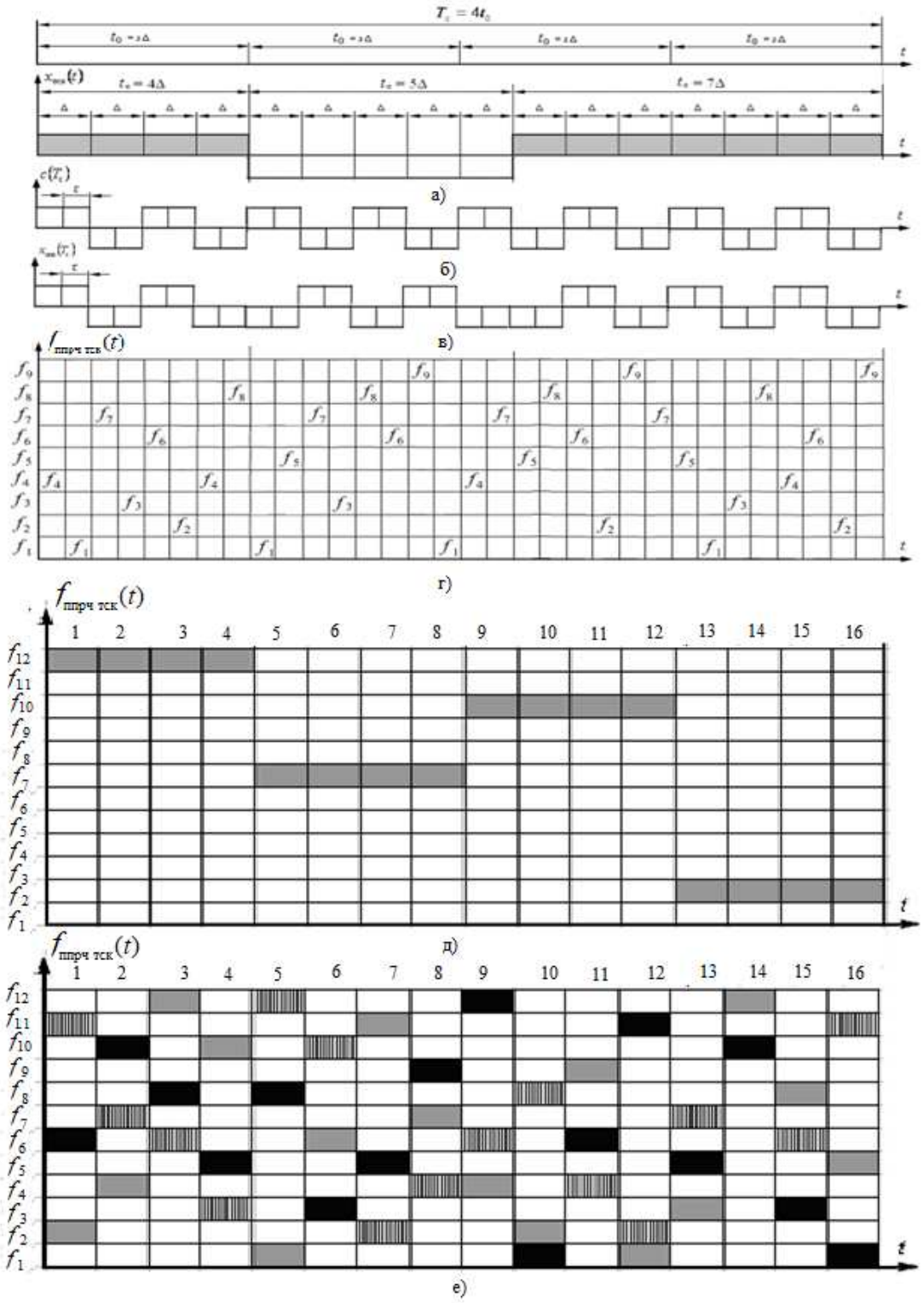


Рис 4.1. Розширення спектра таймерного сигналу $x_{\text{тск}}(t_c)$ за допомогою ПВП (в), швидким (г), повільним (д) та багатоканальним (е) методами ППРЧ на інтервалі $T_c = 4t_0$

4.4 Розширення спектра таймерних сигналів за допомогою повільного методу псевдовипадкового перескоку робочої частоти

Для повільного методу ППРЧ швидкість зміни несної частоти більше інтервалу Найквіста t_0 в кілька разів. В таймерних сигналах $\Delta < t_0$, тому час зміни несної частоти $T_{\text{М ППРЧ}}$ для повільного методу ППРЧ [99] визначається з урахуванням тривалістю часу елемента Δ, тобто:

$$T_{\text{М ППРЧ}} = \Delta z, \tag{4.8}$$

де $z = 2,3,\ldots, M$ – кількість Δ на часовому інтервалі $T_{\text{М ППРЧ}}$; $M = ns$.

При визначенні інтервалу зміни несної частоти слід враховувати, що при збільшенні значення $T_{\text{М ППРЧ}}$ ймовірність ураження в радіоканалі передаваного сигналу завадою підвищується. На рис. 4.2 (д) представлена процедура розширення спектра ТСК повільним методом ППРЧ з інтервалом $T_{\text{М ППРЧ}} = 4\Delta$, де $z = 4$. Якщо $z = M$, тоді зміна несної частоти буде на інтервалі кожної СКК:

$$T_{\text{М ППРЧ}} = T_c, \tag{4.9}$$

Отримаємо, що згідно умови (4.9) кожна складова сигнальної конструкції таймерного сигналу передається на певній несній частоті.

Для визначення ЗМВ фронтів таймерних сигналів [99, 101] в системі радіозв'язку потрібно використовувати маніпуляцію елементів сигнальної конструкцій на інтервалі часу Δ або τ за умови, що $\tau \neq \Delta$. Для цього можна використати наступні види маніпуляції: ФМ-2, ФМ-4 або КАМ-4. За допомогою ФМ-4 або КАМ-4 збільшується швидкість передачі інформації в порівнянні з ФМ-2. Проте, використання КАМ-8 або КАМ-16 може призвести до зниження завадостійкості, тобто потрібно враховувати потоковий стан радіоканалу для визначення умови передавання сигналу.

Для швидкого методу ППРЧ (рис. 4.2 (в)) часовий інтервал несної частоти $T_{\text{Б ППРЧ}}$ співпадає або менше часового елемента Δ:

$$T_{\text{Б ППРЧ}} \leq \Delta. \tag{4.10}$$

Потрібно враховувати той факт, що швидкий метод ППРЧ забезпечує високу завадостійкість. Наприклад, у випадку дії вузькосмугової радіозавади, спотворюються лише частина сигнальної конструкцій у деякому підканалі. Таким чином, не має повного спотворення сигналу тому що рівень імпульсу в межах $t_c = t_0 + k\Delta$ передається декілька разів по Δ на різних підканалах. Таке спотворення може призвести до дроблення одного або декількох імпульсів сигнальної конструкції, що виправляється при деманіпуляції сигналу в приймачі.

При повільному методі ППРЧ впливання вузькосмугової завади може призвести до більшого спотворення ТСК в неможливості його відновлення в приймачі. Реалізація цього методу більш простіша, ніж швидкий метод ППРЧ.

4.5 Розширення спектра таймерних сигналів за допомогою багатоканального методу псевдовипадкового перескоку робочої частоти

На рис. 4.1 (е) представлена діаграма багатоканального швидкого методу ППРЧ розширення спектра ТСК. Шляхом передачі одного стану сигнальної конструкції елемента Δ на різних несних частотах f_i забезпечується підвищення завадостійкості системи радіозв'язку. Доцільним є використання непарного числа підканалів f_i: w = 3, 5 або 7 (рис. 4.1 г). Це дозволить за мажоритарним підходом аналізувати прийнятий елемент сигнальної конструкції Δ. Такий спосіб оцінки якості прийнятого елемента додатково підвищить завадостійкість системи радіозв'язку. Рішення про стан прийнятого сигналу буде здійснюватися за допомогою таймерного декодування, при якому визначається його приналежність до підмножини дозволених комбінацій.

На рис. 4.2 представлена структурна схема системи зв’язку з таймерними шумоподібними сигналами. Пристрій завадостійкого кодування (ПЗК) отримає від джерела повідомлення (ДП) двійкову послідовність РЦК k. В результаті завадостійкого кодування ПЗК додає перевірочні біти r до інформаційної послідовності для формування загальної комбінації:

$$n = k + r. \tag{4.11}$$

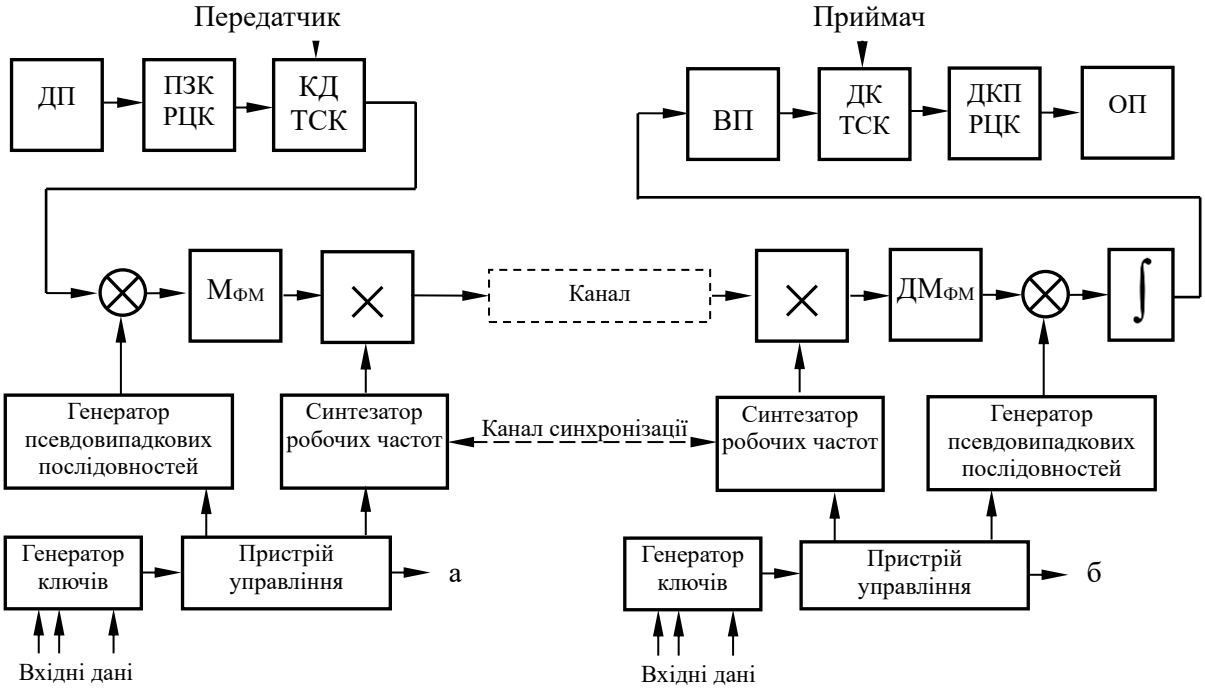


Рис. 4.2. Структурна схема системи зв’язку з таймерними шумоподібними сигналами

Далі закодовані завадостійким кодом комбінації потрапляють на кодер таймерних сигналів (КДТСК), де відбувається формування таймерних сигналів, які потім подаються на помножувач ⊠. Помножувач виконує розширення спектра ТСК за допомогою ПВП. Як ПВП можуть бути використані послідовності Уолша або послідовності з невизначеною структурою. Формування шумоподібного сигналу відбувається за рахунок фазової маніпуляції в пристрої $М_{ФМ}$, на який поступає послідовність з виходу помножувача.

В наданому алгоритмі використовується інтеграція двох методів розширення спектра ТСК: ПРС за допомогою ПВП та швидкого методу ППРЧ. Параметри ТСК формуються завдяки пристрою генераторів ключів на основі вхідних даних, що вводяться користувачем.

4.6 Розширення спектра таймерних сигналів за допомогою лінійної частотної модуляції

Особливість ЛЧМ [4,5] полягає в тому, що при модуляції біту тривалістю t_0 несна частота сигналу змінюється за лінійним законом:

$$s_{\text{ЛЧМ}}(t) = U_0 \cos\big(\phi_0 + \phi(t)\big) = U_0 \cos\left(\phi_0 + 2\pi\left(f_0 t + \frac{b}{2}t^2\right)\right), \qquad (4.12)$$

де U_0 – амплітуда сигналу; $f_0 = (F_{\max}+F_{\min})/2$ – центральне значення несучої частоти; $b = (F_{\max}+F_{\min})/T_c$ – параметр, що дорівнює швидкості зміни частоти в часі; T_c – тривалість сигналу; $F_{\max}$, $F_{\min}$ – максимальне та мінімальне значення частоти радіосигналу; ϕ_0 – початкова фаза. При цьому використовується лінійно зростаючий та спадаючий закони зміни частоти для передавання логічного нуля та одиниці.

Проте використати аналогічний алгоритм ЛЧМ для таймерного сигналу не представляється можливим, тому що базовим елементом для формування сигнальної конструкції є часовий інтервал Δ, який менше за t_0. ЗММ імпульсів в таймерному сигналі [102, 103] на відміну від РЦК кратні ні t_0, а деякому базовому часовому елементу Δ (де $\Delta = t_0/s$; $s = 1,\ 2,\ 3,\ \ldots,\ l$ – цілі числа). Тривалість імпульсів таймерних сигналів не менше інтервалу Найквіста, тобто $t_c = t_0 + k\Delta$ (де $k = 0{,}1,\ 2,\ \ldots,\ s\cdot(n-2)$). На інтервалі $T_c = 4t_0$ (рис. 4.3, а) надано приклад формування ТСК (рис. 4.3, б).

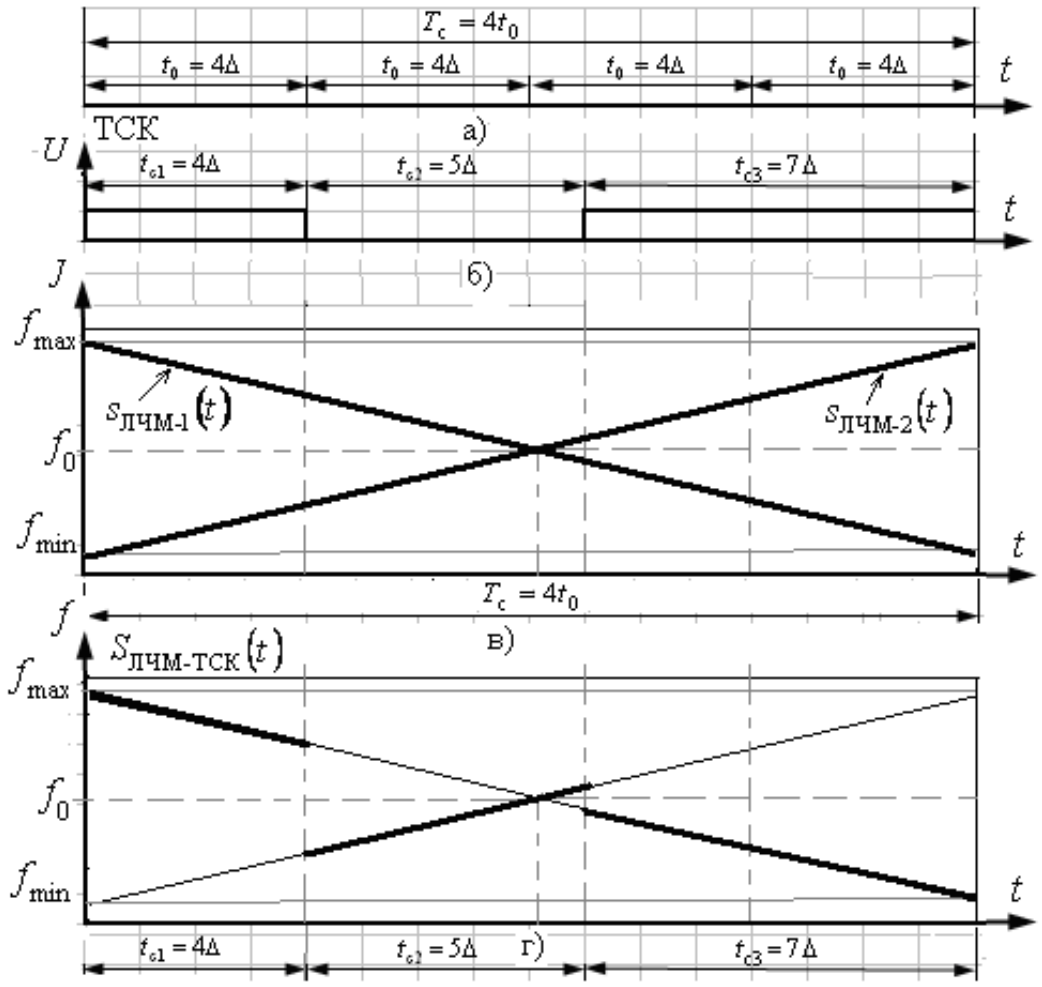


Рис. 4.3. Часові діаграми формування широкосмугових ТСК на основі ЛЧМ

На рис. 4.3 (г) представлена часова діаграма розширення спектра таймерного сигналу за допомогою двох несних частот $S_{ЛЧМ\text{-}1}(t)$ і $S_{ЛЧМ\text{-}2}(t)$. Бачимо, що процес перемикання двох генераторів ЛЧМ передавача (рис. 4.4) залежить від стану імпульсів в межах сигнальної конструкції. При цьому передбачається, що система повинна мати ідеальну тактову синхронізацію за елементами Δ, а відновлення фронтів таймерних сигналів здійснюється на інтервалі $T_c = 4t_0$. Для прийому таймерного ШПС застосовуються два кореляційних приймача з опорними ЛЧМ сигналами $S_{ЛЧМ\text{-}1}(t)$ і $S_{ЛЧМ\text{-}2}(t)$ (рис. 4.5).

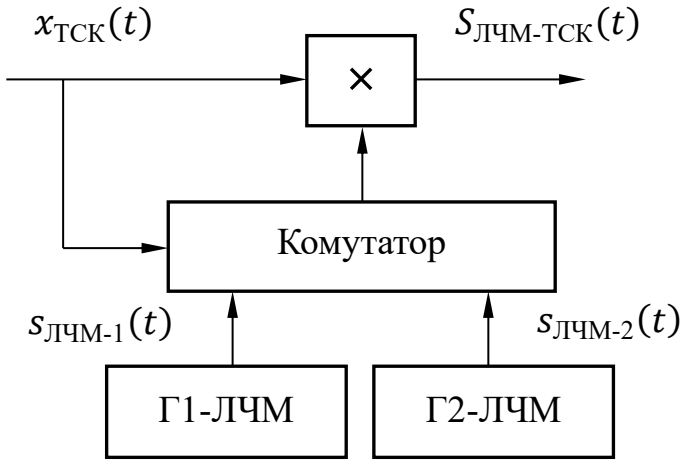


Рис. 4.4. Структурна схема передавача таймерних широкосмугових сигналів на основі ЛЧМ

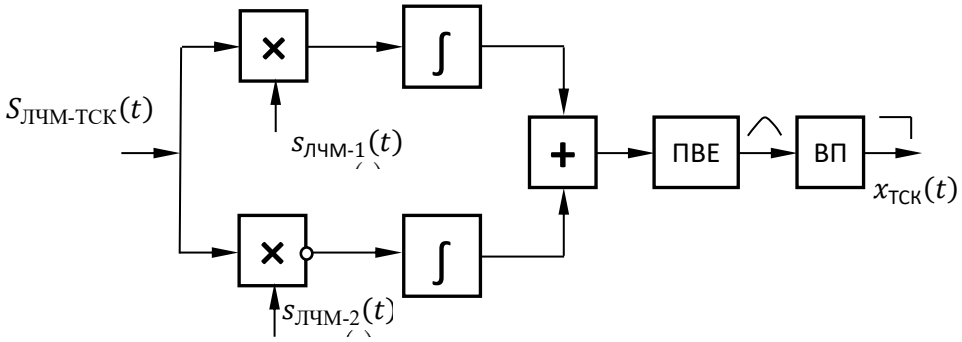


Рис. 4.5. Структурна схема кореляційного приймача таймерних широкосмугових сигналів на основі ЛЧМ

Результуючий сигнал з виходу пристрою складання «+» надходять на вхід пристрою визначення екстремуму (ПВЕ). З виходу ПВЕ по максимальним та мінімальним рівням напруги сигналу в межах інтервалу Δ за допомогою вирішального пристрою (ВП) приймається рішення о передніх і задніх фронтів ТСК. При цьому через кожен інтервал часу $T_c = 4t_0$ здійснюється обнуління стану інтеграторів приймача імпульсами циклової синхронізації.

Розглянемо імітаційне моделювання лінійно-модульованих таймерних сигналів в умовах передавання по каналу з шумом. На рис. 4.6 надано часові діаграми відновлення фронтів таймерного сигналу з використанням кореляційного приймача: (а) – шумоподібний таймерний сигнал $U_{\text{шпс}}$ на вході приймача $h = P_c/P_i = 0{,}25$;

(б) – вихід інтегратора кореляційного приймача; (в) – відновлення фронтів таймерних сигналів по максимальним та мінімальним пікам напруги сигналу з виходу інтегратора «∫». З діаграм бачимо, що відновлення фронтів сигналу можливо навіть за умови, коли шум набагато більше корисного сигналу.

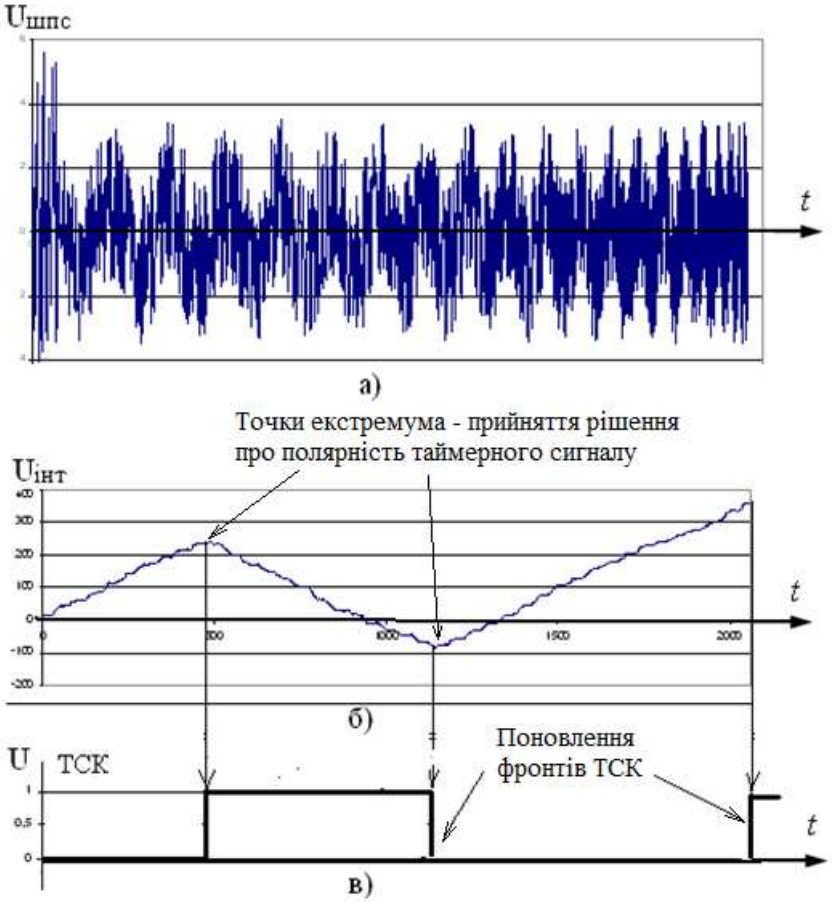


Рис. 4.6. Відновлення фронтів таймерного сигналу з використанням кореляційного приймача: а) ЛЧМ сигнал на вході приймача $h = P_c/P_ш = 0{,}25$;
б) вихід інтегратора кореляційного приймача; в) відновлення фронтів ТСК по пікам сигналу з виходу інтегратора

Таким чином, результати отриманих досліджень в роботі дозволяють встановити наступне: можливість синтезу шумоподібних таймерних сигналів на основі ЛЧМ; застосування кореляційного прийому для виділення фронтів ТСК; забезпечення енергетичної прихованості, тобто можливість передавання за умови, що шум набагато більше корисного сигналу в каналі.

Висновки до розділу 4

1. Використання непозиційних сигналів, прикладом яких є таймерні сигнальні конструкцій, дозволяє вирішити завдання підвищення основних показників завадозахищеності при формуванні шумоподібних сигналів.

2. Запропоновано використовувати комбіноване розширення спектра таймерних сигналів з використанням ПРС за допомогою ПВП та методу ППРЧ. Такий підхід розширення спектра дозволить підвищити структурну прихованість сигнальних конструкцій у випадку використання ПВП невідомої структури вже на першому етапі перетворення.

3. Другий етап розширення спектра пропонується виконувати за допомогою відомих методів ППРЧ. При цьому потрібно враховувати доцільність використання того або іншого методу з урахуванням умов передавання сигналу і складності реалізації системи зв'язку.

4. Запропоновано метод розширення спектра таймерних сигналів на основі ЛЧМ. Встановлена можливість застосування кореляційного прийому для виділення фронтів таймерного сигналу при відношенні сигнал-завада на вході приймача $h = P_c/P_i = 0{,}25$. Енергетична прихованість забезпечується за умови передавання сигналу, що шум перевішує корисний сигнал в 2-4 рази. Використання таймерних сигналів дає змогу збільшити структурну прихованість у порівнянні з розрядно-цифровим кодом.

ВИСНОВКИ

У дисертаційній роботі розв’язана актуальна науково-технічна задача, яка пов’язана з підвищенням прихованості передавання інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції позиційних та непозиційних сигналів з використанням статистичного шифрування, завадостійкого кодування, декореляції помилок, таймерних шумоподібних сигналів та хаотичних коливань.

До основних науково-практичних результатів, одержаних в дисертаційній роботі, можна віднести наступні:

1. Отримала подальший розвиток теорія динамічного хаосу для систем захисту та передавання конфіденційної інформації, що дало змогу в результаті досліджень дати оцінку варіаційним можливостям дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів, а також для систем маніпуляції, в яких для маскування процесу передавання непозиційних цифрових комбінацій використовуються хаотичні коливання. Встановлено, що незначні зміни параметрів дискретного генератора дають можливість створювати квазіортогональні послідовності чисел, взаємний коефіцієнт кореляції складає в межах $6{,}9\ 10^{-4}$ - $8{,}1\ 10^{-3}$.

2. Отримано подальший розвиток методів підвищення інформаційної прихованості та завадостійкості сигнально-кодових конструкцій на основі інтегрованих методів перетворення даних: сумісного використання статистичного шифрування, завадостійкого кодування та декореляції помилок. Це дало змогу інтегрувати в єдиний процес захист інформації від несанкціонованого доступу та випадкових завад в каналі. Так застосування декореляції помилок дозволили зменшити кратність помилок у кодових комбінаціях та використовувати режим

виявлення помилок великої кратності $t_{\text{вияв}} = 2 \ldots 3$ в сполученні з виправленням помилок кратністю $t_{\text{вип}} = 1$.

3. Вперше запропонований метод синтезу таймерних шумоподібних сигналів на основі ЛЧМ. Встановлена можливість застосування кореляційного прийому для виділення фронтів ТСК при відношенні сигнал-завада на вході приймача $h = P_c/P_i = 0{,}25$. Енергетична прихованість забезпечується за умови передавання сигналу, що шум перевішує корисний сигнал в 2-4 рази. Застосування таймерних сигналів дало змогу підвищити структурну прихованість у порівнянні з розрядно-цифровим кодом.

4. Розроблені методи синтезу шумоподібних сигналів ефективно реалізуються на практиці програмно-апаратними пристроями.

5. Розроблено низку програм для апаратно-програмного синтезу шумоподібних сигналів, які практично реалізують запропонований метод.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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).

2. Боднар І. Р. "Інформаційна безпека як основа національної безпеки." Mechanism of Economic Regulation 1 (2014): с. 68-75.

3. 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.

4. Горохов С.М. Критерії ефективності прихованих методів передачі / С.М. Горохов, М.В. Захарченко, В.В. Корчинський // Цифрові технології: Збірник / Кол. авт.: Одеса: Одес. нац. академія зв’язку ім. О.С.Попова, 2012. – Вип. 12. – С. 147-150.

5. Лісовський П.М. Криптосистема військ радіоелектронної боротьби України / П.М. Лісовський, Ю.П. Лісовська // Навчальні посібники, Військове право, Ліра-К, 2024. – 130 с.

6. Shamanov D. Аналіз сучасних методів радіоелектронної боротьби / D. Shamanov, A. Sorokin // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2024. – Т. 1 (75). – С. 211-214.

7. 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.

8. 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.

9. Камінський, А. А. Теорія і практика радіоелектронної боротьби: навчальний посібник. Київ: НАУ, 2016. – 240 с.

10. Тимошенко, В. І. Радіоелектронна боротьба: навчально-методичний посібник. Харків: ХНУПС, 2017. 176 с.

11. Сидоренко, О. В. Сучасні аспекти радіоелектронної боротьби: досвід і перспективи. Київ: ВПЦ "Київський університет", 2020. 220 с.

12. Poisel, R. A. Modern Communications Jamming: Principles and Techniques. Boston: Artech House, 2011. 450 p.

13. Наконечний Т. А., & Євграфов Д. В. (2018). Перехоплення сигналу витоку інформації з екрану монітора. Захист інформації, том 23, №3, липень-вересень 2021. С. 160-167.

14. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019.Вип. 19. 160 с.

15. Friedman, Avram. Cognitive Electronic Warfare: An Artificial Intelligence Approach. – Artech House Publishers, 2020. – 250 с.

16. Cooper, J., & McGill, K. Probability Methods of Signal and System Analysis. Cambridge University Press, 1987, – 376 p.

17. Лізунов С. І., Кадулін М. О. Використання аналізаторів спектра для захисту інформації. Запорізький національний технічний університет. Тиждень науки-2019. Факультет радіоелектроніки та телекомунікацій. Збірник тез доповідей щорічної науково-практичної конференції. 15-19 квітня 2019 року. – С. 110-112.

18. Adamy, D. L. EW 101: A First Course in Electronic Warfare. Boston: Artech House, 2001. 320 p.

19. Poisel, R. A. Modern Communications Jamming: Principles and Techniques. Boston: Artech House, 2011. 450 p.

20. Schleher, D. C. Electronic Warfare in the Information Age. Boston: Artech House, 1999. 550 p.

21. Knott, E. F., Shaeffer, J. F., Tuley, M. T. Radar Cross Section. 2nd ed. Boston: Artech House, 2004. 590 p.

22. Математичні основи оптимізації телекомунікаційних систем: підручник. За загальною редакцією Захарченко М.В. / Захарченко М.В., Горохов С.М., Балан М.М., Гаджієв М.М., Корчинський В.В., Ложковський А.Г. Одеса: ОНАЗ ім. О.С. Попова, 2010. – 240 с.

23. Proakis, J. G., & Manolakis, D. K. Digital Signal Processing: Principles, Algorithms, and Applications. – 4th ed. – Upper Saddle River, NJ: Prentice Hall, 2007. – 1002 p.

24. Sklar, B. Digital Communications: Fundamentals and Applications.* – 2nd ed. – Upper Saddle River, NJ: Prentice Hall, 2001. – 1100 p.

25. Oppenheim, A. V., Willsky, A. S., & Nawab, S. H. Signals and Systems. – 2nd ed. – Upper Saddle River, NJ: Prentice Hall, 1996. – 957 p.

26. Кононович В.Г., Тардаскін М.Ф. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування // Захист інформації, № 1, 2006. – 18-30 с.

27. 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.

28. Лунтовський А.О. Мультисервісні мобільні платформи / А.О. Лунтовський, М.В. Захарченко, А.І. Семенко – К.: ПВП «Задруга», 2014. – 214 с.

29. 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.

30. Корчинський В.В. Прогнозування та оцінки ризиків інсайдерських загроз / Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В., Валигурський Ю.П. //«Перспективні напрями захисту інформації : Матеріали шостої міжнародної всеукраїнської наук. пр. конф.», тези доповідей. – м. Одеса, 02-06 вересня 2020 р. – Одеса, Бондаренко М.О. ОНАЗ, 2020. – С.64-65.

31. Корчинський В.В. Мінімізація ризиків інсайдерських загроз в системах захисту /В.В. Корчинський, Аль-Файюми Халед // Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів, ОНАЗ ім. О.С. Попова. Ч.І., Одеса, 12-14 грудня. – 2019. – С. 139.

32. Корчинський В.В. Ризики інсайдерських загроз у системах захисту інформації підприємств /В.В. Корчинський, Аль-Файюмі Х., Копитін Ю.В., Копитіна М.В.// Наукові праці ОНАЗ ім. О. С. Попова – Одеса: ОНАЗ, 2019, № 2. – С. 112-116.

33. Політанський, Л.Ф. Система передавання даних з використанням генераторів хаосу [Текст] / С. Д. Галюк, Л.Ф. Політанський, О. В. Гресь, Р. Л. Політанський // Радиотехника, 2011. – №164. – С. 66-71.

34. Pecora L.M. Synchronization in chaotic systems [Текст] / L. M. Pecora, T. L. Carroll // Phys. Rev. Lett, 1990. – Vol. 64. – № 8. – P. 821-824.

35. Mao, Y. Chaos-based image encryption. Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics / Y. Mao, G. Chen. – Springer-Verlag, NY. – 2004.

36. Pareek, N. K. Image encryption using chaotic logistic map / N. K. Pareek, P. Vinod, K. K. Sud // Image and Vision Computing. – 2006. –№ 24. – P. 926-934.

37. Pareek, N. K. Cryptography using multiple one-dimensional chaotic maps / N. K. Pareek, V. Patidar, K. Sud // Commun. Non-linear Sci. Numer. Simul. – 2005. – № 10(7). – P. 715-723.

38. Bo, M. A novel chaotic encryption scheme based on arithmetic coding / L. Xiaofeng, C. Yong // Chaos, Solitons and Fractals. – 2008. – № 38. – PP. 1523-1531.

39. Радзімовський Б. К. Синтез телекомунікаційних сигналів на основі хаотичних коливань : автореф. дис. ... канд. техн. наук : 05.12.13 / Б. К. Радзімовський; Одес. нац. акад. зв'язку ім. О.С. Попова. – Одеса, 2014. – 20 с.

40. Голевич О. Б. Спосіб детектування хаотичних сигналів в умовах дії завад / О. Б. Голевич // 14 міжнародній науково-технічній конференції «Вимірювальна та

обчислювальна техніка в технологічних процесах (ВОТТП_14_2015)» (Одеса, 5 - 9 червня 2015 р.).

41. Голевич О. Б. Застосування прямохаотичних надширокосмугових технологій у телекомунікаційних системах / О. Б. Голевич, О. С. Пивовар // Международная научно-практическая конференция Информационные процессы и технологии, 22-26 апреля, Севастополь, Украина, 2013г. – С 109.

42. Голевич О. Б. Дослідження використання хаотичних коливань для телекомунікацій інформаційних сигналів / О. Б. Голевич // 7-а Міжнародна науково – технічна конференція АПКТ-2013, 23 травня, Хмельницький, Україна, 2013 р. – С. 71.

43. Голевич О. Б. Результати порівняння деяких генераторів хаосу по кореляціним властивостям їх сигналів / О. Б. Голевич, О. С. Пивовар, І. В. Троцишин // 14 міжнародній науково-технічній конференції «Вимірювальна та обчислювальна техніка в технологічних процесах (ВОТТП_14_2015)» (Одеса, 5 - 9 червня 2015 р.).

44. Ruelle, D. Chance and Chaos. Translated from French. Izhevsk: R&C Dynamics, 2001. 192 p.

45. Crownover, R. Fractals and Chaos in Dynamic Systems. Translated from English. Moscow: Technosphere, 2006. 488 p.

46. Lukin K. A. Noise Radar Technology: The principles and short overview / K. A. Lukin // Appl. Radio Electronics. – 2005. – 4, N 1. – P. 4–13.

47. . Кислов В. Я. Новый класс сигналов для передачи информации. Широкополосные хаотические сигналы / В. Я. Кислов, В. В. Кислов // Радиотехника и электрон. 1997. – 42, № 8. – С. 962□973.

48. . Lukin K. A. New method for generation of quasi-orthogonal chaotic sequences / K. A. Lukin, V. Ye. Shcherbakov, D. V. Shcherbakov // Appl. Radio Electronics. – 2013. – 12, № 1. – P. 17–24.

49. Chaotic electronics in telecommunications / edited by M. P. Kennedy, R. Rovatti, G. Setti. – CRC Press, 2000. – 445 p.

50. Cuomo K. Circuit Implementation of Synchronized Chaos with Application to Communications / K. Cuomo, A. Oppenheim // Phys. Rev. Lett. – 1993. – 71, N 1. – P. 65–68.

51. Transmission of digital signals by chaotic synchronization / U. Parlitz, L. Chua, L. Kosarev et al. // Int. J. Bifurcation and Chaos. – 1992. – 2, N 4. – P. 973–977.

52. Бобало, Ю.Я. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р.Л. Політанський. – Дрогобич – Львів: Коло, 2015. – 184 с.

53. Політанський, Р.Л. Система передачі даних з використанням хаотичної маніпуляції / Р.Л. Політанський, Л.Ф. Політанський, О.В. Гресь, М. Г. Рождественська // IV Міжнародна науково-технічна конференція молодих вчених «Комп'ютерні науки та інженерія». – Львів, Україна. – 2010. – С. 127-128.

54. 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.

55. 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.

56. Politansky, L. Data Transmission System Using Pseudorandom Sequences / L. Politansky, R. Politansky, P. Shpatar, A. Gres // VII Міжнародна Науково-технічна конференція «Сучасні інформаційно-комунікаційні технології». – Ялта, Крим. – Жовтень, 2012. – С.76-78.

57. 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.

58. Шпатар, П. М. Система передавання даних з шифруванням хаотичними послідовностями / П. М. Шпатар, Р. Л. Політанський, О. В. Гресь, Є. І. Болонна // IV Міжнародна науково-практична конференція «Обробка сигналів і негаусівських процесів». – Черкаси, Україна. – Травень, 2013.

59. Іванюк, П.В. Оцінки чисельних характеристик систем детермінованого хаосу / П.В. Іванюк, Р.Л. Політанський // І-а Всеукраїнська науково-практична конференція «Фізико-технологічні проблеми радіотехічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки». – Чернівці, Україна. – Жовтень, 2011. – С. 107-110.

60. 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.

61. Dedieu H. Chaos Shift Keying Modulation and Demodulation of a Chaotic Carrier Using Self-synchronizing Chua's Circuits / H. Dedieu, M. P. Kennedy, M. Hasler // IEEE Trans. Circuits and Systems. – 1993. – 40, № 10. – P. 634–642.

62. Dmitriev A. S. Experiments on speech and music signals transmission using chaos / A. S. Dmitriev, A. I. Panas, S. O. Starkov // Int. J. of Bifurcation and chaos. – 1995. – 5, № 4. – P. 1249–1254.

63. Information transmission by chaotizing / F. Bohme, U. Feldman, W. Schwarz, A. Bauer // Proc. 2nd Int. Workshop on Nonlinear Dynamics of Electronic Systems (NDES'94). – Krakov, 1994. – P. 163–168.

64. Feldman U. Communication by Chaotic Signals: the Inverse System Approach / U. Feldman, M. Hasler, W. Schwarz // Int. J. on Circuit Theory and Applications. – 1996. – 24, Iss. 5. – P. 551-579.

65. Ryabov V. B. Chaotic masking without synchronization / V. B. Ryabov, P. V. Usik, D. M. Vavriv // Радиофизика и радиоастрономия. – 1997. – 2, № 4. – С. 473-479.

66. Schweizer J. Predictive Poincare Control: a Control Theory for Chaotic Systems / J. Schweizer, M. P. Kennedy // Phys. Rev. E. – 1995. – 52, Iss. 5. – P. 4865–4876.

67. Kolumban G. Nonlinear dynamics and chaotic behavior of sampling phase-locked loops / G. Kolumban, R. Vizvari // IEEE Trans. Circuits and Systems. – 1994. – 41, N 4. – P. 333-337.

68. Multi-User Communication using Chaotic Frequency Modulation / A. R. Volkovskii, S. C. Young, L. S. Tsimring, N. F. Rulkov // Proc. Int. Symp. Nonlinear Theory and Its Applications (NOLTA'01). – Miyagi, 2001. – P. 561–564.

69. Pecora L. M. Synchronization in Chaotic Systems / L. M. Pecora, T. L. Carroll // Phys. Rev. Lett. – 1990. – 64, N 8. – P. 821–824.

70. Kennedy M. P. Chaotic Modulation for Robust Digital Communications over Multipath Channels / M. P. Kennedy, G. Columban // Int. J. Bifurcation Chaos. – 2000. – 10, N 4. – P. 695–719.

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

72. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// Наукові праці ОНАЗ. – Одеса: ОНАЗ, 2020. – № 2, – P. – 65-69.

73. Корчинський В.В. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційними системах веб-сервісів / В.В. Корчинський, В.Й. Кільдішев, В.В. Онищук, Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». No 2 (02) 2021, - С. 195-201.

74. 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.

75. 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.

76. 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.

77. Blahut, R. Theory and Practice of Error Control Codes. Addison-Wesley, 1983. – 576 p.

78. Корчинський В.В., Казакова Н.Ф., Трінтіна Н.А. Аналіз статистики помилок у системах передавання зі змінними параметрами // Наукові праці ОНАЗ ім. О.С.Попова. – 2002. - № 1. С. 85-93.

79. 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.

80. Захарченко М.В. Порівняння синдромних методів для коригуючих блокових позиційних і таймерних кодів / М.В. Захарченко, М.М. Гаджієв, Б.К. Радзімовський, Ю. С. Горохов, Д. О. Шпак // Восточно-Европейский журнал передовых технологий. – 2014. – № 2/9(68). – С. 4–8.

81. Volodymyr Korchynskyi, Valerii Hordiichuk, Vitalii Kildishev, Oleksandr Riabukha, Sergii Staikutsa, Khaled Alfaiomi. Method of information protection based on the integration of probabilistic encryption and noise immune coding. – Radioelectronic and computer systems, 2023.4.13, P.184-185.

82. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. Constructing Symmetric Operations of Cryptographic Information Encoding. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021), October 26, 2021, Kyiv, Ukraine. CEUR Workshop Proceedings. 2022. P. 182-194.

83. Rudnytskyi V., Korchenko O., Lada N., Ziubina R., Wieclaw L., Hamera L. Cryptographic encoding in modern symmetric and asymmetric encryption. 2022 IEEE

26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2022) Procedia Computer Science 207 (2022) pp. 54–63.

84. Rudnytskyi V., Lada N., Pochebut M., Melnyk O., Tarasenko Ya. Increasing the cryptographic strength of CETencryption by ensuring the transformation quality of the information block. 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), October 13-15, 2023, Athens, Greece. 2023. P. 1-6.

85. Корчинський В.В. Метод захисту інформації на основі ймовірнісного шифрування / В.В. Корчинський, О.М. Рябуха, Х.О. Аль-Файюмі, А.Ю. Василенко // 78-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів, Одесса, ДУІЗ, 21-22 листопада 2023 року.

86. Volodymyr Korchynskyi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services / Valentyn Onyshchuk, Vitalii Kildishev, Volodymyr Korchynskyi and Khaled Alfaiomi // Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – Lviv-Slavske, Ukraine February 22-26, 2022 P. 331-334.

87. Корчинський В.В. Ефективність j-кратного повторення надлишкових таймерних сигнальних конструкцій / В.В. Корчинський, В.Й. Кільдішев, С.В. Хомич, Ю.В. Бєлова // Вестник НТУ «ХПИ». – Харьков: ХПИ, 2012. – Вип. 26. – С. 88-95.

88. Корчинський В.В. Ефективність трансформації швидкості передачі в нову якість у каналах зв'язку з моделлю Гільберта / В.В. Корчинський, В.Й. Кільдішев, М.М. Гаджієв // Наукові праці ОНАЗ ім. О. С. Попова, 2009, № 1. – С. 92–95.

89. Haykin, S. Communication Systems. – 5th ed. – Hoboken, NJ: John Wiley & Sons, 2009. – 608 p.

90. Lathi, B. P., & Ding, Z. Modern Digital and Analog Communication Systems. – 4th ed. – New York, NY: Oxford University Press, 2009. – 964 p.

91. Hsu, H. P. Schaum's Outline of Signals and Systems. – 3rd ed. – New York, NY: McGraw-Hill Education, 2014. – 504 p.

92. Захарченко М.В. Статистичні параметри спотворень таймерних сигнальних конструкцій в каналах моделі Гільберта / М В. Захарченко, О.М.Мартинова, Ю.С. Горохов, Д.Н. Бектурсунов, А.С. Кріль // Збірник наукових праць ОНАЗ ім. О. С. Попова. –2015. – № 1. – С. 42–47.

93. Горохов Ю.С., Оцінка потужності таймерних кодів з урахуванням кількості інформаційних відрізків і значення твірного елемента Δ / Ю.С. Горохов, Д.Н. Бектурсунов, М.В. Захарченко, В.В. Корчинський, Б.К. Радзімовський // Міжнародний науково-технічний журнал Вимірювальна та обчислювальна техніка в технологічних процесах. – 2015 – №2 – С. 198-201

94. Захарченко М.В. Ефективність прямого розширення спектра в системах зв'язку з таймерними сигналами / М.В. Захарченко, В.В. Корчинський, Б.К. Радзімовський, Ю.С. Горохов // Вісник НУ «Львівська політехніка». 2015. – № 818. – С.76-79.

95. Захарченко М.В. Кодове ущільнення при таймерних сигналах / М.В. Захарченко, Ю.С. Горохов, А.С. Кріль, С.В. Ковальчук // Науковий журнал. Сучасні інформаційні технології у свері безпеки та оборони. 2015. – № 3(24). – С.38-42.

96. Zakharchenko N.V. Assessing the Impact of the Noise on the Throughput Communication Channel with Timing Signals/ N.V. Zakharchenko, V.V. Korchinskiy, B.K. Radzimovskiy, D. N. Bektursunov, Y. S. Gorokhov // Eastern European Scientific Journal: AURIS Kommunikations- und Verlagsgesellschaft mbH. – Düsseldorf – Germany – 2015. - №4. - С. 209-214.

97. 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.

98. 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.

99. 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.

100. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012). – Lviv: Publishing House of Lviv Polyteshnic, 2012. – С. 317.

101. Корчинський В.В. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції /В.В. Корчинський Кільдішев В.И., Аль-Файюми Халед, Валігурський Ю.П // Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня - 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 31-33.

102. Корчинський В.В. Дослідження ефективності таймерних шумоподібних сигналів на основі лінійної частотної модуляції / Корчинський В.В., Рябуха О. М., Бердніков О.М., Аль-Файюми Халед, Поліщук К.В.// Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня - 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв'язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 27-30.

103. 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.

104. Shannon, C. E. A Mathematical Theory of Communication. – University of Illinois Press, 1948. – 144 pp.

105. V. Hordiichuk, V. Korchynskyi, V. Kildishev, B. Molodetskyi, S. Staikutsa and K. Alfaiomi, "Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare," 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024, pp. 1-4.

106. Голдвассер С., Мікалі С. Ймовірнісне шифрування та як грати в ментальний покер, зберігаючи в секреті всю часткову інформацію // *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*. – 1982. – С. 365–377.

107. Голдвассер С., Мікалі С. Криптографія та теорія обчислень. – К.: Видавництво «Наукова думка», 2016. – 320 с.

108. Молдован А. Гомофонний шифр: принципи побудови та застосування // *Журнал криптографічних досліджень*. – 2002. – №4. – С. 56–72.

109. Молдован А. Гомофонний шифр: Теоретичні основи та практичне застосування. – К.: Видавництво технічної літератури, 2002. – 250 с.

110. Мальцев Г. Н., Чернявський Є. В. Шляхи підвищення достовірності передачі повідомлень в умовах односторонньої радіопередачі // Системи і технології зв'язку, інформатизації та кібербезпеки. – 2021. – №1. – С. 56–72.

111. Гольдвассер Ш., Мікалі С. Ймовірнісне шифрування та семантична стійкість // *Журнал криптографічних досліджень*. – 1982. – №3. – С. 45–65.

112. Гольдвассер Ш., Мікалі С. Криптографія: Теоретичні основи та ймовірнісне шифрування. – К.: Видавництво технічної літератури, 2010. – 280 с.

113. Савчук М. М. Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень // *Звіт про науково-дослідну роботу*. – Київ: Фізико-технічний інститут, 2016. – 120 с.

ДОДАТКИ

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у фахових виданнях, що входять до переліку, затвердженого МОН України

1. Volodymyr Korchynskyi, Valerii Hordiichuk, Vitalii Kildishev, Oleksandr Riabukha, Sergii Staikutsa, Khaled Alfaiomi. Method of information protection based on the integration of probabilistic encryption and noise immune coding. – *Radioelectronic and computer systems*, 2023.4.13, P.184-185. http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2023.4.13. (**SCOPUS**)

2. 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.

https://www.viti.edu.ua/files/science/II_konf_2022/II_konf_2022_theses.pdf

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

https://vottp.khmnu.edu.ua/index.php/vottp/issue/view/9.

4. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// *Наукові праці ОНАЗ*. – Одеса: ОНАЗ, 2020. – № 2,

– P. – 65-69.

https://ojs.onat.edu.ua/index.php/sbornik_onat/issue/view/84.

5. Корчинський В.В. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційними системах веб-сервісів / В.В. Корчинський, В.Й. Кільдішев, В.В. Онищук, Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». No 2 (02) 2021, – С. 195-201.

https://ela.kpi.ua/server/api/core/bitstreams/69ad0866-c78c-47d3-a6d4-00369c3c478d/content.

6. Корчинський В.В. Ризики інсайдерських загроз у системах захисту інформації підприємств /В.В. Корчинський, Аль-Файюмі Х., Копитін Ю.В., Копитіна М.В.// *Наукові праці ОНАЗ ім. О. С. Попова* – Одеса: ОНАЗ, 2019, № 2. – С. 112-116.

Наукові праці, які засвідчують апробацію матеріалів дисертації

7. Volodymyr Korchynskyi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services / Valentyn Onyshchuk, Vitalii Kildishev, Volodymyr Korchynskyi and Khaled Alfaiomi // Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – Lviv-Slavske, Ukraine February 22-26, 2022 P. 331-334 (**SCOPUS**).

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

9. 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.

https://archive.interconf.center/index.php/conference-proceeding/article/view/5775

10. 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.

11. Корчинський В.В. Метод захисту інформації на основі ймовірнісного шифрування / В.В. Корчинський, О.М. Рябуха, Х.О. Аль-Файюмі, А.Ю. Василенко // 78-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів, Одесса, ДУІЗ, 21-22 листопада 2023 року. – С.154-156.

12. Корчинський В.В. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції /В.В. Корчинський Кільдішев В.И., Аль-Файюми Халед, Валігурський Ю.П // Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня – 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв’язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 31-33.

13. Корчинський В.В. Дослідження ефективності таймерних шумоподібних сигналів на основі лінійної частотної модуляції / Корчинський В.В., Рябуха О. М., Бердніков О.М., Аль-Файюми Халед, Поліщук К.В.// Перспективні напрямки захисту інформації: матеріали сьомої міжнародної науково-практичної конференції (м. Одеса, 30 серпня - 3 вересня 2021 р., м. Одеса), Державний університет інтелектуальних технологій і зв’язку. – Одеса-Тернопіль: Видавництво "Крок", 2021. – С. 27-30.

14. Корчинський В.В. Прогнозування та оцінки ризиків інсайдерських загроз / Корчинський В.В., Аль-Файюми Халед, Копитін Ю.В., Копитіна М.В., Валигурський Ю.П. //«Перспективні напрями захисту інформації: Матеріали

шостої міжнародної всеукраїнської наук. пр. конф.», тези доповідей. – м. Одеса, 02-06 вересня 2020 р. – Одеса, Бондаренко М.О. ОНАЗ, 2020. – С.64-65.

15. Корчинський В.В. Мінімізація ризиків інсайдерських загроз в системах захисту /В.В. Корчинський, Аль-Файюми Халед // Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів, ОНАЗ ім. О.С. Попова. Ч.І., Одеса, 12-14 грудня. – 2019. – С. 139.

Монографія

16. 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

ТОВ «АЙСАЙБЕРО», Україна, 65062, Одеська обл., місто Одеса, б. Французький, будинок 66/2, офіс 206, тел. +38(093)8234913, info@icybero.com

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

результатів дисертаційної роботи «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека

АЛЬ-ФАЙЮМІ ХАЛЕДА

Комісія у складі: директора Я.А. Семенюк, системного інженера Д. В. Головаченко, системного адміністратора І. Р. Савчинського.

Розглянувши результати дисертаційної роботи «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій», підтверджуємо, що основні наукові та практичні результати можуть застосовуватися в діяльності ТОВ «АЙСАЙБЕРО».

Зокрема, інтерес становлять такі розробки:

– метод підвищення криптографічної стійкості шифрограм на основі інтегрованих методів перетворення даних: сумісного використання статистичного шифрування, завадостійкого кодування та декореляції помилок;

–метод синтезу шумоподібних таймерних сигналів на основі лінійної частотної модуляції для підвищення енергетичної та структурної прихованості;

– метод формування початкових параметрів генераторів хаосу за допомогою гешування символів паролю користувача та перетворення геш-коду в потрібний діапазон чисел.

Директор Я.А. Семенюк

Системний інженер Д. В. Головаченко

Системного адміністратора І. Р. Савчинський

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Державного університету інтелектуальних технологій і зв'язку
проф. д-р. н. держ. управ.
_____ С.К. Хаджирадєва
«18» 11 2024 року

АКТ
впровадження результатів дисертаційної роботи
Аль-Файюмі Халеда
на тему: «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових 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 т ТЗІ Корчинський В.В., к.т.н. доц. каф. КБ та ТЗІ Кільдішев В.Й., к.ф.н. доц. каф. КБ та ТЗІ Стайкуца, секретар каф. КБ та ТЗІ викл. Шпильова М.І.,
склала цей акт про те, що результати дисертаційної роботи здобувача кафедри кібербезпеки та технічного захисту інформації Аль-Файюмі Халеда на тему «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» впроваджені у навчальний процес на кафедрі кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку.
Матеріали дисертації увійшли до складу дисциплін «Забезпечення кібербезпеки у ЗСУ» і «Теоретичні основи передавання та захисту інформації», що викладаються на факультеті інформаційних технологій та кібербезпеки студентам четвертого курсу першого (бакалаврського) рівня, які навчаються за напрямом підготовки спеціальності 125 Кібербезпека та захист інформації.

Голова комісії:
Декан факультету ІТК ДУІТЗ,
д.т.н., проф. Василіу Є.В.

Члени комісії:
д.т.н., проф. зав. каф. КБ та ТЗІ Корчинський В.В.

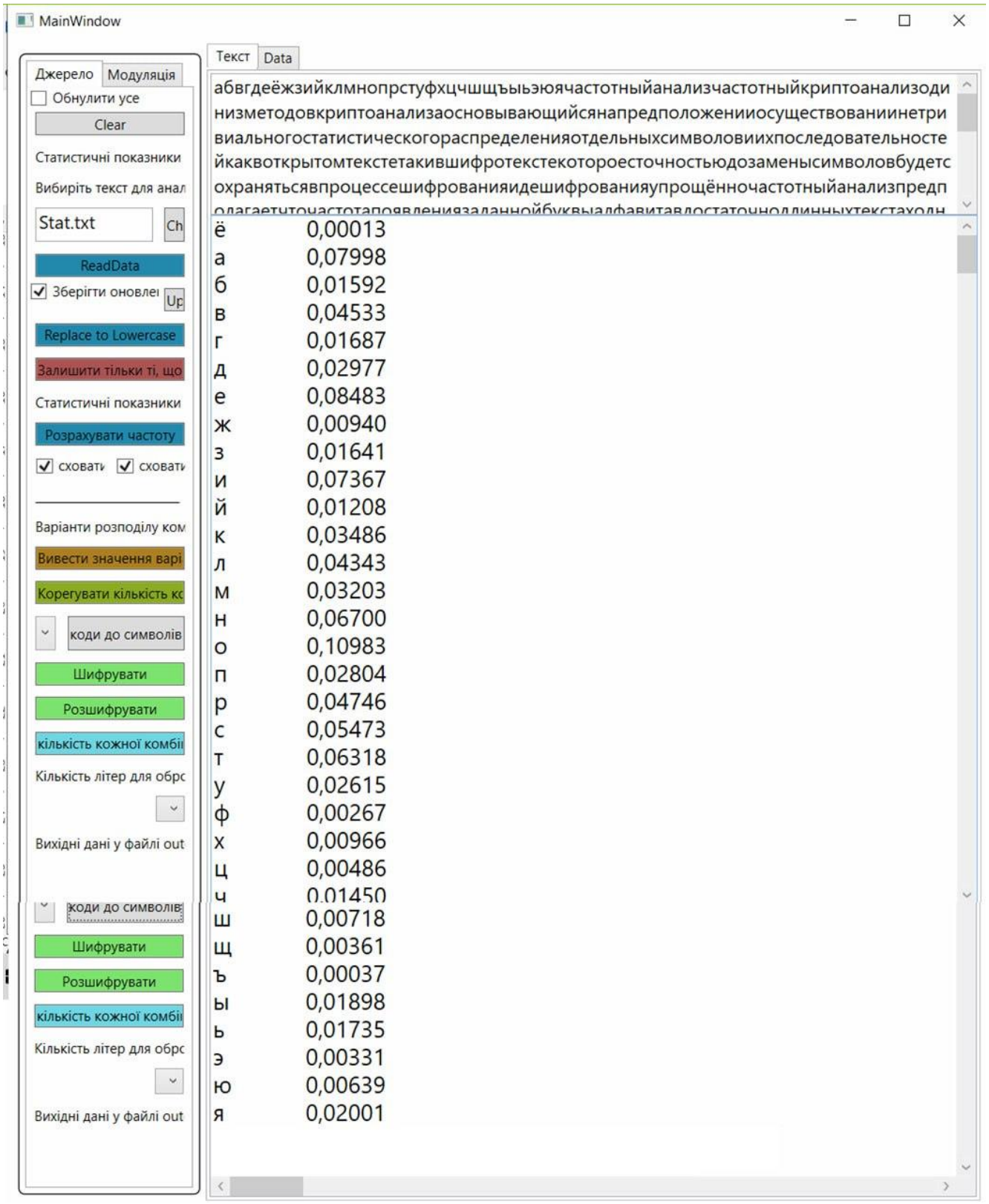
д.т.н., доц. каф. КБ та ТЗІ Кільдішев В.Й.

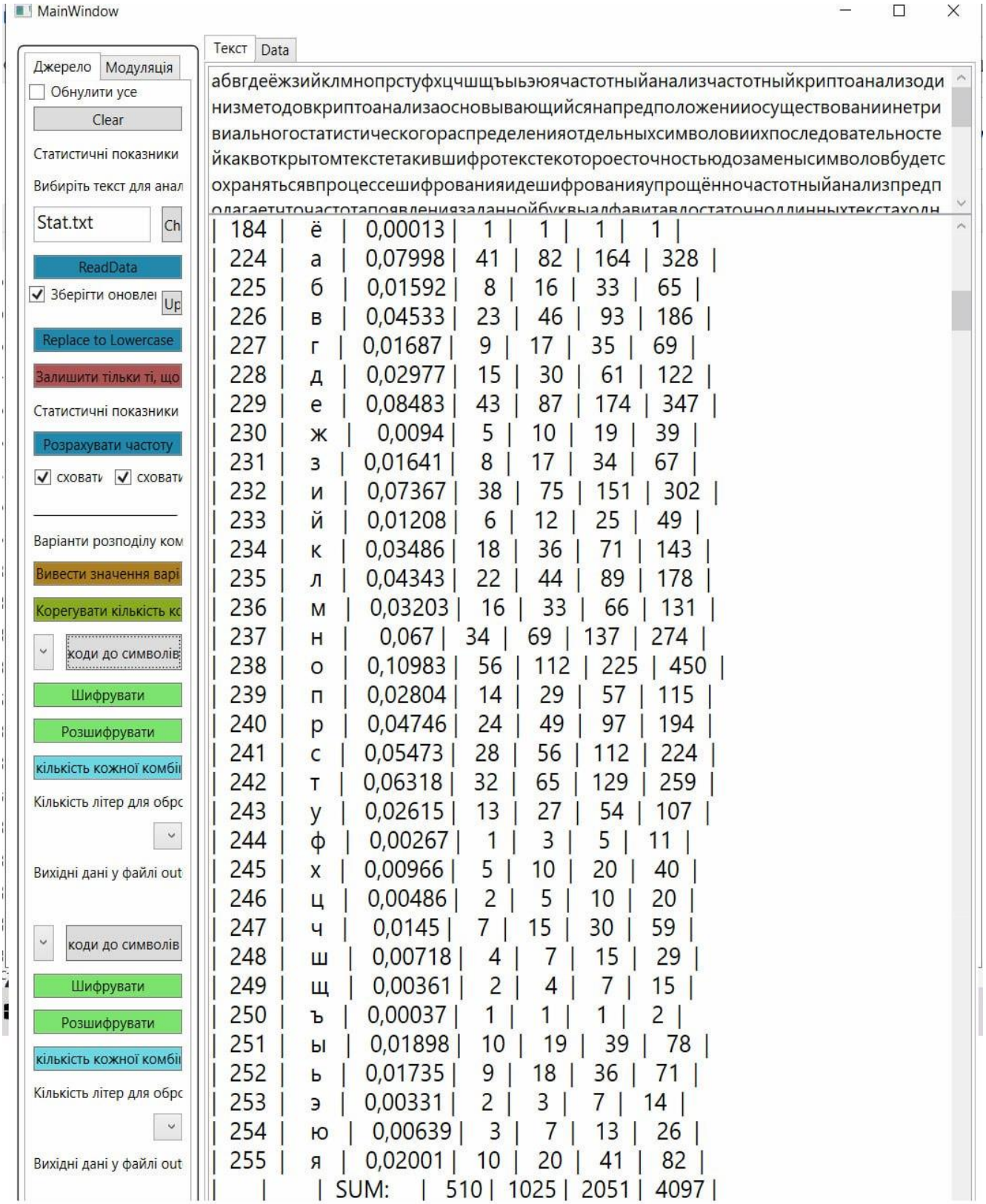
к.ф.н., доц. каф. КБ та ТЗІ Стайкуца С.В.

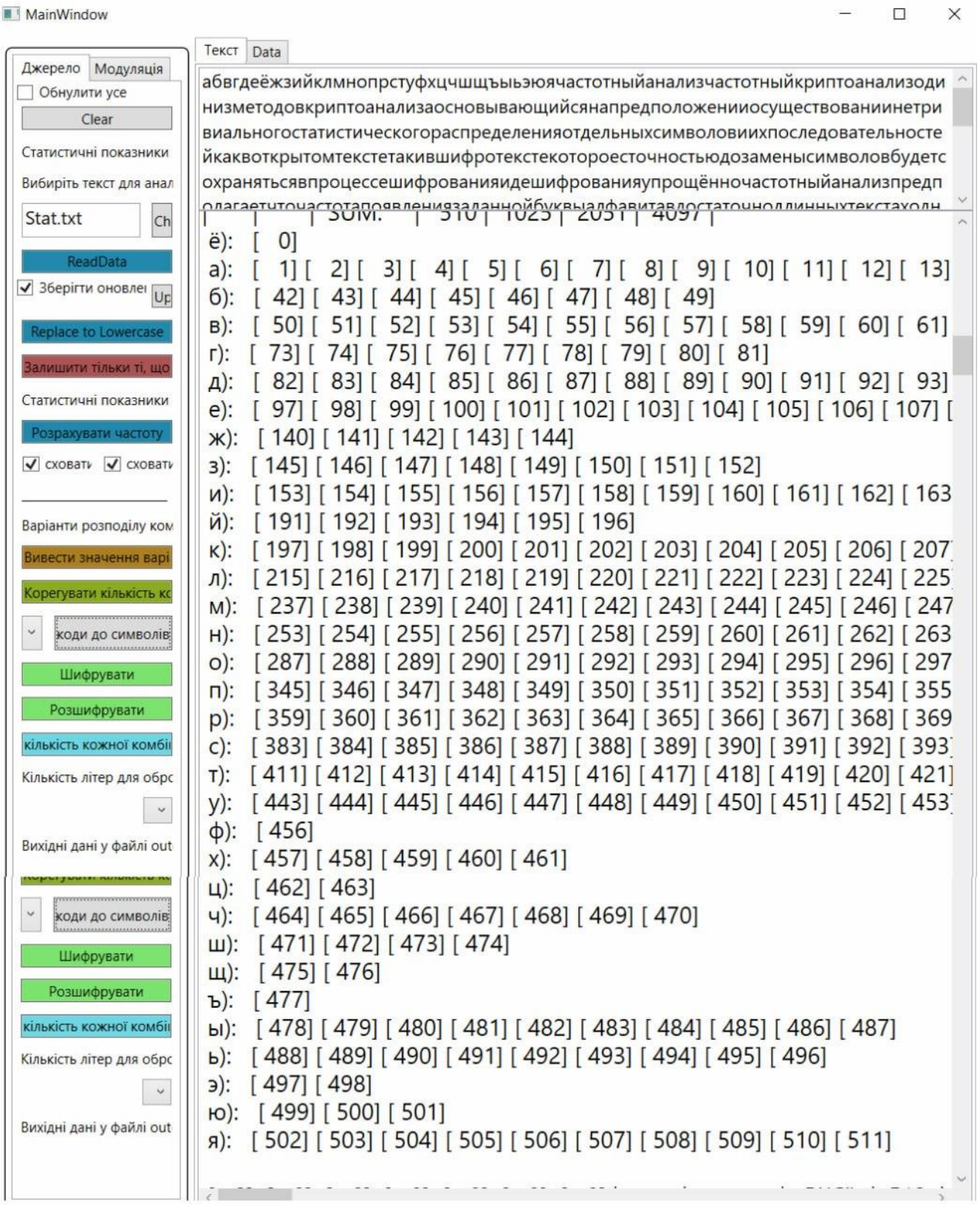
секретар каф. КБ та ТЗІ Шпильова М.І.

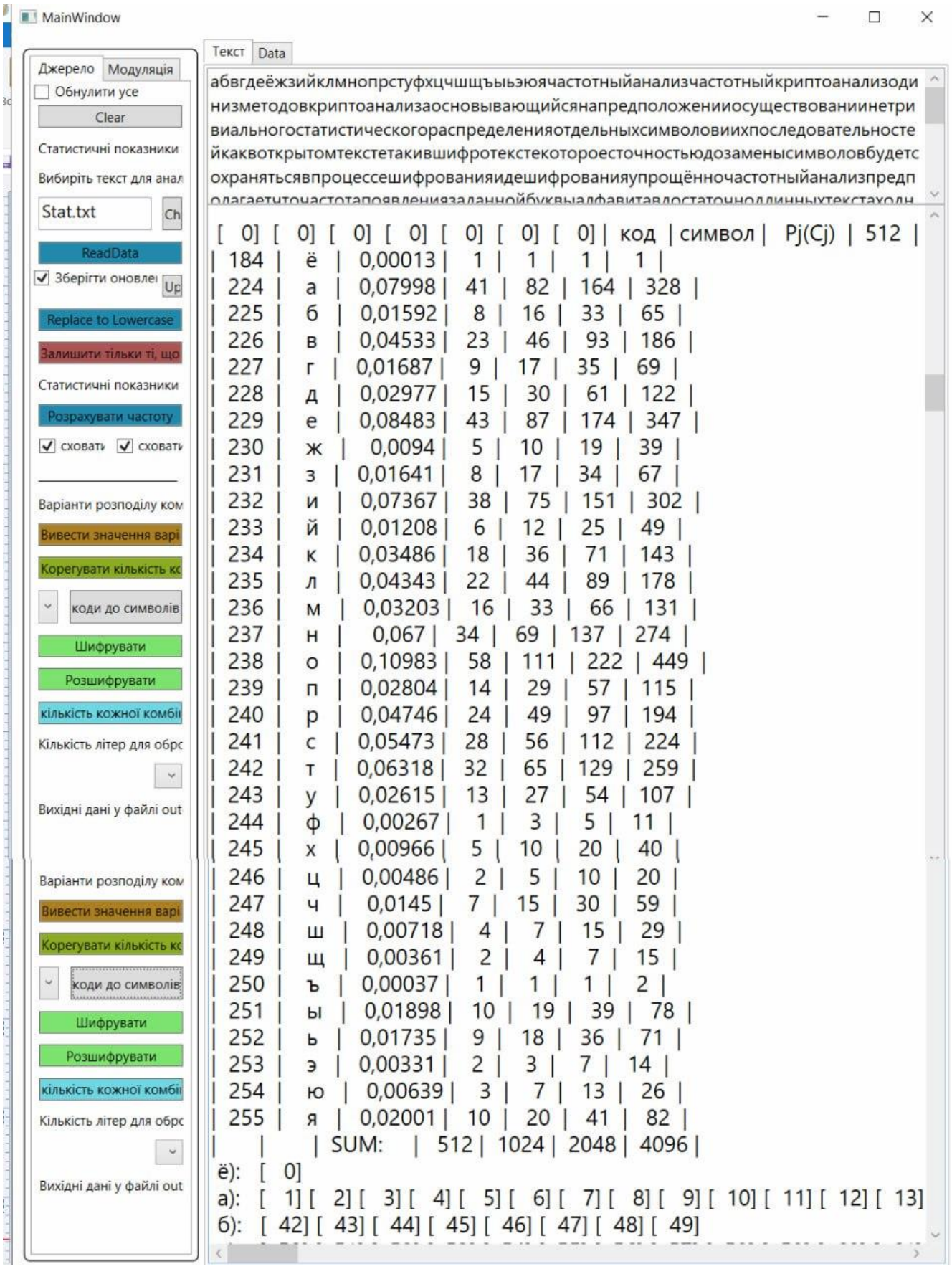
ДОДАТОК В

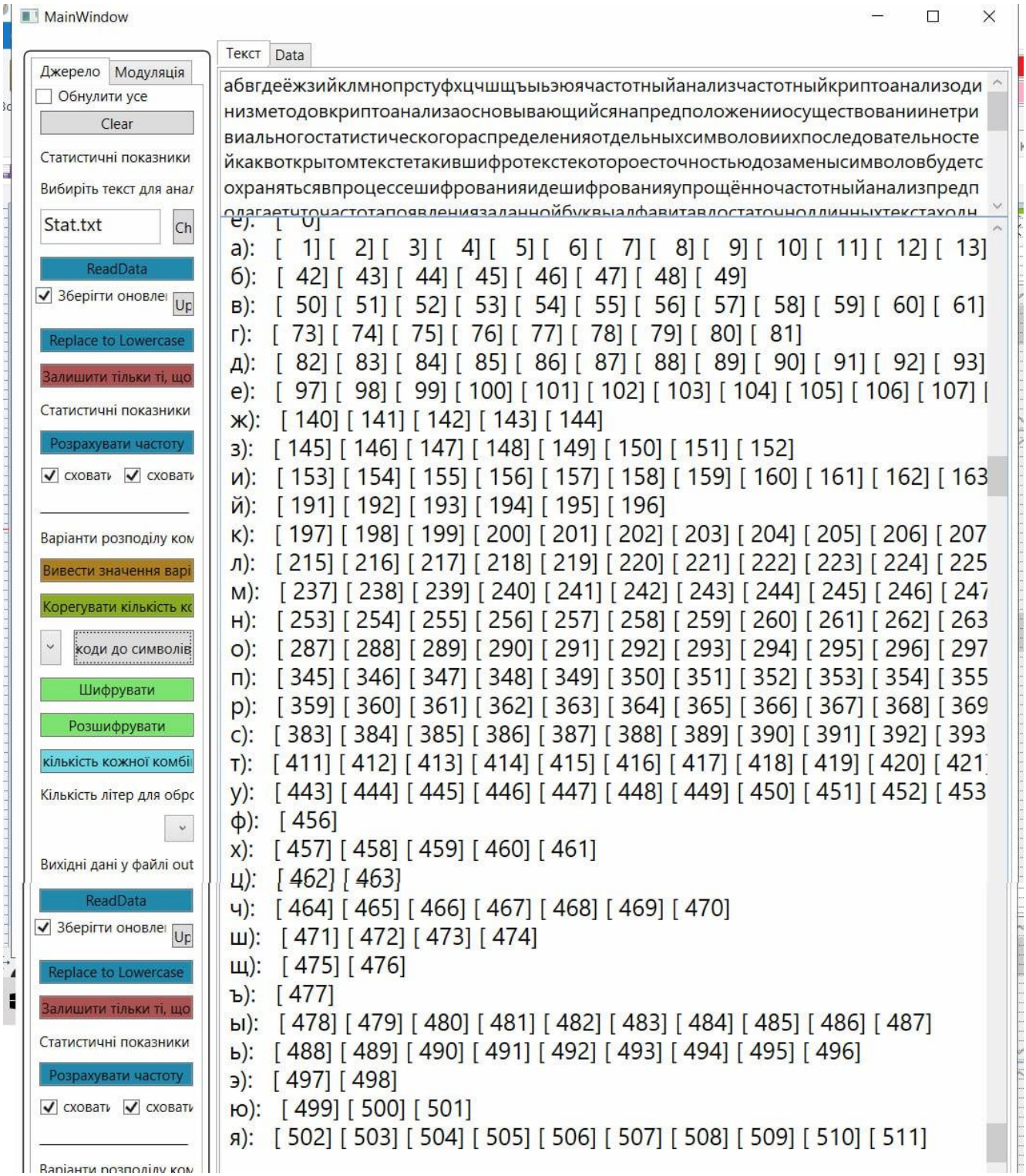
ІНТЕРФЕЙС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СТАТИСТИЧНОГО ШИФРУВАННЯ

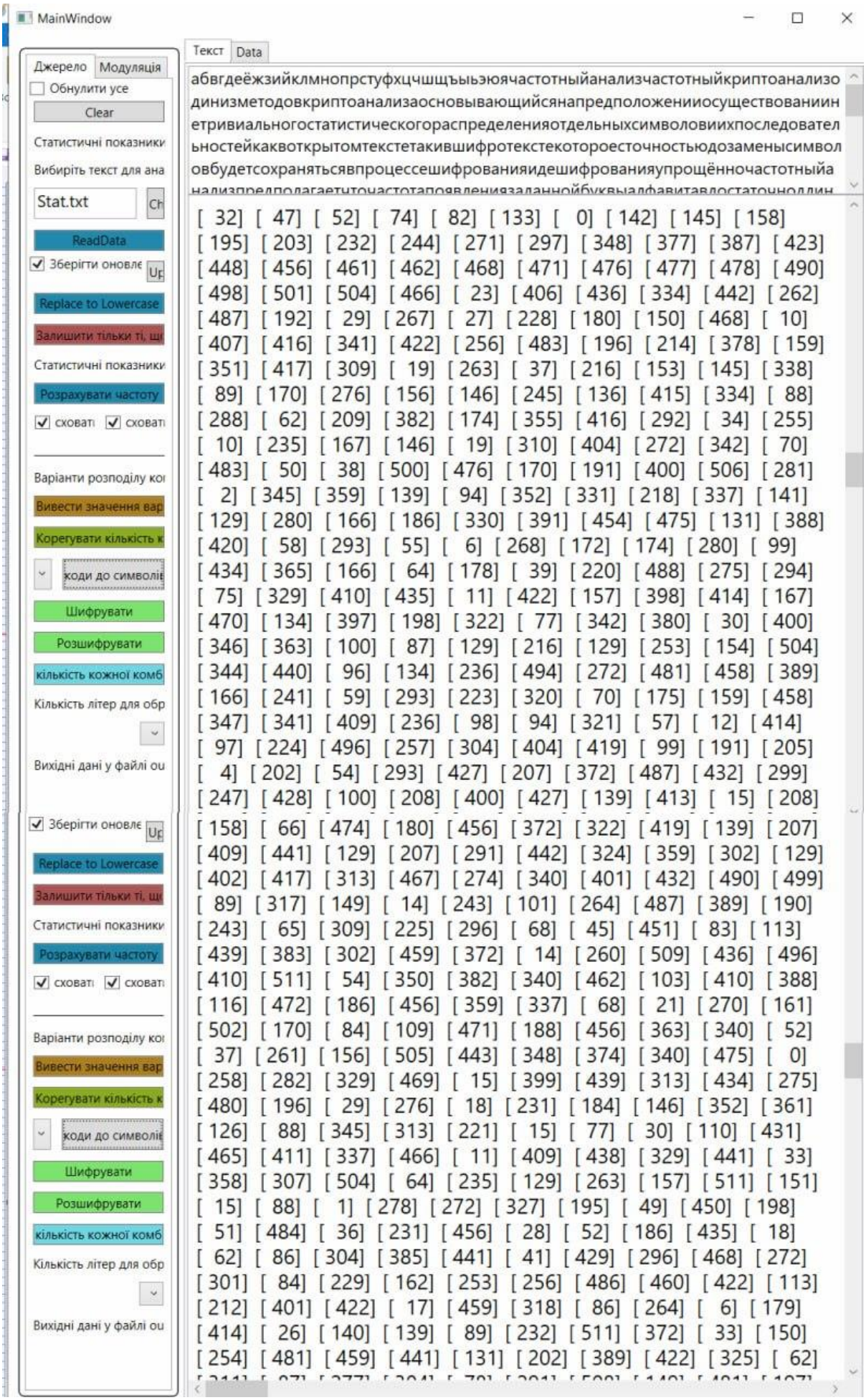


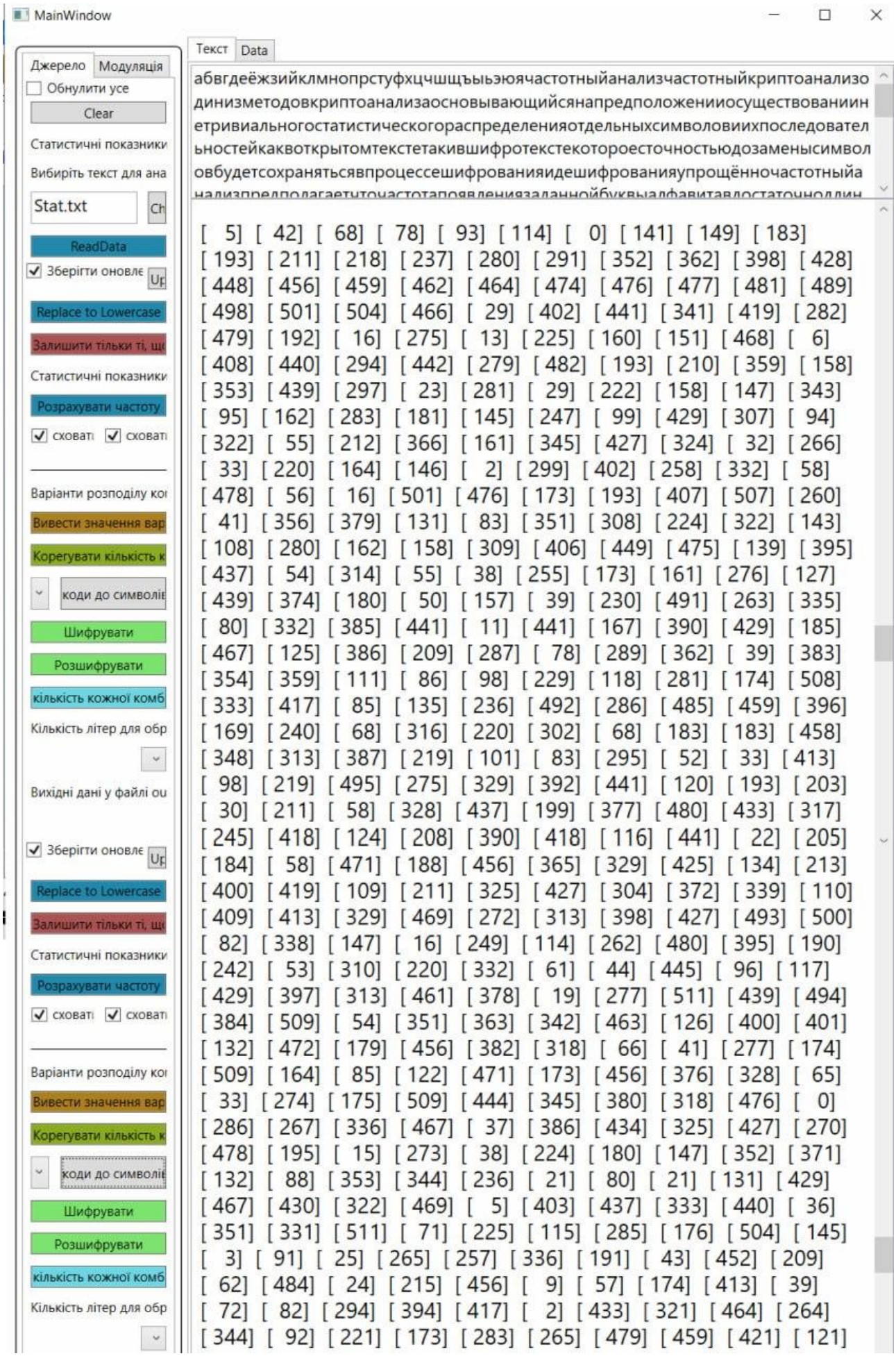

MainWindow
Джерело
Модуляція
Обнулити усе
Clear
Статистичні показники
Вибиріть текст для анал
Stat.txt
Ch
ReadData
Зберігти оновлен
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховати
сховати
Варіанти розподілу ком
Вивести значення варі
Корегувати кількість ко
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбіі
Кількість літер для обро
Вихідні дані у файлі out
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбіі
Кількість літер для обро
Вихідні дані у файлі out
Текст
Data
абвгдеёжзийклмнопрстуфхцчшщъыьэюячастотныйанализчастотныйкриптоанализодинизметодовкриптоанализаосновывающийсянапредположенииосуществованиинетриви
184	ё	0,00013	1	1	1	1
224	а	0,07998	41	82	164	328
225	б	0,01592	8	16	33	65
226	в	0,04533	23	46	93	186
227	г	0,01687	9	17	35	69
228	д	0,02977	15	30	61	122
229	е	0,08483	43	87	174	347
230	ж	0,0094	5	10	19	39
231	з	0,01641	8	17	34	67
232	и	0,07367	38	75	151	302
233	й	0,01208	6	12	25	49
234	к	0,03486	18	36	71	143
235	л	0,04343	22	44	89	178
236	м	0,03203	16	33	66	131
237	н	0,067	34	69	137	274
238	о	0,10983	56	112	225	450
239	п	0,02804	14	29	57	115
240	р	0,04746	24	49	97	194
241	с	0,05473	28	56	112	224
242	т	0,06318	32	65	129	259
243	у	0,02615	13	27	54	107
244	ф	0,00267	1	3	5	11
245	х	0,00966	5	10	20	40
246	ц	0,00486	2	5	10	20
247	ч	0,0145	7	15	30	59
248	ш	0,00718	4	7	15	29
249	щ	0,00361	2	4	7	15
250	ъ	0,00037	1	1	1	2
251	ы	0,01898	10	19	39	78
252	ь	0,01735	9	18	36	71
253	э	0,00331	2	3	7	14
254	ю	0,00639	3	7	13	26
255	я	0,02001	10	20	41	82
		SUM:	510	1025	2051	4097


MainWindow
Джерело
Модуляція
Обнулити усе
Clear
Статистичні показники
Вибиріть текст для анал
Stat.txt
Ch
ReadData
Зберігти оновлен
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховать
сховать
Варіанти розподілу ком
Вивести значення варі
Корегувати кількість кс
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбіі
Кількість літер для обрс
Вихідні дані у файлі out
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбіі
Кількість літер для обрс
Вихідні дані у файлі out
Текст
Data
абвгдеёжзийклмнопрстуфхцчшщъыьэюячастотныйанализчастотныйкриптоанализодинизметодовкриптоанализаосновывающийсянапредположенииосуществованиинетривиальногостатистическогораспределенияотдельныхсимволовиихпоследовательностейкаквоткрытомтекстетакившифротекстекотороесточностьюдозаменысимволовбудетсохранятьсявпроцессешифрованияидешифрованияупрощённочастотныйанализпредполагаетчточастотаполявлениязаданнойбуквыалфавитавдостаточнодлинныхтекстаходи
| | | SUM: | 510 | 1023 | 2031 | 4097 |
ё): [0]
а): [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]
б): [42] [43] [44] [45] [46] [47] [48] [49]
в): [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61]
г): [73] [74] [75] [76] [77] [78] [79] [80] [81]
д): [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93]
е): [97] [98] [99] [100] [101] [102] [103] [104] [105] [106] [107] [
ж): [140] [141] [142] [143] [144]
з): [145] [146] [147] [148] [149] [150] [151] [152]
и): [153] [154] [155] [156] [157] [158] [159] [160] [161] [162] [163
й): [191] [192] [193] [194] [195] [196]
к): [197] [198] [199] [200] [201] [202] [203] [204] [205] [206] [207
л): [215] [216] [217] [218] [219] [220] [221] [222] [223] [224] [225
м): [237] [238] [239] [240] [241] [242] [243] [244] [245] [246] [247
н): [253] [254] [255] [256] [257] [258] [259] [260] [261] [262] [263
о): [287] [288] [289] [290] [291] [292] [293] [294] [295] [296] [297
п): [345] [346] [347] [348] [349] [350] [351] [352] [353] [354] [355
р): [359] [360] [361] [362] [363] [364] [365] [366] [367] [368] [369
с): [383] [384] [385] [386] [387] [388] [389] [390] [391] [392] [393
т): [411] [412] [413] [414] [415] [416] [417] [418] [419] [420] [421]
у): [443] [444] [445] [446] [447] [448] [449] [450] [451] [452] [453
ф): [456]
х): [457] [458] [459] [460] [461]
ц): [462] [463]
ч): [464] [465] [466] [467] [468] [469] [470]
ш): [471] [472] [473] [474]
щ): [475] [476]
ъ): [477]
ы): [478] [479] [480] [481] [482] [483] [484] [485] [486] [487]
ь): [488] [489] [490] [491] [492] [493] [494] [495] [496]
э): [497] [498]
ю): [499] [500] [501]
я): [502] [503] [504] [505] [506] [507] [508] [509] [510] [511]


MainWindow
Джерело
Модуляція
Обнулити усе
Clear
Статистичні показники
Вибіріть текст для анал
Stat.txt
Ch
ReadData
Зберігти оновлен
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховати
сховати
Варіанти розподілу ком
Вивести значення варі
Корегувати кількість кс
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбіі
Кількість літер для обрс
Вихідні дані у файлі out
Варіанти розподілу ком
Вивести значення варі
Корегувати кількість кс
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбіі
Кількість літер для обрс
Вихідні дані у файлі out
Текст
Data
абвгдеёжзийклмнопрстуфхцчшщъыьэюячастотныйанализчастотныйкриптоанализодинизметодовкриптоанализаосновывающийсянапредположенииосуществованиинетривиальногостатистическогораспределенияотдельныхсимволовиихпоследовательностейкаквоткрытомтекстетакившифротекстекотороесточностьюдозаменысимволовбудетсохранятьсявпроцессешифрованияидешифрованияупрощённочастотныйанализпредполагаетчточастотапоявлениязаданнойбуквыалфавитавдостаточнодлинныхтекстаходи
[0] [0] [0] [0] [0] [0] [0] | код | символ | Pj(Cj) | 512 |
184	ё	0,00013	1	1	1	1
224	а	0,07998	41	82	164	328
225	б	0,01592	8	16	33	65
226	в	0,04533	23	46	93	186
227	г	0,01687	9	17	35	69
228	д	0,02977	15	30	61	122
229	е	0,08483	43	87	174	347
230	ж	0,0094	5	10	19	39
231	з	0,01641	8	17	34	67
232	и	0,07367	38	75	151	302
233	й	0,01208	6	12	25	49
234	к	0,03486	18	36	71	143
235	л	0,04343	22	44	89	178
236	м	0,03203	16	33	66	131
237	н	0,067	34	69	137	274
238	о	0,10983	58	111	222	449
239	п	0,02804	14	29	57	115
240	р	0,04746	24	49	97	194
241	с	0,05473	28	56	112	224
242	т	0,06318	32	65	129	259
243	у	0,02615	13	27	54	107
244	ф	0,00267	1	3	5	11
245	х	0,00966	5	10	20	40
246	ц	0,00486	2	5	10	20
247	ч	0,0145	7	15	30	59
248	ш	0,00718	4	7	15	29
249	щ	0,00361	2	4	7	15
250	ъ	0,00037	1	1	1	2
251	ы	0,01898	10	19	39	78
252	ь	0,01735	9	18	36	71
253	э	0,00331	2	3	7	14
254	ю	0,00639	3	7	13	26
255	я	0,02001	10	20	41	82
		SUM:	512	1024	2048	4096
ё): [0]
а): [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]
б): [42] [43] [44] [45] [46] [47] [48] [49]


MainWindow
Джерело
Модуляція
Обнулити усе
Clear
Статистичні показники
Вибиріть текст для анал
Stat.txt
Ch
ReadData
Зберігти оновлен
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховать
сховать
Варіанти розподілу ком
Вивести значення варі
Корегувати кількість ко
коди до символів
Шифрувати
Розшифрувати
кількість кожної комбі
Кількість літер для обро
Вихідні дані у файлі out
ReadData
Зберігти оновлен
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховать
сховать
Варіанти розподілу ком
Текст
Data
абвгдеёжзийклмнопрстуфхцчшщъыьэюячастотныйанализчастотныйкриптоанализодинизметодовкриптоанализаосновывающийсянапредположенииосуществованиинетривиальногостатистическогораспределенияотдельныхсимволовиихпоследовательностейкаквоткрытомтекстетакившифротекстекотороесточностьюдозаменысимволовбудетсохранятьсявпроцессешифрованияидешифрованияупрощённочастотныйанализпредполагаетчточастотаявлениязаданнойбуквыалфавитавдостаточнодлинныхтекстаходи
е): [0]
а): [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]
б): [42] [43] [44] [45] [46] [47] [48] [49]
в): [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61]
г): [73] [74] [75] [76] [77] [78] [79] [80] [81]
д): [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93]
е): [97] [98] [99] [100] [101] [102] [103] [104] [105] [106] [107] [
ж): [140] [141] [142] [143] [144]
з): [145] [146] [147] [148] [149] [150] [151] [152]
и): [153] [154] [155] [156] [157] [158] [159] [160] [161] [162] [163
й): [191] [192] [193] [194] [195] [196]
к): [197] [198] [199] [200] [201] [202] [203] [204] [205] [206] [207
л): [215] [216] [217] [218] [219] [220] [221] [222] [223] [224] [225
м): [237] [238] [239] [240] [241] [242] [243] [244] [245] [246] [247
н): [253] [254] [255] [256] [257] [258] [259] [260] [261] [262] [263
о): [287] [288] [289] [290] [291] [292] [293] [294] [295] [296] [297
п): [345] [346] [347] [348] [349] [350] [351] [352] [353] [354] [355
р): [359] [360] [361] [362] [363] [364] [365] [366] [367] [368] [369
с): [383] [384] [385] [386] [387] [388] [389] [390] [391] [392] [393
т): [411] [412] [413] [414] [415] [416] [417] [418] [419] [420] [421
у): [443] [444] [445] [446] [447] [448] [449] [450] [451] [452] [453
ф): [456]
х): [457] [458] [459] [460] [461]
ц): [462] [463]
ч): [464] [465] [466] [467] [468] [469] [470]
ш): [471] [472] [473] [474]
щ): [475] [476]
ъ): [477]
ы): [478] [479] [480] [481] [482] [483] [484] [485] [486] [487]
ь): [488] [489] [490] [491] [492] [493] [494] [495] [496]
э): [497] [498]
ю): [499] [500] [501]
я): [502] [503] [504] [505] [506] [507] [508] [509] [510] [511]


MainWindow
Джерело
Модуляція
Обнулити усе
Clear
Статистичні показники
Вибиріть текст для ана
Stat.txt
ReadData
Зберігти оновле
Replace to Lowercase
Залишити тільки ті, щ
Статистичні показники
Розрахувати частоту
Варіанти розподілу ко
Вивести значення вар
Корегувати кількість к
коди до символів
Шифрувати
Розшифрувати
кількість кожної комб
Кількість літер для обр
Вихідні дані у файлі ou
Текст
Data
абвгдеёжзийклмнопрстуфхцчшщъыьэюячастотныйанализчастотныйкриптоанализо
динизметодовкриптоанализаосновывающийсянапредположенииосуществованиин
етривиального статистического распределения отдельных символов и их последовател
ьностей как в открытом тексте так и в шифротексте которое точность до замены символ
ов будет сохраняться в процессе шифрования и дешифрования упрощённо частотный а
[32] [47] [52] [74] [82] [133] [0] [142] [145] [158]
[195] [203] [232] [244] [271] [297] [348] [377] [387] [423]
[448] [456] [461] [462] [468] [471] [476] [477] [478] [490]
[498] [501] [504] [466] [23] [406] [436] [334] [442] [262]
[487] [192] [29] [267] [27] [228] [180] [150] [468] [10]
[407] [416] [341] [422] [256] [483] [196] [214] [378] [159]
[351] [417] [309] [19] [263] [37] [216] [153] [145] [338]
[89] [170] [276] [156] [146] [245] [136] [415] [334] [88]
[288] [62] [209] [382] [174] [355] [416] [292] [34] [255]
[10] [235] [167] [146] [19] [310] [404] [272] [342] [70]
[483] [50] [38] [500] [476] [170] [191] [400] [506] [281]
[2] [345] [359] [139] [94] [352] [331] [218] [337] [141]
[129] [280] [166] [186] [330] [391] [454] [475] [131] [388]
[420] [58] [293] [55] [6] [268] [172] [174] [280] [99]
[434] [365] [166] [64] [178] [39] [220] [488] [275] [294]
[75] [329] [410] [435] [11] [422] [157] [398] [414] [167]
[470] [134] [397] [198] [322] [77] [342] [380] [30] [400]
[346] [363] [100] [87] [129] [216] [129] [253] [154] [504]
[344] [440] [96] [134] [236] [494] [272] [481] [458] [389]
[166] [241] [59] [293] [223] [320] [70] [175] [159] [458]
[347] [341] [409] [236] [98] [94] [321] [57] [12] [414]
[97] [224] [496] [257] [304] [404] [419] [99] [191] [205]
[4] [202] [54] [293] [427] [207] [372] [487] [432] [299]
[247] [428] [100] [208] [400] [427] [139] [413] [15] [208]
[158] [66] [474] [180] [456] [372] [322] [419] [139] [207]
[409] [441] [129] [207] [291] [442] [324] [359] [302] [129]
[402] [417] [313] [467] [274] [340] [401] [432] [490] [499]
[89] [317] [149] [14] [243] [101] [264] [487] [389] [190]
[243] [65] [309] [225] [296] [68] [45] [451] [83] [113]
[439] [383] [302] [459] [372] [14] [260] [509] [436] [496]
[410] [511] [54] [350] [382] [340] [462] [103] [410] [388]
[116] [472] [186] [456] [359] [337] [68] [21] [270] [161]
[502] [170] [84] [109] [471] [188] [456] [363] [340] [52]
[37] [261] [156] [505] [443] [348] [374] [340] [475] [0]
[258] [282] [329] [469] [15] [399] [439] [313] [434] [275]
[480] [196] [29] [276] [18] [231] [184] [146] [352] [361]
[126] [88] [345] [313] [221] [15] [77] [30] [110] [431]
[465] [411] [337] [466] [11] [409] [438] [329] [441] [33]
[358] [307] [504] [64] [235] [129] [263] [157] [511] [151]
[15] [88] [1] [278] [272] [327] [195] [49] [450] [198]
[51] [484] [36] [231] [456] [28] [52] [186] [435] [18]
[62] [86] [304] [385] [441] [41] [429] [296] [468] [272]
[301] [84] [229] [162] [253] [256] [486] [460] [422] [113]
[212] [401] [422] [17] [459] [318] [86] [264] [6] [179]
[414] [26] [140] [139] [89] [232] [511] [372] [33] [150]
[254] [481] [459] [441] [131] [202] [389] [422] [325] [62]


MainWindow
Джерело
Модуляція
Обнулити усе
Clear
Статистичні показники
Вибиріть текст для ана
Stat.txt
Ch
ReadData
Зберігти оновле
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховаті
сховаті
Варіанти розподілу ко
Вивести значення вар
Корегувати кількість к
коди до символів
Шифрувати
Розшифрувати
кількість кожної комб
Кількість літер для обр
Вихідні дані у файлі ou
Зберігти оновле
Up
Replace to Lowercase
Залишити тільки ті, що
Статистичні показники
Розрахувати частоту
сховаті
сховаті
Варіанти розподілу ко
Вивести значення вар
Корегувати кількість к
коди до символів
Шифрувати
Розшифрувати
кількість кожної комб
Кількість літер для обр
Текст
Data
абвгдеёжзийклмнопрстуфхцчшщъыьэюячастотныйанализчастотныйкриптоанализо
динизметодовкриптоанализаосновывающийсянапредположенииосуществованиин
етривиального статистического распределения отдельных символов и их последовател
ьностей как в открытом тексте так и в шифротексте которое сточностью до замены символ
ов будет сохраняться в процессе шифрования и дешифрования упрощённо частотный а
нализ предполагает что частота появления заданной буквы алфавита достаточно для
[5] [42] [68] [78] [93] [114] [0] [141] [149] [183]
[193] [211] [218] [237] [280] [291] [352] [362] [398] [428]
[448] [456] [459] [462] [464] [474] [476] [477] [481] [489]
[498] [501] [504] [466] [29] [402] [441] [341] [419] [282]
[479] [192] [16] [275] [13] [225] [160] [151] [468] [6]
[408] [440] [294] [442] [279] [482] [193] [210] [359] [158]
[353] [439] [297] [23] [281] [29] [222] [158] [147] [343]
[95] [162] [283] [181] [145] [247] [99] [429] [307] [94]
[322] [55] [212] [366] [161] [345] [427] [324] [32] [266]
[33] [220] [164] [146] [2] [299] [402] [258] [332] [58]
[478] [56] [16] [501] [476] [173] [193] [407] [507] [260]
[41] [356] [379] [131] [83] [351] [308] [224] [322] [143]
[108] [280] [162] [158] [309] [406] [449] [475] [139] [395]
[437] [54] [314] [55] [38] [255] [173] [161] [276] [127]
[439] [374] [180] [50] [157] [39] [230] [491] [263] [335]
[80] [332] [385] [441] [11] [441] [167] [390] [429] [185]
[467] [125] [386] [209] [287] [78] [289] [362] [39] [383]
[354] [359] [111] [86] [98] [229] [118] [281] [174] [508]
[333] [417] [85] [135] [236] [492] [286] [485] [459] [396]
[169] [240] [68] [316] [220] [302] [68] [183] [183] [458]
[348] [313] [387] [219] [101] [83] [295] [52] [33] [413]
[98] [219] [495] [275] [329] [392] [441] [120] [193] [203]
[30] [211] [58] [328] [437] [199] [377] [480] [433] [317]
[245] [418] [124] [208] [390] [418] [116] [441] [22] [205]
[184] [58] [471] [188] [456] [365] [329] [425] [134] [213]
[400] [419] [109] [211] [325] [427] [304] [372] [339] [110]
[409] [413] [329] [469] [272] [313] [398] [427] [493] [500]
[82] [338] [147] [16] [249] [114] [262] [480] [395] [190]
[242] [53] [310] [220] [332] [61] [44] [445] [96] [117]
[429] [397] [313] [461] [378] [19] [277] [511] [439] [494]
[384] [509] [54] [351] [363] [342] [463] [126] [400] [401]
[132] [472] [179] [456] [382] [318] [66] [41] [277] [174]
[509] [164] [85] [122] [471] [173] [456] [376] [328] [65]
[33] [274] [175] [509] [444] [345] [380] [318] [476] [0]
[286] [267] [336] [467] [37] [386] [434] [325] [427] [270]
[478] [195] [15] [273] [38] [224] [180] [147] [352] [371]
[132] [88] [353] [344] [236] [21] [80] [21] [131] [429]
[467] [430] [322] [469] [5] [403] [437] [333] [440] [36]
[351] [331] [511] [71] [225] [115] [285] [176] [504] [145]
[3] [91] [25] [265] [257] [336] [191] [43] [452] [209]
[62] [484] [24] [215] [456] [9] [57] [174] [413] [39]
[72] [82] [294] [394] [417] [2] [433] [321] [464] [264]
[344] [92] [221] [173] [283] [265] [479] [459] [421] [121]