МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

Фауре Еміль Віталійович

УДК 004.056.53:004.056.2:004.421.5(043.3)

ДИСЕРТАЦІЯ

МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

05.13.21 – системи захисту інформації

Подається на здобуття наукового ступеня доктора технічних наук

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

Е.В. ФАУРЕ

Науковий консультант:
Рудницький Володимир Миколайович
доктор технічних наук, професор

Черкаси – 2018

АНОТАЦІЯ

Фауре Е.В. Методологія захисту інформації на основі факторіального кодування даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Національний авіаційний університет, Київ, 2018.

Дисертаційна робота спрямована на вирішення актуальної науково-технічної проблеми створення методології захисту інформації на основі факторіального кодування даних з необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

У роботі проведено аналіз існуючих методів захисту інформації, що реалізують сумісний захист від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу. Показано, що розвинутими є методи інтеграції канального кодування та шифрування для широкосмугових телекомунікаційних систем. Разом з тим, ці методи не дозволяють контролювати цілісність даних. Аналіз інших методів поєднання функцій криптографії та завадостійкого кодування свідчить про те, що на сьогоднішній день вони вимагають розвитку та вдосконалення. Вирішення проблеми забезпечення інтегрованого захисту інформації від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу передбачає розв'язання супутніх задач, пов'язаних з удосконаленням існуючих і розробкою нових методів криптографічного перетворення інформації, а також методів формування й оцінювання послідовностей випадкових і псевдовипадкових чисел. Результати проведеного аналізу дали можливість чітко визначити задачі дисертаційного дослідження щодо розробки методології захисту інформації на основі факторіальної системи числення. З урахуванням того, що такий захист інформації передбачає введення надлишковості, що за своїми фізичними принципам відноситься до завадостійкого кодування, процес перетворення інформації для її захисту на основі

факторіальної системи числення отримав назву факторіального кодування. Відповідно, отриманий у результаті факторіального кодування код названо факторіальним кодом.

Для розробки базису факторіального кодування вдосконалено метод формування випадкової послідовності перестановок порядку M, який дозволив уникнути проблеми порушення рівномірності розподілу перестановок внаслідок виключення необхідності приведення випадкового числа до потрібного діапазону зі змінною верхньою межею та зменшити розрядність додаткового генератора псевдовипадкових чисел не менш ніж на $\log_2 M$ біт. Реалізація алгоритму формування випадкових послідовностей перестановок дозволила підвищити швидкість роботи генератора порівняно з алгоритмом Фішера-Йєтса для $M = 5$ – у 2,1 рази; $M = 10$ – у 2,6 рази; $M = 20$ – у 2,8 рази.

Розроблено методи роздільного факторіального кодування інформації, які за рахунок використання множини змінних констант в якості ключа дозволяють забезпечити захист інформації від модифікації внаслідок випадкових і умисних деструктивних дій, забезпечити властивість самосинхронізації коду та підвищити показники достовірності в умовах обмежень пропускної здатності каналів зв'язку.

Розроблено методи нероздільного факторіального кодування інформації, які дозволяють забезпечити її захист від несанкціонованого читання та помилок каналу зв'язку, забезпечити властивість самосинхронізації коду та підвищити показники достовірності в умовах обмежень пропускної здатності каналів зв'язку.

Розроблено математичну модель процесу декодування факторіальних кодів, яка дозволяє оцінити достовірність передавання інформації в результаті застосування факторіального кодування. Показано, що в порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості для ймовірності помилки в каналі зв'язку $p_0 = 10^{-3}$ повний факторіальний код дозволяє досягти енергетичний виграш до 2,7 дБ для довжини інформаційної частини $k = 1024$ біти та довжини перевірної частини $r = 64$ біти, комбінований факторіальний код – до 1,6 дБ для $k = 1024$ біти та $r = 16$ біт, факторіальний код з відновленням даних за перестановкою – до 0,821 дБ,

факторіальний код з заданим числом інверсій – до 3,295 дБ (для порядку перестановки 8).

Розроблено модель узагальненого графа станів лінійного конгруентного генератора, яка дозволяє виконати класифікацію типів компонент зв'язності графа його станів та дослідити вплив параметрів на його топологію. Розроблена модель дозволила удосконалити метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів лінійного конгруентного генератора та, як наслідок, мінімізувати часові витрати на вибір його параметрів та збільшити розмір простору їх допустимих значень для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів. Реалізація алгоритму формування ПВП перестановок на основі лінійного конгруентного генератора з будь-яким типом графа його станів дозволила підвищити швидкість роботи генератора порівняно з генератором перестановок на основі ГПВЧ LFIB78 із застосуванням алгоритму Фішера-Йєтса для порядку перестановки $M \le 125$: зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази.

Удосконалено метод симетричного криптографічного захисту інформації, який дозволяє виключити можливість виносу гами, не вимагає рандомізації відкритого повідомлення, має трек помилки, що не перевищує довжину блоку, а також дозволяє підвищити стійкість до статистичного криптоаналізу в порівнянні з одноконтурним шифруванням. Розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації. Реалізація алгоритму в режимі формування ПВП дозволяє отримати послідовність, яка успішно проходить тести NIST STS, Diehard, TestU01.

Теоретично обґрунтовано принципи побудови комбінаційного генератора, який використовує підсумовування за модулем M в якості комбінаційної функції, для чого визначено закон розподілу дискретної випадкової величини на виході комбінаційного генератора, що містить n первинних генераторів випадкових чисел як з необмеженими, так і з обмеженими періодами, а також перестановок, що

циклічно повторюються. Це дозволило обґрунтувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення рівномірного розподілу чисел у заданому діапазоні, а також розробити методику вибору параметрів первинних генераторів для забезпечення необхідних статистичних властивостей формованої послідовності чисел і її використання в реалізаціях запропонованого методу формування перестановок на основі факторіальної системи числення. Виконана оцінка статистичних властивостей ПВП на виході комбінаційного генератора підтверджує, що запропонований комбінаційний метод формування ПВП може бути використаний у задачах, що вимагають їх високої якості.

Розроблено метод, критерії та методики оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, які дозволяють виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами випадкових чисел, і не притаманні штучно згенерованим ПВП. Застосування розроблених методів і критеріїв дозволило виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ.

Розроблено методологію захисту інформації на основі факторіального кодування даних, яка дозволяє забезпечити підтримку процесів створення систем захисту інформації, що реалізують сумісний захист інформації від помилок каналу зв’язку, несанкціонованої модифікації та/або несанкціонованого доступу. Застосування методології дає можливість використовувати розроблені методи та моделі в єдиній стратегії досліджень в галузі інтегрованого захисту інформації в телекомунікаційних системах і мережах та ефективно будувати відповідні системи захисту з заданими властивостями.

Результати дисертаційної роботи впроваджено в діяльність державних і комерційних підприємств та університетів України.

Ключові слова: захист інформації, конфіденційність, цілісність, достовірність, факторіальне кодування, псевдовипадкова послідовність, генератор випадкових чисел, оцінювання випадкових послідовностей.

SUMMARY

Faure E. Methodology of information security based on factorial data coding. – Qualifying scientific work as a manuscript.

Thesis for a Doctor of Technical Science degree in specialty 05.13.21 «Information security systems». – National Aviation University, Kyiv, 2018.

The thesis is devoted to the actual scientific and technical problem of creating the methodology of information security in telecommunication systems and networks based on factorial data coding with necessary ensemble, statistical, and structural properties of code sequences for building systems of information security against communication channels errors, unauthorized modifications and/or unauthorized access.

In the work, existing methods of information security implementing joint protection against communication channel errors, unauthorized modifications and/or unauthorized access are analyzed. It has been shown that to date, methods of integrating channel coding and encryption are developed only for broadband telecommunication systems. However, these methods do not allow controlling data integrity. An analysis of other methods of combining the functions of cryptography and error control indicates that they require development and improvement. Solving the problem of providing integrated information security from communication channel errors, as well as unauthorized modification and/or unauthorized access, involves solving related problems associated with the improvement of existing and development of new methods of cryptographic transformation and methods of generating and estimating sequences of random and pseudorandom numbers. The results of the analysis made it possible to define clearly the tasks of the research to develop a methodology of information security based on factorial number system. Given the fact that this kind of information security involves the introduction of redundancy, relating by it physical principles to error control, the process of converting information for its protection based on factorial number system is called factorial coding. Accordingly, the factorial coding resulting code is named as factorial code.

To develop the basis of factorial coding, it is improved the method of permutation sequence formation. This method allows to generate reproducible sequence of unpredictable permutations of order M, to avoid the problem of disruption of

permutations uniform distribution due to the elimination of need to transform a random number to a given range with variable upper limit, and reduce capacity of additional pseudorandom number generator at least by $\log_2 M$ bit. The implementation of the algorithm of permutation sequence formation allowed to increase the generator speed, compared with the Fisher–Yates shuffle for $M = 5$ – by 2.1 times; $M = 10$ – by 2.6 times; $M = 20$ – by 2.8 times.

The methods of separable factorial coding of information are developed. These methods, by using a set of variable constants as a key, can provide information security from modifications due to accidental and intentional destructive actions, provide the property of code self-synchronization, and improve the measures of security in conditions of bandwidth restrictions.

The methods of inseparable factorial coding of information are developed. These methods allow providing information security against unauthorized reading and channel errors, providing the property of code self-synchronization, and increasing the reliability of information in conditions of bandwidth restrictions.

The mathematical model of decoding of factorial codes is developed. The model allows evaluating the reliability of information transmission with factorial coding. It is shown that compared to cyclic redundancy code for the same amount of input redundancy and bit error rate $p_0 = 10^{-3}$ full factorial code achieves energy gain to 2.7 dB for the length of information part $k = 1024$ bits and the length of check part $r = 64$ bits, combined factorial code – up to 1.6 dB with $k = 1024$ bits and $r = 16$ bits, factorial code with data recovery by permutation – up to 0.821 dB, factorial code with a given number of inversions – up to 3.295 dB (for permutation order 8).

The model of generalized states graph of linear congruential generator is developed. It allows to perform classification of connected components of its states graph and to investigate the impact of parameters on its topology. The model allowed to improve the method of pseudo-random sequences (PRS) forming based on linear congruential method, which allows to form uniformly distributed PRS of numbers independently from topology of linear congruent generator graph and, consequently, minimize the time for choosing its

parameters and increase by $M/\varphi(M)$ times the size of space of their permissible values to achieve a PRS period $T = M$. Implementation of the algorithm of forming of PRS of permutation based on linear congruential generator with any type of its states graph allowed to increase the generator speed, compared with the generator of permutations based on LFIB78 PRNG using Fisher–Yates shuffle for $M \le 125$: specifically, for $M = 20$ – by 2.1 times; $M = 50$ – by 1.6 times; $M = 100$ – by 1.2 times.

The method of symmetric cryptographic protection is improved. It allows combining the advantages of streaming and blocking cryptographic transformation and increasing the resistance to statistical cryptanalysis compared to single-encryption. The structure scheme and algorithm of two-circuit cryptographic transformation device make enable its implementation. Implementation of the algorithm in the mode of PRS forming provides a sequence that successfully passes tests of NIST STS, Diehard, TestU01.

It is theoretically grounded the principles of construction of combination generator that uses a summation modulo M as a combining function. For this, it is defined the distribution law of a discrete random variable formed by combination generator containing n initial random number generators with both limited and not limited periods and also permutations that cyclically repeat. It made possible to prove general requirements for primary sequences and combining function to ensure uniform distribution of numbers in a given range. In addition, it allowed developing a technique for choosing the parameters of primary generators to provide the necessary statistical properties of the formed sequence of numbers and its use in the proposed method of permutations forming based on factorial number system. The estimation of statistical properties of PRS of combination generator confirms that the proposed combination method of PRS forming can be used in tasks that require their high quality.

The method, criteria and techniques of estimating of uniformly distributed random and pseudo-random sequences that can detect statistical properties inherent to sequences generated by natural sources of random numbers and no inherent to artificially generated PRS. Implementation of the developed methods and criteria allowed identifying statistical deviations for some PRS generators, which successfully pass all autocorrelation tests of TestU01 package, as well as for one implementation of quantum RNG.

The methodology of information security based on factorial data coding has been developed. It allows supporting the processes of creation of information security systems that implement the joint data protection from communication channel errors, unauthorized modifications and/or unauthorized access. Application of the methodology makes it possible to use the developed methods and models in a united research strategy in the field of integrated information security in telecommunication systems and networks and to effectively build appropriate security systems with given properties.

The results of the work are implemented to the activities of public and commercial enterprises and universities in Ukraine.

Keywords: information security, confidentiality, integrity, reliability, factorial coding, pseudorandom sequence, random number generator, random sequence estimation.

Список основних публікацій здобувача

[1] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография, под ред. В. М. Безрук, и В. В. Баранник, Харьков: Лидер, 2017, с. 291-323.

[2] Е. В. Фауре, "Методологія захисту інформації на основі факторіального кодування даних", в Криптографічне кодування: обробка та захист інформації: колективна монографія, під ред. В. М. Рудницький, Харків: Щедра садиба плюс, 2018, с. 85-95.

[3] Э. В. Фауре, В. В. Швыдкий и В. А. Щерба, "Комбинированное факториальное кодирование и его свойства", Радіоелектроніка, інформатика, управління, № 3, с. 80-86, 2016.

[4] E. V. Faure, A. I. Shcherba, and V. M. Rudnytskyi, "The Method and Criterion for Quality Assessment of Random Number Sequences", Cybernetics and Systems Analysis, vol. 52, no. 2, pp. 277-284, 2016.

[5] Е. В. Фауре, "Факториальное кодирование с исправлением ошибок", Радіоелектроніка, інформатика, управління, № 3, с. 130-138, 2017.

[6] E. V. Faure, A. I. Shcherba, and A. A. Kharin, "Factorial code with a given number of inversions", Radio Electronics, Computer Science, Control, no. 2, pp. 143-153, 2018.

[7] N. Alishov, E. Faure, D. Faure, and V. Shadkhin, "Method of linear formation of pseudorandom processes", Journal of Qafqaz University. Mathematics and computer science, no. 30, pp. 17-24, 2010.

[8] Р. О. Бивзюк, Д. В. Фауре и Э. В. Фауре, "Устройство формирования остатков в многоканальных помехоустойчивых кодеках", Вісник Хмельницького національного університету, № 4, с. 75-78, 2010.

[9] Є. В. Ланських, Е. В. Фауре і А. В. Очеретяна, "Метод організації ключового обміну з використанням прихованого каналу в телефонних мережах загального користування", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 4, с. 18-21, 2010.

[10] Е. С. Лисицына, В. В. Швыдкий, А. И. Щерба и Э. В. Фауре, "Разделение векторной смеси сигнала и помехи по методу максимального правдоподобия", Системи обробки інформації, № 8(89), с. 62-67, 2010.

[11] Э. В. Фауре, Д. В. Фауре и И. Н. Коротеев, "Выбор параметров генератора конгруэнтных чисел", Сучасна спеціальна техніка, № 1(20), с. 30-35, 2010.

[12] Э. В. Фауре, Д. В. Фауре, М. В. Сторчак и В. А. Кучеренко, "Исследование и оптимизация методов формирования контрольной суммы помехоустойчивых кодов", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 4, с. 63-67, 2011.

[13] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Прихована передача інформації у полосі звукових частот", Сучасний захист інформації, № 2, с. 22-30, 2011.

[14] Э. В. Фауре, Е. В. Ланских, Д. А. Коляда и Ю. И. Черевко, "Преобразование процессов на выходе генераторов М-последовательности и конгруэнц-генераторов", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 1, с. 17-21, 2012.

[15] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Ансамбль ортогональних

шумоподібних сигналів для скритних систем з обмеженим спектром", Наукові записки УНДІЗ, № 1(21), с. 33-38, 2012.

[16] А. С. Береза, А. А. Лавданский, В. В. Швыдкий и Э. В. Фауре, "Генерация конгруэнтных последовательностей чисел с заданными свойствами", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 2, с. 3-8, 2012.

[17] Э. В. Фауре, А. С. Береза и Е. А. Ярославская, "Оценка точности воспроизведения закона распределения дискретной случайной величины при ее преобразовании", Вестник Хмельницкого национального университета, № 5, с. 176–182, 2012.

[18] В. Ю. Шадхін, Е. В. Фауре і О. В. Костомаров, "Криптографічні засоби захисту інформації в автоматизованих системах дистанційного навчання", Вісник Хмельницького національного університету, № 1, с. 126-130, 2012.

[19] В. В. Швыдкий, Э. В. Фауре, В. В. Веретельник и В. А. Щерба, "Генерация стохастической последовательности генератором конгруэнтных чисел", Системи обробки інформації, № 3, с. 74-80, 2012.

[20] Ю. Г. Лега, Э. В. Фауре и А. А. Лавданский, "Технология генерации случайных последовательностей с большой разрядностью чисел", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 3, с. 3-8, 2012.

[21] А. А. Лавданский, В. В. Швыдкий и Э. В. Фауре, "Метод формирования последовательностей случайных чисел и его использование в системах потокового шифрования", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 1, с. 5-10, 2013.

[22] Э. В. Фауре, Е. С. Лисицына и Д. Ю. Нестеренко, "Метод повышения стойкости электронных кодовых замков", Вісник Інженерної академії України, № 2, с. 137-141, 2013.

[23] Е. В. Фауре, М. І. Вишня і В. А. Чорнобай, "Оцінка закону розподілу випадкових чисел комбінаційного генератора у k-вимірному просторі", Вісник Херсонського національного технічного університету, № 4(51), с. 169-173,

2014.

[24] Э. В. Фауре, В. В. Швыдкий и А. И. Щерба, "Метод формирования воспроизводимой непредсказуемой последовательности перестановок", Безпека інформації, т. 20, № 3, с. 253-258, 2014.

[25] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе комбинационного генератора", Безпека інформації, т. 20, № 2, с. 153-158, 2014.

[26] А. А. Лавданский и Э. В. Фауре, "Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов", Системні дослідження та інформаційні технології, № 2, с. 39-50, 2015.

[27] Е. В. Фауре, С. В. Сисоєнко і Т. В. Миронюк, "Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення", Системи управління, навігації та зв'язку, № 4(36), с. 85-87, 2015.

[28] Э. В. Фауре, В. В. Швыдкий и В. А. Щерба, "Метод формирования имитовставки на основе перестановок", Захист інформації, т. 16, № 4, с. 340, 2015.

[29] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Анализ корреляционных свойств последовательностей (псевдо) случайных чисел", Наука і техніка Повітряних Сил Збройних Сил України, № 1(18), с. 142-150, 2015.

[30] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором", Комп'ютерно-інтегровані технології: освіта, наука, виробництво, № 18, с. 165-171, 2015.

[31] В. М. Рудницький, Е. В. Фауре і С. В. Сисоєнко, "Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем", Вісник Інженерної академії України, № 3, с. 219-221, 2016.

[32] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 2, с. 33-39, 2016.

[33] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с

восстановлением данных", Вісник Черкаського державного технологічного університету. Серія: Технічні науки, № 4, с. 57-61, 2016.

[34] Э. В. Фауре, "Факториальное кодирование с несколькими контрольными суммами", Вісник Житомирського державного технологічного університету. Серія: Технічні науки, № 3 (78), с. 104-113, 2016.

[35] Э. В. Фауре, В. В. Швыдкий и А. И. Щерба, "Контроль целостности информации на основе факториальной системы счисления", Journal of Baku Engineering University. Mathematics and computer science, т. 1, № 1, с. 3-13, 2017.

[36] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб комбінованого кодування інформації", патент України №107657, 24.06.2016.

[37] Е. В. Фауре, Д. В. Фауре і Р. О. Бівзюк, "Пристрій формування залишків у багатоканальних завадостійких кодеках", патент України №55711, 27.12.2010.

[38] В. В. Швидкий, А. І. Щерба, Е. В. Фауре і В. В. Веретельник, "Спосіб формування некорельованої послідовності рівномірно розподілених чисел", патент України №74628, 12.11.2012.

[39] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, А. І. Щерба і А. О. Лавданський, "Спосіб двоконтурного поточного шифрування", патент України №82044, 25.07.2013.

[40] Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування випадкової послідовності перестановок", патент України №106668, 10.05.2016.

[41] Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування імітовставки", патент України №106669, 10.05.2016.

[42] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб контролю цілісності інформації", патент України №107655, 24.06.2016.

[43] А. О. Лавданський, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування послідовності рівномірно розподілених випадкових чисел", патент України №86718, 10.01.2014.

[44] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, О. С. Лісіцина і А. О. Лавданський, "Спосіб формування послідовності випадкових чисел", патент України №86705, 10.01.2014.

[45] Е. В. Фауре, О. О. Харін, В. В. Швидкий і А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", патент України №117004, 12.06.2017.

[46] Е. В. Фауре, О. О. Харін, В. В. Швидкий і А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", патент України №121361, 11.12.2017.

[47] Е. В. Фауре і О. О. Харін, "Пристрій кодування та декодування факторіальних кодів з виявленням і виправленням помилок", патент України №123640, 12.03.2018.

[48] Э. В. Фауре и А. А. Лавданский, "Способ определения структуры графа состояний линейного конгруэнтного генератора", в Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 18-22 березня 2013 р., Черкаси, 2013, с. 110-112.

[49] E. Faure, V. Chornobai, and M. Vyshnia, "Some statistical properties of pseudorandom number sequences formed by combination generator", in Современные достижения в науке и образовании : сб. тр. IX междунар. науч. конф., 22-29 сентября 2014 г., Нетания (Израиль)., Хмельницкий, 2014, pp. 56-58.

[50] А. А. Лавданский и Э. В. Фауре, "Комбинационный метод формирования последовательности псевдослучайных чисел", в Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014 р., К., 2014, с. 403-404.

[51] Э. В. Фауре и В. В. Швыдкий, "Формирование имитовставки на основе перестановок", в Проблеми інформатизації: Матеріали другої міжнародної науково-технічної конференції, Черкаси, 25-26 листопада 2014 р., Черкаси, 2014, с. 12.

[52] Е. В. Фауре і А. М. Ткаченко, "Дослідження здатності виявлення помилок завадостійким кодом на основі перестановок", в Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ;

Полтава : ПНТУ, 2015, с. 17.

[53] Э. В. Фауре, "Статистические характеристики оценок нормированных коэффициентов автокорреляции последовательностей (псевдо) случайных чисел", в Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 16-20 березня 2015 р., Черкаси, 2015, с. 46-47.

[54] Э. В. Фауре и А. В. Магуров, "Исследование способности обнаружения ошибок комбинированным факториальным кодом", в Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 13.

[55] Е. В. Фауре і С. В. Сисоєнко, "Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу", в The scientific potential of the present [text]: Proceedings of the International Scientific Conference, St. Andrews, Scotland, UK, December 1, 2016, Vinnytsia, 2016, с. 119-122.

[56] Э. В. Фауре и Р. К. Еременко, "Исследование способности обнаружения ошибок полным факториальным кодом", в Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 12.

[57] Е. В. Фауре і О. О. Харін, "Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних", в Актуальні задачі та досягнення у галузі кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції, Кропивницький, 23-25 листопада 2016 р., Кропивницький, 2016, с. 178-179.

[58] Э. В. Фауре, "Методика оценки вероятности преобразования перестановки чисел в перестановку при ее передаче по каналу связи", в Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-

конференції, Черкаси, 14-20 березня 2016 р., Черкаси, 2016, с. 78-80.

[59] Е. В. Фауре, О. О. Харін і М. О. Качалова, "Дослідження процедури формування контрольної суми повного факторіального коду на основі ітераційного перетворення", в Проблеми інформатизації: Тези доповідей П’ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 17.

[60] Е. В. Фауре і В. С. Рузальонок, "Дослідження структури графа станів лінійного конгруентного генератора", в Проблеми інформатизації: Тези доповідей П’ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 15-16.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АКФ – автокореляційна функція;

ВЗЗ – вирішувальний зворотний зв’язок;

ВПЗ – вектор початкового завантаження;

ГВЧ – генератор випадкових чисел;

ГПВЧ – генератор псевдовипадкових чисел;

КС – комп’ютерні системи;

КФК – комбінований факторіальний код;

КЦІ – контроль цілісності інформації;

ЛКГ – лінійний конгруентний генератор;

ЛКМ – лінійний конгруентний метод;

ОЗП – оперативний запам’ятовувальний пристрій;

ПВП – псевдовипадкова послідовність;

ПФК – повний факторіальний код;

РЗЛЗЗ – регістр зсуву з лінійними зворотними зв’язками;

СКК – сигнально-кодова конструкція;

ФКВД – факторіальний код з відновленням даних за перестановкою;

ФКВДвп – ФКВД з виправленням помилок;

ФКВДд – ФКВД з доповненням;

ФКДКСн – факторіальний код з декількома контрольними сумами (нероздільний);

ФКДКСр – факторіальний код з декількома контрольними сумами (роздільний);

ФКЗЧІ – факторіальний код з заданим числом інверсій;

ФКП – факторіальний код з проріджуванням;

ФСЧ – факторіальна система числення;

CFC – Combined Factorial Code;

CRC – Cyclic Redundancy Code;

FCD – Factorial Code with Decimation;

FCDR – Factorial Code with Data Recovery by Permutation;

FCDRadd – FCDR with addition;

FCDRec – FCDR with error correction;

FCGNI – Factorial Code with a Given Number of Inversions;

FCSCs – Factorial Code with Several Checksums (separable);

FCSCi – Factorial Code with Several Checksums (inseparable);

FFC – Full Factorial Code;

IIC – Information Integrity Control;

LCG – Linear Congruential Generator.

ВСТУП

Актуальність тими дослідження. Інтенсивна комп’ютеризація всіх видів виробничої, управлінської та інформаційної діяльності призводить до повсюдного впровадження телекомунікаційних систем і мереж. Їх використання в сферах оборони, комерційної діяльності, дистанційного керування фінансовими операціями й електронного документообігу вимагає передавання конфіденційної інформації та забезпечення її цілісності, що досягається засобами криптографічного захисту.

Через безперервне зростання об’ємів передавання інформації, в тому числі конфіденційної, а також сформоване конкурентне середовище процесів створення й удосконалення систем атаки та систем захисту зростає математико-логічна складність і ступінь інтелектуалізації використовуваних алгоритмів, процесів і технічних засобів. Це призводить до необхідності підвищення ефективності та гарантоздатності (надійності та безпеки) телекомунікаційних систем і мереж, а також їх компонентів, що реалізовують функції захисту інформації.

Під час передавання інформації в системах зв’язку й управління різноманітного призначення, у тому числі на основі тунельованих протоколів комп’ютерних мереж, одночасно вирішуються декілька задач захисту інформації – забезпечення аутентифікації, конфіденційності, цілісності. Окреме вирішення цих задач пов’язане з застосуванням різних математичних методів і алгоритмів, а також послідовною обробкою інформації, що призводить до збільшення навантаження на засоби перетворення інформації та підвищення вимог до їх швидкодії, збільшення введеної надлишковості і, як наслідок, до зменшення відносної швидкості передавання. Ці обставини актуалізують проблему забезпечення захисту інформації під час її зберігання та передавання в телекомунікаційних системах і мережах за рахунок інтеграції методів канального кодування та криптографічного захисту, що реалізують сумісний захист переданих даних від помилок каналу зв’язку, а також несанкціонованої модифікації та/або несанкціонованого доступу. Актуальність зазначеної проблеми підтверджується також тим, що за даними NIST одними з найбільш перспективних напрямів постквантової криптографії є криптографія на

основі кодів виправлення помилок та на основі решіток.

Забезпечення інтегрованого захисту інформації від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу передбачає розв'язання супутніх задач, пов'язаних з удосконаленням існуючих і розробкою нових методів формування й оцінювання послідовностей випадкових і псевдовипадкових (ПВП) чисел. Зауважимо, що якість цих послідовностей має вирішальне значення в питаннях забезпечення безпеки зберігання, транспортування й обробки даних, у тому числі тих, що розглядаються в цій роботі.

Фундаментальні основи теорій криптографічного захисту інформації та її завадостійкого кодування розробив C.E. Shannon. Значний вклад у їх розвиток внесли дослідники: H. Feistel, W. Diffie, M. E. Hellman, R. L. Rivest, A. Shamir, L. Adleman, R. Hamming, W. W. Peterson, A. Hocquenghem, R. Bose, D. K. Ray-Chaudhuri, R. J. McEliece, С. А. Осмоловський, О. П. Стахов, М. І. Мазурков, В. Я. Чечельницький, О. А. Борисенко, В. А. Лужецький, В. М. Рудницький. Задачам формування послідовностей випадкових і псевдовипадкових чисел, а також їх оцінки присвячено роботи D. H. Lehmer, R. C. Tausworthe, R.R. Coveyou, G. Marsaglia, D.E. Knuth, P. L'Ecuyer, H. Niederreiter, S. K. Park, K. W. Miller, M. Matsumoto, T. Nishimura, M. J. B. Robshaw, І. Д. Горбенка, М. О. Іванова, І. В. Чугункова та ін.

Відомі підходи до поєднання завадостійкого кодування та криптографічного захисту на сьогоднішній день базуються на: криптосистемі McEliece, універсальному стохастичному кодуванні, «золотій» криптографії, досконалих алгебраїчних конструкціях, використанні перестановок. Перші три підходи мають складнощі в їх практичній реалізації. Підхід на основі досконалих алгебраїчних конструкцій є одним з найбільш розвинутих, проте призначений для широкосмугових систем зв'язку та не дозволяє контролювати цілісність даних. Використання ж перестановок і, відповідно, позиційної системи числення з факторіальною основою (факторіальної системи числення – ФСЧ) є перспективним, проте найменш розвинутим підходом.

Таким чином, на сучасному етапі розвитку науки та техніки існує *об'єктивне*

протиріччя між потребою в реалізації декількох видів захисту інформації та максимізації достовірності передавання даних, з одного боку, та обмеженою смугою пропускання каналів зв'язку, необхідністю максимізації відносної швидкості передавання й швидкості коду та мінімізації введеної надлишковості, з іншого.

Вирішення цього протиріччя вважається можливим на основі розроблення теоретичних і методологічних засад інтеграції канального кодування та криптографічного захисту на основі перестановок і ФСЧ. Оскільки такий інтегрований захист передбачає введення надлишковості, що за своїми фізичними принципами відноситься до завадостійкого кодування, процес перетворення інформації для її захисту на основі ФСЧ будемо називати факторіальним кодуванням. Відповідно, отриманий у результаті факторіального кодування код будемо називати факторіальним кодом.

Враховуючи викладене, *актуальною науково-технічною проблемою* є розробка методології захисту інформації на основі факторіального кодування даних з необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу із забезпеченням підвищення достовірності передавання інформації за однакових обсягів введеної надлишковості.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, результати яких представлені в дисертаційній роботі, відповідають пріоритетному напряму розвитку науки і техніки України «Інформаційні та комунікаційні технології» та його тематичному напряму «Технології та засоби захисту інформації» і виконувалися відповідно до програм і планів науково-дослідних робіт Черкаського державного технологічного університету, у тому числі в рамках науково-дослідної теми «Синтез операцій криптографічного перетворення із заданими характеристиками» (номер державної реєстрації 0116U008714), держбюджетної науково-дослідної теми «Розробка мобільного високоефективного ультразвукового хірургічного інструменту для військової та цивільної медицини» (номер державної реєстрації 0117U007474), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Метою роботи є розробка методології захисту інформації на основі факторіального кодування даних для побудови систем захисту інформації від помилок каналу зв’язку, несанкціонованої модифікації та/або несанкціонованого доступу.

Аналіз існуючого стану науково-технічних, методологічних і практичних положень поєднання операцій захисту інформації від несанкціонованого доступу, захисту від нав’язування хибних даних і завадостійкого кодування, а також формування ПВП і оцінювання їх якості породжують наступні проблемні задачі:

− удосконалення методу формування випадкової послідовності перестановок та створення теоретичного базису для методів факторіального кодування даних;

− розробка методів роздільного факторіального кодування інформації для забезпечення її захисту від нав’язування хибних даних і помилок каналу зв’язку;

− розробка методів нероздільного факторіального кодування інформації для забезпечення її захисту від несанкціонованого доступу і помилок каналу зв’язку;

− розробка математичної моделі процесу декодування факторіальних кодів з метою оцінки ймовірності не виявленої декодером помилки;

− удосконалення методу формування ПВП на основі конкатенації зв’язних компонентів графа станів лінійного конгруентного генератора (ЛКГ) для створення елементів перетворення інформації в процесі факторіального кодування;

− удосконалення методу симетричного криптографічного захисту інформації для забезпечення її конфіденційності;

− теоретичне обґрунтування принципів побудови комбінаційного генератора, що використовує підсумовування за модулем у якості комбінаційної функції, для забезпечення необхідних статистичних властивостей під час вирішення задач захисту інформації; аналіз якості ПВП залежно від параметрів комбінаційного генератора і властивостей початкових послідовностей;

− розробка методу і критеріїв кореляційного аналізу часових рядів для тестування ПВП з метою оцінювання їх статистичних відхилень від теоретичних розподілів показників випадкового процесу;

− розробка методології захисту інформації на основі факторіального

кодування даних.

Об’єктом дослідження є процеси захисту інформації в телекомунікаційних системах і мережах в умовах обмеженості пропускної здатності каналів зв’язку.

Предметом дослідження є моделі, методи та засоби забезпечення захисту інформації на основі факторіального кодування даних.

Методи досліджень, які використовуються в роботі, ґрунтуються на теорії факторіального числення для розробки методу формування випадкової послідовності перестановок; теорії криптографічного захисту інформації, теорії завадостійкого кодування для розробки методів факторіального кодування; теорії ймовірностей для оцінки показників достовірності передавання інформації в результаті застосування факторіальних кодів; теорії алгебри монад і топології їх графів для дослідження топології графа станів ЛКГ, розвитку методу формування ПВП на основі ЛКГ та удосконалення методу двоконтурного криптографічного перетворення даних; теорії ймовірностей і статистичного аналізу для доведення тверджень щодо рівномірності розподілу дискретної випадкової величини (д.в.в.) комбінаційного генератора з комбінаційною функцією підсумовування за модулем; теорії статистичного аналізу коефіцієнтів автокореляції і їх знаків для розробки методу оцінювання послідовностей рівномірно розподілених випадкових чисел.

Наукова новизна отриманих результатів:

– *удосконалено* метод формування випадкової послідовності перестановок на основі використання ФСЧ, який за рахунок введення додаткового генератора випадкових чисел (ГВЧ), символи якого підсумовуються з модифікованим синдромом попередньої перестановки та визначають синдром наступної перестановки, дозволяє зменшити обсяг внутрішньої пам’яті додаткового ГВЧ не менш ніж на кількість біт, що дорівнює логарифму двійковому від порядку генерованих перестановок, уникнути порушення рівномірності їх розподілу та підвищити швидкість їх формування;

– *вперше розроблено* методи роздільного факторіального кодування інформації (метод повного факторіального кодування, метод комбінованого факторіального кодування, метод факторіального кодування з проріджуванням, метод роздільного

факторіального кодування з декількома контрольними сумами), які за рахунок реалізації єдиної процедури завадостійкого кодування та захисту від нав'язування хибних даних шляхом використання перестановки в якості перевірної частини кодового слова дозволяють забезпечити контроль цілісності інформації та підвищити її достовірність під час передавання в телекомунікаційних системах в умовах обмежень пропускної здатності каналів зв'язку;

– *вперше розроблено* методи нероздільного факторіального кодування інформації (метод факторіального кодування з відновленням даних за перестановкою, метод факторіального кодування з відновленням даних за перестановкою з доповненням, метод нероздільного факторіального кодування з декількома контрольними сумами, метод факторіального кодування з відновленням даних за перестановкою з заданим числом інверсій, метод факторіального кодування з відновленням даних за перестановкою та виправленням помилок), які за рахунок реалізації єдиної процедури завадостійкого кодування та шифрування шляхом бієктивного перетворення інформаційної послідовності в перестановку чисел заданого порядку, параметри якого тримаються в таємниці, дозволяють забезпечити захист інформації від помилок каналу зв'язку та несанкціонованого доступу, а також підвищити її достовірність під час передавання в телекомунікаційних системах в умовах обмежень пропускної здатності каналів зв'язку;

– *вперше розроблено* математичну модель процесу декодування факторіальних кодів, яка за рахунок дослідження механізмів перетворення одного кодового слова в інше в симетричному двійковому каналі з незалежними бітовими помилками дозволяє оцінити показники достовірності передавання інформації в результаті застосування факторіального кодування та підтвердити його переваги порівняно з іншими методами завадостійкого кодування;

– *удосконалено* метод формування ПВП на основі лінійного конгруентного методу, який за рахунок розробленої моделі узагальненого графа станів ЛКГ та представлення кожної зв'язної компоненти графа у вигляді циклів, оснащених добутками дерев, шляхом конкатенації в графі станів ЛКГ не лише відособлених непересічних циклів, а і передциклів (дерев), якщо вони в ньому містяться, дозволяє

формувати ПВП рівномірно розподілених чисел максимального періоду незалежно від топології графа станів ЛКГ, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду в число разів, що дорівнює відношенню потужності алфавіту ЛКГ до її функції Ейлера;

– *удосконалено* метод симетричного криптографічного захисту інформації на основі операції гамування, який за рахунок введення другого контуру шифрування та використання в ньому принципів конкатенації зв'язних компонентів у графі станів ЛКГ дозволяє виключити можливість винесення гами, зменшити ймовірність зламу шифру методом повного перебору ключового простору та підвищити стійкість до статистичного криптоаналізу;

– *вперше теоретично обґрунтовано* принципи побудови комбінаційного генератора з комбінаційною функцією підсумовування за модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел як з необмеженими, так і з обмеженими періодами, а також перестановок, які циклічно повторюються, за рахунок визначення закону розподілу д.в.в. на виході такого комбінаційного генератора, що дозволило сформувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення необхідних статистичних властивостей послідовності чисел, зокрема, в реалізаціях запропонованого методу формування перестановок на основі ФСЧ;

– *вперше розроблено* метод оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, який за рахунок дослідження закону розподілу знаків емпіричної автокореляційної функції відносно кількості символів в перекритих частинах відрізків, на які розбивається послідовність чисел, і визначення допустимого «порогу» перекриття, нижче якого спостерігається рівномірний розподіл знаків автокореляційної функції, дозволяє виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами дискретного білого шуму, і не притаманні штучно згенерованим ПВП;

– *вперше розроблено* методологію захисту інформації на основі факторіального кодування даних, яка за рахунок формалізованого механізму використання

розроблених методів і моделей роздільного та нероздільного факторіального кодування, а також методів і моделей формування ключових послідовностей для факторіального кодування дозволяє забезпечити підтримку процесів створення систем інтегрованого захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

Практичне значення отриманих результатів:

– розроблено структурну схему та алгоритм роботи пристрою формування випадкової послідовності перестановок порядку M, що забезпечують можливість його практичної реалізації та дозволяють уникнути приведення випадкових чисел до діапазону зі змінною верхньою межею, зменшити розрядність внутрішнього стану додаткового ГВЧ не менш ніж на $\log_2 M$ біт, а також підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса (зокрема, для додаткового генератора псевдовипадкових чисел (ГПВЧ) LFIB78 і $M = 5$ – у 2,1 рази; $M = 10$ – у 2,6 рази; $M = 20$ – у 2,8 рази);

– розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування факторіальних кодів (повного факторіального коду (ПФК), комбінованого факторіального коду (КФК), роздільного та нероздільного факторіальних кодів з декількома контрольними сумами (ФКДКСр і ФКДКСн відповідно), факторіального коду з відновленням даних за перестановкою (ФКВД), факторіального коду з заданим числом інверсій (ФКЗЧІ), факторіального коду з виявленням і виправленням помилок (ФКВДвп)), що надають можливість їх практичної реалізації, дозволяють забезпечити захист інформації та досягти енергетичного виграшу в порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості, зокрема, для ймовірності помилки в каналі $p_0 = 10^{-3}$ та роздільного факторіального кодування: ПФК – до 2,7 дБ для довжини інформаційної частини $k = 1024$ біти та довжини перевірної частини $r = 64$ біти, КФК – до 1,6 дБ для $k = 1024$ біти та $r = 16$ біт; нероздільного факторіального кодування: ФКВД – до 0,821 дБ, ФКЗЧІ – до 3,295 дБ (для порядку перестановки 8);

– розроблено структурну схему та алгоритм роботи пристрою формування ПВП

перестановок на основі ЛКГ з будь-яким типом графа його станів, що забезпечують можливість його практичної реалізації та дозволяють мінімізувати часові витрати на вибір параметрів ЛКГ і збільшити розмір простору їх допустимих значень для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів. Швидкість роботи розробленого генератора перевищує швидкість роботи генератора перестановок на основі ГПВЧ LFIB78 із застосуванням алгоритму Фішера-Йєтса для $M \le 125$ (зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази);

− розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації і дозволяють виключити можливість винесення гами, забезпечити скінченний трек помилки та зменшити в порівнянні з використанням тільки першого контуру ймовірність зламу шифру методом повного перебору ключового простору в $2^{4n} \cdot (n!)^2$ разів, де n – розрядність блоку даних;

− розроблено методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем M, що дозволяє забезпечити рівномірний розподіл сформованої д.в.в. на множині цілих чисел потужності M та проходження пакетів статистичного тестування ПВП NIST STS, Diehard, TestU01;

− розроблено критерії та методики перевірки послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що можуть бути використані під час оцінювання випадкових послідовностей, у тому числі сумісно з пакетами статистичного тестування. Застосування розроблених критеріїв дозволило виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ.

Результати досліджень знайшли практичне застосування в ДП «НДІ «Акорд» (система дистанційного зв’язку, контролю та управління віддаленими об’єктами, м. Черкаси), ТОВ «Діджитал Мастер» (імітатор модуля керування метеорологічним локатором «Буран-А» авіаційного тренажера КТС-148, м. Київ); Департаменті освіти та гуманітарної політики Черкаської міської ради (система обліку кадрів,

м. Черкаси), а також використані в навчальному процесі Черкаського державного технологічного університету, Черкаського інституту пожежної безпеки імені Героїв Чорнобиля та Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

Особистий внесок здобувача. Дисертація є самостійно виконаною завершеною працею здобувача. Наукові положення і практичні результати, що в ній містяться та виносяться на захист, отримані автором самостійно.

У роботах, опублікованих у співавторстві, автором: [1]–[3] – розроблено та досліджено метод комбінованого факторіального кодування інформації; [4] – розроблено метод і критерій оцінювання якості послідовностей випадкових чисел; [5] – розроблено метод факторіального кодування з заданим числом інверсій; [6], [7] – досліджено статистичні властивості послідовностей комбінаційного генератора; [8]–[10] – запропоновано використати підхід до виділення комбінаційної частини та пам’яті в структурі пристрою формування залишку; [11] – розроблено метод організації ключового обміну; [12] – виконано дослідження кореляційних властивостей послідовностей; [13] – досліджено ізоморфізм графів ЛКГ та циклічної групи в $\mathbb{Z}_M$ з операцією множення; [14], [15] – виконано розробку генератора ПВП; [16] – сформульовано правила визначення кількості нуль-циклів у графі станів ЛКГ; [17] – розроблено та досліджено критерій оцінювання точності відтворення закону розподілу д.в.в.; [18] – визначено засоби захисту інформації для дистанційної навчальної системи; [19], [20] – запропоновано принципи формування основної матриці стохастичного генератора; [21] – теоретично обґрунтовано підхід до формування ПВП підвищеної розрядності; [22], [23] – запропоновано підхід та розроблено метод двоконтурного криптографічного перетворення інформації; [24] – розроблено метод підвищення стійкості електронних кодових замків; [25], [26] – розроблено та застосовано алгоритм дослідження рівномірності розподілу псевдовипадкових послідовностей у *k*-вимірному просторі; [27], [28] – розроблено та досліджено метод формування випадкової послідовності перестановок; [29], [30] – виконано аналіз ефективності використання операції суми за модулем в якості комбінаційної функції; [31], [32] – запропоновано методику дослідження

псевдовипадкових послідовностей; [33] – формалізовано алгоритм побудови псевдовипадкової послідовності; [34]–[36] – розроблено та досліджено метод формування імітовставки; [37] – виконано дослідження коефіцієнтів автокореляції випадкових послідовностей чисел; [38] – запропоновано методику оцінки статистичних характеристик ПВП; [39]–[43] – розроблено та досліджено метод повного факторіального кодування інформації; [44], [45] – досліджено методи формування ПВП; [46], [47] – розроблено та досліджено метод факторіального кодування з відновленням даних за перестановкою; [48], [49] – розроблено та досліджено метод і пристрій факторіального кодування з виявленням і виправленням помилок; [50], [51] – досліджено топологію ЛКГ. З робіт, опублікованих у співавторстві, для вирішення задач, поставлених у дисертаційному дослідженні, використано результати, отримані здобувачем особисто.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи докладалися і обговорювалися на XI, XVI Міжнародній науково-технічній конференції «Системний аналіз та інформаційні технології» (Київ, 2009, 2014); II Міжвузівській науково-практичній конференції «Актуальні проблеми технічних і природних наук у забезпеченні цивільного захисту» (Черкаси, 2009); Міжнародній науково-практичній конференції «Інформаційні технології та комп'ютерна інженерія» (Вінниця, 2010); Науково-технічній конференції «Проблеми телекомунікацій» (Київ, 2011); V Міжнародній науково-технічній конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування» (Вінниця, 2011); Міжнародній науково-практичній конференції «Інформаційні технології в освіті, науці і техніці» (Черкаси, 2012); Міжнародній науковій конференції «Информационные технологии и системы» (Мінськ, Білорусь, 2012); Міжнародній науково-практичній інтернет-конференції «Сучасність, наука, година. Взаємодія та взаємовплив» (Київ, 2012); Всеукраїнській науково-практичній Internet-конференції «Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку» (Черкаси, 2013-2017); Міжнародній науково-практичній конференції «Обробка сигналів і негауссівських процесів» (Черкаси, 2013); IX Міжнародній науковій конференції

«Сучасні досягнення в науці і освіті» (Нетанія, Ізраїль, 2014); Doctoral Summer School (Berlin, Germany, 2015); II, III, IV, V Міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси, 2014, 2015, 2016, 2017); International Scientific Conference «The scientific potential of the present» (St. Andrews, Scotland, UK, 2016); Всеукраїнській науково-практичній конференції «Актуальні задачі та досягнення у галузі кібербезпеки» (Кропивницький, 2016).

Публікації. Основний зміст, наукові положення та результати дисертаційного дослідження викладено в 80 наукових працях, основні 60 з яких наведено в авторефераті, в тому числі: 2 розділи в колективних монографіях [52], [53], 4 наукові статті у виданнях, що входять до наукометричних баз даних Scopus та / або Web of Science [1], [4], [5], [54], 2 наукові статті в фахових виданнях інших країн [6], [39] та 27 статей у наукових виданнях, що входять до переліку МОН України та інших наукометричних баз даних [7]–[9], [11]–[19], [21], [22], [24], [25], [27], [29], [31], [32], [34], [37], [38], [55]–[58], 12 патентів України [2], [10], [20], [23], [28], [35], [40], [44]–[46], [48], [49] та 13 матеріалів і тез доповідей наукових конференцій [3], [26], [30], [33], [36], [41]–[43], [47], [50], [51], [59], [60].

Структура і об’єм дисертаційної роботи. Дисертаційна робота складається з анотації, вступу, шести розділів, висновків, додатків і списку використаних джерел (355 найменувань). Повний об’єм дисертації складає 477 сторінок, у тому числі 312 сторінок основного тексту. Робота містить 104 таблиці та 80 рисунків.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ. ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1. Вступ

Існування сучасного суспільства неможливе без повсюдного використання телекомунікаційних систем і мереж, що реалізують зберігання, обробку, передавання та виведення інформації. За цих обставин однією з найбільш важливих характеристик будь-якої системи незалежно від її призначення є безпека циркулюючої в ній інформації.

Проблема забезпечення безпеки інформації в сучасних умовах розвитку телекомунікаційних систем і компонентів повинна вирішуватися з урахуванням ряду специфічних особливостей, найбільш важливими з яких є наступні:

− великі масиви інформації, що циркулює та зберігається в базах даних;

− доступність масивів даних у сховищах за допомогою комп'ютерних мереж;

− широке використання бездротових (супутникових, радіо-) каналів зв'язку, в яких присутні завади в умовах взаємного впливу абонентів один на одного, робота на граничній дальності зв'язку, несанкціоноване прослуховування переданих даних і навмисний вплив на канал зв'язку й інформацію, що транспортується, з метою придушення обміну або нав'язування хибної інформації.

За цих обставин основною вимогою, що пред'являються до телекомунікаційних систем, є їх надійне функціонування в сучасних умовах. Представлені особливості призводять до необхідності застосування одночасно декількох видів захисту інформації. Так, міжнародні стандарти телекомунікаційних мереж визначають комплекс функцій системи захисту інформації, що включає захист від помилок у каналах зв'язку за допомогою завадостійких кодів, аутентифікацію повідомлень, контроль цілісності інформації (забезпечує захист від помилок каналу зв'язку і захист від нав'язування хибної інформації), рандомізацію сигналів, захист від несанкціонованого ознайомлення з інформацією (криптозахист).

Послідовне застосування двох і більше зазначених видів захисту інформації призводить до підвищення вимог до швидкодії компонентів, що реалізують ці

процедури, а також до зростання введеної надлишковості і, як наслідок, до зменшення пропускної здатності каналу зв’язку. Тому поєднання в єдиних процедурах функцій криптографії та завадостійкого кодування є актуальним напрямком для вирішення проблеми підвищення ефективності операцій захисту інформації під час її зберігання та передавання в телекомунікаційних системах і мережах.

Врахуємо також, що всі задачі захисту інформації в телекомунікаційних системах і мережах вирішуються за допомогою послідовностей псевдовипадкових чисел – псевдовипадкових послідовностей (ПВП). Під ПВП будемо розуміти послідовність чисел або об’єктів, яка отримана за допомогою деякого детермінованого алгоритму, проте володіє властивостями істинно випадкової ("truly random" [61]) послідовності чисел. Основні вимоги, що пред’являються до формованих ПВП, можуть відрізнятися залежно від умов їх застосування.

Як показано в [62], під стохастичними методами захисту в широкому сенсі прийнято називати методи захисту інформації, прямо або побічно засновані на використанні генераторів ПВП. За такої умови ефективність захисту в значній мірі визначається якістю використовуваних алгоритмів формування ПВП. Таким чином, роль генераторів ПВП є вирішальною, і саме від якості формованих послідовностей залежить ефективність механізмів захисту інформації в телекомунікаційних системах. Тому актуальною також є наукова проблема, яка полягає в розвитку теорії формування ПВП, розробці нових, ефективних, що враховують тенденції розвитку комп’ютерних систем і компонентів, методів, алгоритмів і засобів формування випадкових чисел і об’єктів, оцінці їх якості і застосування для задач захисту інформації в телекомунікаційних системах і мережах.

У першому розділі для постановки задач дисертаційного дослідження необхідно:

- дослідити існуючі методи інтегрованого захисту інформації від випадкових і навмисних деструктивних впливів;
- виконати аналіз методів формування послідовностей перестановок для забезпечення захисту інформації;

- виконати аналіз властивостей генераторів ПВП – лінійного конгруентного генератора та генератора на основі регістра зсуву з лінійними зворотними зв’язками;
- виконати аналіз методів підвищення ефективності та поліпшення якості генераторів ПВП на основі їх комбінації;
- виконано аналіз методів і програмних засобів оцінювання якості послідовностей випадкових чисел.

1.2. Методи поєднання функцій криптографії та завадостійкого кодування

Під час передавання даних незахищеними каналами зв’язку вирішується кілька задач захисту інформації, включаючи взаємну аутентифікацію, забезпечення конфіденційності, достовірності та цілісності циркулюючих даних, а також виявлення або виправлення помилок каналу зв’язку. Причому рішення кожної з цих завдань забезпечується застосуванням різних математичних методів і алгоритмів обробки інформації, а також може вимагати введення в блок даних додаткової надлишковості, орієнтованої на виконання заданої функції. Тому є виправданим під захистом інформації розглядати технічні та організаційні заходи щодо запобігання завданню шкоди процесам управління, що викликається будь-яким впливом на інформацію під час її зберігання або передавання [63]–[65].

Розробка та дослідження методів кодування інформації, в тому числі і завадостійкого, бере свій початок з роботи К. Шеннона [66]. У теперішній час для задач завадостійкого кодування найбільш широко застосовуються циклічні коди з виявленням помилок, які використовуються в стандартних протоколах HDLC, X.25/2 (LAP-B, LAP-M), SLIP, PPP [67]. Коди Боуза-Чоудхурі-Хоквінгема і Ріда-Соломона [68]–[70], що виправляють помилки, успішно використовуються в радіоканалах. Згорткові коди знаходять застосування в супутниковому зв’язку.

В основі сучасної криптографії лежить робота К. Шеннона [71]. Сучасні методи криптографічного захисту інформації від несанкціонованого доступу базуються на використанні стандартів шифрування DES [72], AES [73],

ДСТУ 7624:2014 [74], ГОСТ 28147-89 [75] (ДСТУ ГОСТ 28147:2009 [76]), RSA [77] та інших [78], [79].

Сучасні методи криптографії, що забезпечують імітозахист і підтвердження достовірності інформації, передбачають введення додаткової надлишковості. Зокрема, для захисту від нав'язування хибних даних у повідомлення вводиться імітовставка – відрізок фіксованої довжини, обчислений на основі даних, що передаються, і секретного ключа. Імітовставка, наприклад, може бути вироблена за допомогою алгоритмів DES [72], AES [73] або ГОСТ 2814789 [75] у режимі зчеплення блоків (CBC) або посиленого гамування (CFB). Для підтвердження достовірності інформації та її авторства, а також захисту від нав'язування хибних даних використовують електронний цифровий підпис. Найбільш відомі на сьогоднішній день алгоритми: RSA [80]; Ель-Гамаля [81]; алгоритми на еліптичних кривих [82], [83].

У роботі [84] запропоновано криптосистему на основі алгебраїчної теорії кодування. Подібний підхід використано також у роботах [85]–[87]. Однак, як зазначається в [88], наведені методи розглядають завадостійкі коди в якості теоретичної бази для обґрунтування захисту даних від несанкціонованого доступу і ніяк не використовують основне призначення цих кодів – захист від внесених каналом зв'язку спотворень у передані дані.

У роботах [89]–[91] представлено способи, що забезпечують виявлення факту модифікації переданих даних як у результаті навмисних дій зловмисника, так і внаслідок впливу завад у каналі зв'язку. Одним з таких способів є код умовних залишків [89], [91]. Контрольна сума, яка формується відповідно до цього коду, представляє число, утворене з символів даних і записане в системі залишкових класів. У системах передавання даних блок, складений з інформаційної та перевірної (контрольної суми) частин, доповнюється спеціальним символом – прапором або маркером (який визначає початок блоку і служить для циклової синхронізації), – після чого блок даних виводять у канал зв'язку. Перераховані способи вимагають збільшеного обсягу надлишковості, що призводить до великих втрат пропускної здатності каналу даних. Крім того, недоліком наведених способів є невисока

швидкість роботи алгоритму, що особливо проявляється під час збільшення довжини блоку та кількості контрольних ознак, а також необхідність виконання обчислень у класах лишків за модулем, відмінним від степеня числа два, що ускладнює роботу алгоритму.

Серед робіт, присвячених розробці та дослідженню підходів до перетворення інформації для її сумісного захисту від помилок каналу зв'язку, несанкціонованого доступу та/або модифікації, які передбачають введення мінімальної надлишковості, необхідно виділити роботи [63]–[65], [92]–[114]. Розглянемо викладені в них принципи більш докладно.

1.2.1. Стохастичні методи захисту інформації

Стохастичні методи захисту інформації базуються на використанні стохастичного кодування, вперше запропонованого в [115].

Основні підходи до стохастичних методів захисту інформації викладено в [63]–[65]. Вони передбачають застосування випадкових сигналів для всіх видів захисту інформації: забезпечення взаємної аутентифікації, конфіденційності, достовірності та цілісності.

Зокрема, в [92] метод комплексного захисту інформації передбачає наступну послідовність дій:

1) до передавання в канал зв'язку або перед записом у пам'ять аналізується стан використовуваного каналу зв'язку або середовища зберігання інформації;

2) визначаються з M можливих кодів параметри оптимального для визначеного стану каналу або середовища зберігання інформації (n,k)-коду;

3) інформація, яка підлягає захисту, розбивається на символи довжиною l біт $\left(q=2^l\right)$. Для кожного q-ічного символу виробляється комбінація гами довжиною l біт від незалежного від інформацією джерела;

4) для кожної сукупності з k інформаційних q-ічних символів формуються $(n-k)$ надлишкових q-ічних символів за правилами обраного двійкового (n,k)-коду;

5) кожен q-ічний символ піддається шифрувальному стохастичному перетворенню за участю гами;

6) після прийому з каналу зв'язку або після зчитування з пам'яті для кожного q-ічного символу виробляється комбінація гами довжиною l, виконується зворотне стохастичне дешифрувальне перетворення кожного q-ічного символу за участю гами;

7) за допомогою перевірних співвідношень двійкового коду локалізуються правильно прийняті або зчитані з пам'яті q-ічні символи;

8) перевіряється правильність локалізації q-ічних символів кодового блоку, недостовірно локалізовані символи стираються, відновлюється цілісність повідомлення шляхом виправлення нелокалізованих і стертих q-ічних символів кожного блоку, виражаючи їх значення через значення достовірно локалізованих або вже виправлених q-ічних символів;

9) за неможливості достовірного відновлення цілісності кодового блоку він стирається, підраховується число стертих блоків, визначається оптимальність на інтервалі спостереження застосовуваного коду з виправленням помилок поточного стану каналу. У випадку виходу критерію оптимальності коду за задані мінімальну або максимальну межу синхронно на передавальній і приймальній частинах каналу код змінюється на оптимальний за критерієм максимуму швидкості передавання.

У роботі [93] запропоновано метод передавання та комплексного захисту інформації, який передбачає такі дії:

1) на передавальній стороні до початку передавання інформації визначаються тип і якість каналу, встановлюються оптимальні значення параметрів n, k і m використовуваного стохастичного q-ічного (n,k,q,m)-коду на основі базового двійкового (n,k)-коду з l-перемежуванням $\left(q=2^l\right)$, де m – число повторень кодового блоку з однаковими значеннями інформаційної частини;

2) інформація кодується за допомогою обраного стохастичного q-ічного коду;

3) виконується пряма рандомізація q-ічних символів;

4) на приймальній стороні виконується зворотна рандомізація q-ічних символів, контролюється цілісність q-ічних символів, контролюється достовірність цілісності q-ічних символів, відновлюється цілісність q-ічних символів з m кодових блоків;

5) накопичуються для видачі споживачеві достовірні q-ічні символи після обробки m кодових блоків;

6) контролюється оптимальність значень параметрів n, k і m і коригуються їх значення.

Запропоноване в [63]–[65], [92], [93] стохастичне кодування, по суті, включає послідовно виконувані дві операції: кодування за допомогою завадостійкого коду і стохастичне перетворення за допомогою таблиць з випадковим заповненням. Крім того, запропоновані методи комплексного захисту інформації використовують операцію гамування, що не завжди є прийнятним в реальних системах передавання даних у зв'язку з обмеженнями, характерними для потокових шифрів.

Для дослідження питання максимального суміщення в часі процесів завадостійкого кодування та потокового шифрування з метою прискорення передавання даних також заслуговує на увагу робота [88].

1.2.2. Захист інформації на основі матриць Фібоначчі

Основні підходи до захисту інформації на основі кодів Фібоначчі викладено в роботах [94]–[100]. Відзначимо, що й самі фібоначчієві числа мають надлишковість і є об'єктом дослідження для застосування в завадостійких системах [116], [117].

Відповідно до робіт [96], [98], сутність «золотої» криптографії (на основі «золотої пропорції» та Q-матриць Фібоначчі [95]) полягає в наступному. Метод криптографічного перетворення може бути застосований для захисту дискретних сигналів, що представляють послідовність відліків деякої неперервної функції: $a_1, a_2, a_3, a_4, a_5, a_6, \ldots$. Шифрування повідомлення полягає в послідовному поданні четвірок «відліків» типу a_1, a_2, a_3, a_4 у вигляді квадратної матриці

$M=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ і подальшому її множенні на пряму «золоту» матрицю $Q(2x)=\begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix}$, де x – неперервна змінна, що приймає значення з множини дійсних чисел; $sFs(x)$, $cFs(2x)$ – відповідно, симетричний гіперболічний синус і косинус, які задаються виразами $sFs(x)=\left(\tau^x-\tau^{-x}\right)/\sqrt{5}$, $cFs(x)=\left(\tau^x+\tau^{-x}\right)/\sqrt{5}$, $\tau=\left(1+\sqrt{5}\right)/2$. Після цього утворюється «кодова матриця» E: $M\cdot Q(2x)=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\cdot\begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix}=\begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix}=E(x)$, яка є зашифрованим повідомленням, що передається каналом зв'язку.

Розшифрування зашифрованого повідомлення, отриманого з каналу зв'язку, відбувається шляхом множення «кодової матриці» E на інверсну матрицю $Q(-2x)=\begin{pmatrix} cFs(2x-1) & -sFs(2x) \\ -sFs(2x) & cFs(2x+1) \end{pmatrix}$. Між детермінантами вихідної матриці M і «кодової матриці» E існує наступний зв'язок: $\det(E)=\det(M)$.

Відповідно до [95], [97], [118], підхід до завадостійкого кодування на основі матриць Фібоначчі полягає в наступному. Перший крок кодування передбачає подання вихідного повідомлення у вигляді квадратної матриці розміром $(p+1)\times(p+1)$, де $p=1,2,3,\ldots$ визначає структуру узагальнених чисел (p-чисел) Фібоначчі: $F_p(n)=F_p(n-1)+F_p(n-p-1)$. Потім сформована матриця M множиться на кодуючу матрицю Фібоначчі $Q_p^n=\begin{pmatrix} F_p(n+1) & F_p(n) & \cdots & F_p(n-p+2) & F_p(n-p+1) \\ F_p(n-p+1) & F_p(n-p) & \cdots & F_p(n-2p+2) & F_p(n-2p+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_p(n-1) & F_p(n-2) & \cdots & F_p(n-p) & F_p(n-p-1) \\ F_p(n) & F_p(n-1) & \cdots & F_p(n-p+1) & F_p(n-p) \end{pmatrix}$, утворюючи кодову матрицю E. Декодування полягає в множенні кодової матриці E на декодуючу матрицю Фібоначчі Q_p^{-n}. Між елементами вихідної матриці M і

кодової матриці E встановлюються строгі математичні співвідношення, які можуть бути використані для виявлення і виправлення помилок: $\det(E)=(-1)^{pn}\det(M)$. Використання детермінанта $\det(M)$ в якості перевірної частини блоку E під час передавання каналом зв'язку дозволяє використовувати цю властивість для виявлення та виправлення помилок.

Разом з тим, варто зазначити, що під час дослідження завадостійкості запропонованого коду авторами не виконано аналіз імовірнісних характеристик коду (імовірності виявленої помилки, імовірності невиявленої помилки, імовірності правильного декодування), що не дозволяє в повній мірі оцінити його ефективність. Крім того, в режимі виправлення помилок під час збільшення довжини блоку значно збільшується кількість вирішуваних діофантових рівнянь, що може призвести до надмірної складності алгоритму декодування.

Представлений код також має неочевидний зв'язок між його швидкістю (надлишковістю) і ступенем підвищення достовірності інформації. Так, довжина кодової комбінації, а також виявляюча та виправляюча здатності коду залежать від степені кодуючої матриці. За цих умов характер залежності залишається невідомим, що ускладнює вибір параметрів коду. У [95] підтверджується, що проблема вибору оптимального значення степені кодуючої матриці є найбільш важливою проблемою практичного застосування запропонованого методу кодування Фібоначчі («Fibonacci coding method» [95]).

1.2.3. Захист інформації на основі досконалих алгебраїчних конструкцій

Цікавим і вартим уваги підходом до інтегрованого захисту інформації є підхід на основі використання досконалих алгебраїчних конструкцій з ідеальними кореляційними і дистанційними властивостями: досконалих багаторівневих решіток, досконалих двійкових решіток (ДДР) [101]–[110]. Пояснимо принцип запропонованого захисту на прикладі методів з [103], [106].

Перш за все, зауважимо, що досконалими двійковими решітками називають [119]–[122] двовимірні таблиці (матриці) порядку N: $H(N)=\|h_{i,j}\|$, де $h_{i,j}\in\{-1;+1\}$,

які мають ідеальну двовимірну періодичну автокореляційну функцію: $R(N)=\|r_{m,n}\|=\begin{cases} N^2 \ \textit{для} \ m=n=0; \\ 0 \ \textit{для інших} \ m \ i \ n. \end{cases}$

Запропоновані в [103], [106] методи завадозахищеного передавання інформації передбачають такі процедури:

1) передане повідомлення формується з дискретних символів, кожен з яких обирається з алфавіту $A=\{a_0,a_1,a_2,\ldots,a_{q-1}\}$ потужності q. Порядок N для ДДР обирається з умови $N^2 \geq q$;

2) інформаційна модуляція здійснюється шляхом циклічних зсувів поточної породжувальної решітки по рядках і (або) стовпчиках. За такої умови кожному переданому символу a_i ставиться у відповідність одна ДДР з використовуваного еквівалентного $E(N)$-класу [122];

3) для забезпечення захисту інформації від несанкціонованого доступу для кожного нового переданого символу відкритого тексту використовується нова породжувальна ДДР. Порядок використання породжувальних ДДР визначається псевдовипадковою послідовністю. Ключем перетворення є ключ формування цієї псевдовипадкової послідовності.

У результаті перетворення інформаційного символу формується двовимірне кодове слово, яке послідовно рядок за рядком подається на вхід передавача, де здійснюється модуляція несучої частоти. Таким чином, у канал зв'язку випромінюється одновимірний дискретний сигнал довжини N^2 елементів – шумоподібний сигнал (ШПС) з базою $B=N^2$.

Криптографічна стійкість запропонованих методів захисту інформації на основі досконалих алгебраїчних конструкцій базується на тому, що для перехоплення формованих сигналів необхідно знати структуру цих сигналів, а вона для кожного переданого символу відкритого тексту постійно змінюється. Таким чином, стійкість перетворення залежить від стійкості використовуваного ГВЧ.

Завадостійкість запропонованої системи визначається, по-перше, властивостями ШПС і, по-друге, властивостями двовимірних періодичних

взаємокореляційних функцій між ДДР еквівалентного $E(N)$-класу.

Оскільки кожна ДДР складається з N^2 біт, а фактично переносить не більш $\log_2(N^2)$ інформаційних біт повідомлення, швидкість коду розглянутої схеми складає $\nu_1 = \dfrac{\log_2(N^2)}{N^2}$. Очевидно, що ця швидкість коду дуже швидко зменшується з ростом порядку N. Крім того, для блокових $(n;k)$-кодів на основі ДДР характерно обмеження $n = N^2 \geq q = 2^k$ або $k \leq \log_2(N^2)$. Це обмеження призводить до того, що, наприклад, за довжини кодової комбінації $n = N^2 = 1024$ біт інформаційні блоки, на які розбивається повідомлення, обмежені довжиною $k \leq 10$ біт.

Таким чином, розглянуті методи захисту інформації на основі досконалих алгебраїчних конструкцій забезпечують параметричну прихованість передавання інформації та її завадостійке кодування, проте обмежені застосуванням у системах зв'язку з ШПС.

1.2.4. Використання перестановок у криптографічних перетвореннях і завадостійкому кодуванні

Операції перестановки і підстановки (заміни) є одними з основних апробованих століттями розвитку тайнопису найпростіших операцій сучасних алгоритмів криптографічного захисту інформації. Шифри, побудовані на основі цих операцій, відповідно, називаються шифрами перестановки і шифрами замін.

Перестановочні шифри будуються на основі:

1) перестановки біт (бітові перестановки);
2) перестановки символів тексту (байтові перестановки);
3) перестановки випадкових за розміром груп символів. Цей метод також називають методом «тасування карт».

У перестановочних шифрах криптограма утворюється шляхом перестановки біт, символів або їх груп за певним правилом, яке задається таблицею перестановок. У шифрі заміни символи відкритого тексту замінюються символами з таблиці замін. Таблиці перестановок і замін є ключами шифру. Обидві вони представляють собою

перестановку (упорядкований набір (послідовність) з M чисел множини $\{0;1;...;M-1\}$, кожне з яких застосовується в ній тільки один раз). Відмінність полягає лише в тому, що для перестановочного шифру порядок перестановки дорівнює кількості символів (сегментів) у повідомленні (блоці), а для шифру заміни порядок перестановки дорівнює потужності використовуваного алфавіту.

Зазначимо, що процедури підстановок і перестановок не руйнують статистику повідомлення і тому не змінюють його ентропію, що істотно знижує їх стійкість. Тому в чистому вигляді шифри перестановок і підстановок не використовуються в реальних криптографічних алгоритмах, однак представляють собою основні операції для блокового симетричного шифрування (див., наприклад, опис стандартів DES [72], AES [73], ДСТУ 7624:2014[74], ГОСТ 28147-89[75]).

У області завадостійкого кодування перестановки використовуються для перемежування в алгоритмах виявлення і виправлення помилок, зокрема, для турбо-кодів [123]. Стандарт мобільного телекомунікаційного зв'язку 3GPP Long Term Evolution (LTE) використовує ці ідеї під час кодування інформації (див. технічну специфікацію 3GPP 36.212 [124]).

Крім того, перестановки є основою для оптимального хешування в алгоритмі «унікального перестановочного хешування» [125].

Перестановки використовуються також у «золотій» криптографії [96].

У роботах [111]–[114] для завадостійкого кодування інформації пропонується використовувати сильніший в плані завадостійкості код, ніж відомі нероздільні коди, в якому повідомлення представляються перестановками. Цей код не вимагає введення додаткових перевірних розрядів і забезпечує велику довжину кодової комбінації.

Коротко наведемо основні результати досліджень з [111]–[114].

Під перестановкою будемо розуміти упорядкований набір (послідовність) з M чисел множини $\{0;1;...;M-1\}$, кожне з яких зустрічається в ній тільки один раз. Число M у цьому випадку є порядком перестановки.

У роботі [111] розглянуто можливі помилки, що виникають під час передавання перестановок: помилки, пов'язані з переходом одного з елементів

перестановки в інший дозволений елемент; помилки, пов'язані з переходом одного з елементів перестановки в заборонений елемент. Наводяться алгоритми виявлення помилок.

Представимо властивості перестановок, описані в роботі [112].

Властивість 1. Число перестановок порядку M дорівнює $M!$.

Властивість 2. Сума всіх елементів перестановки порядку M дорівнює $\frac{M \cdot (M-1)}{2}$.

Властивість 3. Серед елементів перестановки $\pi = (\pi_0; \pi_1; ...; \pi_{M-1})$ не може бути два таких π_i і π_j $(i, j = 0,1,\ldots, M-1; i \neq j)$, що $\pi_i = \pi_j$.

Властивість 4. Мінімальна кількість інформації, необхідна для кодування перестановки, дорівнює $\log_2(M!)$ біт.

Властивість 5. Кількість інформації, необхідна для кодування перестановки в універсальному коді, дорівнює $M \cdot \log_2 M$.

Властивість 6. Абсолютна надлишковість інформації в елементах перестановки під час її кодування універсальним кодом змінюється від

$i_0 = \log_2 M - \log_2 M = 0$ біт для нульового елементу,

$i_1 = \log_2 M - \log_2 (M-1)$ біт для першого елементу

до значення

$i_{M-1} = \log_2 M - \log_2 1 = \log_2 M$ біт для останнього, $(M-1)$-го, елементу.

Властивість 7. Величина абсолютної надлишковості, що міститься в перестановці у випадку її кодування універсальним кодом, дорівнює $I = M \cdot \log_2 M - \log_2 (M!)$ біт.

Властивість 8. Елементи перестановки порядку M, представлені в рівномірному двійковому коді, містять відносно універсального коду надлишкову інформацію $I_d = M \cdot \lceil \log_2 M \rceil - M \cdot \log_2 M$ біт ($\lceil a \rceil$ – функція «стеля» [126], [127] (ceil) від числа a, що дорівнює найменшому цілому, не меншому a).

Властивість 9. Значення абсолютної надлишковості двійкових перестановок відносно перестановок з мінімальною надлишковістю дорівнює

$I_{\Sigma} = M \cdot \lceil \log_2 M \rceil - \log_2 (M!)$ біт.

Властивість 10. За порядку перестановки M, кратного степені двійки, будь-який з елементів двійкової перестановки може бути отриманий шляхом додавання за модулем два значень розрядів інших її $(M-1)$ елементів.

У роботі [113] показано, що перестановка в силу своєї надлишковості не вимагає доповнення контрольної сумою під час передавання каналом зв'язку, оскільки в якості контрольної суми може виступати сума її елементів, яка завжди дорівнює $M \cdot (M-1)/2$. Разом із тим, більш ефективним є спосіб виявлення помилок шляхом перевірки властивості 3, зазначеного вище. Додаткова надлишковість, введена в кожен елемент перестановки, дозволяє виявляти і виправляти більшість помилок навіть за високої ймовірності спотворення даних. Структура перестановок дозволяє виявляти окремі елементи, що містять помилки, і здійснювати для їх виправлення повторне передавання тільки цих елементів.

У роботі [114] виконано аналіз методів виправлення помилок у перестановках: метод контрольних сум з індикацією помилкових елементів, метод перехресного контролю елементів перестановок.

Разом із тим, у роботах [111]–[114] наведено тільки деякі основи використання перестановок у нероздільних кодах для задач захисту інформації під час її передавання та зберігання, вказуючи на ефективність представлених підходів.

1.2.5. Аналіз існуючих методів поєднання функцій криптографії та завадостійкого кодування

Зведемо розглянуті вище особливості існуючих методів захисту інформації в таблицю 1.1.

У [101] зазначається, що відсутні завадостійкі коди, які можна використовувати для шифрування інформації, і методи шифрування, за допомогою яких можна забезпечити завадостійке кодування. Таким чином, науково-технічна проблема побудови телекомунікаційних систем і мереж на основі інтеграції завадостійкого кодування та шифрування даних представляється особливо актуальною для теорії і практики завадозахищених систем, оскільки її вирішення

дозволяє підвищити їх ефективність за рахунок об’єднання операцій, які в них використовуються.

Таблиця 1.1

Особливості існуючих методів поєднання функцій комп’ютерної криптографії та завадостійкого кодування

Метод	Особливості
Криптографія з відкритим ключем на основі кодів виправлення помилок (McEliece R.J.)	− Є асиметричною криптографією; − забезпечує низьку швидкість коду; − вимагає надто великої довжини ключа; − легко дешифрується у випадку повторного використання ключа.
Стохастичні методи захисту (Осмоловський С.А.)	Включає послідовно виконувані операції кодування за допомогою завадостійкого коду і шифрувального стохастичного перетворення за участю гами.
«Золота» криптографія (Стахов О.П.)	− Не виконано аналіз імовірнісних характеристик коду, що не дозволяє оцінити його ефективність; − код має неочевидний зв’язок між швидкістю і ступенем підвищення достовірності інформації; − невирішеною є проблема вибору оптимального значення степені кодуючої матриці, що унеможливлює практичне застосування запропонованого методу.
Методи захисту інформації на основі досконалих алгебраїчних конструкцій (Чечельницький В.Я.)	− Забезпечують параметричну прихованість передавання інформації та її завадостійке кодування; − не забезпечують захист від нав’язування хибних даних; − обмежені застосуванням у системах зв’язку з ШПС.
Метод завадостійкого передавання інформації на основі перестановок (Борисенко О.А.)	− Код не вимагає введення додаткових перевірних розрядів; − забезпечує велику довжину кодової комбінації.

Водночас у [101] вирішено проблему розробки методології інтеграції процесів завадостійкого кодування та шифрування даних на основі розробки методів синтезу повних класів досконалих алгебраїчних конструкцій з ідеальними кореляційними і дистанційними властивостями. Разом з тим, запропоновані методи захисту

інформації не забезпечують захист від нав’язування хибних даних і обмежені застосуванням у широкосмугових системах зв’язку.

Аналіз інших методів поєднання функцій криптографії та завадостійкого кодування свідчить про те, що на сьогоднішній день вони вимагають розвитку та вдосконалення. Зокрема:

– криптосистема McEliece R.J. передбачає високу надлишковість, вимагає надто великої довжини ключа та частої його зміни;
– стохастичні методи захисту Осмоловського С.А. базуються на послідовному застосуванні методів криптографічного перетворення та завадостійкого кодування і не вирішують проблему їх інтеграції в єдину процедуру;
– «золота» криптографія Стахова О.П. визначає тільки можливий напрям захисту інформації та вимагає ґрунтовних досліджень;
– метод завадостійкого передавання інформації на основі перестановок Борисенка О.А. визначає тільки деякі основи використання перестановок у нероздільних кодах для задач захисту інформації та також вимагає ґрунтовних досліджень. Разом з тим використання перестановок для зазначених цілей представляється найбільш перспективним напрямком досліджень і вимагає подальшого розвитку.

1.2.6. Факторіальне кодування та вимоги, які до нього висуваються

Однією з задач дисертаційної роботи є розробка теоретичних і методологічних основ забезпечення захисту інформації від несанкціонованого доступу, нав’язування хибних даних і помилок у каналі зв’язку на основі використання факторіальної системи числення (ФСЧ). З урахуванням того, що такий захист інформації передбачає введення надлишковості, що за своїми фізичними принципам відноситься до завадостійкого кодування, процес перетворення інформації для її захисту на основі ФСЧ будемо називати факторіальним кодуванням. Відповідно, отриманий у результаті факторіального кодування код будемо називати факторіальним кодом.

Вимоги, які висуваються до факторіального коду:

1) код повинен мати властивості виявлення та/або виправлення помилок із забезпеченням наперед заданого енергетичного виграшу;

2) код повинен забезпечувати захист від нав'язування хибних даних з наперед заданою ймовірністю підміни інформації;

3) код повинен забезпечувати криптографічний захист інформації від несанкціонованого читання з наперед заданої стійкістю;

4) код повинен забезпечувати циклову синхронізацію без застосування роздільника (прапора) між блоками;

5) код повинен забезпечувати організацію замкнутого угруповання абонентів у відкритій мережі.

Крім того, реалізація факторіального кодування повинна бути легко здійсненна на сучасній технічній базі.

1.3. Генератори випадкових чисел

Питанням теорії побудови генераторів випадкових чисел присвячено багато робіт зарубіжних і вітчизняних дослідників [61], [62], [64], [128]–[153]. Разом із тим, як показано в [61], у обчислювальній статистиці формування випадкових величин, як правило, здійснюється в два етапи:

1) формування незалежних і однаково розподілених випадкових величин, що мають рівномірний розподіл на інтервалі $(0;1)$;
2) застосування перетворень до цих випадкових величин для формування випадкових величин і випадкових векторів для довільних розподілів.

Ці два етапи є, по суті, незалежними, і кращі світові експерти з кожного з них представляють дві різні групи вчених з невеликим перекриттям. Вираз «генератор випадкових чисел» (ГВЧ), як правило, відноситься до процедури, яка використовується на першому етапі. Історія розвитку методів і засобів формування рівномірно розподілених випадкових і псевдовипадкових чисел до 2017 року детально проаналізована і викладена в [154].

Розглянемо класифікацію генераторів рівномірно розподілених випадкових

чисел згідно [61], [154].

1.3.1. ГВЧ на основі апаратної реалізації

Випадкові числа можуть бути отримані за допомогою фізичних механізмів, таких як час між послідовними подіями в атомному розпаді або теплової шум у напівпровідниках. Ключовим питанням під час побудови ГВЧ на основі апаратної реалізації є те, що наявності «випадкового» або «хаотичного» характеру виходу виявляється недостатньо – отримані числа повинні з заданим ступенем точності наближатися до реалізацій незалежних і рівномірно розподілених випадкових величин. Якщо пристрій генерує потік бітів, що найбільш часто має місце на практиці, то кожен біт повинен приймати значення 0 або 1 з однаковою ймовірністю і не залежати від усіх інших бітів. Ця вимога не може бути теоретично гарантованою, тому необхідно покладатися на результати емпіричних статистичних випробувань, щоб отримати підтвердження,

Одним з найбільш значущих недоліків фізичних пристроїв у порівнянні з гарними алгоритмічними ГВЧ є те, що вони не можуть повторно відтворювати одну і ту ж послідовність. Ця обставина має важливе значення в різних контекстах, у тому числі під час перевірки та налагодження програмних засобів, порівнянні аналогічних систем шляхом моделювання з однаковим набором випадкових чисел або під час використання в якості ключових послідовностей у комп’ютерній криптографії. Проте, апаратні (фізичні) ГВЧ можуть бути корисні для ініціалізації алгоритмічного ГВЧ, зокрема, для застосування в комп’ютерній криптографії, де часта повторна ініціалізація ГВЧ із зовнішнім джерелом ентропії має важливе значення. Гарний алгоритмічний ГВЧ, у якому початкове значення («зерно» або вектор початкового завантаження – ВПЗ) обирається випадковим чином, можна розглядати як «розширювач» випадковості.

1.3.2. ГВЧ на основі детермінованої рекурсії

ГВЧ, які використовуються для моделювання, комп’ютерної криптографії та інших статистичних додатків, майже завжди базуються на детермінованих алгоритмах. Алгоритмічні ГВЧ будемо називати генераторами псевдовипадкових

чисел (ГПВЧ). Теоретична модель ГПВЧ, згідно з якою сформульовано наступне визначення, представлена в [153], [155].

Визначення 1.1. ГПВЧ є структурою

$$(S, \mu, f, U, g),$$

де S – простір станів генератора (скінченна множина станів генератора);

μ – розподіл імовірностей на S, що використовується для вибору початкового стану (ВПЗ) s_0;

$f : S \to S$ – функція переходу;

U – простір виходу;

$g : S \to U$ – функція виходу.

Зазвичай $U = (0;1)$. Стан ГПВЧ змінюється відповідно до рекурентного виразу $s_i = f(s_{i-1})$, $i \geq 1$, а вихідне значення на i-му кроці $u_i = g(s_{i-1}) \in U$. Вихідні значення u_0, u_1, u_2, ... є псевдовипадковими числами, виробленими ГПВЧ.

Оскільки множина S скінченна, повинні існувати деякі скінченні $l \geq 0$ і $j > 0$ такі, що $s_{l+j} = s_l$. Тоді, оскільки функції f і g детерміновані, для всіх $i \geq l$ справедливо $s_{i+j} = s_i$ і $u_{i+j} = u_i$. Таким чином, стани ГПВЧ і вихідні послідовності в кінцевому рахунку є періодичними.

Визначення 1.2. Найменше позитивне значення $j > 0$, для якого $s_{i+j} = s_i$ за всіх $i \geq l$, $l \geq 0$, називається періодом ГПВЧ.

Період ГПВЧ будемо позначати символом T.

Визначення 1.3. Якщо $l = 0$, то послідовність називається чисто періодичною.

Очевидно, що $T \leq |S|$, де $|S|$ – потужність S. Якщо стан має k-бітове представлення, то $T \leq 2^k$. Гарні ГПВЧ спроектовані таким чином, що їх період прямує до верхньої межі. У загальному випадку значення T може залежати від ВПЗ s_0, проте якісні ГПВЧ, як правило, сконструйовані таким чином, що тривалість періоду повторення слів однакова для всіх допустимих ВПЗ.

У практичній реалізації важливо, щоб вихідні значення ГПВЧ були строго між 0 і 1, оскільки значення $F^{-1}(U)$ часто рівне нескінченності для U, що дорівнює 0

або 1. Тим не менш, для математичного аналізу ГПВЧ, часто передбачається, що вихідний простір $U=[0;1)$, тобто 0 є допустимим. Це значно спрощує аналіз і не вимагає внесення модифікацій у математичну структуру генератора.

1.4. Найпростіші ГПВЧ і їх властивості

Одними з найбільш поширених на сьогоднішній день ГПВЧ є лінійний конгруентний генератор (ЛКГ) і генератор на основі регістра зсуву з лінійними зворотними зв'язками (РЗЛЗЗ).

1.4.1. Лінійний конгруентний генератор

Лінійний конгруентний генератор запропонований Д.Г. Лемером у 1949 році [131] і реалізує рекурентне співвідношення (функцію переходу $f: S \to S$) виду:

$$s_i = \left| K \cdot s_{i-1} + C \right|_M , \tag{1.1}$$

де K – множник;

C – приріст;

M – модуль, $K, C, s_0 \in \mathbb{Z}_M$.

Очевидно, що $s_i \in [0; M-1]$, а потужність простору станів ЛКГ $|S| = M$.

Конгруентна послідовність завжди утворює повторювані цикли [156, с. 10].

Приймемо, що для ЛКГ за (1.1) $u_i = s_i$, а $U \equiv S$.

Визначення 1.4. Циклом ГПВЧ (і ЛКГ, зокрема) називається періодично повторювана впорядкована за часом послідовність породжуваних генератором слів з множини потужності M.

Довжина циклу є періодом ГПВЧ.

Визначення 1.5. Словом ГВЧ називається елемент простору виходу ГВЧ.

Лінійний конгруентний метод з $C = 0$ називається мультиплікативним конгруентним методом.

ЛКГ дуже чутливі щодо зміни параметрів. Так, в роботі [156] показано, що вибір в якості модуля M довжини комп'ютерного слова $w = a^e$, де a – основа

системи числення, e – розрядність обчислювального пристрою, негативно позначається на статистичних властивостях породжуваної конгруентної послідовності. Зокрема, молодші розряди слів ЛКГ поводяться менш випадково, ніж старші. Для $M = w \pm 1$, а також для простого M подібна ситуація не спостерігається.

Неналежний вибір множника K також може призвести до погіршення властивостей послідовності слів на виході ЛКГ. Найвідомішим прикладом такого генератора є добре відомий генератор IBM RANDU. Іншим прикладом є ЛКГ з $M = 2^{32}$, $K = 477211307$, $C = 0$ і $s_0 = 0$, який запропонований у [157]. Спектральні тестові значення цього генератора виявляються ще гірше, ніж RANDU.

У [156] розглянуто методи вибору множника K для створення циклу максимальної довжини. Показано, що якщо модуль M є добутком різних простих чисел, тільки значення $K = 1$ забезпечує період $T = M$. Водночас показано, що за $K = 1$ конгруентна послідовність не поводиться як випадкова і для практичних цілей обирають $K \geq 2$. Тому для простого M і $K \geq 2$ побудова циклу довжини $T = M$ за допомогою ЛКГ не представляється можливим.

Якщо ж модуль M ділиться на просте число у великому степені, вибір параметрів K і C стає більш вільним. Так, у [156] представлена доведена в [158], [159] теорема, згідно з якою лінійна конгруентна послідовність за (1.1) має період $T = M$ тоді і тільки тоді, коли:

- $НСД(C, M) = 1$;
- $|K - 1|_p = 0$ для кожного простого $p : |M|_p = 0$;
- якщо $|M|_4 = 0 \Rightarrow |K - 1|_4 = 0$.

Максимальний період $T_{\max}$ мультиплікативного конгруентного генератора (за $C = 0$ у формулі (1.1)) визначений у [160] і дорівнює $T_{\max} = \lambda(M)$, де $\lambda(M)$ – порядок первісного елементу за модулем M. Тому максимальний період такого генератора досягається за умови, якщо $НСД(s_0, M) = 1$ і K – первісний елемент за модулем M. За такої умови

$$\lambda(2) = 1,\ \lambda(4) = 2,\ \lambda(2^e) = 2^{e-2} \text{ для } e \geq 3;$$

$$\lambda\left(p^e\right)=p^{e-1}\left(p-1\right) \text{ для } p>2;$$

$$\lambda\left(p_1^{e_1}\ldots p_t^{e_t}\right)=НСК\left(\lambda\left(p_1^{e_1}\right),\ldots,\lambda\left(p_t^{e_t}\right)\right).$$

Очевидно, що якщо M – просте, то $T_{\max}=M-1$.

У [156] також показано, що число K є первісним елементом за модулем p^e тоді і тільки тоді, коли виконується одна з наступних умов:

1) $p=2$, $e=1$ і K – непарне число;

2) $p=2$, $e=2$ і $\left|K\right|_4=3$;

3) $p=2$, $e=3$ і $\left|K\right|_8=\{3,5,7\}$;

4) $p=2$, $e\geq 4$ і $\left|K\right|_8=\{3,5\}$;

5) $\left|p\right|_2=1$, $e=1$, $\left|K\right|_p\neq 0$ і $\left|K^{(p-1)/q}\right|_p\neq 1$ для будь-якого простого q: $\left|p-1\right|_q=0$;

6) $\left|p\right|_2=1$, $e>1$, K задовольняє умові (5) і $\left|K^{p-1}\right|_{p^2}\neq 1$.

Численні роботи з теорії і застосування ЛКГ спрямовані на вибір параметрів ЛКГ і на оцінку якості отриманих ПВП. У результаті цих досліджень запропоновано і експериментально перевірено наступні реалізації ЛКГ:

- ANSIC ($M=2^{31}$, $K=1103515245$, $C=12345$ і $s_0=12345$) [138], [161];
- MINSTD ($M=2^{31}-1$, $K=16807$, $C=0$ і $s_0=1$) [129], [150], [162];
- RANDU ($M=2^{31}$, $K=65539$, $C=0$ і $s_0=1$) [163], [164];
- SIMSCRIPT ($M=2^{31}-1$, $K=630360016$, $C=0$ і $s_0=1$) [164], [165];
- BCSLIB ($M=2^{35}$, $K=5^{15}$, $C=7261067085$ і $s_0=0$) [156], [166];
- URN12 ($M=2^{31}$, $K=452807053$, $C=0$ і $s_0=1$) [130], [163], [167];
- APPLE ($M=2^{35}$, $K=5^{13}$, $C=0$ і $s_0=1$) [167], [168];
- SUPER-DUPER ($M=2^{35}$, $K=5^{13}$, $C=0$ і $s_0=1$) [134], [150], [167];
- FishmanLCGs [169], [170];
- DERIVE ($M=2^{32}$, $K=3141592653$, $C=1$ і $s_0=0$) [171];

- Turbo C ++ Library ($M = 2^{32}$, $K = 22695477$, $C = 1$ і $s_0 = 0$) [172];
- NAG Fortran ($M = 2^{59}$, $K = 13^{13}$, $C = 0$ і $s_0 = 123456789\left(2^{32}+1\right)$) [173];
- L'EcuyerLCGs [129], [174];
- MATH [175] та ін.

Список з 30 ЛКГ, включаючи RANDU, BCSLIB, APPLE, SUPER-DUPER, і результати їх спектральних випробувань наведено в [156]. Ці ЛКГ були обрані відповідно до різних критеріїв («випадковий» множник; множник, що гарантує швидку реалізацію; множник, близький до ступеня двійки, що виробляє погані решітчасті конструкції). Деякі з них ґрунтуються на результатах пошуку оптимальних множників відносно двовимірних невідповідностей [176].

Слід відзначити також роботи [177], [178], де представлені рандомізаційні методи формування ПВЧ на основі лінійного конгруентного методу зі змінними коефіцієнтами та його нелінійного розширення.

Водночас, незважаючи на велику кількість досліджень, присвячених вибору параметрів ЛКГ і експериментальній оцінці його властивостей, у своїй більшості вони спрямовані на вирішення задач поліпшення «випадковості» формованої послідовності слів ЛКГ і не беруть до уваги структуру його простору станів S.

Серед робіт, присвячених аналізу структури простору станів ЛКГ варто виділити ґрунтовну наукову роботу G. Marsaglia [150]. У цій роботі показано, що якщо $НСД\left(K, M\right) = 1$, то перше значення, яке повториться в конгруентній послідовності, породженій (1.1), буде значення s_0. У термінах, визначених вище, така послідовність буде чисто періодичною. Якщо ж $НСД\left(K, M\right) \neq 1$, послідовність на виході ЛКГ може не бути чисто періодичною.

Визначення 1.6. Послідовність значень $s_0, s_1, \ldots, s_{l-1}$ для ЛКГ з параметрами K, C, M і s_0, де $l \geq 0$ – найменше значення, таке, що $s_{i+T} = s_i$ для всіх $i \geq l$, T – період, називається передциклом (передперіодом), значення l – довжиною передциклу, а значення s_{l-1} – особливою точкою входу в цикл.

Таким чином, якщо $НСД\left(K, M\right) = 1$, лінійна конгруентна послідовність має

нульову довжину передциклу – $l=0$.

Робота [150] також вказує на те, що вибір параметра C і ВПЗ s_0 не має значення, а послідовність за (1.1) може бути отримана з афінного перетворення «фундаментальної послідовності» 0, 1, K, $K+1$, K^2+K+1, ..., $y_i=\left|K\cdot y_{i-1}+1\right|_M$, … Крім того, якщо $НСД\left(K,M\right)=1$, період ЛКГ відповідає періоду «фундаментальної послідовності» для модуля M/D, де $D=НСД\left(M,s_0\left(K-1\right)+C\right)$.

У [150] встановлено також наступне:

- якщо $НСД\left(K,M\right)=1$ і t – мультиплікативний порядок числа K за модулем M, період «фундаментальної послідовності» $T=tr$, де $r=M\Big/НСД\left(\left|1+K+K^2+\ldots+K^{t-1}\right|_M,M\right)$ – адитивний порядок числа C за модулем M $\left(\left|rC\right|_M=0\right)$;
- якщо $НСД\left(K,M\right)=1$, $M=2^e$ і t – мультиплікативний порядок числа K за модулем M, тоді:
  - $t=1$, якщо $\left|K\right|_M=1$;
  - $t=2^{e+1}\Big/НСД\left(K^2-1,M\right)$, якщо $\left|K\right|_M\neq 1$;
- для знаходження періоду ЛКГ, якщо $НСД\left(K,M\right)=1$ необхідно розкласти модуль M/D, де $D=НСД\left(M,s_0\left(K-1\right)+C\right)$, на добуток ступенів різних простих чисел: $M/D=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$, де p_i – просте число. Тоді період ЛКГ $T=НСК\left(q_1,q_2,\ldots,q_k\right)$, де $q_i=НСД\left(K-1,p_i^{e_i}\right)\cdot t_i$, t_i – мультиплікативний порядок числа K за модулем $p_i^{e_i}$.

Аналізу структури простору станів ЛКГ присвячена також робота [179], яка спрямована на дослідження процедури перетворення псевдовипадкової лінійної конгруентної послідовності, породженої рівнянням (1.1), у рівномірно розподілену на відрізку $\left[0;M-1\right]$ послідовність з M чисел.

У цій роботі також визначено поняття, для яких наведемо наступні визначення.

Визначення 1.7. Нуль-циклом називається цикл, що містить один елемент множини цілих чисел відрізка $[0; M-1]$.

Визначення 1.8. Надциклом називається послідовність слів ЛКГ, отримана шляхом конкатенації всіх циклів ЛКГ в єдиний цикл довжиною M.

Визначення 1.9. Гіперциклом називається послідовність слів ЛКГ, отримана шляхом конкатенації надциклів з різним порядком слідування елементів у них.

У роботі [179] сформульовано та доведено наступне твердження.

Твердження 1.1 (з [179]**).** Один або група слів з множини $\{0;1;\ldots;M-1\}$ не може належати двом або більше циклам ЛКГ.

Внаслідок цього:

1) цикли ЛКГ в сукупності з усіма своїми передциклами розбивають множину цілих чисел відрізка $[0; M-1]$ на непересічні підмножини;
2) цикли можуть бути об'єднані в надцикл. Для цього в кінці кожного циклу в якості ВПЗ в ЛКГ записується число-представник іншого циклу. За умови, якщо кожен з циклів ЛКГ не містить передциклу, після перебору представників усіх циклів (включаючи нуль-цикл) без повторень і вилучень, утворюється надцикл, що включає всі M елементів множини;
3) надцикли можуть бути об'єднані в гіперцикл, якщо в кожному надциклі змінювати ВПЗ циклів і порядок їх слідування.

У роботі [180] розроблено метод формування ПВП на основі ЛКМ, що передбачає конкатенацію циклів ЛКГ. Розроблений метод свідчить про те, що існує можливість побудови на базі ЛКГ генератора перестановок – послідовностей чисел множини $\{0;1;\ldots;M-1\}$ без повторів і пропусків.

У роботі [179] доведено наступну теорему.

Теорема 1.1 (з [179]**).** Множина станів ЛКГ з простим M містить один нуль-цикл і рівні за довжиною ненульові цикли. Число ненульових циклів d і їх довжина T є дільниками числа $M-1$:

$$M-1=d\cdot T. \tag{1.2}$$

Таким чином, множина M цілих чисел відрізка $[0, M-1]$ на виході ЛКГ

розбивається на d непересічні підмножини M_j однакової потужності T, причому $M = \bigcup_{j=1}^{d} M_j$, $\bigcap_{i \neq j} M_i M_j = \varnothing$, і один нуль-цикл.

З огляду на те, що ВПЗ у кожному з циклів, крім нуль-циклу, може бути обраний T способами, порядок обходу контурів, з урахуванням нуль-циклу, може бути обраний $(d+1)!$ способами, довжина гіперциклу ЛКГ становить

$$L_{gc} = M \cdot (d+1)! \cdot T^d . \tag{1.3}$$

Якщо нуль-цикл розміщувати в довільному місці надциклу (між будь-якими символами після обходу всіх інших циклів) вираз (1.3) набуває такого вигляду:

$$L_{gc} = M^2 \cdot d! \cdot T^d . \tag{1.4}$$

Очевидно, що $L_{gc} < M!$ для будь-якого з виразів (1.3) або (1.4). Тому такий метод формування послідовності перестановок не дозволяє сформувати всі можливі перестановки порядку M. Водночас формованого обсягу може бути достатньо для практичних застосувань.

Таким чином, незважаючи на те, що проблемі вибору параметрів ЛКГ приділено достатньо велику кількість публікацій, до теперішнього часу недостатньо вивченими є питання, пов'язані з формуванням на основі ЛКГ послідовностей, що складаються з усіх цілих чисел діапазону $[0, M-1]$, (перестановок порядку M) шляхом послідовного обходу контуру графа його станів.

1.4.2. Генератор на основі регістра зсуву з лінійними зворотними зв'язками

ГПВЧ на основі РЗЛЗЗ запропоновано Р. Таусвортом у 1965 році [140]. Цей генератор формує двійкову послідовність $S = \{s_k\}$ шляхом вирішення характеристичного рівняння (реалізації функції переходу $f : S \to S$) виду

$$s_k = \sum_{i=1}^{n} s_{k-i} g_i \tag{1.5}$$

для будь-якого набору значень $g_i \in \{0;1\}$ $(i = 1,2,\ldots,n)$, причому $g_n = 1$.

РЗЛЗЗ за рахунок наявності зворотного зв'язку має нескінченну імпульсну реакцію і за будь-якого ненульового ВПЗ видає періодичну послідовність.

Приймемо, що для ГПВЧ на основі РЗЛЗЗ $u_i = s_i$, а $U \equiv S$.

Максимальний період сформованої послідовності дорівнює $T_{\max} = 2^n - 1$.

Для забезпечення максимального періоду $T = T_{\max} = 2^n - 1$ необхідно і достатньо, щоб утворюючий багаточлен степені n

$$G(x) = \sum_{i=0}^{n} g_i x^i$$

був примітивним у полі $GF(2)$ [181], [182]. У цьому випадку РЗЛЗЗ є генератором послідовності максимальної довжини (М-послідовності).

У роботі [183] показано, що математична модель формування М-послідовності $\Phi_0(x)$, яка породжується генераторним багаточленом $G(x)$, має вигляд:

$$\Phi_0(x) = \left(x^T + 1\right) \big/ G\hat{}(x), \tag{1.6}$$

де $G\hat{}(x)$ – несиметричний багаточлен, взаємний до $G(x)$.

Практична реалізація генераторів М-послідовності дуже проста, а їх швидкодія дуже велика. Ці послідовності відтворювані – фрагмент послідовності і вся послідовність відтворюються абсолютно точно при зміщенні подій у просторі і часі. Ця сукупність факторів визначила широке застосування М-послідовностей у всіх областях комп'ютерної техніки і техніки зв'язку. Водночас неможливість отримання на виході генератора М-послідовності n-розрядного псевдовипадкового числа $(u_{k-1}, u_{k-2}, \ldots, u_{k-n}) = (0, 0, \ldots, 0)$ призводить до спотворення рівномірного закону розподілу. Така псевдовипадкова послідовність символів (слів) рівномірно розподілена в діапазоні $\left[1; 2^n - 1\right]$ і не може бути послідовністю де Брейна [184].

Під час використання М-послідовностей у системах криптографічного захисту істотне значення має ще один недолік – М-послідовність не забезпечує стійкість до розкриття закону формування за її відрізком. Це означає, що М-послідовність передбачувана і, як наслідок, не є криптографічно стійкою.

Згадані недоліки породжують безперервний процес вдосконалення методів

формування псевдовипадкових послідовностей чисел на основі РЗЛЗЗ.

У роботі [185] показано можливість введення нульової комбінації в послідовність, що породжується РЗЛЗЗ, за рахунок використання в комбінаційній схемі додаткового ГВЧ. За цих обставин імовірність появи будь-якого n-розрядного слова на виході генератора однакова і дорівнює $1/2^n$. Водночас реалізація запропонованого генератора рандомізованих псевдовипадкових чисел виявляється можливою тільки для примітивного утворюючого багаточлена.

У роботі [186] поліпшення статистичних параметрів породжуваної РЗЛЗЗ послідовності досягається тим, що в генератор додатково вводять аналоговий формувач шуму, вихідний сигнал якого за допомогою порогового пристрою перетворюють у двійкову послідовність, яку підсумовують за модулем два з сигналом в ланцюзі зворотного зв'язку регістра зсуву. У результаті сама послідовність стає непередбачуваною.

Недоліком цього методу є те, що випадковий процес, породжений аналоговим генератором шуму, невідтворюваний, тобто жоден фрагмент його не можна точно відтворити під час рознесення в часі і в просторі. Це призводить до того, що стає неможливим виконання серії випробувань складних об'єктів за одних і тих самих заважаючих факторів або виконання процедури розшифрування (раніше зашифрованого повідомлення) з рознесенням у просторі і часі.

Таким чином, представлені вище методи підвищення ефективності РЗЛЗЗ покращують статистичні характеристики вихідної послідовності, проте обмежені використанням примітивних утворюючих багаточленів, а також не володіють властивістю відтворюваності за рахунок застосування додаткових джерел ентропії.

Відомий [187] метод формування на основі РЗЛЗЗ двійкових послідовностей довільної довжини, меншої або рівної 2^n. Незважаючи на те, що цей метод забезпечує досягнення періоду, рівного 2^n, він також обмежений використанням примітивного утворюючого багаточлена.

У роботі [180] розроблено метод формування ПВП на основі РЗЛЗЗ, що передбачає конкатенацію його циклів. Розроблений метод свідчить про те, що існує можливість побудови на базі РЗЛЗЗ генератора перестановок – послідовностей

чисел множини $\{0;1;\ldots;M-1\}$ без повторів і пропусків.

1.4.3. Аналіз ефективності найпростіших ГПВЧ

Аналіз найпростіших ГПВЧ – ЛКГ і РЗЛЗЗ – свідчить про їх обмеження, пов'язані з необхідністю підбору параметрів для забезпечення необхідних статистичних властивостей ПВП. Зокрема, допустимі значення параметрів генераторів для забезпечення максимального періоду ПВП наведено в таблиці 1.2.

Таблиця 1.2

Параметри ГПВЧ для досягнення максимального періоду ПВП

Метод	Період	Допустимі значення параметрів ГПВЧ	Розмір простору допустимих значень параметрів ГПВЧ
Лінійний конгруентний метод	$T=M$	1) $НСД(C,M)=1$; 2) $\lvert K-1\rvert_p=0$ для $\forall$ простого $p:\lvert M\rvert_p=0$; 3) якщо $\lvert M\rvert_4=0\Rightarrow\lvert K-1\rvert_4=0$. Приклади реалізації: Java: $M=2^{48}$, $K=25214903917$, $C=11$; C/C++: $M=2^{32}$, $K=22695477$, $C=1$; Delphi: $M=2^{32}$, $K=134775813$, $C=1$.	$\varphi(M)\cdot P$, де P – кількість значень K, що задовольняють умовам 2 і 3. Для $M=2^{32}$ – 2^{61}. Для простого M – $M-1$.
Метод на основі РЗЛЗЗ	$T=2^n-1$	Генераторний поліном $G_n(x)$ – примітивний.	Відповідає кількості примітивних поліномів степені n
Метод формування ПВП на основі конкатенації циклів ЛКГ	$T=M$	$НСД(K,M)=1$.	$\varphi(M)\cdot M$. Для $M=2^{32}$ – 2^{63}. Для простого M – $(M-1)\cdot M$.

Продовження таблиці 1.2

Метод формування ПВП на основі конкатенації циклів РЗЛЗЗ	$T = 2^n$	Генераторний поліном $G_n(x)$ – породжує циклічну структуру графа станів РЗЛЗЗ.	Відповідає кількості поліномів степені n, які породжують циклічну структуру графа станів РЗЛЗЗ

Для подальшого дослідження та аналізу побудови ГПВЧ на основі послідовного обходу всіх вершин графа станів ЛКГ необхідно:

1) виконати поглиблене дослідження структури графа станів ЛКГ;
2) виконати розширений аналіз впливу параметрів ЛКГ на структуру його графа;
3) розвинути метод формування послідовностей псевдовипадкових чисел на основі лінійного конгруентного методу шляхом послідовного обходу контуру графа станів генератора.

1.5. Комбінаційний генератор

Недоліком багатьох існуючих методів формування послідовностей рівномірно розподілених псевдовипадкових чисел (наприклад, послідовностей, утворених РЗЛЗЗ, вихором Мерсенна й ін.) є їх мала лінійна складність і, як наслідок, простота розкриття закону утворення послідовності за її відрізком. Крім того, ряд методів (РЗЛЗЗ, ЛКГ й ін.) мають занадто малий період повторення послідовності і не дозволяють отримати рівномірний розподіл д.в.в. на множині значень, що включає значення нуля. У такому випадку слід вдаватися до операції рандомізації, що ускладнює процедуру формування випадкових чисел. Обмежений період також може бути недоліком у разі використання попередньо сформованої і записаної послідовності істинно випадкових чисел.

Крім того, всі ГПВЧ формують числа певної розрядності. У ряді випадків, у тому числі й для задач формування перестановок під час факторіального кодування, необхідно забезпечити рівномірний розподіл чисел у діапазоні з довільною верхньою межею. Приведення ж випадкових чисел до потрібного діапазону може призводити до порушення рівномірності.

Для усунення зазначених недоліків в ряді відомих робіт ([156], [188]–[190] та ін.), докладно висвітлених і систематизованих у [78], пропонується використання комбінації декількох випадкових процесів.

Для підвищення криптографічного стійкості генераторів ПВП використовують функцію ускладнення [187], вхідними змінними для якої є елементи послідовностей, що формуються на виходах первинних генераторів. Виходи деяких первинних генераторів можуть управляти синхронізацією інших первинних генераторів. Така схема, наприклад, може забезпечувати роботу первинних генераторів за принципом «stop-and-go», з різною частотою і т.п. Ключовою інформацією є параметри схеми синхронізації та функції ускладнення, а також ВПЗ первинних генераторів.

Генератор, що містить у своєму складі кілька первинних автономних генераторів (псевдо) випадкових чисел і забезпечує їх комбінування, будемо називати комбінаційним генератором [78], а функцію ускладнення – комбінаційною функцією [78]. Розглянемо деякі відомі комбінаційні генератори.

1.5.1. Комбінація конгруентних генераторів

У [78] зазначено, що ЛКГ не можна використовувати в криптографії, оскільки вони передбачувані. Методи їх злому вперше продемонстровані в [191]–[194]. У роботах [195]–[197] розроблено способи розкриття будь-якого поліноміального генератора, в [198]–[200] – усічених ЛКГ, у [201], [202] – усічених ЛКГ з невідомими параметрами. Водночас ЛКГ ефективні для некриптографічних додатків і в більшості емпіричних тестів демонструють задовільні характеристики.

У роботах [129], [203] зроблено спроби об’єднання ЛКГ. У цих роботах показано, що криптографічна стійкість отриманих послідовностей не підвищується, проте вони володіють великими періодами і кращими показниками в деяких тестах.

Так, у роботі [129] запропоновано комбінаційний генератор для 32-бітових комп’ютерів з періодом, близьким до 10^{18}. Цей генератор працює, якщо комп’ютер може представити все цілі числа між $-2^{31}+85$ і $2^{31}-249$. Для 16-бітового комп’ютера в [129] запропоновано інший генератор з періодом $1.6\cdot10^{13}$.

У роботі [204] запропоновано комбінаційний генератор, який використовує в

якості первинних генераторів генератори на основі інверсного конгруентного методу [205]. Комбінаційною функцією є арифметичне підсумовування з подальшим виділенням деякої кількості найменш значущих біт суми. В результаті використання запропонованого алгоритму гарантується генерація бітових потоків з максимальною лінійної складністю. Всі первинні інверсні генератори комбінаційного генератора, отримані відповідно до описаного алгоритму, повинні мати максимальні періоди, рівні лінійних складностей, задовільні статистичні властивості і швидкість генерації, що перевищує 1,5 Мбіт/с.

Зауважимо, що представлений генератор орієнтований на формування тільки двійкового потоку псевдовипадкових біт, а комбінаційна функція обмежена сімейством функцій підсумовування за модулем 2^k.

1.5.2. Комбінаційний генератор на основі регістрів зсуву з лінійними зворотними зв'язками

Основний підхід під час проектування комбінаційного генератора ПВП на основі РЗЛЗЗ простий [78]. Спочатку береться один або кілька РЗЛЗЗ, зазвичай з різними періодами і різними утворюючими багаточленами. Якщо періоди взаємно прості, а всі утворюючі багаточлени примітивні, то утворений комбінаційний генератор має максимальний період. Ключем є початкові стани РЗЛЗЗ. Під час формування нового біта виконується зсув послідовності біт первинних РЗЛЗЗ. Біт виходу є результатом функції, бажано нелінійної, деяких бітів первинних РЗЛЗЗ.

Приклади комбінаційних генераторів на основі РЗЛЗЗ [78]:

- генератор Геффа [188];
- узагальнений генератор Геффа;
- генератор Дженнінгса [206], [207];
- генератор «стоп-пішов» [189];
- генератор «стоп-пішов», що чергується [208];
- двосторонній генератор «стоп-пішов» [209];
- пороговий генератор [210];
- самопроріджуваний (self-decimated) генератор [190], [211];

- підсумовуючий генератор [212];
- каскад Голлманна [213];
- A5 [78] та інші.

Водночас, незважаючи на досить велику різноманітність комбінаційних генераторів на основі РЗЛЗЗ, вони уразливі до атак [78].

1.5.3. Комбінаційний генератор на основі регістра зсуву зі зворотним зв'язком за перенесенням

Регістр зсуву зі зворотним зв'язком за перенесенням (РЗЗЗП) схожий на РЗЛЗЗ [78]. В обох є регістр зсуву та функція зворотного зв'язку. Різниця полягає в тому, що в РЗЗЗП є також регістр перенесення, і замість виконання підсумовування за модулем два над усіма бітами відвідної послідовності ці біти підсумовуються між собою і з вмістом регістра перенесення. Значення отриманої суми за модулем два є новим бітом. Значення суми, поділеної на два, заноситься в регістр перенесення.

Згідно [78] комбінаційні генератори на основі РЗЗЗП використовують змінну кількість РЗЗЗП і/або РЗЛЗЗ і множину функцій, які об'єднують регістри. Оскільки операція XOR руйнує алгебраїчні властивості РЗЗЗП, має сенс використовувати цю операцію для їх об'єднання.

Інші комбінаційні генератори на основі РЗЗЗП, які розвивають описані принципи [78]:

- генератор парності РЗЗЗП. Усі регістри – РЗЗЗП, комбінаційна функція – XOR;

- генератор парності РЗЛЗЗ/РЗЗЗП. Використовується суміш РЗЛЗЗ і РЗЗЗП, комбінаційна функція – XOR;

- пороговий генератор РЗЗЗП. Усі регістри – РЗЗЗП, комбінаційна функція – мажорування;

- пороговий генератор РЗЛЗЗ/РЗЗЗП. Використовується суміш РЗЛЗЗ і РЗЗЗП, а комбінаційна функція – мажорування;

- підсумовуючий генератор РЗЗЗП. Усі регістри – РЗЗЗП, а комбінаційна функція – додавання з переносом;

− підсумовуючий генератор РЗЛЗЗ/РЗЗЗП. Використовується суміш РЗЛЗЗ і РЗЗЗП, а комбінаційна функція – додавання з переносом.

1.5.4. Рандомізація перемішуванням

Рандомізація перемішуванням базується на операції перемішування (перестановки) символів послідовності первинного генератора відповідно до визначеного правила. Найбільш відомими алгоритмами формування ПВП, що реалізують рандомізацію перемішуванням, є алгоритми М і В, назви яких запропоновані в [156].

Алгоритм М описано в [214], [215]. Алгоритм представляє собою спосіб об’єднання кілька псевдовипадкових потоків, збільшуючи їх безпеку. Вихід одного генератора використовується для зміни порядку елементів на виході іншого.

Довжина послідовності в результаті реалізації алгоритму М дорівнює найменшому спільному кратному довжин вихідних послідовностей.

У [216] показано, що алгоритм М здатний породжувати задовільну послідовність навіть тоді, коли він застосовується до такої невипадкової послідовності, як послідовність Фібоначчі. Водночас для алгоритму М також можливе отримання послідовності, менш випадкової, ніж вихідна послідовність. Такі проблеми не виникають з алгоритмом В.

Алгоритм В описано в [217]. На відміну від алгоритму М, алгоритм В вимагає на вході тільки одну послідовність, однак може дати кращі результати.

Водночас, як показано в [156], методи перемішування мають «вроджений дефект» – вони змінюють порядок проходження чисел, але не самі числа. Це є причиною, що подібні перетворення не дозволяють ліквідувати деякі статистичні нерегулярності вихідних послідовностей. Крім того, рандомізація перемішуванням не дозволяє стартувати з заданого місця в циклі або швидко в ньому переміщатися.

1.5.5. Комбінаційний генератор на основі конкатенації слів первинних генераторів

У роботі [21] розроблено метод формування рівномірно розподіленої

випадкової послідовності чисел на основі конкатенації слів, утворених незалежними первинними генераторами рівномірно розподілених випадкових чисел, який дозволяє без зменшення продуктивності генератора формувати послідовність рівномірно розподілених випадкових чисел з розрядністю, що виходить за межі розрядності обчислювальної платформи первинних генераторів.

Наведемо основні положення роботи [21].

Твердження 1.2 (з [21])**.** Д.в.в., сформована шляхом конкатенації k рівномірно розподілених незалежних д.в.в., що приймають цілі невід'ємні значення, має також рівномірний розподіл.

Нехай $k=2$, а вихідні рівномірно розподілені д.в.в. X і Y представимо в деякій позиційній системі числення з основою $a: X=\alpha_{n_x-1}\alpha_{n_x-2}\ldots\alpha_1\alpha_0=\sum_{i=0}^{n_x-1}\alpha_i a^i$, $Y=\beta_{n_y-1}\beta_{n_y-2}\ldots\beta_1\beta_0=\sum_{j=0}^{n_y-1}\beta_j a^j$, де $\alpha_i,\beta_j\in[0;a-1]$. Розрядність д.в.в. X становить n_x розрядів, д.в.в. Y – n_y розрядів.

Результатом конкатенації є д.в.в. $Z=Y\cdot a^{n_x}+X=\gamma_{n_x+n_y-1}\gamma_{n_x+n_y-2}\ldots\gamma_1\gamma_0=\gamma_{n_x+n_y-1}a^{n_x+n_y-1}+\gamma_{n_x+n_y-2}a^{n_x+n_y-2}+\ldots+\gamma_1 a^1+\gamma_0=$ $=\sum_{k=0}^{n_x+n_y-1}\gamma_k a^k$, де $\gamma_k\in[0;x-1]$; $\begin{cases}\gamma_k=\alpha_k \text{ при } k\in[0;m-1];\\ \gamma_k=\beta_{k-m} \text{ при } k\in[m;n+m-1].\end{cases}$

Розрядність д.в.в. Z становить n_x+n_y розрядів.

Якщо д.в.в. X і Y рівномірно розподілені на відрізках $[A_x,B_x]$ і $[A_y,B_y]$, то д.в.в. Z рівномірно розподілена на множині цілих чисел з діапазону $\bigcup_{l=A_y}^{B_y}\left[la^{n_x}+A_x,la^{n_x}+B_x\right]$ з потужністю множини значень N_xN_y, де $N_x=B_x-A_x+1$, $N_y=B_y-A_y+1$. Тоді функція розподілу д.в.в. $Z=Y\cdot a^{n_x}+X$ дорівнює $F(z)=\frac{1}{N_xN_y}\left(\frac{z'-|z'|_{a^{n_x}}}{a^{n_x}}\cdot N_x+|z'|_{a^{n_x}}\right)$, де $z'=z-A_y\cdot a^{n_x}-A_x$.

Якщо в операції конкатенації беруть участь k рівномірно розподілених

незалежних д.в.в. з потужностями множин значень $N_0, N_1, \ldots, N_{k-1}$, то закон розподілу конкатенації має вигляд: $P(Z = z_i) = 1/(N_0 N_1 \ldots N_{k-1})$. Функція розподілу:

$$F(z) = \frac{1}{N_0 N_1 \ldots N_{k-1}} \left(\sum_{i=1}^{k-1} \frac{|z'|_{a^{p_{i+1}}} - |z'|_{a^{p_i}}}{a^{p_i}} \cdot N_i + |z'|_{a^{p_1}} \right), \text{ де } z' = z - \sum_{j=0}^{k-1} A_i \cdot a^{p_j}$$

За рівномірного розподілу чисел на виході i-го первинного генератора на відрізку $[A_i, B_i]$ $(i \in [0, k-1])$ конкатенація чисел з виходів генераторів рівномірно розподілена на множині чисел діапазону $\bigcup_{l_{k-1}=A_{k-1}}^{B_{k-1}} \ldots \bigcup_{l_2=A_2}^{B_2} \bigcup_{l_1=A_1}^{B_1} \begin{bmatrix} l_{k-1} a^{p_{k-1}} + \ldots + l_2 a^{p_2} + l_1 a^{p_1} + A_0, \\ l_{k-1} a^{p_{k-1}} + \ldots + l_2 a^{p_2} + l_1 a^{p_1} + B_0 \end{bmatrix}$, де $p_m = \sum_{l=0}^{m-1} n_l \ (m > 0), p_0 = 0$.

Таким чином, у залежності від розрядностей слів вихідних джерел випадкових чисел і діапазонів їх розподілу можна легко визначити розрядність і діапазон рівномірного розподілу конкатенації цих слів. Указану операцію можна зробити і в зворотному напрямку – в залежності від необхідних значень розрядності і діапазону розподілу складених чисел можна визначити параметри первинних послідовностей.

1.5.6. Комбінаційний генератор на основі підсумовування за модулем

У [156] показано, що простим способом, позбавленим дефектів перемішування, є спосіб, який реалізує комбінаційну функцію

$$Z_n = |X_n + Y_n|_M, \tag{1.7}$$

де X_n, Y_n – елементи послідовностей двох первинних генераторів, $0 \le X_n < M$, $0 \le Y_n < M' \le M$.

Період послідовності $\{Z_n\}$ дорівнює

$$T_Z = НСК(T_X; T_Y), \tag{1.8}$$

де T_X, T_Y – періоди первинних генераторів.

Очевидно, що якщо T_X і T_Y взаємно прості, то $T_Z = T_X \cdot T_Y$.

Крім того, в [156] показано наступну закономірність. Нехай розкладання T_X на прості множники має вигляд $T_X = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot \ldots$, а $T_Y = 2^{f_2} \cdot 3^{f_3} \cdot 5^{f_5} \cdot \ldots$. Нехай

$$g_p = \begin{cases} \max\left(e_p; f_p\right) \ при \ e_p \neq f_p; \\ 0 \ при \ e_p = f_p. \end{cases}$$

Нехай також $T_0 = 2^{g_2} \cdot 3^{g_3} \cdot 5^{g_5} \cdot \ldots$. Тоді період T_Z послідовності $\{Z_n\}$ кратний T_0 і є дільником $T = НСК\left(T_X; T_Y\right)$. Зокрема, $T_Z = T = НСК\left(T_X; T_Y\right)$, якщо $e_p \neq f_p$ або $e_p = f_p = 0$ для кожного простого p.

У роботах [218], [219] показано, що період послідовності-суми неявно обмежений наступною умовою:

$$НСК\left(T_X; T_Y\right) / НСД\left(T_X; T_Y\right) \leq T_Z \leq НСК\left(T_X; T_Y\right). \quad (1.9)$$

Як наслідок, $T_Z = T_X \cdot T_Y$ тоді і тільки тоді, коли $НСД\left(T_X; T_Y\right) = 1$ – періоди двох первинних послідовностей взаємно прості [220].

Межі для лінійної складності $\Lambda(z)$ суми послідовностей згідно [218]:

$$\Lambda(x) + \Lambda(y) - 2 \cdot НСД\left(T_X; T_Y\right) \leq \Lambda(z) \leq \Lambda(x) + \Lambda(y), \quad (1.10)$$

де $\Lambda(x)$, $\Lambda(y)$ – лінійні складності первинних послідовностей.

У [156] також показано, що комбінування (1.7) має тенденцію до збільшення випадковості, якщо початкові значення X_0 і Y_0 є незалежними випадковими величинами.

Крім того, такий генератор, на відміну від інших, може дозволити формувати рівномірно розподілену послідовність чисел у довільному діапазоні значень.

Водночас теорія побудови комбінаційних генераторів на основі підсумовування по модулю в літературі висвітлена недостатньо. Зокрема, цікавість представляє комбінування генераторів, що породжують послідовності цілих чисел заданого відрізка без повторів і пропусків (перестановок). Такими генераторами, наприклад, можуть служити генератори на основі лінійного конгруентного методу в режимі циклічного формування надциклу.

Однією з задач цього дисертаційного дослідження є теоретичне обґрунтування принципів побудови комбінаційних ГПВЧ, які використовують перестановки чисел в якості первинних послідовностей і підсумовування за модулем у якості комбінаційної функції. Для цього необхідно:

− дослідити закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем у залежності від параметрів первинних генераторів;

− обґрунтувати загальні вимоги до первинних генераторів для отримання рівномірного закону розподілу д.в.в. на виході комбінаційного генератора;

− виконати аналіз послідовності на виході комбінаційного генератора за допомогою графічних і статистичних методів тестування для різних первинних послідовностей.

1.6. Генератор перестановок

Вирішення задач захисту інформації на основі ФСЧ, а також інших задач сортування масивів, пошуку оптимальних шляхів обходу вершин графа, складання розкладів, інших задач комп'ютерної криптографії тощо зводиться до автоматизації процесу формування послідовності перестановок.

Під випадкової перестановкою будемо розуміти випадкову послідовність $\pi = (\pi_0; \pi_1; ...; \pi_{M-1})$, усі елементи якої приймають значення від 0 до $M-1$. За цих обставин імовірність збігу будь-яких двох елементів дорівнює нулю.

1.6.1. Нумерація перестановок

Одним із способів подання перестановок порядку M є ціле число $B: 0 \le B < M!$ за умови, що існують зручні методи для прямого і зворотного перетворення між числом B і поданням перестановки у вигляді впорядкованої послідовності чисел. Цей підхід дозволяє найбільш компактно подавати довільні перестановки. Обмеженням його є те, що B має вміщатися в машинному слові. Тоді для 32-розрядних систем порядок перестановки обмежений виразом $M \le 12$, а для 64-бітових $M \le 20$. Перетворення $B \leftrightarrow \pi$ може бути виконано через проміжну форму послідовності чисел $b_i: 0 \le b_i \le i$, $i \in [0, M-1]$. Таке подання використовує позиційну систему числення з факторіальною основою (надалі – факторіальну систему числення). Інший підхід використовує множину $\{b_i\}$ для формування коду

Лемера або (що майже еквівалентно) таблицю інверсій.

Розглянемо властивості цих подань більш докладно.

1.6.1.1. Подання перестановки в факторіальній системі числення

Підхід до побудови перестановок на основі використання ФСЧ, докладно викладено в роботах [221], [222].

ФСЧ забезпечує виконання арифметичних операцій і взаємно однозначний зв'язок довільного числа B, що належить числовому відрізку $[0, M!-1]$ і позначає номер перестановки, з перестановкою π. Для формування перестановки її номер у ФСЧ для випадку розташування символів від молодшого розряду до старшого записується наступним чином:

$$B = \sum_{i=0}^{M-1} b_i \cdot i! = \sum_{i=0}^{M-1} b_{M-1-i} \cdot (M-1-i)! \qquad (1.11)$$

За розташування символів від старшого розряду до молодшого номер перестановки записується у вигляді:

$$B = \sum_{i=0}^{M-1} b_i \cdot (M-1-i)! = \sum_{i=0}^{M-1} b_{M-1-i} \cdot i! \ . \qquad (1.12)$$

Для визначеності надалі будемо використовувати подання (1.11) з розташуванням символів від молодшого розряду до старшого.

Визначення 1.10. Послідовність чисел b_i у поданні перестановки π в ФСЧ будемо називати синдромом перестановки S_F і записувати його у вигляді

$$S_F = (b_{M-1}; b_{M-2}; \ldots; b_0). \qquad (1.13)$$

Зазначимо, що вираз (1.11) описує модель лототрону з M кулями всередині, пронумерованими числами $\{0;1;...;M-1\}$.

Формування перестановки проводиться послідовним витяганням куль, причому вибір першого символу проводиться довільним вибором однієї з M можливих куль (це є старший розряд суми (1.11)), вибір другого символу проводиться довільним вибором однієї з $(M-1)$ можливих куль і т.д. Вибір передостаннього символу проводиться вільним вибором одного з двох куль, що

залишилися, а останній символ визначається єдиним чином – останньою залишеною кулею (це є молодший розряд суми (1.11)). Описана модель процесу формування перестановок дозволяє пронумерувати всі можливі перестановки під час багаторазового повторення процесу їх синтезу і служить основою (моделлю) для побудови генератора перестановок.

Перевагою використання ФСЧ для формування перестановок є можливість швидкого перебору факторіальних чисел у порядку зростання або зменшення їх значень, отримання перестановок великого порядку, формування перестановок заданого діапазону їх номерів. Серед робіт, присвячених вирішенню задач ефективного перетворення десяткових і двійкових чисел у факторіальні, а також перетворення факторіальних чисел у перестановки, слід виділити роботи [223]–[228]. Запропоновані в них методи і підходи дозволяють підвищити швидкодію операцій перетворення $B \leftrightarrow S_F$, $S_F \leftrightarrow \pi$ і, тим самим, підвищити ефективність формування перестановок на основі ФСЧ.

1.6.1.2. Подання перестановки в коді Лемера

Кодова комбінація для перестановки $\pi = (\pi_0; \pi_1; ...; \pi_{M-1})$ в коді Лемера [229] являє собою послідовність чисел $(\beta_{M-1}; \beta_{M-2}; \ldots; \beta_0)$, які визначаються наступним чином. Число β_{M-1} дорівнює кількості чисел множини $\{0;1;\ldots;M-1\}$, менших, ніж перший елемент перестановки π_0. Число β_{M-2} дорівнює кількості чисел, менших, ніж другий елемент перестановки π_1 серед інших $M-1$ елементів множини $\{0;1;\ldots;M-1\}$. Таким чином, кожне значення β_{M-1-i} визначається кількістю залишених у множині $\{0;1;\ldots;M-1\}$ елементів, менших за π_i. Оскільки ці залишені елементи з'являються в перестановці як деякий більш пізній елемент π_j, число β_{M-1-i} визначає кількість інверсій (i, j) (кількість значень j, для яких $i < j$ і $\pi_i > \pi_j$).

1.6.1.3. Подання перестановки у вигляді таблиці інверсій

Таблиця інверсій для перестановки $\pi = (\pi_0; \pi_1; ...; \pi_{M-1})$ схожа з кодом Лемера.

Відмінністю є те, що значення β_{M-1-k} відповідає числу інверсій (i, j), де $k = \pi_j$ зустрічається як менше з двох значень, що входять в інвертований порядок [230]. Обидва види кодування (код Лемера та таблиця інверсій) можуть бути візуалізовані за допомогою діаграми $M \times M$ Роте [231].

Перетворення послідовних натуральних чисел у ФСЧ формує послідовність факторіальних чисел у лексикографічному порядку. Подальше перетворення їх у перестановки зберігає лексикографічне впорядкування за умови використання коду Лемера (за використання таблиць інверсій формується інше впорядкування, де аналіз починається з пошуку позиції 1 в запису, а не зі значення на першій позиції). Сума чисел у поданні перестановки в ФСЧ визначає кількість інверсій перестановки, а парність цієї суми визначає парність перестановки. Більш того, позиції нулів у таблиці інверсій визначають максимальні значення елементів перестановки під час руху зліва направо, а положення нулів у коді Лемера – це позиції мінімальних значень елементів перестановки під час руху справа наліво. Це дозволяє обчислити розподіл таких екстремумів у будь-яких перестановках.

1.6.2. Методи формування послідовностей перестановок

Методи формування послідовностей перестановок класифікуються залежно від того, які перестановки потрібні – обрані випадковим чином або всі можливі. У останньому випадку потрібно конкретне їх впорядкування.

1.6.2.1. Детермінований порядок

Існують способи систематичного формування всіх перестановок заданої множини. Багато з них представлено в [221], [232].

Класичний алгоритм систематичного порядку перебору перестановок винайдено Пандіта Нарайан у 14 столітті в Індії і докладно описано в [221].

Для формування послідовності перестановок у лексикографічному порядку на основі ФСЧ попередньо за номером попередньої перестановки обчислюється номер наступної перестановки: $B \leftarrow B+1$, а потім і сама перестановка. Такий підхід визначає двоетапну процедуру перетворення порядкового номера перестановки в перестановку:

– на першому етапі створюється образ (синдром) перестановки;

– на другому етапі синдром трансформується в перестановку.

Такий принцип формування послідовності перестановок використано в [224] для розробки електронної системи формування перестановок, структурна схема якої зображена на рис. 1.1.

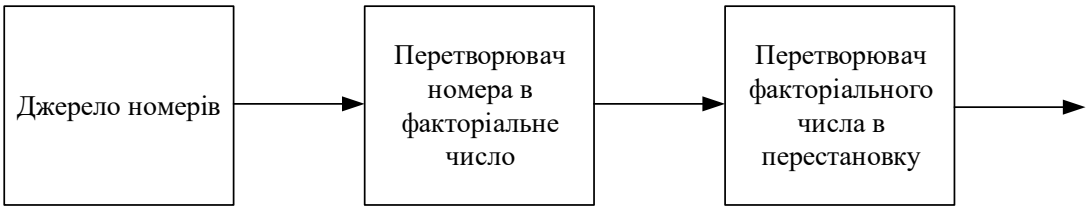


Рис. 1.1. Електронна система формування перестановок (з [224])

Метод перебору перестановок [233], а також метод, реалізований у пристрої для перебору перестановок [234], базуються на використанні ФСЧ і передбачають виконання операцій $B \to S_F \to \pi$. Пристрій містить факторіальний лічильник, на вхід якого подається +1 для обчислення номера кожної наступної перестановки.

Альтернативою методам формування перестановок у лексикографічному порядку є метод Штайнхауса-Джонсона-Троттера (алгоритм P) [221], який передбачає формування послідовності перестановок таким чином, що будь-які дві послідовні перестановки можуть бути отримані шляхом перестановки двох суміжних елементів. Такий порядок послідовності перестановок до 17-го століття був відомий англійським дзвонарям, серед яких він мав назву «прості зміни». Одним з переваг цього методу є те, що невелика кількість змін від однієї перестановки до наступної дозволяє реалізувати метод за постійний час на кожну перестановку. Так само можна легко згенерувати підмножину парних перестановок, пропускаючи кожну другу вихідну перестановку [221].

Альтернативою алгоритму P є алгоритм Хіпа [235].

Меандрові системи призводять до меандрових перестановок – спеціальній підмножині чергованих перестановок. Такі перестановки визначені на множині $\{0;1;\ldots;2M-1\}$ і є циклічними перестановками (без фіксованих точок).

Меандрові перестановки корисні під час аналізу вторинної структури РНК [236]. Варто зазначити, що не всі черговані перестановки меандрові.

Очевидно, що описані принципи формування наступної перестановки призводить до того, що послідовності перестановок є передбачуваними. Це означає, що з будь-якої перестановки можна обчислити всі наступні перестановки. Як наслідок, генератори перестановок, що реалізують описані методи, не володіють криптографічного стійкістю і не можуть бути використані в ряді практичних застосувань, наприклад, таких як електронні системи розіграшу лотерей, жеребкування спортивних змагань, тасування карт в електронних іграх, системи криптографічного захисту інформації.

Такі програми вимагають використання засобів формування послідовностей перестановок, що породжують випадковий порядок їх перебору і володіють властивостями відтворюваності і непередбачуваності. Зауважимо, що під властивістю відтворюваності мається на увазі можливість відтворення послідовності перестановок під час рознесення в просторі і (або) часу процесу їх формування.

1.6.2.2. Випадковий порядок

Основна ідея формування випадкової перестановки полягає в тому, щоб генерувати випадковим чином одну з $M!$ послідовностей цілих чисел $(b_{M-1};b_{M-2};\ldots;b_0)$, $0 \le b_i \le i$, і перетворити її в перестановку π за допомогою бієктивної відповідності. Для такого алгоритму в [224] запропоновано використовувати систему, структурна схема якої представлена на рис. 1.1.

У якості послідовності $(b_{M-1};b_{M-2};\ldots;b_0)$ може бути використано код Лемера. Такий метод формування послідовності випадкових перестановок називається тасуванням Фішера-Йєтса (тасуванням Кнута) [237]. Алгоритм тасування Фішера-Йєйтса незміщений – має рівномірний закон розподілу ймовірностей появи кожної перестановки. Час реалізації алгоритму пропорційний числу елементів множини M і не використовує додаткового простору.

Оригінальний метод Фішера-Йєтса передбачає наступну послідовність дій:

1) записуються числа від 0 до $M-1$;

2) обирається випадкове число k між одиницею і числом чисел, що залишилися;

3) викреслюється k-е залишене число. Викреслене число записується в якості наступного елементу перестановки;

4) повторюється крок 2, поки всі числа не будуть викреслені.

Таким чином, послідовність записаних на кроці 3 чисел є випадковою перестановкою чисел множини $\{0;1;\ldots;M-1\}$.

Модифікація алгоритму тасування Фішера-Йєтса для використання в комп'ютерах запропоновано Р. Дуршенфельдом в [238] під назвою «Algorithm 235: Random permutation». Цей алгоритм передбачає на кожній ітерації перенесення обраних чисел у кінець списку шляхом перестановки з останнім невибраний числом. Така модифікація скорочує часову і просторову складність алгоритму.

Ще однією модифікацією алгоритму Фішера-Йєтса є алгоритм Саттоло [239] для формування випадкових рівномірно розподілених циклічних перестановок. Різниця між алгоритмами Дуршенфельда і Саттоло полягає в кроці 2 – в алгоритмі Саттоло випадкове число k на i-ій ітерації обирається з множини $\{1;\ldots;M-i\}$, не з $\{1;\ldots;M-i+1\}$. Ця проста модифікація призводить до перестановок з одного циклу.

Аналіз існуючих методів формування послідовності перестановок показує, що найбільш розвиненими є методи формування перестановок у детермінованому порядку, зокрема, лексикографічному. Випадковий же порядок перестановок забезпечується за допомогою додаткового генератора рівномірно розподілених випадкових чисел в діапазоні зі змінною верхньою межею, максимальне значення якої дорівнює M. Реалізація такого генератора (особливо на основі детермінованого алгоритму) може викликати значні труднощі, пов'язані з приведенням випадкового числа до потрібного діапазону. Більш того, щоб уникнути появи нерівномірності розподілу під час використання ГПВЧ число його внутрішніх станів повинно перевищувати число перестановок на кілька порядків. Наприклад, для $M=52$ необхідно використовувати генератор, який має не менше 250-бітного числа станів. Таким чином, існуючий стан предметної області вимагає розробки нових методів формування відтворюваних випадкових послідовностей перестановок, частково або повністю позбавлених зазначених недоліків.

Задачею дослідження є розробка методу формування випадкової послідовності перестановок на основі використання ФСЧ без приведення випадкового числа до діапазону зі змінною верхньою межею. Породжувана послідовність перестановок повинна задовольняти вимогам:

– відсутність кореляції між символами всередині перестановки і між суміжними перестановками;

– послідовність перестановок повинна бути невідтворюваною без знання ключа взаємного зв'язку суміжних перестановок;

– закон розподілу перестановок повинен бути рівномірним – кожна з $M!$ можливих перестановок повинна зустрічатися з імовірністю $1/M!$.

1.7. Вимоги до ГПВЧ

Однією з проблемних і важливих задач під час проектування та дослідження ГВЧ і ГПВЧ є розробка вимог, які до них пред'являються.

Одне з перших формулювань основних вимог, що пред'являються до статистичних властивостей двійкових періодичних псевдовипадкових послідовностей, представлено в [240]. Три основних правила отримали у відкритій криптографії популярність як постулати Голомба [241]:

1) кількість одиниць у кожному циклі повинно відрізнятися від кількості нулів не більше, ніж на одиницю;

2) у кожному циклі половина серій (з однакових символів) повинна мати довжину один, одна чверть повинна мати довжину два, одна восьма повинна мати довжину три і т.д. Більш того, для кожної з цих довжин має бути однакова кількість серій з одиниць і нулів;

3) нехай існують дві копії однієї і тієї ж послідовності періоду T, зсунуті відносно один одного на деяке значення d. Тоді для кожного d, $0 \le d \le T-1$, можна підрахувати кількість узгодженостей (співпадінь) між цими двома послідовностями A_d і кількість неузгодженостей D_d. Коефіцієнт автокореляції для кожного d визначається співвідношенням $(A_d - D_d)/T$. Ця функція автокореляції

приймає різні значення в процесі того, як d приймає всі допустимі значення. Тоді для будь-якої послідовності, що задовольняє третьому правилу, функція автокореляції повинна приймати лише два значення (бути двозначною).

Варто відзначити, що сформульовані Голомбом правила характерні для класу послідовностей, що генеруються РЗЛЗЗ.

Набір вимог, які пред'являються до ГВЧ і ГПВЧ, визначається областю застосування генератора. Наприклад, для задач комп'ютерної криптографії згідно ДСТУ ISO/IEC 18031:2015 [242] набір цілей і вимог для генераторів випадкових біт складається з наступних пунктів:

− неможливість відрізнити послідовність генератора від послідовності істинно однорідно розподілених випадкових біт. Усі комбінації біт генератора повинні виникати з однаковою ймовірністю, а серії комбінацій – мати однорідний розподіл;

− послідовність повинна бути важко передбачуваною – повинна бути виключена практична можливість обчислення будь-якого наступного або попереднього елементу послідовності генератора без знання його параметрів;

− вихідний потік не повинен повторюватися протягом життєвого циклу ГВЧ;

− вихідні дані генератора не повинні містити інформацію про приховувані параметри генератора (внутрішній стан, параметри і т.п.).

Таким чином, однією з найбільш важливих характеристик ГПВЧ є його період, після якого генеровані числа будуть повторюватися і їх можна легко передбачити. Період практично визначає можливе число ключів криптосистеми. Чим він більший, тим складніше підібрати ключ.

Друга із зазначених вище вимог пов'язана з проблемою визначення механізмів підтвердження факту, що послідовність чисел генератора дійсно є непередбачуваною. У теперішній час у світі не існує універсальних і практично перевірених критеріїв для перевірки цієї властивості. Тому для того, щоб послідовність вважалася випадковою і непередбачуваною, необхідно, щоб її період був дуже великим, а різні комбінації елементів зустрічалися з однаковою частотою.

Очевидно, що наведених правил і вимог недостатньо для вирішення проблеми визначення «випадковості» аналізованої послідовності. Додаткові вимоги, що

пред’являються до ГВЧ і ГПВЧ, визначаються національними і промисловими стандартами США: FIPS PUB 140-2, зокрема, NIST Special Publication 800-90A [243], ANSI X9.17, ANSI X9.31, ANSI X9.44, рекомендаціями органу з стандартизації Німеччини: AIS-20, AIS-31 та іншими.

Для тестування послідовностей чисел застосовується широкий спектр тестів і критеріїв. Такі тести і критерії детально описані в [156], [187], [241], [244] і спрямовані на перевірку гіпотези про використання для генерації послідовності природного джерела білого шуму. Звернемо увагу, що термін «білий шум» є неоднозначним (див., наприклад, визначення в [245, с. 90] або [246]). У цій роботі використовується визначення з [246] і під дискретним білим шумом розуміється стаціонарний дискретний випадковий процес, чиї вибірки некорельовані.

Багато тестів і критеріїв реалізовано в спеціалізованих прикладних пакетах тестів, найбільш відомими є DIEHARD [247], NIST STS [248], TestU01 [249].

Розглянемо більш докладно цілі та методи тестування ГПВЧ. Врахуємо також, що статистичні критерії і тести для послідовностей ГПВЧ можуть також бути успішно застосовані для аналізу ГВЧ з метою виявлення неоптимальних процедур перетворення фізичних процесів у послідовності випадкових чисел. Крім того, методи тестування ГПВЧ також ефективно застосовуються для аналізу якості криптографічних перетворень.

1.8. Тестування ГПВЧ

У процесі тестування ГПВЧ проводиться оцінка міри близькості заданої псевдовипадкової послідовності до випадкової. Існує дві групи методів тестування ПВП: графічні та статистичні.

1.8.1. Графічні методи тестування

До цієї категорії відносяться методи, результати яких відображаються у вигляді графіків, що характеризують властивості досліджуваної послідовності. Згідно [187], основними графічними методами тестування є:

1) гістограма розподілу елементів послідовності;

2) розподіл на площині;

3) перевірка серій;

4) перевірка на монотонність;

5) автокореляційна функція;

6) профіль лінійної складності;

7) графічний спектральний тест.

Слід зазначити, що результати графічних тестів інтерпретуються людиною і є суб'єктивними. Тому висновки на їх основі можуть бути неоднозначними.

1.8.2 Статистичні методи тестування

На відміну від графічних тестів, статистичні тести оцінюють чисельну характеристику послідовності і дозволяють із заданою довірчою ймовірністю визначити, пройдений тест чи ні. Найбільш відомі набори тестів:

- набір статистичних тестів Д. Кнута [156];
- DIEHARD Дж. Марсальї [247];
- NIST Statistical Test Suite [248];
- TestU01 [249].

Крім того, існують і інші набори, серед яких можна виділити CRYPT-X [250] і NIST PUB FIPS 140-2 [251].

На рис. 1.2, запозиченому з [252], показано найбільш відомі збірки статистичних тестів для оцінки якості роботи ГВЧ.

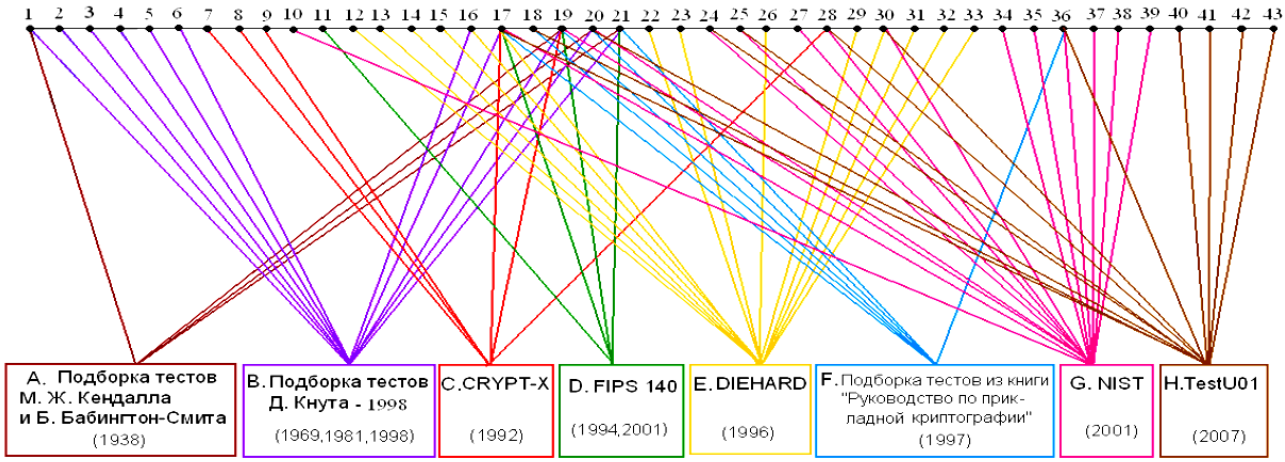


Рис. 1.2. Збірки статистичних тестів (рисунок запозичено з [252])

Представлені на рис. 1.2 тести:

1. Тест інтервалів (Gap test).

2. Тест конфліктів (Collision test).

3. Тест «максимум *t*» (Maximum-of-*t* test).

4. Тест серійної кореляції (Serial correlation test).

5. Тест збирача купонів (Coupon collector's test).

6. Тест перестановок (Permutation test).

7. Перевірка бінарної похідної (Binary derivative test).

8. Тест точок переходу (Change point test).

9. Тест складності послідовності (Sequence complexity test).

10. Перевірка кумулятивних сум (Cumulative sums (Cusum) test).

11. Тест довгих підпослідовностей (Long run test).

12. Тест на паркування (Parking lot test).

13. Мавпячі тести (Monkey tests).

14. Тест стиснення (Squeeze test).

15. Тест 3D-сфер (3D spheres test).

16. Тест проміжків між днями народження (Birthday spacings test).

17. Тест підпослідовностей (Run test або Runs test).

18. Перевірка автокореляції (Autocorrelation test).

19. Частотний тест (Frequency test).

20. Тест серій (Serial Test).

21. Тест покеру (Poker test).

22. Тест пересічних сум (Overlapping sums test).

23. Тест гри в кості (Craps test).

24. Спектральний тест (Spectral test).

25. Перевірка стиснення за допомогою алгоритму Лемпеля-Зіва (Lempel-Ziv complexity test або Lempel-Ziv compression test).

26. Підрахунок числа одиниць в певних байтах (Count the 1's in specific bytes).

27. Перевірка апроксимованої ентропії (Approximate entropy test).

28. Перевірка лінійної складності (Linear complexity test).

29. Перевірка потоку біт (Bitstream test).

30. Перевірка рангів матриць (Binary matrix rank test).

31. Підрахунок 1 в потоці байт (The count-the-1’s test on a stream of byte).

32. Тест на мінімальну відстань (Minimum distance test).

33. Перевірка пересічних перестановок (Overlapping 5-permutations test).

34. Частотний тест в підпослідовність (Frequency test within a block).

35. Перевірка випадкових відхилень (Random excursion test).

36. Універсальний тест Маурера (Maurer’s «Universal Statistical» test).

37. Тест «блоків» в підпослідовність (Test for longest run of ones in a block).

38. Перевірка пересічних шаблонів (Overlapping template matching test).

39. Перевірка непересічних шаблонів (Non-overlapping template matching test).

40. Перевірка випадкових блукань (Random walk test).

41. CAT-тест (CAT-test).

42. Перевірка ваг Хеммінга (Hamming weights).

43. Тест найдовшою послідовності (Longest run of 1’s test).

Методики тестування генераторів запропоновані також у [253], [254].

Тести Д. Кнута [156], здебільшого, базуються на статистичному критерії χ^2. Обчислене значення статистики χ^2 порівнюється з табличними результатами, і в залежності від імовірності появи такої статистики робиться висновок про її якість. Перевагою цих тестів є їх невелика кількість і швидкі алгоритми їх виконання.

Тести Diehard [247] розроблені Дж. Марсалья. Представлені в роботі [249] результати аналізу тестів Diehard свідчать про їх недоліки та обмеження:

– послідовність тестів, а також їх параметри (розмір вибірки і т.д.) фіксовані;

– розміри вибірки не дуже великі: весь набір тестів запускається за кілька секунд процесорного часу на стандартному настільному комп’ютері. В результаті вони не дуже строгі, і у користувача мало гнучкості для їх зміни;

– пакет також вимагає, щоб випадкові числа, що підлягають тестуванню, перебували в двійковому файлі у вигляді 32-бітних цілих чисел. Цей файл повинен бути переданий процедурам тестування. Ця вимога обмежує сферу застосування пакета: наприклад, багато ГВЧ формують числа з точністю менше 32 біт (наприклад,

часто можна зустріти 31 біт), а DIEHARD не допускає цього.

Пакет статистичних тестів NIST STS [248] розроблено спільно Відділом комп'ютерної безпеки і Статистичним відділом Національного інституту стандартів і технологій (NIST) США. До складу пакету входять 15 статистичних тестів.

TestU01 – пакет статистичних емпіричних тестів, реалізований на мові ANSI C, який пропонує набір утиліт для тестування генераторів випадкових чисел [249]. Він містить загальні реалізації класичних статистичних тестів, кілька запропонованих у літературі і кілька оригінальних.

TestU01 пропонує кілька батарей тестів, що включають SmallCrush (складається з 10 тестів), Crush (96 тестів) і BigCrush (106 тестів). Як показано в [249], час роботи батареї тестів SmallCrush на комп'ютері з процесором AMD Athlon 64 з частотою 2.4 GHz займає 14 секунд, Crush – 1 годину, BigCrush – 5,5 годин.

Тести класифікуються за двома категоріями:

- тести, які стосуються послідовностей дійсних чисел в діапазоні $(0;1)$;
- тести, призначені для послідовностей біт.

1.8.3. Постановка задачі розробки методу та критерію оцінювання ГПВЧ

Незважаючи на велику кількість розглянутих вище критеріїв, вони визначають лише деякі з умов, необхідних для забезпечення нерозрізненості послідовностей псевдовипадкових чисел від послідовностей випадкових чисел. Тому досліджувана ПВП може задовольняти відомій множині умов, проте не задовольняти деякій умові, що не входить в цю множину [244].

Таким чином, актуальною проблемою є проблема створення повного і комплексного набору критеріїв, застосування яких здатне віднести будь-яку з досліджуваних послідовностей чисел до категорії випадкової або псевдовипадкової.

Зауважимо, що статистичні критерії і тести, спрямовані на виявлення нерегулярностей у ПВП, можуть також бути успішно застосовані для аналізу ГВЧ. Такий аналіз використовується для виявлення неоптимальних процедур перетворення фізичних процесів у послідовності випадкових чисел і знаходить відображення в багатьох дослідженнях, серед яких можна виділити [255]–[257].

Через те, що повноту критеріїв аналізу послідовностей випадкових і псевдовипадкових чисел оцінити і довести надзвичайно складно, будь-який новий метод тестування послідовностей чисел з метою виявлення статистичних особливостей, властивих тільки послідовностям випадкових чисел, дозволяє наблизитися до вирішення цієї проблеми.

Виходячи з раніше наведеного визначення дискретного білого шуму [246], одним з найбільш поширених тестів, що дозволяє виявити статистичні нерегулярності досліджуваних послідовностей чисел, є автокореляційний тест.

У літературі широко досліджене це питання. Так, у [156], як і в [187], рекомендується використовувати критерій серійної (циклічної) кореляції між циклічно зсунутими копіями досліджуваної послідовності; у [249], [258], [259] оцінки коефіцієнтів автокореляції формуються на підставі порівняння підпослідовностей, відлік яких ведеться від початку і кінця досліджуваної послідовності. Незважаючи на різні підходи до знаходження емпіричних коефіцієнтів автокореляції, що формують оцінку автокореляційної функції (АКФ), основним завданням автокореляційного тесту є визначення відповідності оцінки АКФ досліджуваної послідовності АКФ випадкової послідовності чисел, описуваній дельта-функцією Дірака [260]. Таким чином, оцінки коефіцієнтів автокореляції в ненульових точках повинні прямувати до нуля, а їх значущість найбільш часто оцінюється згідно з t-критерієм Стьюдента [261].

Зазначимо також, що в [249] передбачається перевірка відповідності розподілу оцінок коефіцієнтів автокореляції в ненульових точках біноміальному закону, який за великої кількості значень може бути апроксимувати нормальним.

У роботах [262], [263] запропоновано статистичні критерії комплексного оцінювання бічних пелюсток АКФ, що передбачають замість тестування значущості кожного окремого коефіцієнта автокореляції перевірку на відміну від нуля відразу кількох коефіцієнтів автокореляції. Разом з тим, запропоновані критерії не адаптовані для аналізу послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел.

Таким чином, питання оцінки коефіцієнтів автокореляції все ще недостатньо

вивчене. Це призводить до необхідності проведення більш глибокого аналізу з метою виявлення кореляційних властивостей, властивих послідовностям, породженим природними джерелами дискретного білого шуму, і не властивих штучно згенерованим ПВП.

Тому однією з задач дисертаційного дослідження є розвиток існуючого методу і критерію комплексного оцінювання бічних пелюсток АКФ, а також розробка нового методу і критерію оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що дозволяє виявити в них не виявлені до теперішнього часу статистичні нерегулярності.

1.9. Цілі та задачі дисертаційного дослідження

Мета дослідження полягає в забезпеченні захисту та підвищенні достовірності передавання інформації в телекомунікаційних системах і мережах за рахунок розробки методологічних основ факторіального кодування даних з необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей.

У першому розділі виконано аналіз існуючих методів захисту інформації, що реалізують сумісний захист від помилок каналу зв’язку, несанкціонованої модифікації та/або несанкціонованого доступу. Показано, що розвинутими є методи інтеграції канального кодування та шифрування тільки для широкосмугових телекомунікаційних систем. Разом з тим, ці методи не дозволяють контролювати цілісність даних. Аналіз інших методів поєднання функцій криптографії та завадостійкого кодування свідчить про те, що на сьогоднішній день вони вимагають розвитку та вдосконалення. Встановлено, що використання перестановок для зазначених цілей є перспективним напрямком досліджень і вимагає подальшого розвитку.

Тому задачами роботи є:

– удосконалення методу формування псевдовипадкових послідовностей перестановок та створення теоретичного базису для методів факторіального

кодування даних;

– розробка методів роздільного факторіального кодування інформації для забезпечення її захисту від нав'язування хибних даних і помилок каналу зв'язку;

– розробка методів нероздільного факторіального кодування інформації для забезпечення її захисту від несанкціонованого доступу і помилок каналу зв'язку;

– розробка математичної моделі процесу декодування факторіальних кодів з метою оцінки ймовірності не виявленої декодером помилки.

Аналіз властивостей найпростіших генераторів ПВП – ЛКГ і генератора на основі РЗЛЗЗ – показує, що в теперішній час недостатньо вивченими є питання, пов'язані з формуванням на основі ЛКГ послідовностей, що складаються з усіх цілих чисел діапазону $[0; M-1]$, (перестановок порядку M) шляхом послідовного обходу вузлів графа його станів. Сформульовано задачі роботи, які полягають у дослідженні топології графа станів ЛКГ, вдосконаленні методу формування ПВП на основі конкатенації зв'язних компонентів графа станів ЛКГ для генерації елементів перетворення інформації в процесі факторіального кодування, а також удосконаленні методу симетричного криптографічного захисту інформації для забезпечення її конфіденційності.

Аналіз методів підвищення якості ПВП на основі їх комбінації показує, що теорія побудови комбінаційних генераторів з комбінаційною функцією підсумовування за модулем у літературі висвітлена недостатньо. Тому сформульовано задачу дисертаційного дослідження, яка полягає в теоретичному обґрунтуванні принципів побудови комбінаційного генератора, що використовує підсумовування за модулем у якості комбінаційної функції, для забезпечення необхідних статистичних властивостей під час вирішення задач захисту інформації на основі факторіального кодування, виконанні аналізу якості ПВП залежно від параметрів комбінаційного генератора і властивостей початкових послідовностей.

Сформульовано вимоги, що пред'являються до ГПВЧ. Виконано аналіз методів і засобів оцінювання їх якості. Показано, що одним з найбільш поширених тестів, що дозволяє виявити статистичні нерегулярності послідовностей чисел, є автокореляційний тест. Разом з тим, питання оцінки коефіцієнтів автокореляції все

ще недостатньо вивчене. Тому наступною задачею дисертаційного дослідження є розвиток існуючого критерію комплексного оцінювання бічних пелюсток АКФ, а також розробка методу і критерію оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що дозволяє виявити статистичні нерегулярності, які не виявляються існуючими методами тестування.

Для забезпечення підтримки процесів створення систем інтегрованого захисту інформації, що реалізують її сумісний захист від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу, необхідно розробити методологію захисту інформації на основі факторіального кодування даних, що є заключною задачею дисертаційної роботи.

Поставлені задачі дисертаційного дослідження несуть наукову новизну і практичну цінність, а їх вирішення дозволить досягти поставленої мети.

1.10. Висновки

У першому розділі:

- досліджено сучасний стан предметної області дисертаційної роботи: виконано аналіз методів поєднання функцій криптографії та завадостійкого кодування, зокрема, на основі використання перестановок; найпростіших ГПВЧ (ЛКГ і генератора на основі РЗЛЗЗ) і їх властивостей, комбінаційних ГПВЧ, генераторів перестановок, вимог до ГПВЧ і їх тестування,;
- сформульовано цілі дисертаційного дослідження;
- визначено коло задач, що підлягають вирішенню для досягнення поставлених цілей.

РОЗДІЛ 2. МЕТОДИ РОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУВАННЯ ІНФОРМАЦІЇ

2.1. Вступ

У першому розділі дисертації поставлено задачу розробки теоретичних і методологічних основ факторіального кодування інформації, що забезпечує її інтегрований захист від несанкціонованого доступу, нав'язування хибних даних і помилок у каналі зв'язку.

Поставлена задача тісно пов'язана ще з однією задачею дослідження – розробкою методу формування випадкової послідовності перестановок на основі використання ФСЧ.

2.2. Метод формування випадкової послідовності перестановок

Представимо розроблений і викладений у [27], [28] метод формування відтворюваної непередбачуваної послідовності перестановок на основі використання ФСЧ. При цьому будемо використовувати принципи подання перестановок у ФСЧ, детально описані в розділі 1.

Позначимо через $B(j)$ і $S_F(j)=\left(b_{M-1}(j);b_{M-2}(j);\ldots;b_0(j)\right)$ відповідно номер і синдром перестановки $\pi(j)$, що має j-у порядкову позицію в послідовності.

Для вирішення поставленої задачі, перш за все:

– відмовимося від виконання операцій (1.10) над числом B і перейдемо до операцій (1.12) над синдромом S_F;

– відмовимося від виконання операцій виду $B(j)=B(j-1)+1$ (відповідно, і від обчислення $S_F(j)=S_F(j-1)+1$), характерних, наприклад, для лексикографічного порядку формування перестановок, і перейдемо до операції виду

$$S_F(j)=S_F(j-1)\dot{+}t_{10}(j), \tag{2.1}$$

де $t_{10}(j)$ – випадкове число, представлене в десятковій системі числення і

позначає зсув порядкового номера формованої j-ої перестановки відносно порядкового номера попередньої перестановки на відрізку $[0, M!-1]$ числовій осі;

символ $\dot{+}$ позначає додавання чисел різних систем числення – факторіальної $(S_F(j-1))$ та десяткової $(t_{10}(j))$.

Випадкову величину $t_{10}(j)$ формує вбудований генератор (псевдо) випадкових чисел. Перехід до обчислення $S_F(j) = S_F(j-1) \dot{+} t_{10}(j)$ для випадкового $t_{10}(j)$ призводить до випадкового порядку проходження перестановок. У отриманій послідовності перестановок ступінь їх кореляції визначається статистичними властивостями послідовності символів $t_{10}(j)$.

2.2.1. Визначення процедури перетворення синдрому перестановки

Для реалізації процедури обчислення $S_F(j)$ за значеннями $S_F(j-1)$ і $t_{10}(j)$ створено правила обчислення:

– кожного з чисел $b_i(j)$ за заданими $b_i(j-1)$ і $t_{10}(j)$,

– символів переносу з молодшого розряду в старший: $\psi_i(j)$.

Правила мають вигляд:

$$b_i(j) = \left| b_i(j-1) + \psi_{i-1}(j) \right|_{i+1}, \tag{2.2}$$

де

$$\psi_i(j) = \left\lfloor \frac{b_i(j-1) + \psi_{i-1}(j)}{i+1} \right\rfloor, \tag{2.3}$$

де $i \in [1; M-1]$,

$\psi_0(j) = t_{10}(j)$.

Якщо прийняти, що $\mathrm{E}\left(\frac{a}{b}\right) = \left\lfloor \frac{a}{b} \right\rfloor$ – ціла частина дробу $\frac{a}{b}$, а $\varepsilon\left(\frac{a}{b}\right) = \frac{a}{b} - \left\lfloor \frac{a}{b} \right\rfloor = \frac{|a|_b}{b}$ – дрібна частина дробу $\frac{a}{b}$, то $\frac{a}{b} = \mathrm{E}\left(\frac{a}{b}\right) + \varepsilon\left(\frac{a}{b}\right)$, а вирази (2.2) і (2.3) приймуть такий вигляд:

$$b_i(j)=\varepsilon\left(\frac{b_i(j-1)+\psi_{i-1}(j)}{i+1}\right)\cdot(i+1), \tag{2.4}$$

$$\psi_i(j)=\mathrm{E}\left(\frac{b_i(j-1)+\psi_{i-1}(j)}{i+1}\right). \tag{2.5}$$

Особливістю наведених правил є те, що операції обчислення чисел за формулами (2.4) і (2.5) виконуються в десятковій системі числення.

Звернемо увагу на те, що всі числа, що входять до виразу (2.2), (2.3), (2.4), (2.5), не перевищують значення, рівного M, тому операції над синдромом навіть для перестановок великої розмірності не викликають складнощів, пов'язаних з обробкою цих слів. У свою чергу, витрати часу на обчислення синдрому $S_F(j)$ визначаються $(M-1)$-кратним виконанням операцій за (2.2), (2.3), (2.4), (2.5) і лінійно залежать від порядку перестановки.

Слід зазначити, що вираз (1.11) може бути модифіковано таким чином:

$$S_F(j)=f\left(S_F(j-1)\right)\dot{+}t_{10}(j). \tag{2.6}$$

де $f\left(S(j-1)\right)$ – деяка функція від значення синдрому $(j-1)$-ої, перестановки.

Відповідно до цього, процедура формування синдрому перестановки допускає можливість використання наступних підходів:

– формування синдрому перестановки з випадковим зміщенням щодо фіксованої нульової точки (формування перестановки з фіксованим нулем): $S_F(j)=S_F(0)\dot{+}t_{10}(j)$;

– формування синдрому перестановки з випадковим зміщенням щодо попередньої умовної нульової точки (формування перестановки з випадковим нулем): $S_F(j)=S_F(j-1)\dot{+}t_{10}(j)$;

– формування синдрому перестановки з модифікацією попередньої умовної нульової точки (формування перестановки з модифікованим випадковим нулем): $S_F(j)=f\left(S_F(j-1)\right)\dot{+}t_{10}(j)$.

Формування перестановки з фіксованим нулем передбачає обчислення всіх перестановок, зміщених на випадкове значення $t_{10}(j)$ щодо умовно обраної

нульової точки $S_F(0)$. Синдром $S_F(0)$ завантажується в момент пуску генератора і не змінюється до завершення його роботи. Таку методику формування послідовності перестановок будемо позначати наступним чином: $\left(S_F(j) = S_F(0) \dot{+} t_{10}(j)\right) \to \pi(j)$.

Особливість зазначеного підходу до синтезу послідовності перестановок полягає в тому, що ступінь кореляції між перестановками визначається статистичними властивостями послідовності символів $t_{10}(j)$ [264], [265]. Зокрема, якщо послідовність символів $t_{10}(j)$ є стохастичною і рівномірно розподіленою на відрізку $[0, M!-1]$, то ступінь кореляції між перестановками буде прямувати до нуля. Якщо, крім того, $t_{10}(j)$ є непередбачуваною (ключ її формування тримається в таємниці), то послідовність перестановок стає непередбачуваною та криптографічно стійкою.

Формування перестановки з випадковим нулем передбачає обчислення кожної наступної перестановки, номер якої зміщений на випадкове число $t_{10}(j)$ відносно номера попередньої перестановки. Таку методику формування послідовності перестановок будемо позначати через $\left(S_F(j) = S_F(j-1) \dot{+} t_{10}(j)\right) \to \pi(j)$.

Особливість зазначеного підходу з випадковим нулем до синтезу послідовності перестановок полягає в тому, що сусідні перестановки корельовані, що особливо проявляється для $t_{10}(j) \ll M!$. Однак якщо величина $t_{10}(j)$ є непередбачуваною і рівномірно розподіленою на відрізку $[0, M!-1]$, то послідовність перестановок також стає непередбачуваною.

Формування перестановки з модифікованим випадковим нулем передбачає обчислення кожної наступної перестановки, синдром якої зміщений на випадкове значення $t_{10}(j)$ відносно модифікованого синдрому попередньої перестановки. Модифікація синдрому виконується відповідно до деякого ключа перетворення, який може триматися в таємниці. Ключ може поширюватися на групу перестановок або піддаватися модифікації від перестановки до перестановки на розсуд

користувача. Таку методику формування послідовності перестановок будемо позначати наступним чином: $\left(S_F(j) = f\left(S_F(j-1)\right) \dot{+} t_{10}(j)\right) \to \pi(j)$.

Особливість такого підходу до синтезу послідовності перестановок полягає в тому, що в порівнянні з режимом формування перестановок з випадковим нулем кореляція між сусідніми перестановками знижується і підвищується їх непередбачуваність. Результати дослідження функції $f\left(S_F(j-1)\right)$ наведено нижче.

2.2.2. Перетворення синдрому в перестановку

Визначимо порядок перетворення синдрому в перестановку для режимів відкритого і прихованого перетворення.

Відкрите перетворення синдрому в перестановку описує оборотну функцію $\pi = G(S_F)$, для якої легко виконується як пряме $\left(\pi = G(S_F)\right)$, так і зворотне $\left(S_F = G^{-1}(\pi)\right)$ перетворення.

Приховане перетворення синдрому в перестановку описує оборотну функцію $\pi = G(S_F)$, для якої за відомого ключа легко виконується як пряме $\left(\pi = G(S_F)\right)$, так і зворотне $\left(S_F = G^{-1}(\pi)\right)$ перетворення, в той час як зворотне перетворення $S_F = G^{-1}(\pi)$ за невідомого ключа є нездійсненним (або, як мінімум, важко виконуваним) за прийнятний час і з використанням обмежених ресурсів.

Метою прихованого перетворення є приховування правил, що визначають взаємозв'язок символів під час перетворення $S_F \to \pi$.

Спільне застосування операцій виду $S_F(j) = f\left(S_F(j-1)\right) \dot{+} t_{10}(j)$ (за випадкового, приховуваного $t_{10}(j)$) і прихованого перетворення $S_F(j) \to \pi(j)$ забезпечують приховування взаємного зв'язку між перестановками (відповідно, руйнує кореляційний зв'язок між перестановками), а також між $\pi(j)$ і $S_F(j)$ під час перетворення $\pi(j) \to S_F(j)$, що підвищує стійкість послідовності перестановок.

Під час перетворення синдрому в перестановку вхідним об'єктом перетворення є синдром S_F, кінцевим продуктом перетворення – перестановка π.

Для пояснення процесу перетворення будемо використовувати (в якості моделі) лототрон з кулями, що описується виразом (1.10). Замість лототрону з кулями будемо використовувати:

– оперативний запам'ятовувальний пристрій (ОЗП);

– керуючий пристрій (КП).

2.2.2.1. Відкрите перетворення

Використовуємо ОЗП, в яке за адресами $0,1,2,\ldots,(M-2),(M-1)$ запишемо послідовність з M слів у натуральному порядку – $0,1,2,\ldots,(M-2),(M-1)$. Отримаємо таблицю:

Адреса	0	1	2	...	M-2	M-1
Вміст	0	1	2	...	M-2	M-1

Нехай є синдром $S_F = (b_{M-1}; b_{M-2}; \ldots; b_0)$.

На k-ому кроці формування перестановки (під час обчислення k-ого символу перестановки) виконуються наступні дії:

1) обирається k-е слово синдрому – b_{M-k};

2) з ОЗП зчитується слово за адресою b_{M-k}. Це слово є k-им символом перестановки, тобто $\pi_k = R(b_{M-k})$ ($R(i)$ – вміст комірки ОЗП за i-ю адресою);

3) зчитане слово видаляється з ОЗП, а всі інші слова переписуються у відповідності з наступним правилом:

$$R_i \leftarrow R_i \text{ для } 0 \le i \le b_{M-k} - 1;$$
$$R_i \leftarrow R_{i+1} \text{ для } b_{M-k} \le i \le M - k - 1.$$

Зазначена процедура виконується для всіх значень $k \in [1; M-1]$.

Для скорочення часової і просторової складності наведеного алгоритму можна скористатися алгоритмом, запропонованим у [238] Р. Дурштенфельдом для модифікації алгоритму тасування Фішера-Йєтса [237], і зчитаний k-ий символ перестановки переміщувати в кінець списку (блоку ОЗП) шляхом перестановки з останнім невибраний числом.

2.2.2.2. Приховане перетворення

Приховане перетворення відрізняється від відкритого тим, що в ОЗП за адресами $0,1,2,\ldots,(M-2),(M-1)$ заноситься не натуральна послідовність чисел $0,1,2,\ldots,(M-2),(M-1)$, а деяка їх перестановка. Ця перестановка є ключем перетворення і тримається в таємниці. Ключ може бути фіксованим у статусі мережного ключа, поширюватися на групу перестановок у статусі сеансного ключа або піддаватися модифікації за розкладом, встановленим користувачем, у статусі ключа, змінюваного за розкладом.

Перетворення синдрому в перестановку, що використовує в якості ключа перестановку слів натуральної послідовності чисел, еквівалентне двом послідовно виконуваним процедурам: $S_F \to \pi$ і перестановці символів π за деякою таблицею перестановок, що тримається в таємниці.

Крім того, за прихованого перетворення і використання процедури $\left(S_F(j) = f\left(S_F(j-1)\right) \dot{+} t_{10}(j)\right) \to \pi(j)$ ключ модифікації синдрому перетворення $f\left(S_F(j-1)\right)$ також може зберігатися в таємниці та складати частину загального ключа перетворення. У цьому випадку виконання зворотного перетворення $\pi \to S_F$ на невідомому ключі не дозволяє ідентифікувати S_F.

2.2.3. Опис методу формування випадкової послідовності перестановок

Таким чином, метод формування відтворюваної непередбачуваної послідовності перестановок передбачає виконання таких операцій:

1) синдром першої та наступних перестановок представляються в ФСЧ;
2) для формування синдрому наступної перестановки використовується додатковий ГВЧ, символи якого підсумовуються з модифікованим синдромом попередньої перестановки, а результат підсумовування визначає синдром наступної перестановки. Процедура і ключ модифікації синдрому можуть бути як відкритими, так і прихованими і бути елементами загального ключа;
3) для підвищення криптографічної стійкості послідовності перестановок параметри перетворення синдрому в перестановку можуть триматися в

таємниці та бути елементом ключа перетворення.

Виконаємо порівняння розробленого методу формування послідовності перестановок з іншими відомими методами: Фішера-Йєтса [237] та Дуршенфельда [238].

Таблиця 2.1

Порівняльний аналіз методів формування випадкової послідовності перестановок

Метод	**Необхідність приведення випадкових чисел до різних діапазонів**	**Необхідна розрядність внутрішнього стану ГПВЧ**
Фішера-Йєтса	вимагається	$\log_2\left(M!\cdot M\cdot 10^m\right)$
Дуршенфельда	вимагається	$\log_2\left(M!\cdot M\cdot 10^m\right)$
Запропонований метод	не вимагається	1) з фіксованим нулем – $\log_2\left(M!\right)$; 2) з випадковим нулем – $\log_2\left(M!\cdot 10^m\right)$; 3) з модифікованим випадковим нулем – $\log_2\left(M!\cdot 10^m\right)$.

Значення m у таблиці 2.1 вказує на кількість порядків, на яке число внутрішніх станів ГПВЧ має перевищувати число перестановок для запобігання появи нерівномірності розподілу перестановок. Зазвичай $m=7\div 10$.

З таблиці видно, що запропонований метод не потребує багаторазового приведення випадкових чисел до потрібних діапазонів та вимагає меншої розрядності допоміжного ГПВЧ. Це призводить до:

- уникнення порушення рівномірності розподілу перестановок внаслідок приведення випадкових чисел до діапазону зі змінною верхньою межею;
- розширення діапазону значень порядку перестановок для використовуваної обчислювальної платформи або зменшенню вимог до розрядності ГПВЧ для формування послідовності перестановок заданого порядку.

2.2.4. Пристрій формування випадкової послідовності перестановок

Технічний результат від застосування запропонованого методу формування некорельованої послідовності перестановок може бути досягнутий за допомогою

пристрою, спрощена структурна схема якого (адаптована для створення генератора перестановок на однокристальній ЕОМ) показана на рис. 2.1.

Рис. 2.1. Структурна схема пристрою формування випадкової послідовності перестановок

Пристрій містить блок (1) обчислення синдрому $S_F(j)$ за заданим значенням $S_F(j-1)$ і $t_{10}(j)$, блок (2) обчислення перестановки $\pi(j)$ за заданим $S_F(j)$, генератор (3) випадкових чисел (формувач числа $t_{10}(j)$) і пристрій керування (4).

У початковий момент часу з зовнішнього пристрою у блок (1) обчислення синдрому $S_F(j)$ завантажується довільно обрана на розсуд оператора послідовність $S_F(0)$ із M чисел (наприклад, $0,1,2,\ldots,(M-1)$), яка є ВПЗ. Одночасно ГВЧ (3), формує випадкове число $t_{10}(1)$, яке також завантажується в блок (1).

Блок (1) обчислення синдрому за заданими $S_F(0)$ і $t_{10}(1)$ за формулами (2.2) і (2.3) обчислює значення першого синдрому $S_F(1)=S_F(0)\dotplus t_{10}(1)$. Блок (2) формування перестановки обчислює першу перестановку $\pi(1)$ за заданим $S_F(1)$.

У залежності від обраного режиму роботи (відкрите чи приховане перетворення) для формування наступного синдрому і, відповідно, наступної перестановки, пристрій керування (4) по шині керування (ШК) задає блоку (1) обчислення синдрому значення $S_F(1)$ (яке може бути піддане модифікації для режиму прихованого перетворення) і нове випадкове значення $t_{10}(2)$.

Так, перестановка за перестановкою, формується відтворювана непередбачувана випадкова послідовність перестановок.

Криптографічна стійкість генератора послідовності перестановок визначається наступними прихованими параметрами, що утворюють ключ перетворення:

– ВПЗ $S_F(0)$ з потужністю ключового простору $M!$;

– ключем перетворення синдрому в перестановку з потужністю простору $M!$;

– ключем модифікації синдрому з потужністю простору $M!$.

Виконане дослідження дозволяє сформулювати наступні висновки:

– розроблено задовольняючий поставленим у розділі 1 вимогам метод формування послідовності перестановок на основі використання для представлення синдрому формованої перестановки ФСЧ, який дозволяє формувати відтворену непередбачувану послідовність перестановок, що володіє криптографічного стійкістю, та не потребує приведення випадкового числа додаткового ГВЧ до потрібного діапазону зі змінною верхньою межею, що дозволяє уникнути порушення рівномірності розподілу перестановок;

– розроблено реалізації запропонованого методу для різних процедур обчислення синдрому наступної перестановки: з фіксованим нулем, з випадковим нулем, з модифікованим випадковим нулем;

– розроблено правила обчислення суми факторіального і десяткового числа, що використовується для формування синдрому наступної перестановки;

– розроблено два режими формування послідовності перестановок (відкритий і прихований);

– розроблено пристрій формування випадкової послідовності перестановок, що дозволяє його практичну реалізацію.

Виконаємо дослідження швидкості роботи програмної реалізації генератора перестановок на основі ФСЧ та порівняємо її з швидкістю роботи генератора, що реалізує сучасний алгоритм Фішера-Йєтса. Для об’єктивності оцінки генератори реалізовано на одній платформі та досліджено на одному комп’ютері з фіксованими показниками продуктивності. Результати зведемо в таблицю 2.2.

Таблиця 2.2

Порівняльний аналіз швидкості формування випадкової послідовності перестановок

Метод	Швидкість формування (слів/сек)				
	$M=5$	$M=8$	$M=10$	$M=15$	$M=20$
Фішера-Йєтса	81540	82120	83300	84960	86000
Запропонований метод	167670	200280	220230	233880	241020

Як можна бачити з таблиці, запропонований метод дозволяє підвищити швидкість роботи генератора порівняно з алгоритмом Фішера-Йєтса (зокрема, для $M=5$ – у 2,1 рази; $M=10$ – у 2,6 рази; $M=20$ – у 2,8 рази).

2.3. Метод повного факторіального кодування інформації

Представимо розроблений і досліджений у [39], [35], [40], [34], [36], [41], [42], [60] метод контролю цілісності інформації (КЦІ) на основі перестановки, яка використовується в якості контрольної суми. Виконаємо оцінку достовірності інформації внаслідок його застосування.

Зауважимо, що КЦІ передбачає виявлення факту модифікації переданих даних внаслідок як навмисних дій зловмисника, так і внаслідок помилок у каналі зв’язку. Тому КЦІ є засобом, що об’єднує імітозахист і завадостійке кодування.

Виходячи з цього, задамо вимоги до системи КЦІ, що реалізує запропонований метод:

– повинен забезпечуватися захист інформації від нав’язування хибних даних і помилок, що вносяться каналом зв’язку;

– повинен забезпечуватися ефект «розсіювання»: кожен символ повідомлення повинен впливати на формування перевірної частини блоку; цей вплив має залежати як від самого символу, так і від його розташування в блоці даних;

– рівень колізій повинен бути мінімальним (колізія – ситуація, за якої контрольні суми різних блоків даних збігаються);

– довжина контрольної суми для будь-якої кількості символів повідомлення повинна бути фіксованою та постійною;

– має забезпечуватися відсутність кореляції між контрольними сумами,

обчисленими за цілим повідомленням і його частиною;

– контрольна сума повинна бути невідтворюваною без знання ключа її формування.

2.3.1. Опис методу

Сутність запропонованого методу повного факторіального кодування інформації полягає в наступному:

– контрольна сума кодового слова формується у вигляді перестановки порядку M, яка залежить від кожного символу інформаційної частини кодового слова;

– блок даних містить інформаційну частину і контрольну суму (перестановку) і не містить символ-прапор.

Метод повного факторіального кодування полягає в наступному:

1) контрольна сума представляється у вигляді однієї перестановки порядку M;
2) формування контрольної суми є ітераційним процесом над синдромами перестановок, представленими в ФСЧ:
   a) інформаційна частина розбивається на k_{symb} блоків (укрупнених символів);
   b) значення поточного укрупненого символу підсумовується з модифікованим синдромом попередньої перестановки, а результат цього перетворення визначає синдром наступної перестановки;
   c) початковий синдром тримається в таємниці та є елементом загального ключа перетворення;
   d) процедура і ключ модифікації синдрому тримаються в таємниці та є елементами загального ключа перетворення;
   e) перетворення останнього синдрому в перестановку після перебору всіх укрупнених символів інформаційного повідомлення виконується відповідно до ключа, який також є елементом ключа перетворення;
3) для підвищення стійкості до зламу блок даних, що містить інформаційну та перевірну частини, може піддаватися перестановці біт з метою зміни порядку їх слідування в процесі передавання каналом зв`язку приймачу, правило

перестановки тримається в таємниці і є частиною ключа перетворення.

Таким чином, досягнутий технічний результат – виявлення помилок, внесених каналом зв`язку, і виявлення факту несанкціонованої модифікації інформації – забезпечується за рахунок використання завадостійкого коду, в процесі формування перевірної частини якого використовується множина змінних констант, що використовується в якості ключа. Крім того, ступінь підвищення достовірності може регулюватися шляхом вибору порядку перестановки M.

На основі викладеного вище сформулюємо наступне визначення.

Визначення 2.1. Повним факторіальним кодом (ПФК) називається роздільний надлишковий код, який використовує в якості перевірної частини кодового слова перестановку чисел порядку M, яка визначається інформаційної послідовністю і алгоритмом кодування.

Виконаємо розробку пристрою повного факторіального кодування, дослідимо процедури реалізації запропонованого методу, визначимо основні властивості ПФК.

2.3.2. Пристрій кодування та декодування повних факторіальних кодів

Технічний результат від застосування методу КЦІ на основі ПФК досягається за допомоги пристрою, що містить блок кодування та блок декодування.

Спрощена структурна схема блоку кодування ПФК показана на рис. 2.2.

Рис. 2.2. Структурна схема блоку кодування ПФК

Блок повного факторіального кодування інформації містить блок обчислення синдрому $S_F(j)$ (1) за заданими значеннями $S_F(j-1)$ і $t(j)$ для $j \in [1; k_{symb}]$, блок обчислення перестановки $\pi(j = k_{symb})$ (2) за заданим синдромом $S_F(j = k_{symb})$,

формувач кодового слова (3), що може включати блок перестановки символів.

З рис. 2.2 слідує, що блок повного факторіального кодування має структуру, подібну структурі пристрою формування випадкової послідовності перестановок, і, як наслідок, формування перевірної частини ПФК може бути режимом його роботи.

Режим формування перевірної частини ПФК характеризується тим, що:

- робота ведеться за секретним ключем;
- послідовність $t(j)$ утворюють символи повідомлення;
- перестановка, яка є перевірною частиною ПФК, виводиться одноразово після обробки всього повідомлення.

У початковий момент часу із зовнішнього пристрою у блок обчислення синдрому $S_F(j)$ (1) завантажується ВПЗ $S_F(0)$, що тримається в таємниці. Одночасно джерело інформації видає перший символ блоку даних – число $t(1)$.

Блок обчислення синдрому (1) за заданими $S_F(0)$ і $t(1)$ обчислює значення першого синдрому $S_F(1)$. Процес обчислення синдромів продовжується ітераційно: за заданими $S_F(j-1)$ і $t(j)$ згідно виразу (2.6) обчислюється значення $S_F(j)$. Цей процес продовжується до обчислення $S_F(k_{symb})$.

Блок формування перестановки (2) за синдромом $S_F(k_{symb})$, що надходить від блоку обчислення синдрому (1), і заданим ключем обчислює контрольну суму блоку – перестановку $\pi(k_{symb})$. Формувач кодового слова (3) об`єднує символи інформаційної частини і контрольну суму – перестановку – в єдиний блок даних, а пристрій перестановки символів блоку даних, що може входити до складу формувача кодового слова (3), виконує перестановку символів за деяким ключем, що зберігається в таємниці. Сформований блок даних видається на вихід пристрою.

Спрощена структурна схема блоку декодування ПФК показана на рис. 2.3.

Блок декодування повних факторіальних кодів містить послідовно з'єднані блок обчислення синдрому $S_F'(j)$ (1) за заданими значеннями $S_F'(j-1)$ і $t'(j)$ для $j \in [1; k_{symb}]$, блок обчислення перестановки $\pi'(j = k_{symb})$ (2) за заданим синдромом

$S_F^{'}\left(j=k_{symb}\right)$ і блок прийняття рішення (4).

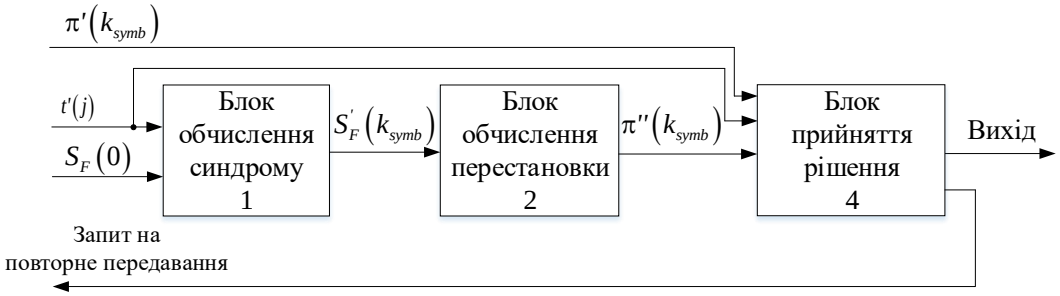


Рис. 2.3. Структурна схема блоку декодування ПФК

Блок декодування ПФК працює наступним чином. Блок обчислення синдрому (1) за заданими $S_F\left(0\right)$ і прийнятими з каналу $t'\left(j\right)$ обчислює значення $S_F^{'}\left(k_{symb}\right)$. Блок формування перестановки (2) за синдромом $S_F^{'}\left(k_{symb}\right)$, що надходить від блоку обчислення синдрому (1), і заданим ключем обчислює контрольну суму блоку – перестановку $\pi''\left(k_{symb}\right)$. Блок прийняття рішення (4) порівнює обчислену $\pi''\left(k_{symb}\right)$ контрольну суму, що надходить на третій вхід блоку (4), та прийняту з каналу $\pi'\left(k_{symb}\right)$ контрольну суму, що надходить на перший вхід блоку (4). Якщо вони співпадають, то на перший вихід блоку прийняття рішення (4) видається отримана з каналу інформаційна частина кодового слова ПФК, що надходить на другий вхід блоку (4). В іншому випадку на другому виході блоку прийняття рішення (4) формується запит на повторне передавання прийнятого з помилкою блоку даних.

2.3.3. Структура кодового слова повного факторіального коду

Приймемо, що КЦІ на основі ПФК використовується в найпростіших системах передавання даних з вирішувальним зворотним зв'язком (ВЗЗ), де прямий канал – двійковий симетричний, зворотний канал – ідеальний (помилки в ньому відсутні), а символи, складові повідомлення, є елементами поля $F_2=\left\{0;1\right\}$.

У системах з ВЗЗ виявлення помилок здійснюється кодовими методами, а їх виправлення – перепитами блоку даних, що містить (виявлену кодом) помилку.

Число перезапитів блоку даних залежить від якості каналу зв'язку і довжини блоку. Врахуємо, що утворюваний код не розрізняє модифікацію даних, обумовлену навмисними діями зловмисника або впливом помилок у каналі зв'язку. І в тому, і в іншому випадку система сприймає модифікацію як помилку в прийнятому блоці і формує сигнал перезапиту (не виводячи інформації одержувачу).

Нехай k і r – число двійкових символів у інформаційній та перевірній частинах кодового слова відповідно, $n = k + r$ – повна довжина кодового слова.

Структуру кодового слова ПФК представлено на рис. 2.4.

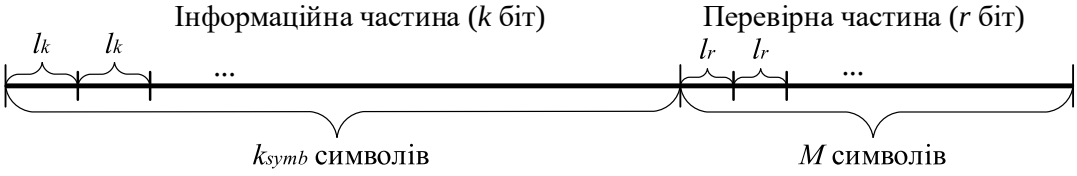


Рис. 2.4. Структура кодового слова ПФК

Інформаційна частина містить k_{symb} укрупнених символів. Кожен укрупнений символ утворюється групою з l_k біт і відповідає елементу поля $F_2^{l_k}$ (числу L-адічної системи числення, де $L = 2^{l_k}$ (четвірковій, вісімковій, шістнадцятковій і т.п.)). Таким чином, довжина інформаційної частини дорівнює $k = l_k \cdot k_{symb}$ біт.

У якості перевірної частини блоку використовується перестановка порядку M. За кодування символів перестановки рівномірним двійковим кодом її довжина становить $l_r = \lceil \log_2 M \rceil$ біт. Таким чином, перевірна частина містить $r = l_r \cdot M$ біт.

Значення M обирається виходячи з вимог до ступеня підвищення достовірності: чим вищий цей ступінь, тим більшим має бути порядок перестановки M і, відповідно, довжина перевірної частини r. Вплив величини M на достовірність передавання в результаті застосування ПФК наводиться нижче.

2.3.4. Процедура формування контрольної суми

Нехай $t(j) \in F_2^{l_k}$ – число, утворене l_k бітами j-го укрупненого символу

інформаційної частини блоку, $j \in \left[1; k_{symb}\right]$. Перевірна частина (перестановка) формується за допомогою послідовного аналізу всіх символів інформаційної частини і повинна залежати як від величини $t(j)$, так і від порядку j їх слідування.

Визначена виразом (2.6) ітераційна процедура формування синдрому перестановки допускає можливість використання наступних варіантів зчеплення символів інформаційної частини блоку під час обчислення синдрому $S_F(j)$:

1) $S_F(j) = S_F(0) \dot{+} t(j)$ – з фіксованим нулем;
2) $S_F(j) = S_F(j-1) \dot{+} t(j)$ – з випадковим нулем;
3) $S_F(j) = f\left(S_F(j-1)\right) \dot{+} t(j)$ – з модифікованим випадковим нулем.

Розглянемо можливість використання цих варіантів для ПФК.

Перший і другий варіанти не забезпечують зчеплення символів і непридатні для поставленої задачі. Вона може бути вирішена за умови, якщо сума символів інформаційної частини блоку буде залежати і від величини $t(j)$, і від порядку слідування символів у блоці j, тобто необхідно забезпечити $\omega = \sum_{j=1}^{k_{symb}} \beta_j\left(t(j)\right)$, де $\beta_j\left(t(j)\right)$ – перетворення, залежне від положення j символу в блоці.

Перетворення $S_F(j) = f\left(S_F(j-1)\right) \dot{+} t(j)$ передбачає модифікацію синдрому.

Операція $f\left(S_F(n-1)\right)$ повинна відповідати таким вимогам:

1) максимальна ентропія результату перетворення;
2) мінімальна ймовірність колізій.

Розглянемо кілька способів її реалізації.

Перший спосіб. Модифікація $f\left(S_F(j-1)\right)$ використовує гамування [266]–[268] синдрому: $S_F(j) = \left(S_F(j-1) + \gamma(j)\right) \dot{+} t(j)$. Така процедура забезпечує зсув контрольної точки спочатку на величину $\gamma(j)$, представлену, наприклад, у ФСЧ, $0 \le \gamma(j) \le M! - 1$, а потім на величину $t(j)$, $0 \le s(j) \le 2^{l_r} - 1$.

Другий спосіб ґрунтується на операції $b_i(j) = \left(b_i(j-1) + Z_i(j)\right) (\mathrm{mod}\, i)$ для

кожного коефіцієнта $b_i(j)$. Ключ модифікації $Z_i(j)$ формується таким чином:

– двійкова послідовність даних t підсумовується за модулем два з двійковою гамою γ, утворюючи гамовану послідовність даних $z = t \oplus \gamma$;

– група з k_{symb} двійкових символів послідовності z накопичується в буферній пам'яті і після зчитування паралельним кодом утворює символ $Z_i(j)$.

Третій спосіб модифікації синдрому $f\left(S_F(j-1)\right)$ передбачає перетворення виду $S_F(j-1) \to \pi(j-1) \to S_F'(j-1)$, де $S_F(j-1) \to \pi(j-1)$ і $\pi(j-1) \to S_F'(j-1)$ виконуються на двох ключах.

Виконаємо аналіз наведених способів модифікації синдрому. Зазначимо, що для забезпечення вимог, що пред'являються до системи КЦІ на основі ПФК, ентропія модифікованого синдрому має бути максимальною, а ймовірність виникнення колізій – мінімальною.

Для кожного з наведених варіантів виконано дослідження закону розподілу перевірної частини ПФК, яке представлено в додатку Б.

У результаті проведеного аналізу визначено:

– перетворення $S_F(j) = \left(S_F(j-1) + \gamma(j)\right) \dot{+} t(j)$ забезпечує максимальну інформаційну ентропію формувача перевірної частини ПФК та близьку до мінімальної ймовірність виникнення колізій;

– перетворення $b_i(j) = \left(b_i(j-1) + Z_i(j)\right) (\mathrm{mod}\, i)$ забезпечує близьку до максимальної інформаційну ентропію формувача перевірної частини ПФК та близьку до мінімальної ймовірність виникнення колізій;

– перетворення $S_F(j-1) \to \pi(j-1) \to S_F'(j-1)$ забезпечує максимальну інформаційну ентропію формувача перевірної частини ПФК та близьку до мінімальної ймовірність виникнення колізій.

Разом із тим, зазначимо, що перетворення $S_F(j) = \left(S_F(j-1) + \gamma(j)\right) \dot{+} t(j)$ і $b_i(j) = \left(b_i(j-1) + Z_i(j)\right) (\mathrm{mod}\, i)$ базуються на лінійних операціях і вимагають додаткового ГВЧ. Крім того, перетворення $b_i(j) = \left(b_i(j-1) + Z_i(j)\right) (\mathrm{mod}\, i)$ вимагає

виконання M операцій підсумовування факторіальних коефіцієнтів з гамою і, як наслідок, додаткових ресурсів продуктивності кодера. Натомість перетворення $S_F(j-1) \to \pi(j-1) \to S_F'(j-1)$ не вимагає використання додаткового генератора гами, при цьому ключ модифікації має довжину $2M \cdot l_r$ біт і потужність $(M!)^2$.

Деякі отримані результати аналізу викладено в роботах автора [43], [269].

2.3.5. Оцінка імітостійкості повного факторіального коду

У якості перевірної частини кодового слова ПФК може бути використана група M' слів з M слів сформованої перестановки. Зауважимо, що використання M' слів з M можливих у контрольній сумі виключає можливість самосинхронізації ПФК і збільшує число колізій за рахунок зменшення числа можливих значень контрольної суми зі значення $M!$ до значення $\prod_{i=0}^{M'-1} M-i = M!/(M-M')!$. Зазначимо також, що порядок вибору M' слів (з M слів перестановки) тримається в таємниці.

Таким чином, ключем вироблення контрольної суми ПФК є:

- ВПЗ $S_F(0)$;
- ключ перетворення синдрому в перестановку;
- ключ модифікації синдрому;
- правила вибору M' символів контрольної суми з M можливих.

Зауважимо, що ВПЗ, ключ перетворення синдрому в перестановку і ключ модифікації синдрому є послідовностями з M символів кожна.

Виконаємо орієнтовну оцінку імітостойкості [270] ПФК, виходячи з того, що задача, яка вирішується криптоаналітиком, – злом методом «грубої сили» ключової системи для її множинного застосування.

Будемо вважати, що система буде зламана, якщо криптоаналітик за перехопленими повідомленнями простим перебором усіх можливих значень ВПЗ, ключа перетворення синдрому в перестановку, ключа модифікації синдрому і всіх сполучень вибору M' символів зуміє підібрати ключ формування контрольної суми. Імовірність цих подій (позначимо їх P_1, P_2, P_3, P_4) визначиться так:

$P_1 = P_2 = P_3 = (M!)^{-1}$, $P_4 = (C_M^{M'})^{-1}$. З огляду на статистичну незалежність кожної з них, імовірність злому ПФК буде дорівнювати

$$P_{ПС} = P_1 P_2 P_3 P_4 = \left(M!\right)^{-3} \cdot \left(C_M^{M'}\right)^{-1}.$$

Звідси випливає, що імітостійкість буде тим вища, чим більше M і чим ближче M' до значення $0.5M$ (зауважимо, що для разового злому це не так).

Знаючи ймовірність злому, можна визначити середнє необхідне число спроб злому: $N = 0.5 \cdot P_{ПС}^{-1} = 0.5 \cdot \left(M!\right)^3 \cdot C_M^{M'}$.

Для визначення часу злому будемо виходити з таких передумов:

- продуктивність сучасних комп'ютерів порядку 10^{10} операцій/сек;
- обчислення перевірної частини ПФК вимагає не менше 1000 операцій;
- для злому можна залучити машинне угруповання з 1000 комп'ютерів.

Тоді комп'ютерне угруповання за один рік може виконати $3.15 \cdot 10^{17}$ обчислень перевірної частини, а за мільйон років – $3.15 \cdot 10^{23}$. Імітостійкість (млн. років)

$$T = \frac{0.5 \cdot \left(M!\right)^3 \cdot C_M^{M'}}{3.15 \cdot 10^{23}}.$$

Зокрема, для $M = 256$ і $M! = 8.57 \cdot 10^{506}$ отримаємо $T = \dfrac{0.5 \cdot \left(M!\right)^3 \cdot C_M^{M'}}{3.15 \cdot 10^{23}} \approx C_M^{M'} \cdot 10^{1497}$ млн. років.

Звідси випливає, що якщо не тримати в таємниці правило вибору M' символів перестановки (покласти $C_M^{M'} = 1$), для $M = 256$ імітостійкість – 10^{1497} млн. років.

Зауважимо, що імітостійкість, в першу чергу, визначається порядком перестановки і саме її необхідно визначити для заданої стійкості.

Поклавши $C_M^{M'} = 1$, отримаємо $3.15 \cdot 10^{23} \cdot T = 0.5 \cdot \left(M!\right)^3$, звідки $M! \approx 8.7 \cdot 10^7 \cdot \sqrt[3]{T}$. Звідси випливає, що для забезпечення імітостійкості не менше, наприклад, 10 млн. років розмірність перестановки $M \geq 12$.

Імовірність підбору коду виявлення модифікацій (КВМ) ПФК у одному блоці даних становить $P_{MAC}\left(FFC\right) = \left(M!\right)^{-1}$.

Разом з тим ще раз зауважимо, що представлена оцінка є орієнтовною і базується тільки на методі злому «грубою силою».

2.3.6. Математична модель процесу декодування повного факторіального коду. Оцінка показників достовірності

2.3.6.1. Принципи виникнення помилок на виході декодера повного факторіального коду

Одним з параметрів оцінювання якості завадостійкого коду в системах з ВЗЗ є ймовірність не виявленої декодером помилки в прийнятому блоці даних. Для запропонованого методу КЦІ помилка не буде виявлена кодом, якщо перестановка, обчислена декодером за прийнятою з помилкою інформаційною частиною блоку, збіглася з отриманою перевірною частиною. Іншими словами, невиявлена помилка виникає тоді, коли вектор помилки в перевірній частині трансформує передану перестановку π в іншу перестановку π', яка збігається з перестановкою π'', обчисленою декодером за прийнятою з помилками інформаційною частиною.

Нехай p_0 – перехідна ймовірність прямого (двійкового симетричного) каналу зв'язку $\left(q_0 = 1 - p_0\right)$. Імовірність невиявленої помилки в результаті застосування ПФК (FFC – full factorial code) $P_{ud}\left(FFC, p_0\right) = P\left\{\pi' = \pi''\right\}$ істотно залежить від ступеня статистичного зв'язку інформаційної та перевірної частин, яка, в свою чергу, залежить від способу перетворення інформаційної частини в перестановку. До того ж, від способу формування перестановки залежить і ступінь зчеплення символів інформаційної частини і, як наслідок, стійкість системи КЦІ, яка тим вище, чим більше потужність множини перестановок і чим ближче статистика розподілу їх контрольних точок до рівномірного розподілу.

2.3.6.2. Оцінка достовірності передавання даних під час використання повного факторіального кодування

Далі будемо використовувати широко прийнятий [68, с. 232], [271, с. 601], [272, с. 361] підхід розгляду наборів (векторів) над полем F_2 у вигляді елементів алгебри багаточленів з коефіцієнтами з F_2.

Перш за все, зазначимо, що блок даних, який складається з інформаційної $A(x)$ та перевірної $R(x)$ частин, виводиться в канал зв'язку у вигляді $C(x)=A(x)\coprod R(x)$, де $\coprod$ – символ конкатенації (приєднання).

Під час передавання каналом зв'язку на блок даних впливає вектор помилки $\varepsilon_n(x)$ з потужністю множини векторів $\mu\{\varepsilon_n(x)\}=2^n$. Цей вектор може бути представлений у вигляді конкатенації двох векторів – вектора завади, що покриває інформаційну частину блоку (розмірністю k біт), і вектора завади, що покриває перевірну частину блоку (розмірністю r біт): $\varepsilon_n(x)=\varepsilon_k(x)\coprod\varepsilon_r(x)$.

З урахуванням викладеного, прийнятий з каналу зв'язку вектор має вигляд $D(x)=C(x)\oplus\varepsilon_n(x)=\big(A(x)\oplus\varepsilon_k(x)\big)\coprod\big(R(x)\oplus\varepsilon_r(x)\big)$.

У приймачі за прийнятою з каналу послідовністю $A(x)\oplus\varepsilon_k(x)$ обчислюється контрольна сума – перестановка. Ця перестановка статистично не пов'язана ні з інформаційним вектором, ні з вектором завади і може бути представлена у вигляді $R(x)\oplus\varepsilon_r^{\wedge}(x)$, де $\varepsilon_r^{\wedge}(x)$ – помилка, що виникає на виході формувача перестановки і трансформує контрольну суму – перестановку $R(x)$ – в будь-яку з $M!$ перестановок. Обчислюється синдром $S(x)=\big(R(x)\oplus\varepsilon_r^{\wedge}(x)\big)\oplus\big(R(x)\oplus\varepsilon_r(x)\big)=\varepsilon_r^{\wedge}(x)\oplus\varepsilon_r(x)$.

Якщо $\varepsilon_n(x)=0$, то $S(x)=0$. Тому рівність $S(x)=0$ є ознакою відсутності модифікації блоку даних.

Разом з тим, якщо $\varepsilon_n(x)\neq 0$ і $\varepsilon_r^{\wedge}(x)\oplus\varepsilon_r(x)=0$, виникають помилки декодування. Зауважимо, що $\varepsilon_r^{\wedge}(x)$ і $\varepsilon_r(x)$ статистично незалежні, а помилки декодування за $\varepsilon_k(x)\neq 0$ і $\varepsilon_r^{\wedge}(x)=\varepsilon_r(x)=0$ є результатом виникнення колізій.

Імовірність невиявленої помилки $P_{ud}(FFC,p_0)=P\{\varepsilon_r^{\wedge}(x)=\varepsilon_r(x)\}$ за $\varepsilon_n(x)\neq 0$ залежить від виду використовуваної функції $f\big(S_F(j-1)\big)$. Для визначення $P_{ud}(FFC,p_0)$ приймемо, що вхід і вихід формувача перестановки є статистично незалежними, а закон розподілу помилок $\varepsilon_r^{\wedge}(x)$ за $\varepsilon_k(x)\neq 0$ – рівномірним.

Оцінимо $P_{ud}\left(FFC, p_0\right)$ для різних співвідношень M і k. Зокрема, визначимо показники достовірності для двох випадків:

1) $M! < 2^k$ – відображення $f : A(x) \to R(x)$ сюр'єктівне: потужність множини значень перевірної частини менше потужності множини значень інформаційної частини – в середньому $2^k / M!$ комбінацій інформаційної частини мають однакову перевірну частину, що призводить до колізій;

2) $M! \geq 2^k$ – відображення $f : A(x) \to R(x)$ ін'єкційне або бієктивне: кожному значенню інформаційної частини відповідає унікальне значення перевірної частини, в цьому випадку колізії взагалі відсутні.

Оцінка ймовірності невиявленої помилки для ПФК з $M! < 2^k$

За умови статистичної незалежності даних на вході і виході блоку формування перестановки і $\varepsilon_k(x) \neq 0$ помилка $\varepsilon_r^{\wedge}(x)$ має рівномірний розподіл на множині з $M!$ можливих векторів. У цьому випадку для $\varepsilon_k(x) \neq 0$ імовірність появи кожного з $M!$ векторів помилок $\varepsilon_r^{\wedge}(x)$, включаючи нульовий, дорівнює

$$p_r^{\wedge} = \frac{1 - q_0^k}{M!}. \tag{2.7}$$

Позначимо через p_r імовірність появи помилки $\varepsilon_r(x)$ (включаючи нульову), здатної перетворити перестановку $R(x)$ у будь-яку з $M!$ перестановок (тобто дозволену комбінацію перевірної частини в дозволену).

Тоді за теоремою множення ймовірностей:

$$P_{ud}\left(FFC, p_0\right) = p_r^{\wedge} \cdot p_r. \tag{2.8}$$

Визначимо ймовірність p_r.

Для незалежних бітових помилок помилка $\varepsilon_r(x)$ розподілена за біноміальним законом: імовірність появи вектора з вагою Хеммінга $i \in [0; r]$

$$p_r(i) = C_r^i p_0^i q_0^{r-i}. \tag{2.9}$$

Тоді ймовірність нульової помилки в перевірній частині дорівнює $p_r(0) = q_0^r$.

Частка ненульових помилок перевірної частини, здатних перетворити перестановку $R(x)$ в будь-яку з $M!-1$ перестановок, дорівнює $\frac{M!-1}{2^r-1}$, де $r=l_rM$.

Позначимо через $f_{per}(i)$ кількість помилок ваги $i\in[0;r]$, здатних перетворити перестановку $R(x)$ чисел $\{0;1;2;\ldots;M-1\}$ у перестановку.

Нехай випадкова подія A = {помилка $\varepsilon_r(x)$ в перевірній частині перетворює перестановку чисел в перестановку}, $\mathrm{P}(A)=p_r$; випадкова подія $B_i=$ {поява помилки ваги i}, $\mathrm{P}(B_i)=p_r(i)$. Тоді умовна ймовірність $\mathrm{P}(A|B_i)=f_{per}(i)/C_r^i$ визначає ймовірність перетворення перестановки чисел в перестановку, зумовленого впливом помилки ваги i. З формули повної ймовірності і виразу (2.9)

$$p_r=\mathrm{P}(A)=\sum_{i=0}^{r}p_r(i)\cdot f_{per}(i)/C_r^i=\sum_{i=0}^{r}f_{per}(i)\,p_0^iq_0^{r-i}. \qquad (2.10)$$

Теорема 2.1. Імовірність p_r появи помилки $\varepsilon_r(x)$, здатної перетворити дозволену комбінацію перевірної частини ПФК в дозволену комбінацію (включаючи саму в себе), визначається виразом

$$p_r=\sum_{i=0}^{\lfloor r/2\rfloor}f_{per}(2i)\,p_0^{2i}q_0^{r-2i}, \qquad (2.11)$$

де $\sum_{i=0}^{\lfloor r/2\rfloor}f_{per}(2i)=M!$ і

$$f_{per}(0)=1;\ f_{per}(2)\le l_r\cdot M/2;\ f_{per}(4)\le l_r\cdot M\cdot\left(l_r\cdot(M+8)-10\right)/8. \qquad (2.12)$$

Доведення.

Спочатку покажемо, що вага помилок $\varepsilon_r(x)$, здатних перетворити одну перестановку чисел $\{0;1;2;\ldots;M-1\}$ в іншу, кратна двом.

Без обмеження загальності розгляду, приймемо перестановку $\pi(0)=\{0;1;\ldots;M-1\}$ в якості вихідної. Представимо символи перестановки в двійковому коді і запишемо їх послідовно, як показано на рис. 2.5.

$$
\begin{array}{l}
\pi(0)=\{0\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ \ldots\ ;\ M\text{-}1\} \qquad \sum(\mathrm{mod}\ 2) \\
\left|\begin{array}{cccccc}
\downarrow & \downarrow & \downarrow & \downarrow & & \downarrow \\
0 & 1 & 0 & 1 & \ldots & 1 \\
0 & 0 & 1 & 1 & \ldots & 1 \\
0 & 0 & 0 & 0 & \ldots & 1 \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & 0 & 0 & \ldots & 1
\end{array}\right| \qquad \begin{array}{c} = w_0 \\ = w_1 \\ = w_2 \\ \vdots \\ = w_{lr\text{-}1} \end{array}
\end{array}
$$

Рис. 2.5. Символи перевірної частини

Завада, яка переводить перестановку в перестановку, змінює місцями символи (стовпці) і не порушує їх склад. Тому значення $w_j \in \{0;1\}$, яке дорівнює сумі за модулем два біт j-го рядка, $j \in [0, l_r - 1]$, інваріантне відносно перестановки символів. Це означає, що завада в кожному рядку і, отже, $\varepsilon_r(x)$ мають парну вагу. Тому $f_{per}(2i+1) = 0$, $i \in \mathbb{N}_0$, а $p_r = \sum_{i=0}^{\lfloor r/2 \rfloor} f_{per}(2i)\, p_0^{2i} q_0^{r-2i}$.

Для $M! < 2^k$ потужність множини дозволених комбінацій перевірної частини $R(x)$ відповідає потужності множини перестановок порядку M і дорівнює $\mu(R(x)) = M!$. Перестановка $R(x)$ може бути єдиним чином модифікована помилкою $\varepsilon_r(x)$ в будь-яку з $M!$ перестановок. Тому загальна кількість помилок, здатних перетворити перестановку порядку M у перестановку, дорівнює $M!$.

Оцінимо значення $f_{per}(2i)$ для $i = \{0;1;2\}$.

1. Помилка нульової ваги переводить перестановку саму в себе: $f_{per}(0) = 1$.

2. Помилка ваги 2 перетворює перестановку в перестановку, якщо вона породжує транспозицію (вражає 2 різних символи і перетворює їх один в одного). Якщо $M = 2^{l_r}$, то кількість таких помилок – $f_{per}(2) = l_r \cdot M/2 = l_r \cdot 2^{l_r - 1}$. Якщо $2^{l_r - 1} < M < 2^{l_r}$, то $f_{per}(2) < l_r \cdot M/2$, звідки слідує оцінка $f_{per}(2)$ з (2.12).

3. Помилка ваги $i = 4$, яка призводить до помилки декодування, може вражати 2, 3 або 4 укрупнених символи перестановки, $M \geq 4$. Для $M = 2^{l_r}$ кількість таких помилок, що перетворюють перестановку в перестановку і вражають 2 символи,

дорівнює $C_{l_r}^2 \cdot M/2$; 3 символи – $C_{l_r}^2 \cdot 2 \cdot M$; 4 символи – $C_{l_r}^2 \cdot M/2 + M \cdot l_r \cdot \left(l_r \cdot (M-4)+2\right)/8$. Для $2^{l_r-1} < M < 2^{l_r}$ кількість таких помилок зменшується. Звідси нескладно отримати оцінку $f_{per}(4)$ з (2.12). ■

Приклад. Для $M = 8$ і $l_r = 3$ кількість помилок ваги 2 і 4, які можуть призводити до помилки декодування, дорівнюють, відповідно, $f_{per}(2) = 12$ і $f_{per}(4) = 114$. Частка таких векторів у загальній кількості помилок відповідної ваги дорівнює $f_{per}(2)/C_{24}^2 = 12/276 = 0,043$ і $f_{per}(4)/C_{24}^4 = 114/10626 = 0,011$, що підтверджує ефективність застосування оцінок (2.12).

Розглянемо властивості розподілу $f_{per}(i)$. Для цього сформулюємо теорему.

Теорема 2.2. Для $\log_2 M \in \mathbb{Z}$ розподіл $f_{per}(i)$ числа помилок, здатних перетворити перестановку $R(x)$ чисел $\{0;1;2;\ldots;M-1\}$ у перестановку, в залежності від їх ваги симетричний відносно значення $r/2$, тобто

$$f_{per}(i) = f_{per}(r-i). \tag{2.13}$$

Доведення.

Нехай $\varepsilon_r^{(i)}(x)$ – вектор помилки розмірності r біт і ваги i, для якого $R(x) \oplus \varepsilon_r^{(i)}(x) = R'(x)$, де $R(x)$ і $R'(x)$ – деякі перестановки. Тоді інверсний вектор помилки $\varepsilon_r^{(r-i)}(x) = \varepsilon_r^{(i)}(x) \oplus E_r(x)$, де $E_r(x)$ – вектор помилки розмірності і ваги $r-i$. У результаті впливу інверсної помилки перевірна частина модифікується в такий спосіб: $R(x) \oplus \varepsilon_r^{(n-i)}(x) = R(x) \oplus \varepsilon_r^{(i)}(x) \oplus E_r(x) = R'(x) \oplus E_r(x)$.

Якщо $\log_2 M \in \mathbb{Z}$, то множина з M елементів перестановки $R(x)$, представлених у двійковому рівномірному коді, бієктивно відображається на себе відносно інверсії біт її елементів (що еквівалентне підсумовуванню за модулем два з одиничним вектором). Тому $R'(x) \oplus E_r(x) = R''(x)$, де $R''(x)$ – перестановка.

Таким чином, якщо помилка $\varepsilon_r^{(i)}(x)$ призводить до перетворення перестановки в перестановку, то і інверсна помилка також призводить до перетворення

перестановки в перестановку, звідки слідує вираз (2.13). ■

Наслідок 2.1. Імовірність p_r появи помилки $\varepsilon_r(x)$, здатної перетворити дозволену комбінацію перевірної частини ПФК в дозволену (включаючи саму в себе), для $\log_2 M \in \mathbb{Z}$ дорівнює

$$p_r = \sum_{i=0}^{r/4-1} \left(f_{per}(2i)\left(p_0^{2i} q_0^{r-2i} + p_0^{r-2i} q_0^{2i} \right) \right) + f_{per}(r/2)\, p_0^{r/2} q_0^{r/2}, \tag{2.14}$$

де $f_{per}(0) = 1$.

Подальший розгляд будемо проводити для випадку, коли $\log_2 M \in \mathbb{R}$.

Виконаємо оцінку зверху для ймовірності p_r.

У правій частині (2.11) проведемо послідовно угруповання доданків виду $p_0^j q_0^{r-j}$ по C_r^i штук $\left(i = 2(m_1+1), 2(m_1+2), \ldots\right)$. Враховуючи, що $\sum f_{per}(2i) = M!$, $f_{per}(i) \le C_r^i$ і $p_0^i q_0^{r-i} > p_0^j q_0^{r-j}$ для $i < j$, отримаємо:

$$p_r = \sum_{i=0}^{\lfloor r/2 \rfloor} f_{perm}(2i)\, p_0^{2i} q_0^{r-2i} = q_0^r + \underbrace{p_0^2 q_0^{r-2} + \ldots + p_0^2 q_0^{r-2}}_{f_{per}(2)\ слагаемых} + \underbrace{p_0^4 q_0^{r-4} + \ldots + p_0^4 q_0^{r-4}}_{f_{per}(4)\ слагаемых} + \ldots +$$

$$+ \underbrace{p_0^{2\lfloor r/2 \rfloor} q_0^{r-2\lfloor r/2 \rfloor} + \ldots + p_0^{2\lfloor r/2 \rfloor} q_0^{r-2\lfloor r/2 \rfloor}}_{f_{per}(2\lfloor r/2 \rfloor)\ слагаемых} \le$$

$$\le q_0^r + \underbrace{p_0^2 q_0^{r-2} + \ldots + p_0^2 q_0^{r-2}}_{C_r^2\ слагаемых} + \underbrace{p_0^4 q_0^{r-4} + \ldots + p_0^4 q_0^{r-4}}_{C_r^4\ слагаемых} + \ldots + \underbrace{p_0^m q_0^{r-m} + \ldots + p_0^m q_0^{r-m}}_{C_r^m\ слагаемых} +$$

$$+ \underbrace{p_0^{m+2} q_0^{r-m-2} + \ldots + p_0^{m+2} q_0^{r-m-2}}_{z\ слагаемых},$$

де $z = M! - \sum_{i=0}^{m} C_r^{2i}$, а число $m \in \mathbb{N}$ таке, що

$$\sum_{i=0}^{m} C_r^{2i} \le M! < \sum_{i=0}^{m+1} C_r^{2i}. \tag{2.15}$$

Тоді

$$p_r \le \sum_{i=0}^{m} p_r(2i) + \left(\left(M! - \sum_{i=0}^{m} C_r^{2i} \right) \Big/ C_r^{2m+2} \right) p_r(2m+2), \tag{2.16}$$

де $p_r(i)$ обчислюються за (2.9), а m – за (2.15).

Оцінка (2.16) є грубою. Виконаємо її більш точно.

Відомо, що математичне сподівання біноміального розподілу (2.9) дорівнює $\lambda = r \cdot p_0$. Сам розподіл (2.9) має максимум у точці $i = \lfloor \lambda \rfloor$ і монотонно зменшується для $i < \lfloor \lambda \rfloor$ і $i > \lfloor \lambda \rfloor$. Розділимо суму в виразі (2.11) на дві складові.

Визначення 2.2. Імовірність появи в перевірній частині блоку помилки $\varepsilon_r(x)$, яка перетворює перестановку чисел $\{0;1;2;\ldots;M-1\}$ у перестановку, дорівнює сумі:

$$p_r = \sum_{i=0}^{m_1} f_{per}(2i)\, p_0^{2i} q_0^{r-2i} + \Delta_{per}(m_1), \tag{2.17}$$

де

$$\Delta_{per}(m_1) = \sum_{i=m_1+1}^{\lfloor r/2 \rfloor} f_{per}(2i)\, p_0^{2i} q_0^{r-2i}, \tag{2.18}$$

$0 \le m_1 \le \lfloor r/2 \rfloor - 1$.

Теорема 2.3. Для ймовірності $\Delta_{per}(m_1)$ появи помилки $\varepsilon_r(x)$ з вагою $i \ge 2(m_1+1)$, $0 \le m_1 \le \lfloor r/2 \rfloor - 1$, здатної перетворити дозволену комбінацію перевірної частини ПФК в дозволену комбінацію, має місце наступна оцінка:

$$\Delta_{per}(m_1) \le \sum_{i=m_1+1}^{m_2} p_r(2i) + \frac{M! - \sum_{i=0}^{m_1} f_{per}(2i) - \sum_{i=m_1+1}^{m_2} C_r^{2i}}{C_r^{2(m_2+1)}}\, p_r\big(2(m_2+1)\big), \tag{2.19}$$

де $p_r(i)$ обчислюється за (2.9), а число $m_2 \in \mathbb{N}$ таке, що

$$\sum_{i=m_1+1}^{m_2} C_r^{2i} \le M! - \sum_{i=0}^{m_1} f_{per}(2i) < \sum_{i=m_1+1}^{m_2+1} C_r^{2i}. \tag{2.20}$$

Доведення.

У правій частині (2.18) проведемо послідовно угруповання доданків виду $p_0^j q_0^{r-j}$ по C_r^i штук $\big(i = 2(m_1+1), 2(m_1+2), \ldots\big)$. Враховуючи, що $\sum f_{per}(2i) = M!$, $f_{per}(i) \le C_r^i$ і $p_0^i q_0^{r-i} > p_0^j q_0^{r-j}$ для $i < j$, отримаємо:

$$\Delta_{per}(m_1)=\sum_{i=m_1+1}^{\lfloor r/2\rfloor} f_{per}(2i)\,p_0^{2i}q_0^{r-2i}=$$

$$=\underbrace{p_0^{2(m_1+1)}q_0^{r-2(m_1+1)}+\ldots+p_0^{2(m_1+1)}q_0^{r-2(m_1+1)}}_{f_{per}(2(m_1+1))\ слагаемых}+\underbrace{p_0^{2(m_1+2)}q_0^{r-2(m_1+2)}+\ldots+p_0^{2(m_1+2)}q_0^{r-2(m_1+2)}}_{f_{per}(2(m_1+2))\ слагаемых}+\ldots+$$

$$+\underbrace{p_0^{2\lfloor r/2\rfloor}q_0^{r-2\lfloor r/2\rfloor}+\ldots+p_0^{2\lfloor r/2\rfloor}q_0^{r-2\lfloor r/2\rfloor}}_{f_{per}(2\lfloor r/2\rfloor)\ слагаемых}\le$$

$$\le\underbrace{p_0^{2(m_1+1)}q_0^{r-2(m_1+1)}+\ldots+p_0^{2(m_1+1)}q_0^{r-2(m_1+1)}}_{C_r^{2(m_1+1)}\ слагаемых}+\underbrace{p_0^{2(m_1+2)}q_0^{r-2(m_1+2)}+\ldots+p_0^{2(m_1+2)}q_0^{r-2(m_1+2)}}_{C_r^{2(m_1+2)}\ слагаемых}+\ldots+$$

$$+\underbrace{p_0^{2m_2}q_0^{r-2m_2}+\ldots+p_0^{2m_2}q_0^{r-2m_2}}_{C_r^{2m_2}\ слагаемых}+\underbrace{p_0^{2(m_2+1)}q_0^{r-2(m_2+1)}+\ldots+p_0^{2(m_2+1)}q_0^{r-2(m_2+1)}}_{z\ слагаемых},$$

де $z=M!-\sum_{i=0}^{m_1} f_{per}(2i)-\sum_{i=m_1+1}^{m_2} C_r^{2i}$, а число $m_2\in\mathbb{N}$ таке, що

$$\sum_{i=m_1+1}^{m_2} C_r^{2i}\le M!-\sum_{i=0}^{m_1} f_{per}(2i)<\sum_{i=m_1+1}^{m_2+1} C_r^{2i}.$$

Тоді $\Delta_{per}(m_1)\le\sum_{i=m_1+1}^{m_2} p_r(2i)+\left(z/C_r^{2(m_2+1)}\right)p_r\left(2(m_2+1)\right)$, де $p_r(i)$ обчислюється за (2.9). ■

Зауваження 2.1. Оскільки $z<C_r^{2(m_2+1)}$, справедливо

$$\Delta_{per}(m_1)\le\sum_{i=m_1+1}^{m_2+1} p_r(2i)\le\sum_{i=m_1+1}^{\lfloor r/2\rfloor} p_r(2i)\le\sum_{i=m_1+1}^{\infty} p_r(2i).$$

Наслідок 2.2. В умовах застосування апроксимаційної формули Пуассона для біноміального розподілу має місце оцінка:

$$\Delta_{per}(m_1)\le e^{-\lambda}\cdot\frac{\lambda^{2(m_1+1)}}{(2(m_1+1))!}\cdot\frac{(2m_1+3)^2}{(2m_1+3)^2-\lambda^2},\qquad(2.21)$$

де $\lambda=r\cdot p_0$ і $m_1>(\lambda-3)/2$.

Доведення.

Згідно зауваженню 2.1 і апроксимаційної формули Пуассона

$$p_r(i)\simeq\frac{\lambda^i}{i!}e^{-\lambda},\qquad(2.22)$$

$\lambda=r\cdot p_0$, маємо:

$$\Delta_{per}(m_1) \le \sum_{i=m_1+1}^{\infty} \frac{\lambda^{2i}}{(2i)!} e^{-\lambda} = e^{-\lambda}\left(\frac{\lambda^{2(m_1+1)}}{(2(m_1+1))!} + \frac{\lambda^{2(m_1+2)}}{(2(m_1+2))!} + \frac{\lambda^{2(m_1+3)}}{(2(m_1+3))!} + \dots \right) \le$$

$$\le e^{-\lambda} \frac{\lambda^{2(m_1+1)}}{(2(m_1+1))!}\left(1 + \frac{\lambda^2}{(2m_1+3)^2} + \frac{\lambda^4}{(2m_1+3)^4} + \dots \right).$$

Для $m_1 > \dfrac{\lambda-3}{2}$ виконується $\dfrac{\lambda^2}{(2m_1+3)^2} < 1$. Обчислюючи суму, отримаємо

$$\Delta_{per}(m_1) \le e^{-\lambda} \frac{\lambda^{2(m_1+1)}}{(2(m_1+1))!} \cdot \frac{1}{1-\lambda^2/(2m_1+3)^2} = e^{-\lambda} \cdot \frac{\lambda^{2(m_1+1)}}{(2(m_1+1))!} \cdot \frac{(2m_1+3)^2}{(2m_1+3)^2-\lambda^2}. \blacksquare$$

Зауваження 2.2. Значення $\Delta_{per}(m_1)$ оцінюється за (2.19) або (2.21), де m_1 обирається таким чином, щоб $m_1 > (\lambda-3)/2$ і оцінка $\Delta_{per}(m_1)$ не перевищувала максимальної абсолютної похибки обчислень ε_1.

Нагадаємо, що $\lambda = r \cdot p_0$, $r = l_r \cdot M$, де $l_r = \lceil \log_2 M \rceil$.

Наслідок 2.3. У таблиці 2.3 для кожної пари $(m_1; p_0)$ і заданої точності ε_1 вказано максимальне значення M_0, для якого $\Delta_{per}(m_1) \le \varepsilon_1$ за всіх $M \le M_0$.

Таблиця 2.3

Діапазони значень M у залежності від $(m_1; p_0)$, за яких $\Delta_{per}(m_1) \le \varepsilon_1$ для $\varepsilon_1 = 10^{-3}$

m_1 \ p_0	10^{-3}	10^{-4}	10^{-5}
0	$M \le 11$	$M \le 65$	$M \le 508$
1	$M \le 64$	$M \le 487$	$M \le 3652$
2	$M \le 142$	$M \le 1036$	$M \le 8192$

Зауваження 2.3. Помилка декодування ПФК для $M! < 2^k$ визначається за (2.8): $P_{ud}(FFC, p_0) = p_r^{\wedge} \cdot p_r$, де $p_r^{\wedge}$ обчислюється за (2.7), а p_r оцінюється за (2.17).

Оцінка ймовірності невиявленої помилки для ПФК з $M! \ge 2^k$

За умови статистичної незалежності даних на вході і виході блоку формування перестановки і рівномірного розподілу значень перевірної частини коду $R(x)$ на множині з $2^k \le M!$ перестановок колізії відсутні. У цьому випадку для $\varepsilon_k(x) \ne 0$

імовірність появи кожного з $\left(2^k-1\right)$ ненульових векторів помилок $\varepsilon_r^{\wedge}\left(x\right)$ дорівнює

$$p_r^{\wedge}=\frac{1-q_0^k}{2^k-1}. \tag{2.23}$$

Позначимо через p_r^* імовірність появи помилки $\varepsilon_r\left(x\right)$ (не включаючи нульову), здатної перетворити перестановку $R\left(x\right)$ у будь-яку з $\left(2^k-1\right)$ інших перестановок (тобто дозволену комбінацію перевірної частини в іншу дозволену).

Тоді за теоремою множення ймовірностей для помилки декодування маємо:

$$P_{ud}\left(FFC,p_0\right)=p_r^{\wedge}\cdot p_r^*. \tag{2.24}$$

Визначимо ймовірність p_r^*.

Частка ненульових помилок перевірної частини, здатних перетворити перестановку $R\left(x\right)$ у будь-яку з $\left(2^k-1\right)$ перестановок, дорівнює $\left(2^k-1\right)/\left(2^r-1\right)$.

Позначимо через $f_{per}^*\left(i\right)$ кількість помилок ваги $i\in\left[0;r\right]$, здатних перетворити дозволену перестановку $R\left(x\right)$ у будь-яку з $\left(2^k-1\right)$ дозволених перестановок.

Нехай випадкова подія A* = {помилка $\varepsilon_r\left(x\right)$ у перевірній частини перетворює дозволену перестановку чисел у дозволену перестановку}, $\mathrm{P}\left(A^*\right)=p_r^*$; випадкова подія B_i={поява помилки ваги i}, $\mathrm{P}\left(B_i\right)=p_r\left(i\right)$. Тоді $\mathrm{P}\left(A^*\middle|B_i\right)=f_{per}^*\left(i\right)/C_r^i$ вказує ймовірність перетворення дозволеної перестановки чисел у дозволену перестановку за появи помилки ваги i. Унаслідок формули повної ймовірності та виразу (2.9),

$$p_r^*=\mathrm{P}\left(A^*\right)=\sum_{i=0}^{r}p_r\left(i\right)\cdot f_{per}^*\left(i\right)/C_r^i=\sum_{i=0}^{r}f_{per}^*\left(i\right)p_0^iq_0^{r-i}. \tag{2.25}$$

Теорема 2.4. Імовірність p_r^* появи помилки $\varepsilon_r\left(x\right)$, здатної перетворити дозволену комбінацію перевірної частини ПФК в іншу дозволену комбінацію, дорівнює

$$p_r^*=\sum_{i=1}^{\lfloor r/2\rfloor}f_{per}^*\left(2i\right)p_0^{2i}q_0^{r-2i}. \tag{2.26}$$

де $\sum_{i=1}^{\lfloor r/2 \rfloor} f_{per}^{*}(2i) = 2^k - 1$ і

$$f_{per}^{*}(i) \le f_{per}(i). \tag{2.27}$$

Доведення.

Згідно з теоремою 2.1, вага помилок $\varepsilon_r(x)$, здатних перетворити перестановку чисел $\{0;1;2;\ldots;M-1\}$ у іншу, кратна двом. Тому $p_r^{*} = \sum_{i=1}^{\lfloor r/2 \rfloor} f_{per}^{*}(2i)\, p_0^{2i} q_0^{r-2i}$.

Потужність множини дозволених комбінацій перевірної частини $R(x)$ для $M! \ge 2^k$ відповідає потужності значень інформаційної частини і дорівнює $\mu(R(x)) = 2^k$. Перестановка $R(x)$ може бути єдиним чином перетворена помилкою $\varepsilon_r(x)$ у будь-яку з інших $(2^k - 1)$ дозволених перестановок. Тому загальна кількість помилок, здатних перетворити дозволену перестановку порядку M у іншу дозволену перестановку, дорівнює $(2^k - 1)$. Звідси $\sum_{i=1}^{r} f_{per}^{*}(i) = 2^k - 1$.

Оскільки кількість дозволених комбінацій перевірної частини не перевищує потужності множини перестановок $(2^k \le M!)$, $f_{per}^{*}(i) \le f_{per}(i)$ для $\forall i \in [1; \lfloor r/2 \rfloor]$. ■

Підставляючи вирази (2.23) і (2.26) в (2.24), маємо:

$$P_{ud}^{*}(FFC, p_0) = p_r^{\wedge} \cdot p_r^{*} = \frac{1 - q_0^k}{2^k - 1} \cdot \sum_{i=1}^{\lfloor r/2 \rfloor} f_{per}^{*}(2i)\, p_0^{2i} q_0^{r-2i}. \tag{2.28}$$

Виконаємо оцінку зверху для ймовірності p_{per}^{*}.

У правій частині (2.26) проведемо послідовно угруповання доданків виду $p_0^j q_0^{r-j}$ по C_r^i штук $(i = 2(m_1+1), 2(m_1+2), \ldots)$. Враховуючи, що $\sum f_{per}(2i) = 2^k$, $f_{per}(i) \le C_r^i$ і $p_0^i q_0^{r-i} > p_0^j q_0^{r-j}$ для $i < j$, отримаємо:

$$p_r^{*} = \sum_{i=1}^{\lfloor r/2 \rfloor} f_{per}(2i)\, p_0^{2i} q_0^{r-2i} = \underbrace{p_0^2 q_0^{r-2} + \ldots + p_0^2 q_0^{r-2}}_{f_{per}(2)\ слагаемых} + \underbrace{p_0^4 q_0^{r-4} + \ldots + p_0^4 q_0^{r-4}}_{f_{per}(4)\ слагаемых} + \ldots +$$

$$+ \underbrace{p_0^{2\lfloor r/2 \rfloor} q_0^{r-2\lfloor r/2 \rfloor} + \ldots + p_0^{2\lfloor r/2 \rfloor} q_0^{r-2\lfloor r/2 \rfloor}}_{f_{per}(2\lfloor r/2 \rfloor)\ слагаемых} \le$$

$$\le \underbrace{p_0^2 q_0^{r-2} + \ldots + p_0^2 q_0^{r-2}}_{C_r^2 \text{ слагаемых}} + \underbrace{p_0^4 q_0^{r-4} + \ldots + p_0^4 q_0^{r-4}}_{C_r^4 \text{ слагаемых}} + \ldots + \underbrace{p_0^m q_0^{r-m} + \ldots + p_0^m q_0^{r-m}}_{C_r^m \text{ слагаемых}} +$$

$$+ \underbrace{p_0^{m+2} q_0^{r-m-2} + \ldots + p_0^{m+2} q_0^{r-m-2}}_{z \text{ слагаемых}},$$

де $z = 2^k - 1 - \sum_{i=1}^{m} C_r^{2i}$, а число $m \in \mathbb{N}$ таке, що

$$\sum_{i=1}^{m} C_r^{2i} \le 2^k - 1 < \sum_{i=1}^{m+1} C_r^{2i}. \tag{2.29}$$

Тоді

$$p_r^* \le \sum_{i=1}^{m} p_r(2i) + \left(\left(2^k - 1 - \sum_{i=1}^{m} C_r^{2i} \right) \Big/ C_r^{2m+2} \right) p_r(2m+2). \tag{2.30}$$

де $p_r(i)$ обчислюються за (2.9), а m – за (2.29).

Оцінка (2.30) є грубою. Виконаємо її більш точно.

Розділимо суму в виразі (2.26) на дві складові.

Визначення 2.3. Імовірність появи в перевірній частині блоку помилки $\varepsilon_r(x)$, яка перетворює дозволену перестановку у іншу дозволену перестановку, дорівнює:

$$p_r^* = \sum_{i=1}^{m_1} f_{per}^*(2i)\, p_0^{2i} q_0^{r-2i} + \Delta_{per}^*(m_1), \tag{2.31}$$

де

$$\Delta_{per}^*(m_1) = \sum_{i=m_1+1}^{\lfloor r/2 \rfloor} f_{per}^*(2i)\, p_0^{2i} q_0^{r-2i}, \tag{2.32}$$

$1 \le m_1 \le \lfloor r/2 \rfloor - 1$.

Теорема 2.5. Для ймовірності $\Delta_{per}^*(m_1)$ появи помилки $\varepsilon_r(x)$ з вагою $i \ge 2(m_1+1)$, $0 \le m_1 \le \lfloor r/2 \rfloor - 1$, здатної перетворити дозволену комбінацію перевірної частини ПФК в іншу дозволену комбінацію, має місце наступна оцінка:

$$\Delta_{per}^*(m_1) \le \sum_{i=m_1+1}^{m_2} p_r(2i) + \frac{2^k - 1 - \sum_{i=1}^{m_1} f_{per}^*(2i) - \sum_{i=m_1+1}^{m_2} C_r^{2i}}{C_r^{2(m_2+1)}} p_r(2(m_2+1)), \tag{2.33}$$

де $p_r(i)$ обчислюється за (2.9), а число $m_2 \in \mathbb{N}$ таке, що

$$\sum_{i=m_1+1}^{m_2} C_r^{2i} \le 2^k - 1 - \sum_{i=1}^{m_1} f_{per}^*(2i) < \sum_{i=m_1+1}^{m_2+1} C_r^{2i}. \qquad (2.34)$$

Доведення.

У правій частині (2.32) проведемо послідовно угруповання доданків виду $p_0^j q_0^{r-j}$ по C_r^i штук $\left(i = 2(m_1+1), 2(m_1+2), \ldots\right)$. Враховуючи, що $\sum f_{per}(2i) = 2^k$, $f_{per}^*(i) \le C_r^i$ і $p_0^i q_0^{r-i} > p_0^j q_0^{r-j}$ для $i < j$, отримаємо:

$$\Delta_{per}^*(m_1) = \sum_{i=m_1+1}^{\lfloor r/2 \rfloor} f_{per}^*(2i)\, p_0^{2i} q_0^{r-2i} =$$

$$= \underbrace{p_0^{2(m_1+1)} q_0^{r-2(m_1+1)} + \ldots + p_0^{2(m_1+1)} q_0^{r-2(m_1+1)}}_{f_{per}^*(2(m_1+1))\ доданків} + \underbrace{p_0^{2(m_1+2)} q_0^{r-2(m_1+2)} + \ldots + p_0^{2(m_1+2)} q_0^{r-2(m_1+2)}}_{f_{per}^*(2(m_1+2))\ доданків} + \ldots +$$

$$+ \underbrace{p_0^{2\lfloor r/2 \rfloor} q_0^{r-2\lfloor r/2 \rfloor} + \ldots + p_0^{2\lfloor r/2 \rfloor} q_0^{r-2\lfloor r/2 \rfloor}}_{f_{per}^*(2\lfloor r/2 \rfloor)\ доданків} \le$$

$$\le \underbrace{p_0^{2(m_1+1)} q_0^{r-2(m_1+1)} + \ldots + p_0^{2(m_1+1)} q_0^{r-2(m_1+1)}}_{C_r^{2(m_1+1)}\ доданків} + \underbrace{p_0^{2(m_1+2)} q_0^{r-2(m_1+2)} + \ldots + p_0^{2(m_1+2)} q_0^{r-2(m_1+2)}}_{C_r^{2(m_1+2)}\ доданків} + \ldots +$$

$$+ \underbrace{p_0^{2m_2} q_0^{r-2m_2} + \ldots + p_0^{2m_2} q_0^{r-2m_2}}_{C_r^{2m_2}\ доданків} + \underbrace{p_0^{2(m_2+1)} q_0^{r-2(m_2+1)} + \ldots + p_0^{2(m_2+1)} q_0^{r-2(m_2+1)}}_{z^*\ доданків},$$

де $z^* = 2^k - 1 - \sum_{i=1}^{m_1} f_{per}^*(2i) - \sum_{i=m_1+1}^{m_2} C_r^{2i}$, а число $m_2 \in \mathbb{N}$ таке, що

$$\sum_{i=m_1+1}^{m_2} C_r^{2i} \le 2^k - 1 - \sum_{i=1}^{m_1} f_{per}^*(2i) < \sum_{i=m_1+1}^{m_2+1} C_r^{2i}.$$

Тоді $\Delta_{per}^*(m_1) \le \sum_{i=m_1+1}^{m_2} p_r(2i) + \left(z^* / C_r^{2(m_2+1)}\right) p_r\left(2(m_2+1)\right)$, де $p_r(i)$ обчислюється за (2.9). ■

Зауваження 2.4. Оскільки $z^* < C_r^{2(m_2+1)}$,

$$\Delta_{per}^*(m_1) \le \sum_{i=m_1+1}^{m_2+1} p_r(2i) \le \sum_{i=m_1+1}^{\lfloor r/2 \rfloor} p_r(2i) \le \sum_{i=m_1+1}^{\infty} p_r(2i).$$

Відповідно до наслідку 2.2, в умовах застосування апроксимаційної формули Пуассона для біноміального розподілу оцінка зверху ймовірності $\Delta_{m_1}^*$ появи помилки $\varepsilon_r(x)$ з вагою $i \ge 2(m_1+1)$, $1 \le m_1 \le \lfloor r/2 \rfloor - 1$, здатної перетворити

дозволену комбінацію перевірної частини повного факторіального коду в іншу дозволену комбінацію, має вигляд

$$\Delta^*_{per}\left(m_1\right) \le e^{-\lambda} \cdot \frac{\lambda^{2(m_1+1)}}{\left(2\left(m_1+1\right)\right)!} \cdot \frac{\left(2m_1+3\right)^2}{\left(2m_1+3\right)^2-\lambda^2}, \tag{2.35}$$

де $\lambda = r \cdot p_0$ і $m_1 > \left(\lambda - 3\right)/2$.

Зауваження 2.5. Значення p^*_r обчислюється відповідно до (2.31), де $\Delta^*_{per}\left(m_1\right)$ оцінюється за (2.33) або (2.35). Значення m_1 обирається так, щоб $m_1 > \left(\lambda - 3\right)/2$ і $\Delta^*_{per}\left(m_1\right)$ не перевищувала максимальної абсолютної похибки обчислень ε_1.

Оцінимо зверху ймовірність p^*_r.

Наслідок 2.4. Для ймовірності p^*_r появи помилки $\varepsilon_r\left(x\right)$, здатної перетворити дозволену комбінацію перевірної частини ПФК в іншу дозволену комбінацію, має місце наступна оцінка:

$$p^*_r \le \sum_{i=1}^{m_1} f_{per}\left(2i\right) p_0^{2i} q_0^{r-2i} + \Delta_{per}\left(m_1\right), \tag{2.36}$$

де $\Delta_{per}\left(m_1\right)$ оцінюється за (2.19) або (2.21).

Доведення.

Унаслідок теореми 2.4 і виразу (2.27) $\sum_{i=1}^{\lfloor r/2 \rfloor} f^*_{per}\left(2i\right) p_0^{2i} q_0^{r-2i} \le \sum_{i=0}^{\lfloor r/2 \rfloor} f_{per}\left(2i\right) p_0^{2i} q_0^{r-2i}$, звідки випливає оцінка (2.36). ■

Оскільки величина p^*_r може приймати свої значення в широких межах (тому що $f^*_{per}\left(0\right) = 0$), доцільно для оцінювання точності обчислень використовувати відносну похибку обчислень $\delta_{per}\left(m_1\right) = \dfrac{\Delta_{per}\left(m_1\right)}{\sum_{i=0}^{\lfloor r/2 \rfloor} f_{per}\left(2i\right) p_0^{2i} q_0^{r-2i}}$, яка не повинна перевищувати необхідного значення δ_{per}: $\delta_{per}\left(m_1\right) \le \delta_{per}$.

Наслідок 2.5. Нижче в таблиці 2.4 для кожної пари $\left(m_1; p_0\right)$ і точності δ_{per} вказано максимальне значення M_0, для якого $\delta^{'}_{per}\left(m_1\right) \le \delta_{per}$

$$\left(\delta'_{per}(m_1) = \frac{\Delta_{per}(m_1)}{(l_r \cdot M/2)\, p_0^2 q_0^{r-2}} \geq \delta_{per}(m_1) \right)$$ за всіх $M \leq M_0$.

Таблиця 2.4

Діапазони значень M у залежності від $(m_1; p_0)$, за яких $\delta'_{per}(m_1) \leq \delta_{per} = 10^{-2}$

m_1 \ p_0	10^{-3}	10^{-4}	10^{-5}
1	$M \leq 12$	$M \leq 38$	$M \leq 132$
2	$M \leq 54$	$M \leq 255$	$M \leq 1174$

Зауваження 2.6. Помилка декодування ПФК з $M! \geq 2^k$ визначається за (2.24): $P_{ud}(FFC, p_0) = p_r^{\wedge} \cdot p_r^*$, де $p_r^{\wedge}$ обчислюється за (2.23), а p_r^* оцінюється за (2.36).

Зауваження 2.7. Вираз (2.23) справедливий для $M! \geq 2^k$ за умови відсутності колізій у перевірній частині коду. Тому перед застосуванням цього виразу необхідно переконатися в тому, що обрана функція модифікації синдрому $f(S_F(j-1))$ дійсно не породжує колізії. У інших випадках імовірність помилки декодування перетворюється відповідно до статистики множини перестановок, породжуваних під час використання обраної функції модифікації синдрому.

2.3.6.3. Характеристики системи передавання даних з вирішальним зворотним зв'язком

Визначимо оцінку основних показників системи передавання даних з ВЗЗ:

- відносної швидкості передавання;
- енергетичного виграшу.

Відносна швидкість передавання

Згідно [273, с. 676], під відносною швидкістю передавання ν_0 системи з ВЗЗ розуміється відношення математичного сподівання числа інформаційних символів, що надійшли до одержувача, до загальної кількості кодових символів, що надійшли в прямий канал. Іншими словами,

$$\nu_0 = B/C \tag{2.37}$$

де B – фактична швидкість (швидкість передавання в каналі з помилками);

C – пропускна здатність каналу даних (швидкість передавання в каналі без помилок).

Представимо відносну швидкість передавання ν_0 у вигляді добутку

$$\nu_0 = \nu_1 \nu_2, \tag{2.38}$$

де $\nu_1 = k/n$ – швидкість коду (статична складова втрати швидкості передавання);

ν_2 – динамічна складова втрати швидкості передавання внаслідок перезапитів.

Теорема 2.6. Нехай $\nu_{2\,\min}$ – поріг між станами норми і аварії каналу зв'язку. Тоді для заданих p_0 і $\nu_{2\,\min}$ існує максимальне значення довжини кодової комбінації

$$n_{\max} \approx -\ln \nu_{2\,\min} / p_0, \tag{2.39}$$

таке, що для $\forall n \le n_{\max}$ справедливим є $\nu_2 \ge \nu_{2\,\min}$.

Доведення.

За швидкості передавання C біт/сек час доставки блоку даних від джерела до приймача в найпростішій системі з ВЗЗ становить $t_{block} = n/C + t_{distr}$ (t_{distr} – час поширення сигналу каналом), а ймовірність такої події – $Q + P_{ud}$, де $Q = (1 - p_0)^n$, P_{ud} – імовірність невиявленої помилки. Приймемо, що $t_{distr} \ll n/C$. Тоді $t_{block} = n/C + t_{distr} \approx n/C$. Крім того, врахуємо умову $P_{ud} \ll Q$. Тоді блок з імовірністю Q доставляється без перезапиту за час $t_{block} \approx n/C$, а з імовірністю $1-Q$ – перезапитується. У разі перезапиту повторно переданий блок з імовірністю Q доставляється без помилок за час $t_{block} \approx n/C$, а з імовірністю $1-Q$ – ще раз перепитується. І т.д.

Приймемо, що час доставки зворотним каналом зв'язку сигналу підтвердження або перезапиту, а також час аналізу комбінації і сигналу зворотного зв'язку дуже малий у порівнянні з t_{block}. У цьому випадку загальний час доставки блоку t_{deliv} за одного перепиту дорівнює $2t_{block}$, за двох перепитів – $3t_{block}$ і т.д. Нехай N_{trans} – кількість спроб передавання блоку до його безпомилкового прийому, тоді $t_{deliv} = N_{trans} \cdot t_{block}$. Розподіл імовірностей для N_{trans} і t_{deliv} представлено в таблиці 2.5.

Таблиця 2.5

Розподіл імовірностей для випадкових величин N_{trans} і t_{deliv}

N_{trans}	1	2	3	...	i	...
t_{deliv}	t_{block}	$2t_{block}$	$3t_{block}$	...	it_{block}	...
$P\left(t_{deliv}=i\cdot t_{block}\right)$	Q	$Q(1-Q)$	$Q(1-Q)^2$	...	$Q(1-Q)^{i-1}$	...

Таким чином, функція імовірності для $i\in\{1,2,3,\ldots\}$ $P_i=P\left(N_{trans}=i\right)=P\left(t_{deliv}=i\cdot t_{block}\right)=Q(1-Q)^{i-1}$ відповідає геометричному розподілу з математичним сподіванням $M\left(N_{trans}\right)=1/Q$. Тому в системі з ВЗЗ середня кількість спроб передавання блоку до його безпомилкового прийому дорівнює $\overline{N}_{trans}=1/Q$, середній час доставки блоку – $\bar{t}_{deliv}=t_{block}/Q$, а $\nu_2=t_{block}/\bar{t}_{deliv}=Q$.

Оскільки для $p_0\in[0;0.5]$ і фіксованого n функція $Q(p_0,n)=(1-p_0)^n$ монотонно спадає від 1 до 0.5^n, справедливими є наступні твердження: $\nu_0\le\nu_1$; для $p_0\to 0.5\Rightarrow Q\to 0$, отже, $\nu_2\to 0$ і $\nu_0\to 0$.

Разом з тим функція $Q(p_0,n)=(1-p_0)^n$ за фіксованого $p_0\in[0;0.5]$ монотонно спадає по n, $n>0$. Отже, ν_2 також монотонно спадає по n, $n>0$. Тому для заданого p_0 існує максимальне значення довжини блоку даних $n_{\max}$, для якого виконується умова $\nu_2\ge\nu_{2\min}$: $\exists n_{\max}$: $\nu_2\ge\nu_{2\min}$ для $\forall n\le n_{\max}$, де $\nu_{2\min}$ – поріг між станами «норма» і «аварія» каналу зв'язку. Вирішуючи нерівність $Q\ge\nu_{2\min}$ для $Q=(1-p_0)^n$, зрозуміло, що $n_{\max}=\ln\nu_{2\min}/\ln(1-p_0)$. Для $p_0\ll 1$, що має місце в більшості реальних каналів зв'язку, $\ln(1-p_0)\approx -p_0$, звідки слідує (2.39). ■

Наслідок 2.6. Для каналів ТМЗК з $p_0=10^{-3}$ за $\nu_{2\min}=0.2\div 0.3$ значення $n_{\max}=1609\div 1203$. Для каналів гіршої якості (радіоканалів діапазонів ДВ, СВ, КВ з $p_0\le 10^{-2}$) допустима довжина блоку зменшується, а зменшення ν_1 призводить до зменшення ν_0. Для каналів кращої якості (мікрохвильових, супутникових, оптичних) на порядки збільшується допустима довжина блоку, а $\nu_0\to 1$.

Енергетичний виграш

Енергетичний виграш у випадку застосування завадостійкого кодування визначається різницею рівнів сигналу на вході приймача, що забезпечують однакову ймовірність безпомилкового прийому блоку даних без використання і з використанням завадостійкого кодування.

Визначимо енергетичний виграш ΔP для оптимального некогерентного приймача двійкових сигналів, для якого $p_0 = 0.5 \cdot e^{-0.5h^2}$ [274, с. 45], де h^2 – відношення енергії сигналу до спектральної щільності потужності шуму. Тоді

$$\Delta P = 10\lg\left(h_{eq}^2 / h_0^2\right) = 10\lg\left(\ln\left(2p_{0eq}\right)/\ln\left(2p_0\right)\right), \qquad (2.40)$$

де $h_0^2 = 2\ln\left(2p_0\right)$ – відношення енергії сигналу до спектральної щільності потужності шуму на вході некогерентного приймача, що забезпечує ймовірність бітової помилки p_0 на його виході;

h_{eq}^2 – відношення енергії сигналу до спектральної щільності потужності шуму на вході некогерентного приймача, що забезпечує еквівалентну ймовірність бітової помилки на його виході p_{0eq}, визначену в [273, с. 676] як імовірність помилки в гіпотетичному симетричному постійному двійковому каналі, за якої ймовірність безпомилкового прийому така ж, як і в цій системі: $\left(1-p_{0eq}\right)^k = \left(1-P_{ud}\right)^{1/(Q+P_{ud})}$.

Згідно з [273, с. 677], для $p_{0eq}, P_{ud} \ll 1$ еквівалентна ймовірність бітової помилки

$$p_{0eq} \approx P_{ud} / k\left(Q + P_{ud}\right). \qquad (2.41)$$

Далі p_{0eq} і, відповідно, ΔP оцінюватимемо знизу, використовуючи для обчислення формул (2.41) і (2.40) оцінку зверху для P_{ud}.

2.3.6.4. Оцінка показників достовірності повного факторіального кодування

1. Нижче в таблиці 2.6 представлено приклади ПФК для $n = 1400$ і їх характеристики для $p_0 = 10^{-3}$ (де $k = n - r$ і $r = l_r \cdot M = \lceil \log_2 M \rceil \cdot M$).

Таблиця 2.6

Приклади ПФК для $n=1400$

n	k	M	ν_0	$P_{ud}\left(FFC, p_0\right)$	ΔP
1400	1392	4	0,276	0,031	1,478
1400	1376	8	0,242	$1{,}811\cdot10^{-5}$	4,121
1400	1336	16	0,235	$3{,}305\cdot10^{-14}$	7,646
1400	1240	32	0,218	$2{,}302\cdot10^{-36}$	11,465
1400	1016	64	0,179	$3{,}429\cdot10^{-90}$	15,305
1400	504	128	0,089	$3{,}641\cdot10^{-156}$	17,653

2. Виконаємо порівняння ПФК з систематичним двійковим CRC-кодом за критерієм ефективності виявлення помилок каналу зв'язку. Графіки залежностей оцінок імовірностей невиявленої помилки від k в результаті застосування кодів для $p_0=10^{-3}$ представлено на рис. 2.6. Оцінку ймовірності невиявленої помилки для CRC-коду в системі з ВЗЗ визначено в додатку В.

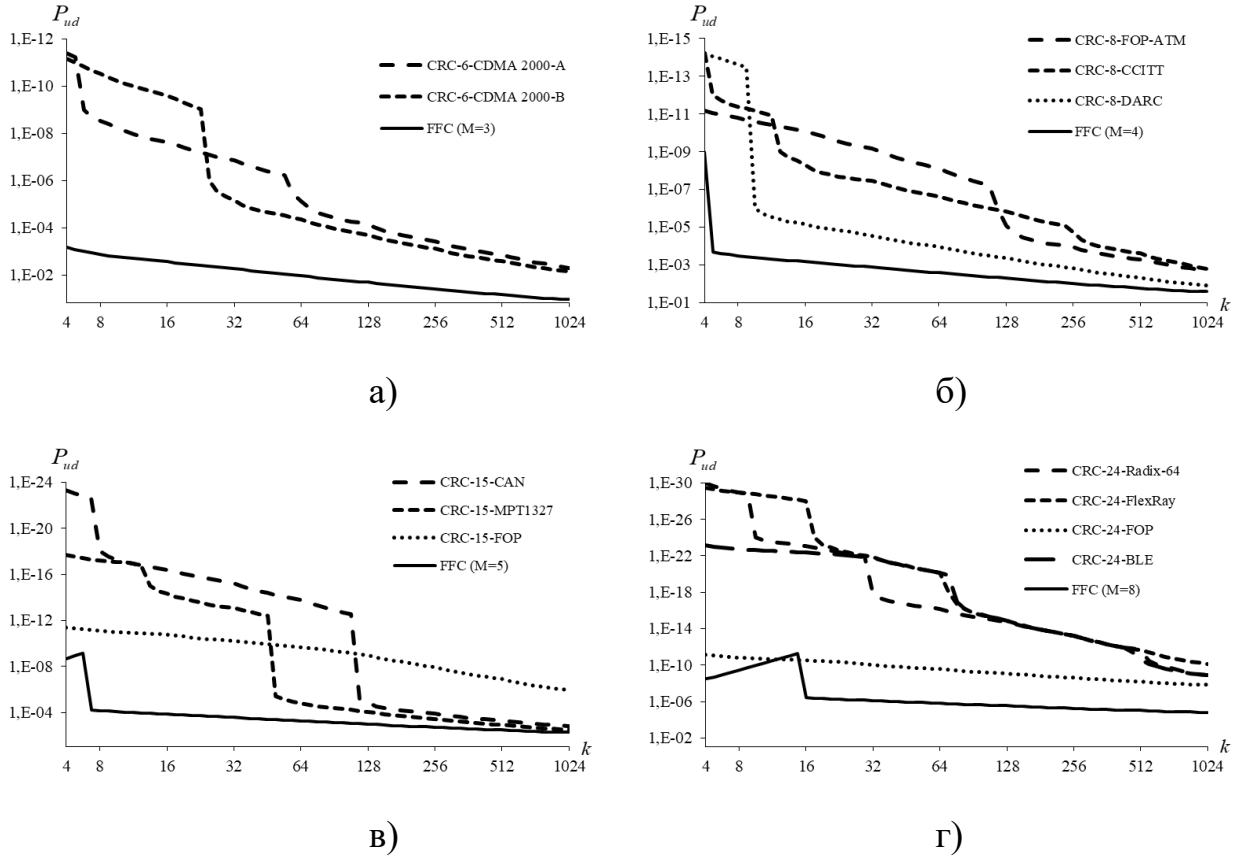


Рис. 2.6. Графіки залежностей оцінок імовірностей невиявленої помилки від довжини інформаційної частини для $p_0=10^{-3}$ і $r=6$ (а); $r=8$ (б); $r=15$ (в); $r=24$ (г)

Графіки на рис. 2.6. свідчать про те, що виявляюча здатність ПФК поступається виявляючій здатності CRC-коду на малих значеннях k і наближається до неї в процесі збільшення k.

Визначимо залежності енергетичного виграшу в результаті застосування ПФК і виявляючого помилки CRC-коду. Результати представимо на рис. 2.7.

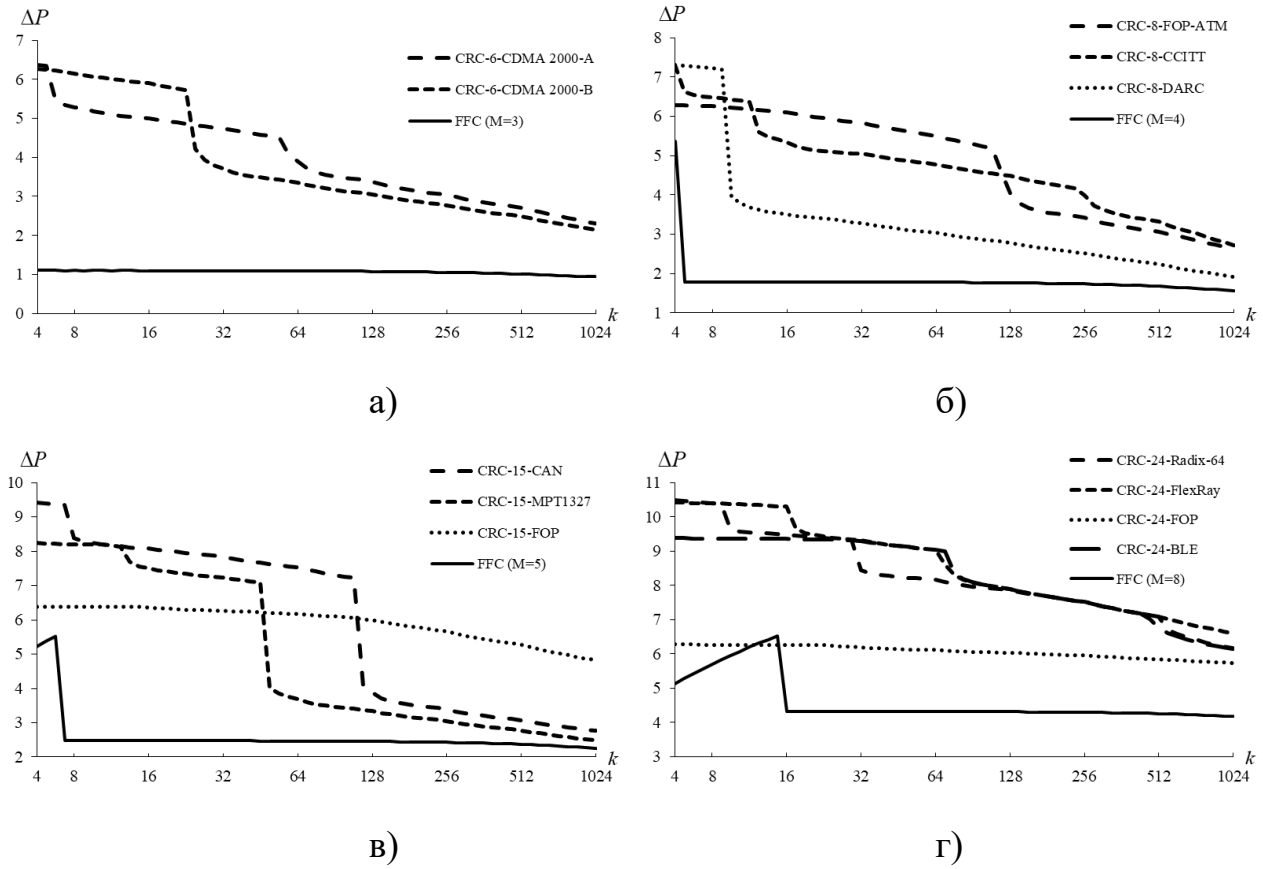
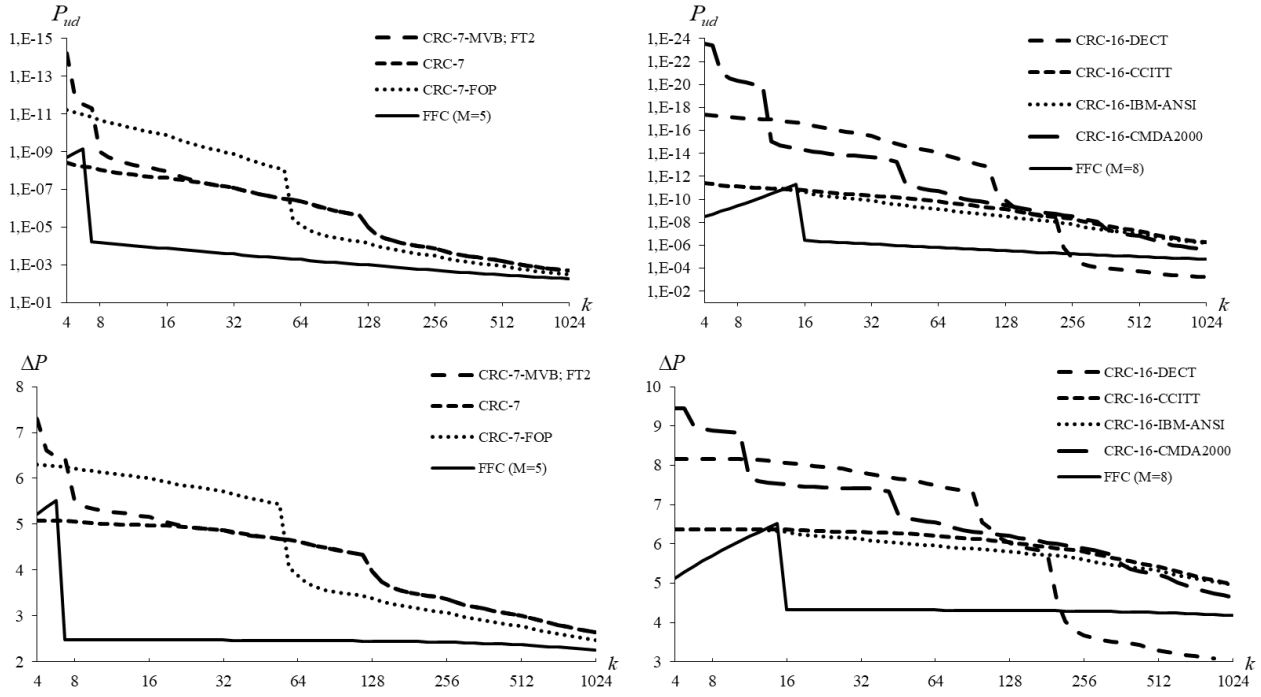


Рис. 2.7. Графіки залежностей оцінок енергетичного виграшу від довжини інформаційної частини для $p_0 = 10^{-3}$ і $r = 6$ (а); $r = 8$ (б); $r = 15$ (в); $r = 24$ (г)

Рис. 2.7 показує, що ПФК поступається CRC-коду. Разом з тим у міру збільшення довжини інформаційної частини енергетичний виграш внаслідок використання ПФК наближається до значення енергетичного виграшу внаслідок використання CRC-коду. Так, для $k = 1024$ і $p_0 = 10^{-3}$ різницю між їх оцінками енергетичного виграшу $\Delta P_{CRC} - \Delta P_{FFC} \le 1.336\,дБ$ для $r = 6$, $\Delta P_{CRC} - \Delta P_{FFC} \le 1.121\,дБ$ для $r = 8$, $\Delta P_{CRC} - \Delta P_{FFC} \le 1.889\,дБ$ для $r = 15$, $\Delta P_{CRC} - \Delta P_{FFC} \le 1.920\,дБ$ для $r = 24$.

3. ПФК самосинхронізований і не вимагає наявності прапора для циклової синхронізації. Ця властивість обумовлена тим, що символи $\{0;1;...;M-1\}$ зустрічаються в перестановці рівно по одному разу, а їх сума дорівнює $\sigma = 0{,}5M(M-1)$. Тому, прийнявши 3-5 блоків даних і підрахувавши суму з r символів у ковзному вікні, можна досить точно визначити циклову фазу. Тому довжину перевірної частини кодового слова ПФК r_{FFC} можна збільшувати на довжину прапора, зберігаючи незмінними k і n (з урахуванням прапора). Для цього випадку на рис. 2.8 представлено приклади залежностей оцінок P_{ud} і ΔP від k у результаті застосування ПФК і CRC-коду для $p_0 = 10^{-3}$ і розміру прапора в 8 біт.



а) б)

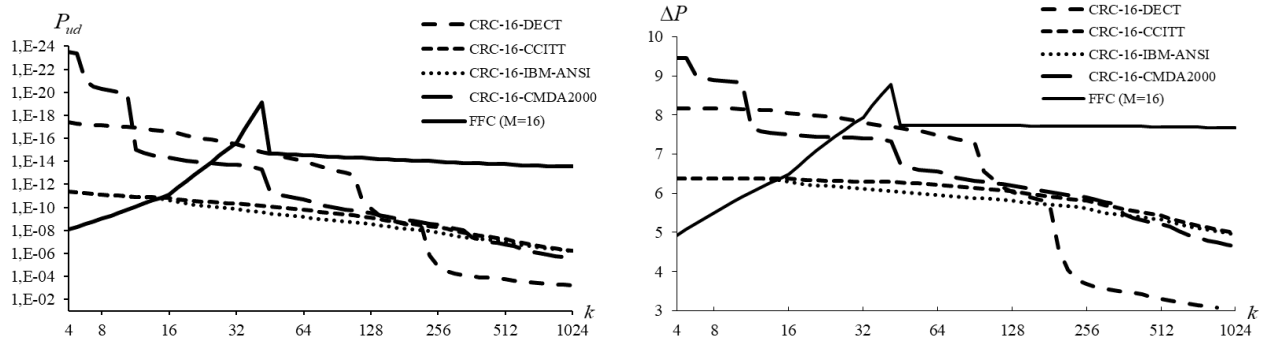
Рис. 2.8. Графіки залежностей оцінок імовірності невиявленої помилки і енергетичного виграшу від довжини інформаційної частини кодового слова для $p_0 = 10^{-3}$ і $r_{CRC} = 7$, $r_{FFC} = 15$ (а); $r_{CRC} = 16$, $r_{FFC} = 24$ (б)

Рис. 2.8 показує, що збільшення довжини перевірної частини кодового слова ПФК за рахунок прапора циклової синхронізації дозволяє підвищити ефективність виявлення помилок і ще більш наблизитися до енергетичного виграшу CRC-коду

(для $k=1024$ і $p_0=10^{-3}$ $\Delta P_{відн}\le 0.384\,дБ$ для $r_{CRC}=7$, $r_{FFC}=15$; $\Delta P_{відн}\le 0.811\,дБ$ для $r_{CRC}=16$, $r_{FFC}=24$), а в деяких випадках і перевищити його (див., наприклад, CRC-16-DECT і FFC $(M=8)$, де $\Delta P_{відн}=-1.089\,дБ$).

4. ПФК забезпечує імітозахист переданого повідомлення. Тому довжину перевірної частини кодового слова ПФК r_{FFC} можна збільшувати на довжину імітовставки, що забезпечує рівну стійкість до злому, зберігаючи незмінними k і n (з урахуванням прапору й імітовставки). У цьому випадку ΔP_{FFC} буде зростати.

Приймемо, наприклад, $M=16$ $(r_{FFC}=64)$. Покладемо, що довжина імітовставки, яка вироблена за відмінним від ПФК методом і забезпечує рівну з ПФК потужність множини її значень, може бути оцінена так: $r_{MAC}\le\lfloor\log_2 M!\rfloor=44$. Приймемо $r_{MAC}=40$. Тоді кількість біт, що залишилися для перевірної частини CRC-коду з урахуванням прапора з 8 біт, становить $r_{CRC}=16$. Для цього випадку на рис. 2.9 представлено залежності оцінок P_{ud} і ΔP від k у результаті застосування ПФК і CRC-коду для $p_0=10^{-3}$ і $M=16$, $r_{CRC}=16$.



а) б)

Рис. 2.9. Графіки залежностей оцінок імовірності невиявленої помилки (а) і енергетичного виграшу (б) від довжини інформаційної частини кодового слова для $p_0=10^{-3}$ і $r_{CRC}=16$, $r_{FFC}=64$

З графіків рис. 2.9 видно, що збільшення довжини перевірної частини кодового слова ПФК за рахунок прапора циклової синхронізації й імітовставки

дозволяє підвищити ефективність виявлення помилок ПФК. Так, для $k \geq 32$ енергетичний виграш ПФК перевершує енергетичний виграш CRC-коду (за $p_0 = 10^{-3}$ $\Delta P_{відн} \leq -0.032\,дБ$ для $k = 32$ і $\Delta P_{відн} \leq -2.683\,дБ$ для $k = 1024$). Зауважимо також, що оцінка ймовірності не виявленої ПФК помилки є грубою оцінкою зверху, в той час як відповідна оцінка для CRC є точною.

Приймемо тепер $M = 8$ $\left(r_{FFC} = 24\right)$. Згідно з описаною вище вимогою до відповідної довжини імітовставки покладемо $r_{MAC} = 16$. Тоді з урахуванням прапора з 8 біт для перевірної частини CRC-коду не залишається жодного біта. Таким чином, зменшення розміру перевірної частини призводить до зростання ефективності використання ПФК.

Зі сказаного випливає, що використання перевірної частини ПФК має більшу ефективність у порівнянні зі спільним використанням у одному блоці даних імітовставки, перевірної частини CRC-коду, а також прапора циклової синхронізації.

2.3.7. Захист інформації від несанкціонованого доступу

Використання перестановки в якості коду виявлення модифікацій створює можливість ефективного захисту інформації від несанкціонованого доступу. Використання властивості самосинхронізації ПФК виключає можливість спільної роботи абонентів, у яких організація кадру відповідає викладеному вище способу, з абонентами, що мають іншу організацію кадру (в тому числі маркер початку блоку). Ця обставина створює можливість на запропонованій основі організувати замкнуту підмережу (угруповання) абонентів у відкритій мережі (наприклад, у радіомережі з однією частотою, як у службі таксі, поліції, швидкої допомоги тощо).

Для створення замкнутого угруповання її абоненти мають єдиний ключ входу в цю підмережу, який невідомий іншим (стороннім) абонентам. Для створення підмережі у відкритій мережі після завершення процедури формування блоку (кадру) додатково може виконуватися операція перестановки біт блоку даних за секретним ключем. Для тих абонентів, яким ключ відомий, зворотна процедура відновлення вихідної структури кадру не представляє складнощів. Для тих, хто

робить несанкціоновану спробу доступу в цю підмережу, необхідно зробити (в середньому) $\eta_1 = 0.5C_n^r$ спроб підбору ключа для того, щоб визначити циклову фазу, а потім $\eta_2 = 0.5k!$ (у середньому) спроб, щоб правильно розставити символи інформаційної частини і мати можливість читання переданих повідомлень. Тільки після злому перестановочного шифру можна приступити до процедури злому КЦІ.

Для $M = 6$ $\left(M! = 720\right)$, $l_k = l_r = 3$, $k = 682$, $r = 18$, $n = 700$ для організації несанкціонованого доступу до інформації потрібно $\eta = 0.5\left(C_n^r + k!\right) = 9.27 \cdot 10^{1637}$ спроб підбору ключа. За продуктивності комп'ютерної угруповання з 1000 комп'ютерів, що використовується для підбору ключа доступу до інформації, яка дорівнює $\lambda = 3{,}15 \cdot 10^{23}$ кл./млн. років (за продуктивності сучасних комп'ютерів 10^{10} операцій/сек і використанні не менше 1000 машинних операцій для кожної спроби підбору ключа), середній час злому ключа доступу до інформації вимагає $T = 0.5\left(C_n^r + k!\right)/\lambda = 9.27 \cdot 10^{1637}/3.15 \cdot 10^{23} = 2.94 \cdot 10^{1614}$ млн. років, що практично виключає можливість доступу до інформації.

2.4. Метод комбінованого факторіального кодування інформації

2.4.1. Опис методу

Факторіальне кодування не обмежується ПФК і може бути суттєво розширено. Зокрема, становить інтерес розроблений і викладений у [1]–[3] метод комбінованого факторіального кодування інформації, який поєднує принципи факторіального і циклічного надлишкового кодування.

Визначення 2.5. Комбінованим факторіальним кодом (КФК) називається роздільний надлишковий код, який використовує в якості перевірної частини кодового слова контрольну суму CRC-коду, обчислену за перевірною частиною кодового слова ПФК.

Виконаємо дослідження методу комбінованого факторіального кодування і представимо оцінку його характеристик для вирішення задач захисту інформації в системах передавання даних з ВЗЗ. Для цього оцінимо такі показники:

- швидкість коду;
- імовірність не виявленої кодом помилки;
- імовірність злому коду методом «грубої сили».

КФК (CFC – Combined Factorial Code) поєднує ПФК з CRC-кодом. За інформаційною послідовністю спочатку обчислюється перевірна частина кодового слова ПФК, після чого за отриманою перестановкою, представленою у вигляді багаточлена $R_{FFC}(x)$ степені $(r_{FFC}-1)$, обчислюється лишок

$$R_{CFC}(x)=\left|R_{FFC}(x)\right|_{G(x)}. \tag{2.42}$$

де $G(x)$ – багаточлен степені r_{CFC}, який утворює CRC-код.

Кодове слово КФК, що складається з інформаційної частини $A(x)$ (розмірності k біт) і перевірної частини $R(x)=R_{CFC}(x)$ (розмірності $r=r_{CFC}$ біт), виводиться в канал зв'язку у вигляді $C(x)=A(x)\coprod R(x)$ $\left(C(x)=x^r\cdot A(x)\oplus R(x)\right)$. Повна довжина блоку $n=n_{CFC}=k+r_{CFC}$ біт. Швидкість КФК

$$\nu_{CFC}=k/(k+r_{CFC}).$$

Таким чином, метод комбінованого факторіального кодування інформації полягає в наступному:

1) образ інформаційної частини блоку даних формується у вигляді однієї перестановки порядку M (або відповідного їй синдрому) на основі прихованої залежності від кожного символу інформаційної частини згідно з механізмами ПФК. Отримана перестановка (синдром) не підлягає передаванню приймачу;
2) представлена в двійковому вигляді перестановка (або її синдром) кодується завадостійким кодом (наприклад, CRC-кодом). Отримана перевірна частина є частиною кодового слова КФК і вводиться в блок даних;
3) для підвищення стійкості до зламу блок даних може піддаватися перестановці біт з метою зміни порядку їх слідування в процесі передавання каналом зв`язку приймачу, при цьому правило перестановки тримається в таємниці.

Досягнутий технічний результат – виявлення факту модифікації інформації внаслідок впливу природних або штучних завад – обумовлений застосуванням

завадостійкого кодування до образу, обчисленому за інформаційною частиною блоку. При цьому ключ перетворення інформаційної частини в синдром (а також синдрому в перестановку) тримається в секреті, забезпечуючи статистичну незалежність перевірної частини блоку від його інформаційної частини і роблячи неможливим несанкціоновану модифікацію будь-якого символу блоку.

Крім того, такий підхід виключає можливість отримання даних користувачем, який не володіє ключем формування перевірної частини блоку.

Виконаємо розробку пристрою комбінованого факторіального кодування інформації та визначимо основні властивості КФК.

2.4.2. Пристрій кодування та декодування комбінованих факторіальних кодів

Заявлений технічний результат від застосування методу комбінованого факторіального кодування інформації досягається за допомогою пристрою, що містить блок кодування та блок декодування. Спрощена структурна схема блоку комбінованого факторіального кодування інформації показана на рис. 2.10.

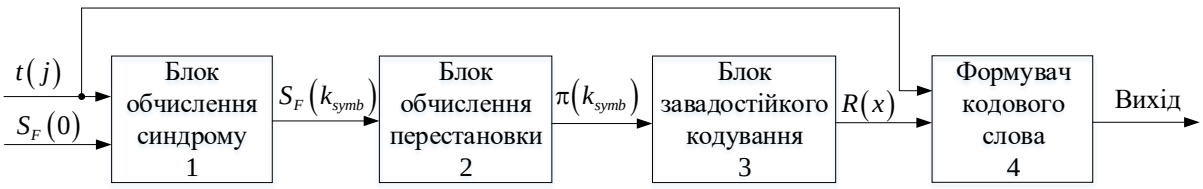


Рис. 2.10. Структурна схема блоку кодування КФК

Блок кодування містить блок обчислення синдрому $S_F(j)$ (1) за заданим значенням $S_F(j-1)$ і $t(j)$ для $j \in [1; k_{symb}]$, блок обчислення перестановки $\pi(j = k_{symb})$ (2) за заданим синдромом $S_F(j = k_{symb})$, блок завадостійкого кодування (3), формувач кодового слова (4). Зауважимо, що у разі формування перевірної частини блоку безпосередньо на основі синдрому перестановки $S_F(j = k_{symb})$ в ланцюгу блоків (1)-(2)-(3)-(4) блок (2) є відсутнім.

Блоки обчислення синдрому (1) та перестановки (2) працюють згідно з принципами ПФК, описаними вище. Завадостійкий кодер (3) за послідовністю $\pi\left(k_{symb}\right)$ (або $S_F\left(k_{symb}\right)$) обчислює перевірну частину блоку. Формувач кодового слова (4) об'єднує символи інформаційної та перевірної частин у блок даних.

Спрощена структурна схема блоку декодування КФК показана на рис. 2.11.

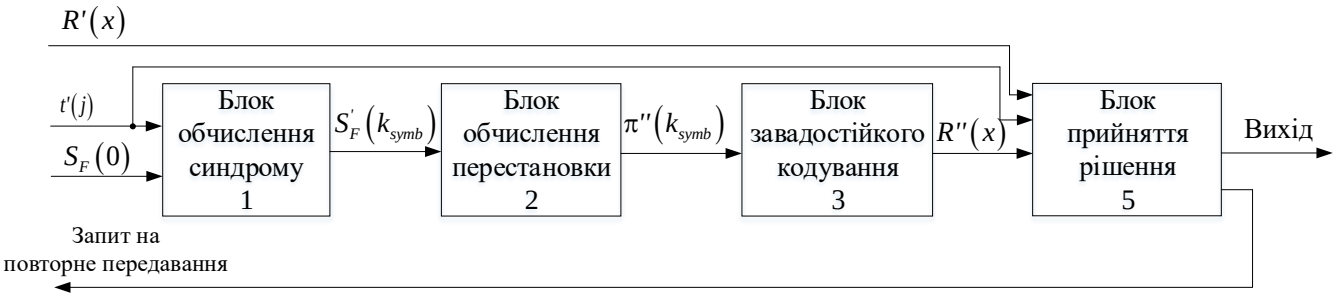


Рис. 2.11. Структурна схема блоку декодування КФК

Блок декодування КФК містить послідовно з'єднані блок обчислення синдрому $S_F^{'}\left(j\right)$ (1) за заданими значеннями $S_F^{'}\left(j-1\right)$ і $t'\left(j\right)$ для $j\in\left[1;k_{symb}\right]$, блок обчислення перестановки $\pi'\left(j=k_{symb}\right)$ (2) за заданим синдромом $S_F^{'}\left(j=k_{symb}\right)$, блок завадостійкого кодування (3), де за послідовністю $\pi'\left(k_{symb}\right)$ обчислюється перевірна частина кодового слова, і блок прийняття рішення (4), де відбувається порівняння обчисленої та прийнятої з каналу контрольних сум.

Блок обчислення синдрому (1) за заданими $S_F\left(0\right)$ і прийнятими з каналу $t'\left(j\right)$ обчислює значення $S_F^{'}\left(k_{symb}\right)$. Блок формування перестановки (2) за синдромом $S_F^{'}\left(k_{symb}\right)$, що надходить від блоку обчислення синдрому (1), і заданим ключем обчислює контрольну суму блоку – перестановку $\pi''\left(k_{symb}\right)$. Завадостійкий кодер (3) обчислює за послідовністю $\pi'\left(k_{symb}\right)$, що надходить від блоку формування перестановки (2), перевірну частину кодового слова $R''\left(x\right)$. Блок прийняття рішення (4) порівнює $R''\left(x\right)$, що надходить на третій вхід блоку (4), та прийняту з каналу

$R'(x)$ контрольну суму, що надходить на перший вхід блоку (4). Якщо вони співпадають, то на перший вихід блоку прийняття рішення (4) видається отримана з каналу інформаційна частина кодового слова КФК, що надходить на другий вхід блоку (4). В іншому випадку на другому виході блоку прийняття рішення (4) формується запит на повторне передавання прийнятого з помилкою блоку даних.

2.4.3. Математична модель процесу декодування комбінованого факторіального коду. Оцінка показників достовірності

Під час передавання каналом зв'язку на кодове слово впливає вектор помилки $\varepsilon_{n_{CFC}}(x)$ з потужністю множини векторів $\mu\left\{\varepsilon_{n_{CFC}}(x)\right\} = 2^{n_{CFC}}$. Цей вектор може бути представлений у вигляді конкатенації двох векторів – вектора завади, що покриває інформаційну частину кодового слова, з k біт, і вектора завади, що покриває перевірну частину кодового слова, з r_{CFC} біт: $\varepsilon_{n_{CFC}}(x) = \varepsilon_k(x) \amalg \varepsilon_{r_{CFC}}(x)$.

Звідси прийнятий з каналу зв'язку вектор суміші кодового слова і помилки має вигляд $D_{CFC}(x) = C_{CFC}(x) \oplus \varepsilon_{n_{CFC}}(x) = \left(A(x) \oplus \varepsilon_k(x)\right) \amalg \left(R_{CFC}(x) \oplus \varepsilon_{r_{CFC}}(x)\right)$.

У приймачі за прийнятою з каналу послідовністю $A(x) \oplus \varepsilon_k(x)$ формується перевірна частина (перестановка) для ПФК. За її двійковим представленням $R^{\wedge}_{FFC}(x)$ згідно (2.42) обчислюється залишок $R^{\wedge}_{CFC}(x) = \left|R^{\wedge}_{FFC}(x)\right|_{G(x)}$. Цей залишок може бути представлений у вигляді $R^{\wedge}_{CFC}(x) = R_{CFC}(x) \oplus \varepsilon^{\wedge}_{r_{CFC}}(x)$, де $\varepsilon^{\wedge}_{r_{CFC}}(x)$ – помилка, що виникає під час формування в приймачі перевірної частини і перетворює передану перевірну частину в будь-яку з $2^{r_{CFC}}$ можливих значень.

Ситуація, коли обчислена в приймачі і прийнята з каналу перевірні частини збігаються $\left(R^{\wedge}_{CFC}(x) = R_{CFC}(x) \oplus \varepsilon_{r_{CFC}}(x)\right)$, є ознакою відсутності помилок у прийнятому кодовому слові і служить підставою для виведення його споживачеві. Відповідно, ситуація $R^{\wedge}_{CFC}(x) \neq R_{CFC}(x) \oplus \varepsilon_{r_{CFC}}(x)$ є ознакою прийому блоку даних з помилкою і служить підставою для його перезапиту.

Звідси синдром помилки отримує вид:

$$S_{CFC}(x)=\left(R_{CFC}(x)\oplus\varepsilon^{\wedge}_{r_{CFC}}(x)\right)\oplus\left(R_{CFC}(x)\oplus\varepsilon_{r_{CFC}}(x)\right)=\varepsilon^{\wedge}_{r_{CFC}}(x)\oplus\varepsilon_{r_{CFC}}(x).$$

Якщо $\varepsilon_{n_{CFC}}(x)=0$, то $S_{CFC}(x)=0$. Тому рівність $S_{CFC}(x)=0$ є ознакою відсутності модифікації блоку даних.

Якщо $\varepsilon_{n_{CFC}}(x)\neq 0$ і $\varepsilon^{\wedge}_{r_{CFC}}(x)\oplus\varepsilon_{r_{CFC}}(x)=0$, виникають невиявлені помилки на виході декодера. Зауважимо, що $\varepsilon^{\wedge}_{r_{CFC}}(x)$ і $\varepsilon_{r_{CFC}}(x)$ статистично незалежні, а помилки декодування для $\varepsilon_k(x)\neq 0$ і $\varepsilon^{\wedge}_{r_{CFC}}(x)=\varepsilon_{r_{CFC}}(x)=0$ є результатом виникнення колізій.

Приймемо, що дані на вході і виході блоку формування перестановки є статистично незалежними, а перестановки, що формуються в ньому, розподілені рівномірно з імовірністю (див. формули (2.7), (2.23)):

$$p^{\wedge}_{r}=\begin{cases}\dfrac{1-q_0^k}{M!} \ \textit{для}\ M!<2^k,\\ \dfrac{1-q_0^k}{2^k-1} \ \textit{для}\ M!\geq 2^k.\end{cases} \tag{2.43}$$

Приймемо також, що $r_{CFC}\leq k$ і $2^{r_{CFC}}\leq M!$. Тоді ймовірність появи кожного з $2^{r_{CFC}}$ векторів $R_{CFC}(x)$, і, відповідно, кожного з $2^{r_{CFC}}$ векторів $\varepsilon^{\wedge}_{r_{CFC}}(x)$, дорівнює $p^{\wedge}_{r_{CFC}}=\left(1-q_0^k\right)/2^{r_{CFC}}$ і визначає ймовірність невиявленої КФК помилки:

$$P_{ud}(CFC,p_0)=P\left\{\varepsilon^{\wedge}_{r_{CFC}}(x)=\varepsilon_{r_{CFC}}(x)\right\}=\left(1-q_0^k\right)/2^{r_{CFC}}. \tag{2.44}$$

Енергетичний виграш ΔP під час застосування КФК для оптимального некогерентного приймача двійкових сигналів визначається згідно виразу (2.40).

Приклад. Оцінимо енергетичний виграш КФК за оптимального некогерентного прийому біт даних для $p_0=10^{-3}$, $n=1400$ і $r_{CFC}=16$, $G(x)=x^{16}+x^{12}+x^5+1$. Тоді $k=1384$, $\nu_{CFC}=1384/1400=0.988$, а $P_{ud}(CFC,p_0)=1.14\cdot 10^{-5}$. Енергетичний виграш $\Delta P=4.25$ дБ.

На рис. 2.12 представлено графіки залежностей оцінок імовірностей невиявленої помилки P_{ud} від довжини інформаційної частини блоку k в результаті застосування КФК, ПФК і CRC-коду для $p_0=10^{-3}$.

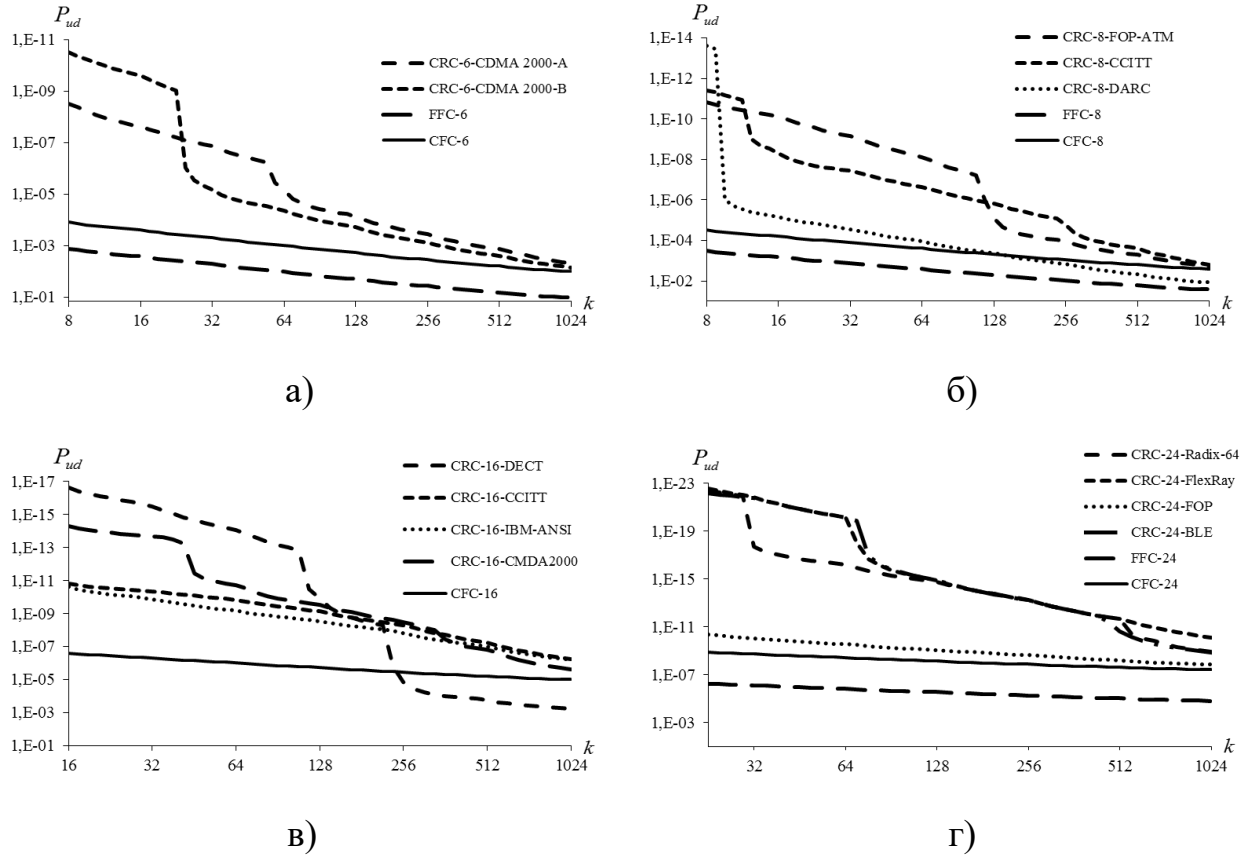


Рис. 2.12. Графіки залежностей оцінок імовірностей невиявленої помилки від k для $p_0 = 10^{-3}$ і $r = 6$ (а); $r = 8$ (б); $r = 16$ (в); $r = 24$ (г)

Графіки залежностей оцінок енергетичного виграшу ΔP від довжини інформаційної частини блоку k в результаті застосування КФК, ПФК і CRC-коду для $p_0 = 10^{-3}$ представлено на рис. 2.13.

Рис. 2.12 і 2.13 свідчать про те, що виявляюча здатність КФК вища, ніж ПФК за однакових швидкостей кодів і кодуванні символів перестановки ПФК рівномірним двійковим кодом. Крім того, довжина перевірної частини КФК визначається тільки кодовим поліномом і може приймати будь-яке ціле позитивне значення (в той час як для ПФК $r_{FFC} = M \cdot \lceil \log_2 M \rceil$: $r_{FFC} \in \{2;6;8;15;18;21;24;36\ldots\}$).

Водночас, КФК, на відміну від ПФК, не володіє властивостями самосинхронізації. Тому, якщо ПФК використовується в якості маркера циклової синхронізації, порівняння показників завадостійкості ПФК і КФК необхідно виконувати з урахуванням збільшення довжини перевірної частини ПФК за рахунок прапора циклової синхронізації. Зокрема, для довжини прапора в 8 біт порівняння

ПФК-24 і КФК-16 показує практично ідентичні значення оцінок енергетичного виграшу, що відрізняються на 0,1 дБ на користь КФК.

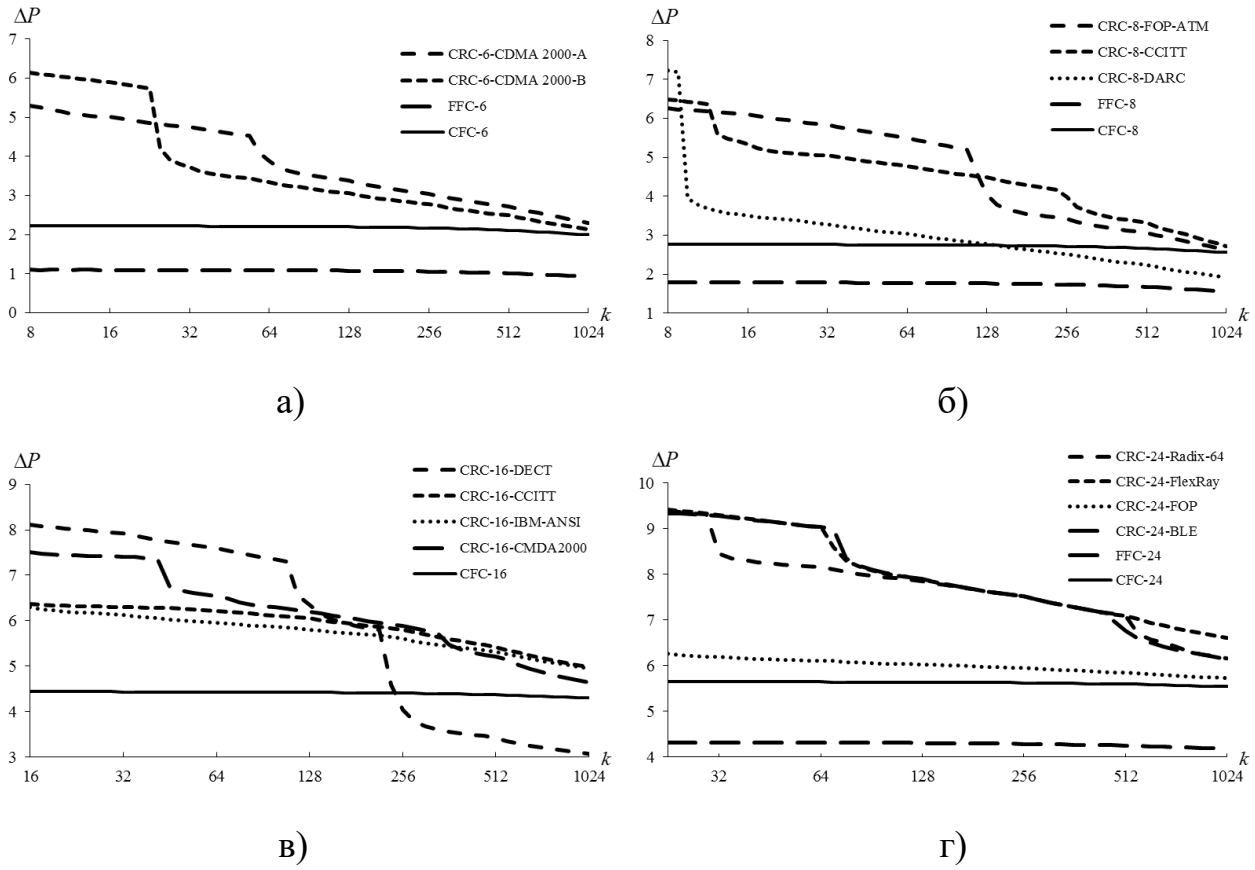


Рис. 2.13. Графіки залежностей оцінок енергетичного виграшу від довжини інформаційної частини для $p_0 = 10^{-3}$ і $r = 6$ (а); $r = 8$ (б); $r = 16$ (в); $r = 24$ (г)

Виявляюча здатність КФК, в цілому, поступається виявляючій здатності CRC-коду, проте для деяких утворюючих поліномів CRC-коду і k $\Delta P_{CFC} > \Delta P_{CRC}$. Так, $\Delta P_{CFC-8} > \Delta P_{CRC-8-DARC}$ для $k \geq 146$ ($\Delta P_{CRC-8-DARC} - \Delta P_{CFC-8} \approx -0.638\,дБ$ для $k = 1024$), а $\Delta P_{CFC-16} > \Delta P_{CRC-16-DECT}$ для $k \geq 243$ ($\Delta P_{CRC-16-DECT} - \Delta P_{CFC-16} \approx -1.219\,дБ$ для $k = 1024$).

Водночас, КФК більш ефективний у порівнянні зі спільним використанням у одному блоці імітовставки і перевірної частини CRC-коду (за $r_{MAC} = 8$ і $p_0 = 10^{-3}$ $\Delta P_{CRC-8} - \Delta P_{CFC-16} \leq -1.573\,дБ$ для $k = 1024$).

Слід зазначити, що оцінка ймовірності невиявленої помилки CRC-коду визначена практично точно, в той час як оцінка КФК (2.44) може бути поліпшена.

Для цього, як і для формування використовуваної оцінки енергетичного виграшу CRC-коду, необхідно визначити $f_{CFC}(j)$ для $j \in [0;n]$.

2.4.4. Оцінка стійкості комбінованого факторіального коду

Виконаємо кількісну оцінку стійкості КФК від несанкціонованого читання і/або нав'язування хибних даних у випадку атаки тільки на дані, що передаються, і злому методом «грубої сили» шляхом перебору множини ключового простору.

Під час використання КФК інформаційна частина блоку даних передається, як і для ПФК, у відкритому вигляді, тому КФК також не забезпечує криптографічний захист даних. Імовірність підбору ключа КЦІ для одноразової спроби $P_{ІІС}(CFC) = P_{ІІС}(FFC) \cdot \left(N_{r_{CFC}}\right)^{-1} \le (M!)^{-3} \cdot \left(N_{r_{CFC}}\right)^{-1}$, де $N_{r_{CFC}}$ – кількість можливих багаточленів $G(x)$ степені r_{CFC}, які утворюють CRC-код. Можливість підбору КВМ для одного блоку даних за одноразової спроби $P_{MAC}(CFC) = 2^{-r_{CFC}}$.

2.5. Метод факторіального кодування інформації з проріджуванням

2.5.1. Опис методу

Представлені факторіальні коди передбачають формування контрольної суми відповідно до k-бітного інформаційного вектора $A(x)$. За цих умов:

- для послідовної обробки символів інформаційного вектора $A(x)$ кількість операцій і час формування контрольної суми збільшуються під час збільшення k;
- для використання таблиці відповідності вектору $A(x)$ перестановки кількість записів у ній дорівнює 2^k і також збільшується під час збільшення k.

Таким чином, під час збільшення розміру блоку даних, що надходить на вхід кодера, час формування перевірної частини, а також обсяг необхідної пам'яті зростають і для деякого значення k можуть перевищувати допустимі межі.

У рамках дисертаційного дослідження виконано розробку методу факторіального кодування даних, що дозволяє скоротити час формування кодового

слова і обсяг використовуваної за цих умов пам’яті за рахунок зменшення кількості біт інформаційного вектора $A(x)$, оброблюваних у процесі формування кодового слова. Основні результати розробки цього методу опубліковано в [58], [275].

Визначення 2.6. Факторіальним кодом з проріджуванням (ФКП) називається роздільний код, який використовує в якості перевірної частини кодового слова перестановку чисел порядку M, яка обчислюється за частиною інформаційних символів, які надходять на вхід кодера.

Примітка. Процедура вибірки k_{FCD} біт з k інформаційних біт $(k_{FCD} < k)$ є процедурою проріджування або децимації.

Перевірна частина ФКП (FCD – Factorial Code with Decimation) формується за прорідженою послідовністю з k_{FCD} біт відповідно до принципів ПФК. За рівномірного двійкового кодування символів перестановки довжина перевірної частини $r_{FCD} = M \cdot \lceil \log_2 M \rceil$ біт. Довжина кодового слова $n_{FCD} = k + r_{FCD}$, швидкість коду $\nu_{FCD} = k/(k + r_{FCD})$.

Таким чином, метод факторіального кодування інформації з проріджуванням базується на методі повного факторіального кодування і полягає в наступному:

1) контрольна сума ФКП представляється у вигляді перестановки порядку M;
2) з інформаційної частини кодового слова відповідно до секретного ключа, який є елементом ключа перетворення, обираються k_{FCD} біт;
3) відповідно до принципів ПФК за обраними k_{FCD} бітами формується контрольна сума – перестановка;
4) для підвищення стійкості до зламу блок даних, що містить інформаційну та перевірну частини, може піддаватися перестановці біт з метою зміни порядку їх слідування в процесі передавання каналом, при цьому правило перестановки тримається в таємниці і є частиною ключа перетворення.

Досягнутий технічний результат – виявлення помилок, внесених каналом зв`язку, і виявлення факту несанкціонованої модифікації інформації – забезпечується за рахунок використання ПФК для прорідженої інформаційної послідовності.

2.5.2. Оцінка достовірності передавання даних

Оскільки контрольна сума охоплює перевіркою тільки k_{FCD} з k інформаційних біт, не виявлена ФКП помилка може виникнути внаслідок:

1) помилки в інших $\left(k - k_{FCD}\right)$ бітах інформаційної частини;

2) невиявленої помилки під час декодування контрольної суми ПФК, обчисленої за k_{FCD} інформаційними бітами.

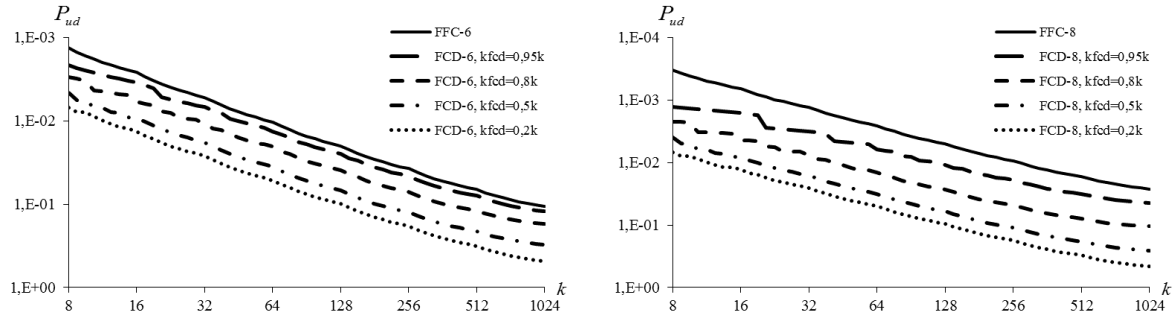
Імовірність не виявленої ФКП помилки обчислюється таким чином:

$$P_{ud}\left(FCD, p_0\right) = P_{ud}\left(FFC, p_0\right) + p_{dec}, \tag{2.45}$$

де $P_{ud}\left(FFC, p_0\right)$ оцінюється за (2.8) або (2.24). Значення k під час розрахунку за цими формулами замінюється на k_{FCD};

$p_{dec} = \left(1 - q_0^{k-k_{FCD}}\right) \cdot q_0^{k_{FCD}+r_{FCD}}$ – імовірність помилки децимації: помилки в $\left(k - k_{FCD}\right)$ бітах інформаційної частини, що не використовуються для формування контрольної суми, за умови, що інші $\left(k_{FCD} + r_{FCD}\right)$ біт завадою не вражені.

На рис. 2.14 представлено графіки залежностей оцінок імовірностей невиявленої помилки (2.45) від довжини інформаційної частини кодового слова в результаті застосування ФКП для $p_0 = 10^{-3}$ і різних співвідношень k_{FCD}/k і M.



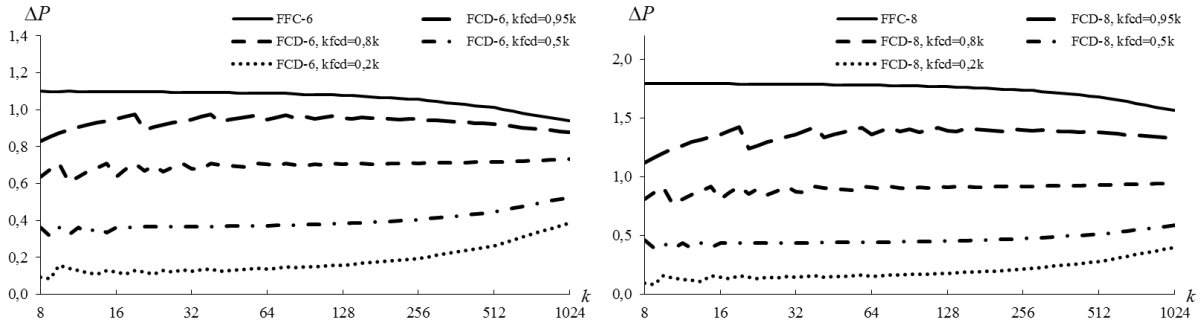
а) б)

Рис. 2.14. Графіки залежностей оцінок імовірностей невиявленої помилки ФКП від k для $p_0 = 10^{-3}$ і різних значень k_{FCD}/k і $M = 3$(а); $M = 4$ (б)

Енергетичний виграш у результаті застосування ФКП будемо оцінювати для оптимального некогерентного приймача двійкових сигналів.

Приклад. Нехай $p_0 = 10^{-3}$, $k = 1376$, $k_{FCD} = 500$, $M = 8$ і $r_{FCD} = 24$. Тоді $\nu_{FCD} = 1376/1400 = 0.983$, $P_{ud}\left(FCD, p_0\right) \le 0.346$, а $\Delta P \ge 0.56$ дБ.

На рис. 2.15 представлено графіки оцінок енергетичного виграшу від довжини інформаційної частини кодового слова в результаті застосування ФКП для $p_0 = 10^{-3}$ та різних співвідношень k_{FCD}/k і величини M.



а) б)

Рис. 2.15. Графіки залежностей оцінок енергетичного виграшу ФКП від довжини інформаційної частини для $p_0 = 10^{-3}$ і різних значень k_{FCD}/k і $M = 3$(а); $M = 4$ (б)

Рис. 2.14 і 2.15 вказують на очевидний програш ФКП у порівнянні з ПФК, який збільшується зі зменшенням співвідношення k_{FCD}/k.

Зазначимо, що достовірність передавання ФКП можна збільшити (за рахунок зменшення швидкості коду), якщо для інформаційної послідовності обчислити N $\left(N \ge 2\right)$ контрольних сум-перестановок за принципами ФКП, охопивши перевіркою всі інформаційні біти. У цьому випадку принципи ФКП є базовими для наступного виду факторіального кодування – з декількома контрольними сумами.

2.5.3. Оцінка стійкості факторіального коду з проріджуванням

Виконаємо кількісну оцінку стійкості ФКП від нав'язування хибних даних для атаки тільки на дані, що передаються, і злому методом «грубої сили».

Імовірність злому системи КЦІ за одноразової спроби підбору ключа $P_{ІІС}\left(FCD\right) \le \left(C_k^{k_{FCD}}\right)^{-1} \cdot \left(M!\right)^{-3}$. Можливість підбору контрольної суми для одного

блоку даних та одноразової спроби $P_{MAC}(FCD)=(M!)^{-1}$. Водночас нав'язування хибних даних можливе у випадку зміни біт інформаційної частини, які не беруть участі у формуванні перевірної частини. Імовірність цієї події $P_{dec}(FCD)=C_{k-k_{FCD}}^{k_{mod}} \Big/ C_k^{k_{mod}}$, де k_{mod} – кількість модифікованих криптоаналітиком біт інформаційної частини.

2.6. Метод роздільного факторіального кодування інформації з декількома контрольними сумами

2.6.1. Опис методу

Достовірність передавання ФКП можна збільшити, якщо для інформаційної послідовності обчислити N $(N \geq 2)$ контрольних сум-перестановок ФКП [58], [275].

Визначення 2.7. Роздільним факторіальним кодом з декількома контрольними сумами (ФКДКСр) називається код, який використовує в якості перевірної частини кодового слова конкатенацію декількох перевірних частин ФКП.

Приймемо, що i-а контрольна сума $(1 \leq i \leq N)$ є перестановкою порядку $M(i)$ і обчислюється за $k_{FCD}(i)$ інформаційними бітами. За цих обставин $\sum_{i=1}^{N} k_{FCD}(i)=k$, а кожен інформаційний біт бере участь у формуванні тільки однієї контрольної суми.

За рівномірного двійкового кодування символів перестановок довжина i-ої перевірної частини $r_{FCD}(i)=M(i)\cdot\lceil \log_2 M(i)\rceil$ біт. Тоді повна довжина кодового слова ФКДКСр (FCSCs – Factorial Code with Several Checksums (separable)) $n_{FCSCs}=k+\sum_{i=1}^{N} r_{FED}(i)$, а швидкість коду $\nu_{FCSCs}=k \Big/ \left(k+\sum_{i=1}^{N} r_{FCD}(i)\right)$.

Таким чином, метод роздільного факторіального кодування інформації з декількома контрольними сумами базується на методі факторіального кодування інформації з проріджуванням і полягає в наступному:

1) контрольна сума ФКДКСр представляється у вигляді конкатенації N

перестановок порядку $M(i)$ $(1 \le i \le N)$;

2) кожна перестановка формується відповідно до принципів ФКП, причому кожен інформаційний біт бере участь у формуванні однієї перестановки;
3) для підвищення стійкості до зламу блок даних, що містить інформаційну та перевірну частини, може піддаватися перестановці біт з метою зміни порядку їх слідування в процесі передавання каналом зв`язку, при цьому правило перестановки тримається в таємниці і є частиною ключа.

Практично реалізувати ФКДКСр для $k_{FCD}(i) = k_{FCD} = const$ можна такий спосіб. Укрупнимо символи джерела таким чином, щоб кожен укрупнений символ утворювався групою з l_k біт. Приймемо, що $k \vdots l_k$, тоді інформаційна частина буде містити $k_{symb} = k_{FCD} = k/l_k$ укрупнених символів. Перша контрольна сума-перестановка формується за двійковою послідовністю, утвореною першими бітами укрупнених інформаційних символів, друга – другими бітами, третя – третіми і т.д.

Зауважимо, що ФКДКСр дозволяє зменшити кореляцію бітових помилок у прийнятому блоці даних, наприклад, під час їх групування.

2.6.2. Пристрій кодування та декодування роздільних факторіальних кодів з декількома контрольними сумами

Пристрій кодування та декодування роздільних факторіальних кодів з декількома контрольними сумами містить блок кодування та блок декодування.

Структурна схема блоку кодування ФКДКСр представлена на рис. 2.16.

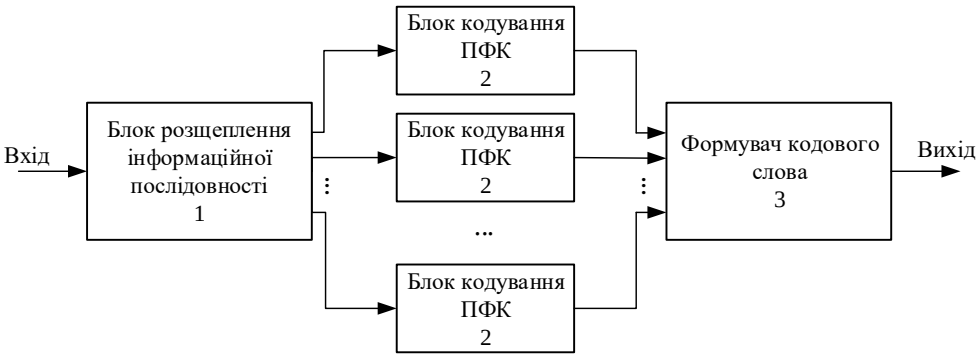


Рис. 2.16. Структурна схема блоку кодування ФКДКСр

Блок кодування містить послідовно з'єднані блок розщеплення інформаційної послідовності (1), набір з N паралельно працюючих блоків кодування ПФК (2) та формувач кодового слова ФКДКСр (3).

Блок кодування працює наступним чином. Інформаційне повідомлення $A(x)$, яке представлене в двійковій системі числення і містить k біт, поступає на вхід блоку розщеплення інформаційної послідовності (1), де поділяється на N блоків довжиною $k_{FCD}(i)$ біт $(1 \le i \le N)$. Правило формування блоків може триматися в таємниці та становити елемент ключа перетворення. Інформаційні блоки з виходу блоку розщеплення інформаційної послідовності (1) поступають на відповідні входи N блоків кодування ПФК (2), де для кожного блоку інформаційної послідовності формується перестановка $\pi(i)$ порядку $M(i)$ відповідно до принципів ПФК. Структура та принцип роботи блоку кодування ПФК (2) відповідає рис. 2.2. Параметри перетворення можуть триматися в таємниці. Отримані N кодових слів ПФК після кодування перевірної частини двійковим кодом поступають на вхід формувача кодового слова ФКДКСр (3), де відбувається їх конкатенація. Вихід формувача кодового слова ФКДКСр (3) є виходом блоку кодування ФКДКСр.

Структурна схема блоку декодування ФКДКСр представлена на рис. 2.17.

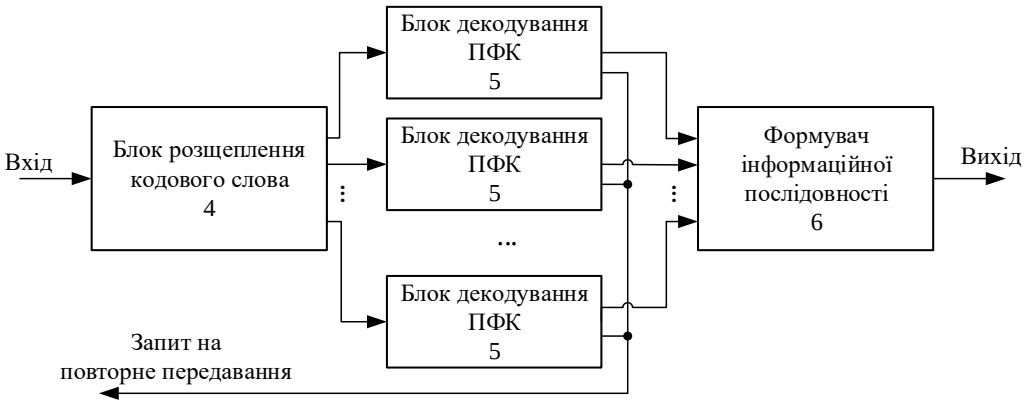


Рис. 2.17. Структурна схема блоку декодування ФКДКСр

Блок декодування складається з послідовно з'єднаних блоку розщеплення кодового слова (4), набору з N паралельно працюючих блоків декодування ПФК (5) та формувача інформаційної послідовності (6). Виходи блоку розщеплення кодового

слова (4) з'єднані з входами блоків декодування ПФК (5), перші виходи яких з'єднані з входами формувача інформаційної послідовності (6), а другі виходи – із зворотним каналом для формування сигналу перезапиту. Вихід блоку формувача інформаційної послідовності (6) є виходом блоку декодування.

Прийнятий з каналу зв'язку блок даних поступає на блок розщеплення кодового слова (4), де виконується виділення N кодових слів ПФК, які поступають на входи відповідних блоків декодування ПФК (5). Структура та принцип роботи блоку декодування ПФК (5) відповідає рис. 2.3. Декодовані послідовності з виходу блоків (5) подаються на вхід формувача інформаційної послідовності (6), де відбувається відновлення інформаційного повідомлення за зворотною процедурою блоку розщеплення інформаційної послідовності (1).

2.6.3. Оцінка достовірності передавання даних

Оскільки кодове слово ФКДКСр представляє собою об'єднання N кодових слів ПФК, не виявлена ним помилка виникає, коли хоча б в одному з N кодових слів ПФК помилку не виявлено, а решта – помилкою не уражені.

Імовірність не виявленої ФКДКСр помилки дорівнює різниці між імовірністю події, за якої в N кодових словах ПФК немає виявлених помилок, і події, за якої всі N кодових слів ПФК прийняті без помилок:

$$P_{ud}\left(FCSCs, p_0\right)=\prod_{i=1}^{N}\left[Q(i)+P_{ud}\left(FFC(i), p_0\right)\right]-\prod_{i=1}^{N}Q(i), \qquad (2.46)$$

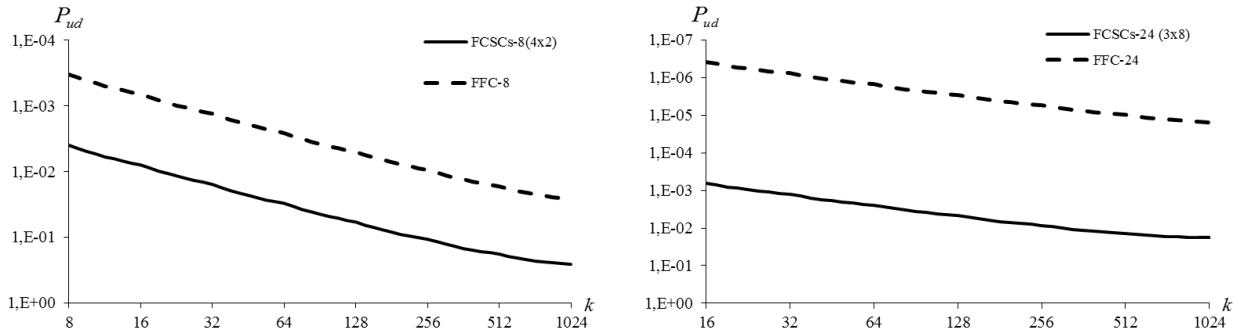
де $Q(i)=q_0^{n_{FCD}(i)}$ – імовірність прийому без помилок $n_{FED}(i)$ біт блоку даних, які відповідають i-му кодовому слову ПФК, $n_{FCD}(i)=k_{FCD}(i)+r_{FCD}(i)$;

$P_{ud}\left(FFC(i), p_0\right)$ – імовірність появи невиявленої помилки в i-му кодовому слові ПФК, яка обчислюється за (2.8) або (2.24). Під час оцінки $p_r^{\wedge}$ і p_r значення k замінюється на $k_{FCD}(i)$, а M – на $M(i)$.

Приклад. Нехай $p_0=10^{-3}$, $k=768$, $N=3$, $k_{FCD}(i)=256$, $M(i)=4$ для $\forall i\in[1;N]$. Тоді $l_r(i)=\lceil\log_2 M(i)\rceil=2$, $\forall i\in[1;N]$, $r_{FCSCs}=\sum_{i=1}^{N}l_r(i)\cdot M(i)=24$, а

$\nu_{FCSCs} = 768/792 = 0.97$. Імовірність не виявленої ФКДКСр помилки $P_{ud}\left(FCSCs, p_0\right) \le 1.67 \cdot 10^{-2}$, а $\Delta P \ge 1.74$ дБ.

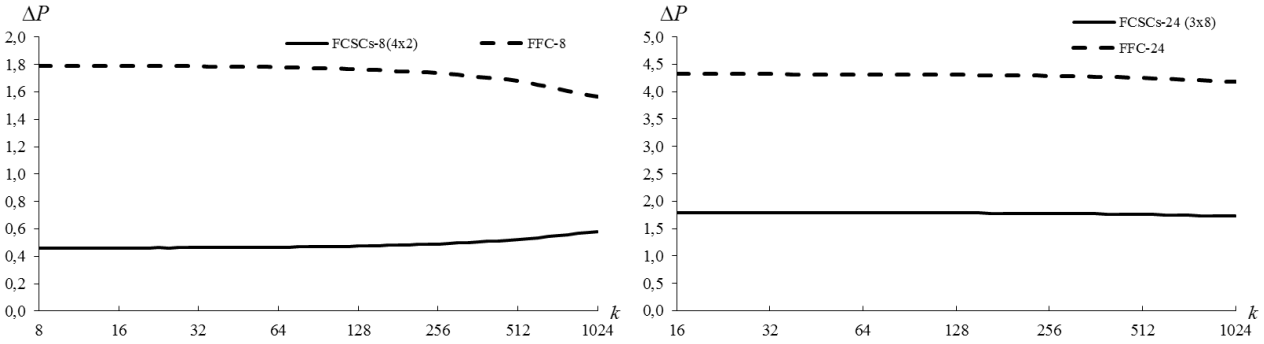
На рис. 2.18 представлено графіки залежностей оцінок імовірностей невиявленої помилки ФКДКСр (2.46) і ПФК (2.8) від довжини інформаційної частини кодового слова для $p_0 = 10^{-3}$ та різних значень N і M.



а) б)

Рис. 2.18. Графіки залежностей оцінок імовірностей невиявленої помилки ФКДКСр і ПФК від k для $p_0 = 10^{-3}$ та $N = 4$, $M = 2$ (а); $N = 3$, $M = 4$ (б)

На рис. 2.19 показано графіки залежностей оцінок енергетичного виграшу для некогерентного прийому від довжини інформаційної частини кодового слова в результаті застосування ФКДКСр і ПФК для $p_0 = 10^{-3}$ та різних значень N і M.



а) б)

Рис. 2.19. Графіки залежностей оцінок енергетичного виграшу ФКДКСр і ПФК від k для $p_0 = 10^{-3}$ та $N = 4$ і $M = 2$ (а); $N = 3$ і $M = 8$ (б)

Порівняння залежностей $\Delta P_{FCSCs}(k)$ і $\Delta P_{FFC}(k)$ за однакових швидкостей кодів вказує на меншу виявляючу здатність ФКДКСр у порівнянні з ПФК.

2.6.4. Оцінка стійкості роздільного факторіального коду з декількома контрольними сумами

Імовірність злому системи КЦІ на основі ФКДКСр за одноразової спроби підбору ключа $P_{ПС}(FCSCs) \le \left(\prod_{i=1}^{N} C^{k_{FCD}(i)}_{k-\sum_{j=1}^{i-1} k_{FCD}(j)} \cdot \left(M(i)!\right)^3 \right)^{-1}$. Можливість підбору контрольної суми для одного блоку даних за одноразової спроби $P_{MAC}(FCSCs) = \prod_{i=1}^{N} \left(M(i)!\right)^{-1}$.

2.7. Порівняльна оцінка методів роздільного факторіального кодування інформації

Усі представлені в цьому розділі методи роздільного факторіального кодування інформації спрямовані на забезпечення КЦІ під час її зберігання та передавання.

Виконаємо порівняльну оцінку представлених методів роздільного факторіального кодування інформації.

Властивості повного факторіального кодування інформації:

– у якості перевірної частини кодового слова використовується перестановка;

– процедура формування перестановки забезпечує зчеплення всіх інформаційних символів, руйнуючи їх статистичні зв’язки;

– закон формування перевірної частини може бути прихований;

– інформаційна частина кодового слова передається в канал зв’язку в початковому вигляді, тому цей код не забезпечує криптографічний захист;

– ПФК самосинхронізований, а його довжина і швидкість регулюються виходячи з вимог до стійкості системи і ступеня підвищення достовірності.

Властивості комбінованого факторіального кодування:

− у якості перевірної частини кодового слова використовується перевірна частина CRC-коду, обчислена за образом інформаційної частини, сформованому відповідно до принципів ПФК;

− процедура формування перестановки забезпечує зчеплення всіх інформаційних символів, руйнуючи їх статистичні зв’язки;

− закон формування перевірної частини може бути прихований;

− інформаційна частина кодового слова передається в канал зв’язку в початковому вигляді, тому цей код не забезпечує криптографічний захист;

− за однакових довжині кодової комбінації і швидкості коду виявляюча здатність КФК вища за ПФК, однак нижча за CRC-код;

− КФК не володіє властивістю самосинхронізації.

Основні властивості ФКП полягають у наступному:

− у якості перевірної частини кодового слова використовується перестановка, яка формується відповідно до принципів ПФК за частиною інформаційних символів;

− інформаційна частина кодового слова передається в канал зв’язку в початковому вигляді, тому ФКП не забезпечує криптографічний захист;

− закон формування перевірної частини може бути прихований;

− оскільки ФКП охоплює перевіркою лише частину інформаційних символів, він не може служити в якості повноцінного засобу КЦІ;

− виявляюча здатність ФКП поступається виявляючій здатності ПФК і CRC-коду;

− ФКП має властивість самосинхронізації.

Властивості ФКДКСр:

− у якості перевірної частини кодового слова використовується конкатенація декількох перевірних частин ФКП;

− інформаційна частина кодового слова передається в канал зв’язку в початковому вигляді, тому цей код не забезпечує криптографічний захист;

− закон формування перевірної частини може бути прихований;

− виявляє здатність ФКДКСр поступається виявляючій здатності ПФК і CRC-

коду;

– ФКДКСр має властивість самосинхронізації.

Результати порівняльного аналізу кодів наведемо в таблиці 2.8.

Таблиця 2.8

Властивості перешкодостійких кодів

Код	Роздільний	Завадо-стійкий	Крипто-стійкий	Імітo-стійкий	Само-синхронізується
ПФК	+	+	-	+	+
КФК	+	+	-	+	-
ФКП	+	+	-	-	+
ФКДКСр	+	+	-	+	+
CRC	+	+	-	-	-

Таким чином, представлені в цьому розділі роздільні факторіальні коди задовольняють наступним сформульованим у пункті 1.8.5 вимогам, що до них пред’являються:

1) ПФК, КФК, ФКП, ФКДКСр забезпечують виявлення помилок;

2) ПФК, КФК, ФКП, ФКДКСр забезпечують захист від нав’язування хибних даних;

3) ПФК, ФКП, ФКДКСр забезпечують циклову синхронізацію без застосування роздільник (прапора) між блоками;

4) ПФК, КФК, ФКП, ФКДКСр забезпечують організацію замкнутої угруповання абонентів у відкритій мережі.

Водночас зазначимо, що роздільні факторіальні коди не забезпечують криптографічний захист від несанкціонованого читання інформації. Крім того, представлені результати досліджень не дозволяють забезпечити виправлення помилок роздільними факторіальними кодами.

Аналіз представлених у таблиці 2.8 властивостей завадостійких кодів дозволяє сформулювати наступні рекомендації щодо їх застосування. За необхідності забезпечення КЦІ під час її передавання або зберігання можуть бути використані ПФК або КФК. Причому, якщо не потрібно самосинхронізації коду, більш ефективно використовувати КФК. ФКДКСр також вирішує поставлену задачу КЦІ,

однак програє ПФК і КФК за показником виявляючої здатності, тому може бути використаний у разі невисоких вимог до обчислювальних ресурсів кодека.

2.8. Висновки

У другому розділі дисертації отримано наступні результати:

- удосконалено метод формування випадкової послідовності перестановок на основі використання ФСЧ, який за рахунок введення додаткового ГВЧ, символи якого підсумовуються з модифікованим синдромом попередньої перестановки та визначають синдром наступної перестановки, дозволяє зменшити обсяг внутрішньої пам'яті додаткового ГВЧ не менш ніж на кількість біт, що дорівнює логарифму двійковому від порядку генерованих перестановок, уникнути порушення рівномірності їх розподілу та підвищити швидкість їх формування;
- розроблено структурну схему та алгоритм роботи пристрою формування випадкової послідовності перестановок порядку M, що забезпечують можливість його практичної реалізації та дозволяють уникнути приведення випадкових чисел до діапазону зі змінною верхньою межею, зменшити розрядність внутрішнього стану додаткового ГВЧ не менш ніж на $\log_2 M$ біт, а також підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса (зокрема, для додаткового ГПВЧ LFIB78 і $M = 5$ – у 2,1 рази; $M = 10$ – у 2,6 рази; $M = 20$ – у 2,8 рази);
- вперше розроблено методи роздільного факторіального кодування інформації (метод повного факторіального кодування, метод комбінованого факторіального кодування, метод факторіального кодування з проріджуванням, метод роздільного факторіального кодування з декількома контрольними сумами), які за рахунок реалізації єдиної процедури завадостійкого кодування та захисту від нав'язування хибних даних шляхом використання перестановки в якості перевірної частини кодового слова дозволяють забезпечити контроль цілісності інформації та підвищити її достовірність під час передавання в телекомунікаційних системах в умовах обмежень пропускної здатності каналів зв'язку;

– вперше розроблено математичну модель процесу декодування роздільних факторіальних кодів, яка за рахунок дослідження механізмів перетворення в симетричному двійковому каналі одного кодового слова в інше дозволяє оцінити показники достовірності передавання інформації в результаті застосування факторіального кодування та підтвердити його ефективність за цими показниками порівняно з іншими методами завадостійкого кодування;

– розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування роздільних факторіальних кодів (ПФК, КФК, ФКДКСр), що надають можливість їх практичної реалізації, дозволяють забезпечити контроль цілісності інформації та досягти енергетичний виграш у порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості, зокрема, для $p_0 = 10^{-3}$: ПФК – до 0,03 дБ для $k = 32$, $r_{FFC} = 64$ і до 2,7 дБ для $k = 1024$, $r_{FFC} = 64$, КФК – до 1,6 дБ для $k = 1024$ та $r_{CFC} = 16$.

Розроблені принципи факторіального кодування інформації дозволяють розширити науково-технічну базу методів і засобів контролю цілісності інформації під час її зберігання та передавання. Виявлення помилок, внесених каналом зв`язку, і виявлення факту несанкціонованої модифікації інформації – забезпечується за рахунок використання завадостійкого факторіального коду, в процесі формування перевірної частини якого використовується множина змінних констант, що використовується в якості ключа.

Водночас представлені роздільні факторіальні коди не забезпечують криптографічний захист від несанкціонованого читання інформації і не дозволяють забезпечити виправлення помилок. Тому необхідно виконати розробку методів факторіального кодування, які будуть задовольняти заданим вимогам. Результати розробки таких методів будуть представлені в наступному розділі дисертації.

РОЗДІЛ 3. МЕТОДИ НЕРОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУВАННЯ ІНФОРМАЦІЇ

3.1. Вступ

У попередньому розділі дисертації представлено методи роздільного факторіального кодування інформації, які забезпечують:

5) виявлення помилок під час передавання повідомлення каналом зв’язку;

6) захист від нав’язування хибних даних;

7) циклову синхронізацію без застосування прапора;

8) організацію замкнутого угруповання абонентів у відкритій мережі.

Однак, як зазначено раніше, роздільні факторіальні коди не дозволяють забезпечити криптографічний захист інформації та виправлення помилок, що впливають на повідомлення під час передавання каналом зв’язку.

Метою цього розділу є представлення розроблених у рамках дисертаційного дослідження методів нероздільного факторіального кодування, які реалізують у собі функції виявлення та виправлення помилок у каналі зв’язку та криптографічного захисту даних, а також оцінка їх характеристик у системах передавання даних з ВЗЗ. Оцінці підлягають: швидкість коду; імовірність не виявленої кодом помилки; імовірність злому коду методом «грубої сили».

3.2. Метод факторіального кодування з відновленням даних за перестановкою

Оскільки розроблюваний код повинен вирішувати задачу криптографічного захисту переданого повідомлення, він не може бути роздільним і містити в кодовому слові інформаційну частину у відкритому вигляді. Тому відкриті дані за допомогою ключа, що тримається в таємниці, повинні бути перетворені в шифртекст, який окрім криптографічного захисту повинен додатково забезпечити функції завадостійкого кодування.

У якості коду, що задовольняє висунутим вимогам, пропонується

факторіальний код з відновленням даних за перестановкою [56], [46], [47], [276].

Визначення 3.1. Факторіальним кодом з відновленням даних за перестановкою (ФКВД) називається нероздільний код, який передбачає заміну інформаційної послідовності з k біт на перестановку чисел порядку M $\left(M! \geq 2^k\right)$, обчислену за всіма k інформаційними бітами.

3.2.1. Опис методу

ФКВД (FCDR – Factorial Code with Data Recovery by Permutation) передбачає заміну інформаційної послідовності з k біт (вектора $A(x)$) на перестановку $R_{FCDR}(x)$ порядку M. У випадку кодування символів перестановки рівномірним двійковим кодом її довжина $r = r_{FCDR} = M \cdot \lceil \log_2 M \rceil$ біт. Перестановка передається каналом зв'язку одержувачу, тому довжина кодового слова ФКВД $n_{FCDR} = r_{FCDR}$. На станції прийому виконується зворотне перетворення, що призводить до відновлення k біт вихідного блоку даних і забезпечує швидкість коду:

$$\nu_{FCDR} = k / r_{FCDR} . \tag{3.1}$$

Графік залежності швидкості ФКВД від розміру блоку даних k на вході кодера показано на рис. 3.1. При цьому значення M вибирається таким чином, щоб

$$(M-1)! < 2^k \leq M!. \tag{3.2}$$

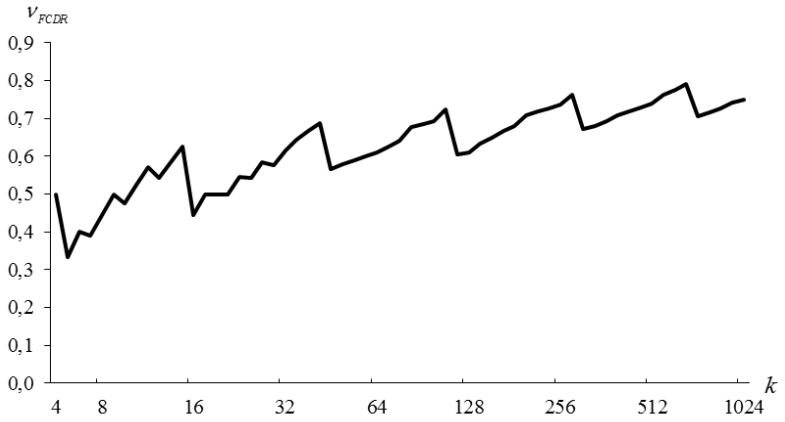


Рис. 3.1. Графік залежності швидкості ФКВД від розміру блоку даних на вході кодера

Очевидно, що максимальна швидкість ФКВД досягається для $\left(M!-2^k\right)\to 0$ і $\left(\log_2 M-\lceil \log_2 M\rceil\right)\to 0$. З цією метою параметри коду доцільно обирати таким чином, щоб $\log_2 M\in\mathbb{Z}$, а значення k задовольняло умові $2^k\le M!<2^{k+1}$.

Для забезпечення можливості відновлення даних за перестановкою необхідно виконання однієї з двох умов:

1) відображення $A(x)\leftrightarrow R_{FCDR}(x)$ має бути бієктивним: кожному значенню інформаційного вектора повинна відповідати одна перестановка, а кожній перестановці має відповідати одне значення інформаційного вектора;
2) відображення $f_{FCDR}: A(x)\to R_{FCDR}(x)$ має бути ін'єктивним, а $f_{FCDR}^{-1}: R_{FCDR}(x)\to A(x)$ – сюр'єктивним. За цих умов повинна забезпечуватися бієкція між 2^k інформаційними векторами і відповідними їм перестановками, інші $\left(M!-2^k\right)$ перестановок у результаті зворотного перетворення $f_{FCDR}^{-1}: R_{FCDR}(x)\to A(x)$ можуть перетворюватися в будь-які вектори.

Таким чином, необхідною умовою забезпечення можливості відновлення даних за перестановкою є бієктивне відображення $A(x)\leftrightarrow R_{FCDR}(x)$ рівнопотужних множин інформаційних векторів $A(x)$ і дозволених перестановок $R_{FCDR}(x)$.

Оскільки $\log_2(M!)\notin\mathbb{Z}$ для $M\ge 3$, рівність $M!=2^k$ справедливо тільки для $M=2$ і $k=1$. Тому в інших випадках, які значно більш цікаві, необхідно дотримуватися умови $M!>2^k$, $\left(M!-2^k\right)$ перестановок повинні бути забороненими.

Дотримання зазначеної умови може бути досягнуто в такий спосіб. Перетворення $f_{FCDR}: A(x)\to R_{FCDR}(x)$ полягає в перетворенні числа $A(x)$, представленого в двійковій системі числення, в число A_F, представлене в ФСЧ, з подальшим його перетворенням в синдром S_F і перестановку π і кодуванням її символів рівномірним двійковим кодом. Тоді $f_{FCDR}: A(x)\to A_F\to S_F\to\pi\to R_{FCDR}(x)$, а $f_{FCDR}^{-1}: R_{FCDR}(x)\to\pi\to S_F\to A_F\to A(x)$. Перетворення $A_F\leftrightarrow S_F\leftrightarrow\pi\leftrightarrow R_{FCDR}(x)$ для означеної вище процедури формування

перестановки за її синдромом з фіксованою базовою перестановкою $\pi(0)$ є взаємно-однозначним. У свою чергу, $A_F \leftrightarrow A(x)$, що передбачає перетворення A_F з ФСЧ в двійкову $\left(A(x)\right)$ і навпаки, також є взаємно-однозначним. Тоді числове значення A_F не перевищує значення $\left(2^k - 1\right)$, а всі значення, більші за $\left(2^k - 1\right)$, є забороненими.

Представлення двійкового вектора $A(x)$ у ФСЧ A_F вирішує задачу формування перевірної частини (перестановки) в залежності від усіх інформаційних символів, виключаючи при цьому колізії. Недоліком такого представлення є невисока швидкість формування перестановки за рахунок необхідності обробки двійкових чисел великої розмірності. Альтернативою прямого перетворення $A(x) \to A_F$ може слугувати наступна процедура:

1) у пам'ять одноразово записуються числа 2^j, $j \in [0, k-1]$, у ФСЧ: $\left\{A_F\left(2^{k-1}\right), A_F\left(2^{k-2}\right), \ldots, A_F\left(2^1\right), A_F\left(2^0\right)\right\}$;
2) $A_F = \sum_{i=0}^{k-1} a_i \cdot A_F\left(2^i\right)$, де a_i – i-ий біт інформаційної послідовності;
3) за отриманим A_F легко визначається синдром S_F і перестановка π.

Така процедура дозволяє скоротити час перетворення $A(x) \to A_F$, однак вимагає додаткової пам'яті для зберігання чисел $A_F\left(2^j\right)$, $j \in [0, k-1]$.

Таким чином, метод факторіального кодування з відновленням даних за перестановкою полягає в наступному:

1) інформаційна послідовність $A(x)$ з k біт перетворюється в перестановку π порядку M: $M! \geq 2^k$, а множина з $M! - 2^k$ перестановок є забороненою;
2) перетворення інформаційного повідомлення в перестановку є бієктивним відображенням $A(x) \leftrightarrow \pi$ рівнопотужних множин інформаційних векторів $A(x)$ і дозволених перестановок π;
3) правило $A(x) \leftrightarrow \pi$ може триматися в таємниці і складати ключ перетворення;
4) символи перестановки π кодуються двійковим кодом, після чого вона передається каналом зв'язку одержувачу.

Для руйнування статистичного зв'язку між інформаційною послідовністю $A(x)$ і відповідною перестановкою $R_{FCDR}(x)$ послідовність $A(x)$ може піддатися скремблюванню або гамуванню. Параметри скремблера або гама можуть зберігатися в таємниці, що додатково підвищує криптографічну стійкість перетворення. Разом з тим зауважимо, що скремблювання, на відміну від гамування, розмножує помилки, однак не вимагає формування рівномірно розподіленої додаткової послідовності випадкових або псевдовипадкових чисел.

Представимо структурні схеми пристрою факторіального кодування з відновленням даних за перестановкою та визначимо основні властивості ФКВД.

3.2.2. Пристрій кодування та декодування факторіальних кодів з відновленням даних за перестановкою

Пристрій кодування та декодування факторіальних кодів з відновленням даних за перестановкою містить блок кодування та блок декодування.

Структурна схема блоку кодування ФКВД представлена на рис. 3.2.

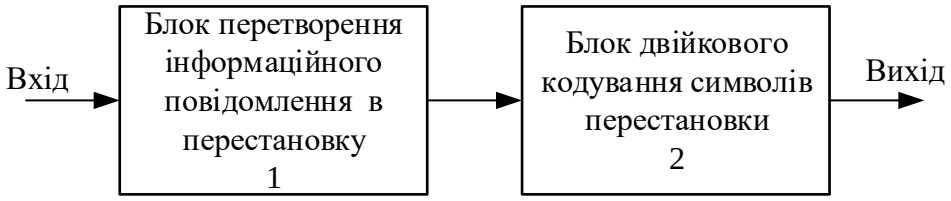


Рис. 3.2. Структурна схема блоку кодування ФКВД

Блок кодування містить послідовно з'єднані блок перетворення інформаційного повідомлення $A(x)$ у перестановку π (1) та блок двійкового кодування символів перестановки (2).

Інформаційне повідомлення $A(x)$, представлене в двійковій системі числення і містить k біт, поступає на вхід блоку перетворення інформаційного повідомлення у перестановку (1), де формується перестановка π порядку M. Інформаційний блок $A(x)$ у блоці перетворення інформаційного повідомлення у перестановку (1) може послідовно перетворюється в число A_F, представлене у ФСЧ, та синдром

перестановки S_F. Сформоване значення S_F відповідно до базової перестановки перетворюється в перестановку π порядку M, $M! \geq 2^k$. Отримана перестановка після кодування її символів двійковим кодом у блоці (2) передається в канал зв'язку.

Перетворення інформаційного блоку в перестановку може також бути виконано табличним способом – створенням таблиці, що має 2^k рядків, в кожній з яких записується одна з перестановок. Проте для великих k реалізація такого способу може вимагати занадто великих об'ємів пам'яті та часу.

Структурна схема блоку декодування ФКВД представлена на рис. 3.3.

Рис. 3.3. Структурна схема блоку декодування ФКВД

Блок декодування містить блок перевірки послідовності (3) та блок вилучення інформації (4). Перший вихід блоку перевірки послідовності (3) з'єднаний з входом блоку вилучення інформації (4), другий вихід блоку перевірки послідовності (3) з'єднаний із зворотним каналом для формування сигналу перезапиту. Вихід блоку вилучення інформації (4) є виходом блоку декодування.

Прийнятий з каналу блок даних поступає на блок перевірки послідовності (3), де перевіряється, чи є отримана послідовність перестановкою. Якщо ця умова не виконується, відбувається формування сигналу запиту на повторне передавання отриманого з помилкою блоку. В іншому випадку прийнята перестановка поступає на вхід блоку вилучення інформації (4). Блок вилучення інформації (4) виконує зворотне перетворення перестановки в інформаційне слово. Зворотне перетворення $\pi \to A(x)$, може представлятися у вигляді $\pi \to S_F \to A_F \to A(x)$, використовуючи $\pi(0)$ на етапі $\pi \to S_F$, або використовувати зворотну таблицю замін.

3.2.3. Оцінка показників достовірності передавання

Перш за все зазначимо, що в приймачі виконується перевірка коректності прийнятої з каналу послідовності. Якщо в прийнятій з каналу послідовності пропущені та повторно застосовані будь-які символи, то ця послідовність не є перестановкою і такий блок у системі з ВЗЗ підлягає перезапиту.

Імовірність не виявленої декодером ФКВД помилки $P_{ud}\left(FCDR, p_0\right)$ визначається ймовірністю появи в каналі зв'язку такого вектора помилок, який перетворює передану перестановку в будь-яку з $\left(2^k-1\right)$ інших дозволених перестановок. Якщо ж усі перестановки дозволені і зворотне перетворення $f_{FCDR}^{-1}: R_{FCDR}\left(x\right) \to A\left(x\right)$ сюр'єктивне, ймовірність невиявленої помилки визначається ймовірністю перетворення перестановки в будь-яку з $\left(M!-z\right)$ інших перестановок, де z – кількість перестановок, які в результаті зворотного перетворення $f_{FCDR}^{-1}: R_{FCDR}\left(x\right) \to A\left(x\right)$ формують передану послідовність.

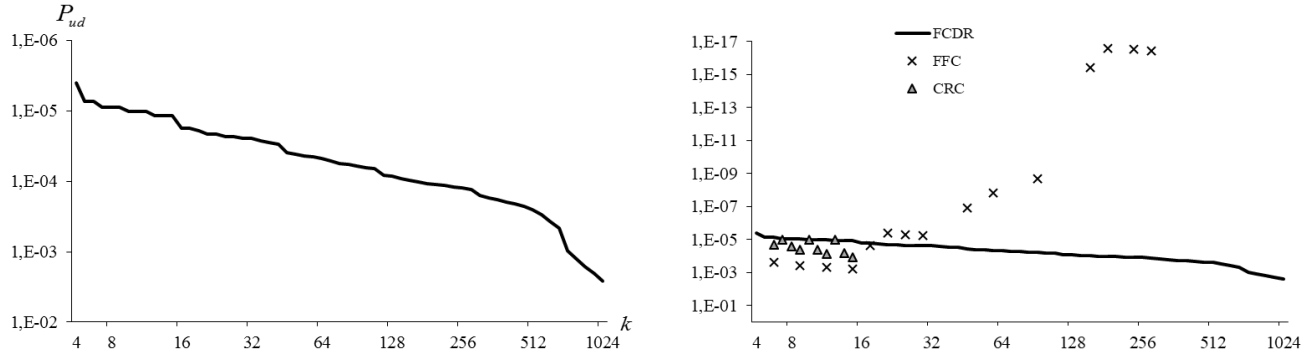
Оскільки $\begin{cases} 2^k-1 \le M!-1, \\ M!-z \le M!-1, \end{cases}$ справедлива оцінка $P_{ud}\left(FCDR, p_0\right) \le p_r^*$, де p_r^* оцінюється за (2.37):

$$P_{ud}\left(FCDR, p_0\right) \le \sum_{i=1}^{m_1} f_{per}\left(2i\right) p_0^{2i} q_0^{r-2i} + \Delta_{per}\left(m_1\right), \tag{3.3}$$

де $f_{per}\left(2i\right)$ оцінюється за (2.13), а $\Delta_{per}\left(m_1\right)$ – за (2.20) або (2.22).

Приклад. Нехай $k=716$, $p_0=10^{-3}$. Для $M=128$ $\nu_{FCDR}=0.799$, а $P_{ud}\left(FCDR, p_0\right) \le 4.814 \cdot 10^{-4}$. Енергетичний виграш ФКВД $\Delta P \ge 3.08$ дБ.

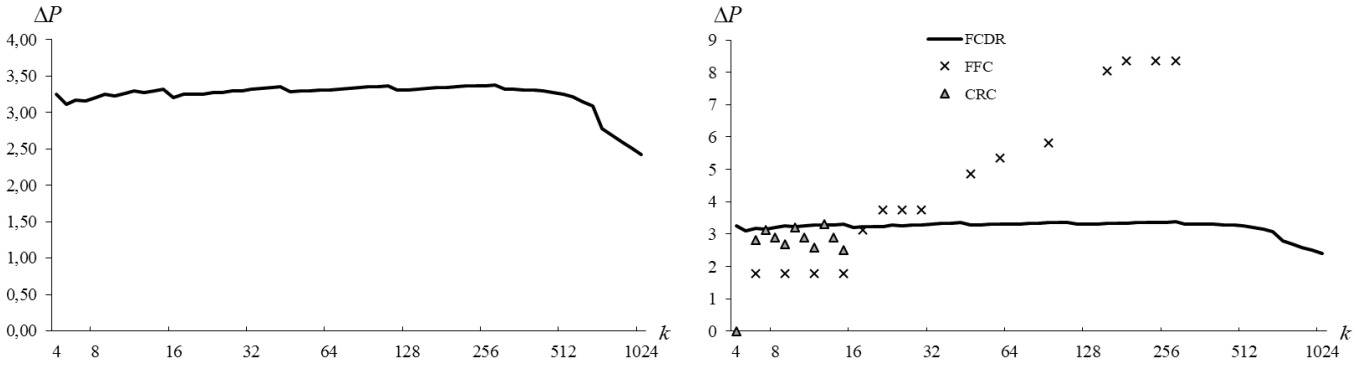
На рис. 3.4, *а* наведено графік залежності оцінки ймовірності невиявленої помилки від розміру блоку даних k на вході кодера ФКВД для $p_0=10^{-3}$ і $M:\left(M-1\right)! < 2^k \le M!$. На рис. 3.4, *б* додатково точками відображено оцінки ймовірності невиявленої помилки для ПФК та CRC за ідентичних ФКВД довжини інформаційної частини блоку k і швидкості коду.



а) б)

Рис. 3.4. Графіки залежностей оцінок імовірностей невиявленої помилки від розміру блоку даних на вході кодера для ФКВД (а); ФКВД, ПФК і CRC (б) для $p_0 = 10^{-3}$

На рис. 3.5, *а* показано графік залежності оцінки енергетичного виграшу ФКВД за оптимального некогерентного прийому двійкових символів від розміру блоку даних k на вході кодера для $p_0 = 10^{-3}$ і $M : (M-1)! < 2^k \le M!$. На рис. 3.5, *б* додатково точками відображено оцінки енергетичного виграшу ПФК і CRC за ідентичних значень довжини інформаційної частини блоку k і швидкості коду.



а) б)

Рис. 3.5. Графіки залежностей оцінок енергетичного виграшу від розміру блоку даних на вході кодера для ФКВД (а); ФКВД і ПФК і CRC (б) при $p_0 = 10^{-3}$

Рис. 3.4 і 3.5 свідчать про те, що для однакових швидкостей кодів і кодуванні символів перестановок рівномірним двійковим кодом:

– за малих значень k ($k \le 18$ для $p_0 = 10^{-3}$) енергетичний виграш ФКВД перевищує відповідний енергетичний виграш ПФК $(\Delta P_{FCDR} - \Delta P_{FFC} \le 1.5 дБ)$;

– за малих значень k ($k \le 15$ для $p_0 = 10^{-3}$) енергетичний виграш ФКВД перевищує відповідний енергетичний виграш CRC $\left(\Delta P_{FCDR} - \Delta P_{FFC} \le 0.821 \partial Б\right)$.

3.2.4. Оцінка стійкості факторіального кодування з відновленням даних за перестановкою

Імовірність злому ФКВД методом грубої сили для одноразової спроби підбору ключа перетворення, який, наприклад, є таблицею замін з $2^k \le M!$ рядків, становить $P_{UR}\left(FCDR\right) = \left(C_{M!}^{2^k} \cdot 2^k !\right)^{-1} = \left(M! - 2^k\right)! / \left(M!\right)!$.

У разі, якщо ключем перетворення є тільки $\pi(0)$, $P_{UR}\left(FCDR\right) = \left(M!\right)^{-1}$.

Середній час злому системи ФКВД $T_{UR}\left(FCDR\right) = 0.5 / \left(P_{UR}\left(FCDR\right) \cdot N\right)$ сек., де N – продуктивність комп'ютерного угруповання (ключів / сек).

Разом з тим, оскільки ФКВД передбачає просту заміну інформаційного повідомлення на перестановку, однакові блоки відкритого тексту перетворюються в однакові перестановки. Тому ефективний криптоаналіз такої системи може бути виконаний шляхом застосування частотного аналізу до виходу перетворювача. Для усунення статистичної надлишковості і зменшення ймовірності появи однакових блоків відкритий текст перед перетворенням доцільно піддати стисненню. Крім того, для вирівнювання статистики інформаційного повідомлення його доцільно піддати скремблюванню або гамуванню. Параметри скремблера або гама можуть зберігатися в таємниці, що додатково підвищує криптографічну стійкість.

Варто також зауважити, що за великого M алгоритм частотного аналізу для $M!$ можливих варіантів перестановок має значну просторову і часову складності, що позбавляє сенсу його реалізації на невеликих обсягах шифртексту. З іншого боку, збільшення M призводить до підвищення складності формування ключа перетворення (особливо, якщо ключем є таблиця замін).

У випадку використання перетворення $f_{FCDR} : A(x) \to A_F \to S_F \to \pi \to R_{FCDR}(x)$ та базової перестановки в якості ключа перетворення останній легко визначається за відомим блоком відкритого тексту та відповідним йому шифртекстом. Тому за таких

умов ФКВД є нестійким до злому на основі відомого відкритого тексту та відповідного йому шифртексту. Крім того, вказане перетворення не забезпечує ефекту розсіювання (зміна молодшого біта інформаційного блоку може призводити лише до зміни позицій двох молодших символів перестановки).

Для усунення вказаних недоліків для ФКВД доцільно використовувати додатковий генератор випадкових перестановок для формування $\pi(0)$.

З огляду на те, що перестановка може бути легко модифікована криптоаналітиком, ФКВД не забезпечує імітозахист повідомлення.

3.3. Метод факторіального кодування з відновленням даних за перестановкою з доповненням

Нехай α – показник надлишковості (за потужністю), що для ФКВД дорівнює

$$\alpha = \frac{M!}{2^k}. \tag{3.4}$$

Оскільки $(M-1)! < 2^k \le M!$ (3.2), справедливо $1 \le \alpha < M$. Разом з тим рівність $\alpha = 1$ виконується тільки для $k = 1$ і $M = 2$, а для $k > 1$ справедливим є $1 < \alpha < M$. Таким чином, використовувана методика вибору M за (3.2) вирішує задачу забезпечення можливості відновлення даних за перестановкою, проте призводить до надлишковості коду. Наявність такої надлишковості створює передумови її використання для підвищення достовірності передавання даних.

У рамках дисертаційного дослідження виконано розробку методу підвищення ефективності ФКВД шляхом підвищення достовірності передавання за рахунок надлишковості коду. Основні результати розробки опубліковано в [46], [57].

3.3.1. Опис методу

З формули (3.4) слідує:

1) $\lfloor \alpha \rfloor$ визначає, скільки разів відрізок $\left[0; 2^k - 1\right]$ укладається в $\left[0; M!-1\right]$;

2) зменшення довжини інформаційного вектора на Δk біт за фіксованого M

призводить до збільшення α в $\alpha_2/\alpha_1 = M!/2^{k_1-\Delta k}/M!/2^{k_1} = 2^{\Delta k}$ раз.

Тому, якщо для заданого k обчислене за (3.2) M таке, що $\alpha > 2$, перед формуванням перевірної частини існує можливість ввести в інформаційну частину додаткові перевірні біти, наприклад, біти паритету. За цих умов M і ν_{FCDR} (див. формулу (3.1)) не зміняться. Кількість додатково введених біт обмежено виразом

$$r_{add} \le \lfloor \log_2 \alpha \rfloor. \qquad (3.5)$$

Оскільки $\alpha < M$, справедлива оцінка $r_{add} \le \lfloor \log_2 M \rfloor$. З іншого боку, допустимі межі зміни довжини k на вході кодера в залежності від M, що задовольняють умові (3.2), мають вигляд: $\lfloor \log_2 (M-1)! \rfloor + 1 \le k \le \lfloor \log_2 M! \rfloor$, звідки також випливає, що кількість додатково введених біт $r_{add} \le \lfloor \log_2 M! \rfloor - \lfloor \log_2 (M-1)! \rfloor - 1 \le \lfloor \log_2 M \rfloor$.

Отже, чим більше k і, відповідно, M (по суті, чим вище якість каналу зв'язку), тим більшою може бути кількість додаткових біт і, відповідно, вище значення внесеної надлишковості і ресурсу підвищення достовірності.

На представленому на рис. 3.6 графіку показано максимальні значення кількості додатково внесених біт r_{add} залежно від M при виконанні умови (3.2).

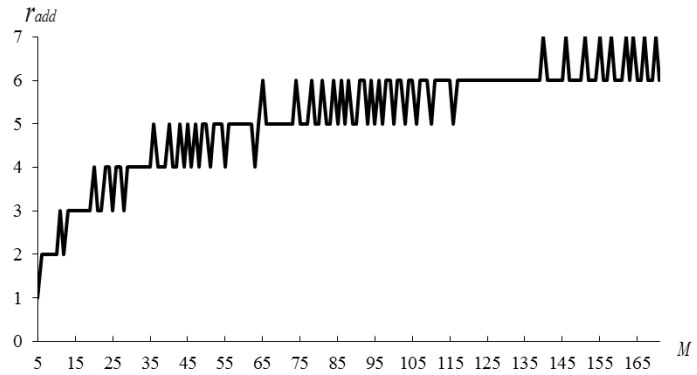


Рис. 3.6. Графік залежності максимальної кількості додатково внесених біт r_{add} від порядку перестановки M

Зазначимо, що в системах передавання даних з фіксованим M достовірність передавання може бути підвищена за рахунок зменшення розміру блоку даних на вході кодера на r_{add} біт і введення замість них додаткових перевірних біт.

Таким чином, метод підвищення ефективності ФКВД за рахунок введення додаткових перевірних біт полягає в наступному:

1) визначаються значення k і M. Наприклад, для заданого k значення M може вибиратися згідно з умовою (3.2);
   a) якщо $\alpha = M!/2^k > 2$, перед формуванням перестановки в інформаційну частину вводяться $r_{add} \le \lfloor \log_2 \alpha \rfloor$ додаткових перевірних біт;
   b) якщо $\alpha = M!/2^k < 2$, підвищення достовірності передавання може бути досягнуто шляхом зменшення довжини інформаційного вектора на r_{add} біт і введення замість них додаткових перевірних біт;
2) доповнена перевірними бітами інформаційна послідовність перетворюється в перестановку відповідно до принципів ФКВД.

ФКВД з використанням додаткових перевірних біт (з доповненням) будемо позначати через ФКВДд (FCDRadd – FCDR with addition).

3.3.2. Оцінка показників достовірності передавання

Розглянемо виявляючу здатність ФКВДд.

Очевидно, що помилка не виявляється ФКВДд тоді і тільки тоді, коли передана перестановка трансформована в іншу перестановку, а додаткові перевірні біти приймають правильні значення.

Нехай подія A={помилку в блоці даних не виявлено ФКВДд}, $P(A) = P_{ud}(FCDRadd, p_0)$; подія B = {перестановка (блок даних) під час передавання каналом зв'язку перетворена в іншу перестановку}, $P(B) = P_{ud}(FCDR, p_0)$.

За умови, що дані на вході і виході блоку формування перестановки є статистично незалежними, в результаті декодування прийнятого з помилкою кодового слова ФКВДд, кожен з додатково введених в інформаційну частину r_{add} перевірних біт з рівними можливостями може приймати значення 0 і 1. Тоді ймовірність того, що після появи події B додаткові перевірні біти приймуть правильні значення, дорівнює $P(A|B) = 2^{-r_{add}}$. З формули повної ймовірності

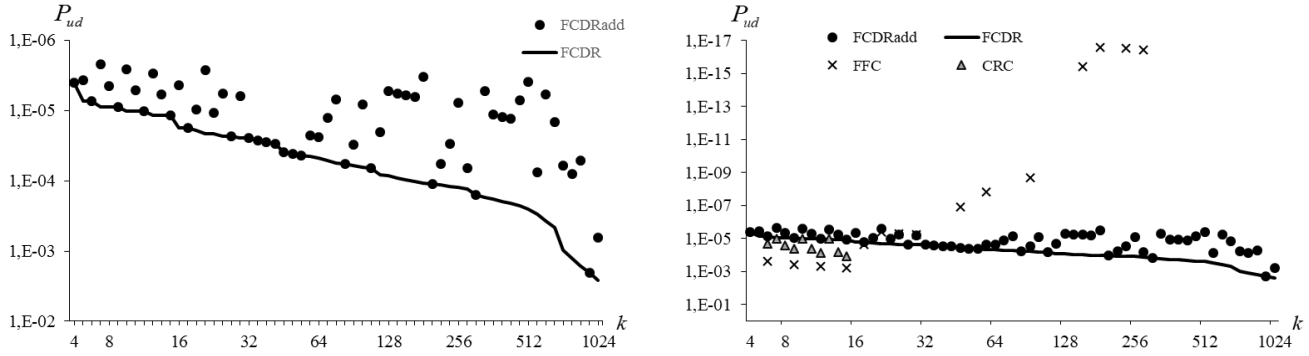
$$P_{ud}(FCDRadd, p_0) = P_{ud}(FCDR, p_0)/2^{r_{add}}, \qquad (3.6)$$

де $P_{ud}(FCDR, p_0)$ оцінюється відповідно до формули (3.3);

r_{add} – кількість додатково введених перевірних біт, обмежена формулою (3.5).

Приклад. Нехай $p_0 = 10^{-3}$ і $M = 128$, $k = 712$, а $r_{add} = 4$. Тоді $v_{FCDR} = 712/896 = 0.795$, $P_{ud}\left(FCDRadd, p_0\right) \le 3.009 \cdot 10^{-5}$, а $\Delta P \ge 3.94$ дБ.

На рис. 3.7, *а* представлено графіки залежностей оцінок $P_{ud}\left(FCDR, p_0\right)$ від розміру блоку даних k на вході кодера в результаті застосування ФКВДд і ФКВД для $p_0 = 10^{-3}$, $M : (M-1)! < 2^k \le M!$ і $r_{add} = \lfloor \log_2 \alpha \rfloor$. На рис. 3.7, *б* додатково відображено оцінки ймовірності невиявленої помилки ПФК за ідентичних ФКВД довжині інформаційної частини блоку k і швидкості коду. Зауважимо, що залежності швидкостей ФКВД і ФКВДд від розміру блоку даних k на вході кодера збігаються і для $M : (M-1)! < 2^k \le M!$ відображаються графіком на рис. 3.1.



а) б)

Рис. 3.7. Графіки залежностей оцінок імовірностей невиявленої помилки від k на вході кодера для ФКВДд, ФКВД (а); ФКВДд, ФКВД, ПФК, CRC (б)

На рис. 3.8, *а* представлено графіки залежностей оцінок енергетичного виграшу від розміру блоку даних k на вході кодера в результаті застосування ФКВДд і ФКВД для $p_0 = 10^{-3}$, $M : (M-1)! < 2^k \le M!$ і $r_{add} = \lfloor \log_2 \alpha \rfloor$. На рис. 3.8, *б* додатково відображено оцінки енергетичного виграшу, що досягаються в результаті застосування ПФК за ідентичних ФКВД значення k і швидкості коду.

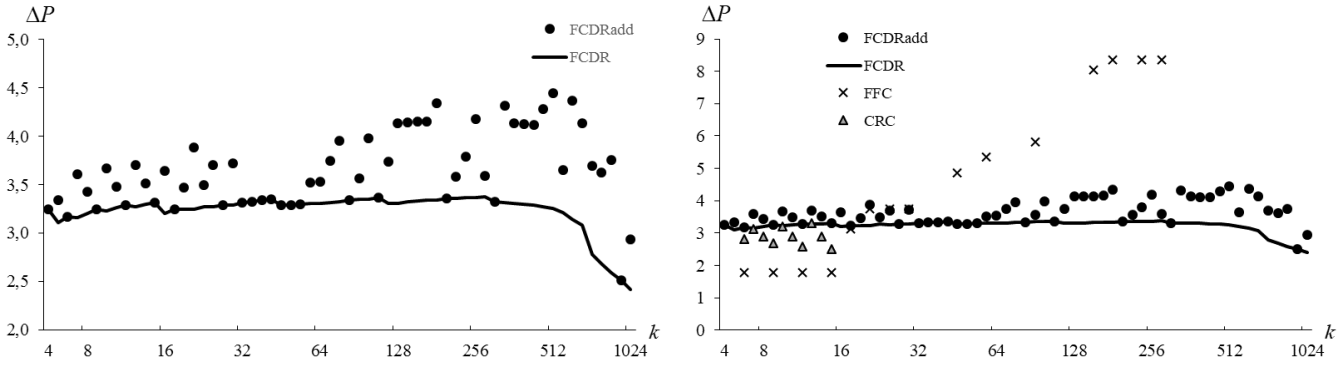


Рис. 3.8. Графіки залежностей оцінок енергетичного виграшу від розміру блоку даних k на вході кодера для ФКВДд і ФКВД (а); ФКВДд, ФКВД, ПФК і CRC (б)

Рис. 3.7 і 3.8 свідчать про те, що введення додаткових перевірних біт під час формування ФКВД дозволяє підвищити виявляючу здатність коду (наприклад, $\Delta P_{FCDRadd} - \Delta P_{FCDR} \approx 1.194 дБ$ для $k = 512$, $\Delta P_{FCDRadd} - \Delta P_{FCDR} \approx 1.601 дБ$ для $k = 1012$) і розширити діапазон значень розміру блоку даних k на вході кодера (з $k \le 18$ до $k \le 22$ для $p_0 = 10^{-3}$), для яких енергетичний виграш ФКВД перевищує відповідний енергетичний виграш ПФК за однакових швидкостей кодів і кодування символів перестановок рівномірним двійковим кодом.

3.4. Метод нероздільного факторіального кодування інформації з декількома контрольними сумами

Формування кодового слова - перестановки для ФКВД або ФКВДд на основі k-бітного інформаційного вектора $A(x)$ характеризується тим, що збільшення розміру вектора $A(x)$ призводить до збільшення часу формування перестановки, а також об’єму пам’яті, які для деякого k можуть перевищувати допустимі межі.

Представимо розроблений і досліджений у [58], [275] метод факторіального кодування даних, що дозволяє скоротити час формування кодового слова і об’єм використовуваної пам’яті за рахунок зменшення кількості біт інформаційного вектора $A(x)$, оброблюваних кодером у процесі формування кодового слова.

3.4.1. Опис методу

Визначення 3.2. Нероздільним ФКДКС (ФКДКСн) називається нероздільний код, який передбачає заміну інформаційної послідовності на конкатенацію $N \geq 2$ кодових слів ФКВД, обчислених за N різними підблоками, на які розбивається інформаційна послідовність символів.

Кодове слово ФКДКСн (FCSCi – Factorial Code with Several Checksums (inseparable)), на відміну від ФКДКСр, складається тільки з контрольних сум-перестановок. Перестановки обчислюються відповідно до принципів ФКВД, а $M(i)! \geq 2^{k_{FCDR}(i)}$, де $k_{FCDR}(i)$ – кількість біт у i-му блоці повідомлення.

За рівномірного двійкового кодування символів $r_{FCDR}(i) = M(i) \cdot \lceil \log_2 M(i) \rceil$, довжина кодового слова $n_{FCSCi} = \sum_{i=1}^{N} r_{FCDR}(i)$, швидкість коду

$$\nu_{FCSCi} = k \Big/ \sum_{i=1}^{N} r_{FCDR}(i). \tag{3.7}$$

Таким чином, метод нероздільного факторіального кодування інформації з декількома контрольними сумами полягає в наступному:

4) кодове слово ФКДКСн представляється у вигляді конкатенації N перестановок порядків $M(i)$ $(1 \leq i \leq N)$;
5) кожна перестановка формується відповідно до принципів ФКВД за окремими блоками, на які розбивається інформаційна послідовність символів. Кожен інформаційний біт входить тільки в один блок і бере участь у формуванні тільки однієї перестановки.

3.4.2. Пристрій кодування і декодування нероздільних факторіальних кодів з декількома контрольними сумами

Кодек ФКДКСн містить блок кодування та блок декодування.

Структурна схема блоку кодування ФКДКСн представлена на рис. 3.9.

Блок кодування містить послідовно з’єднані блок розщеплення інформаційної послідовності (1), набір з N паралельно працюючих блоків кодування ФКВД (2) та формувач кодового слова ФКДКСн (3).

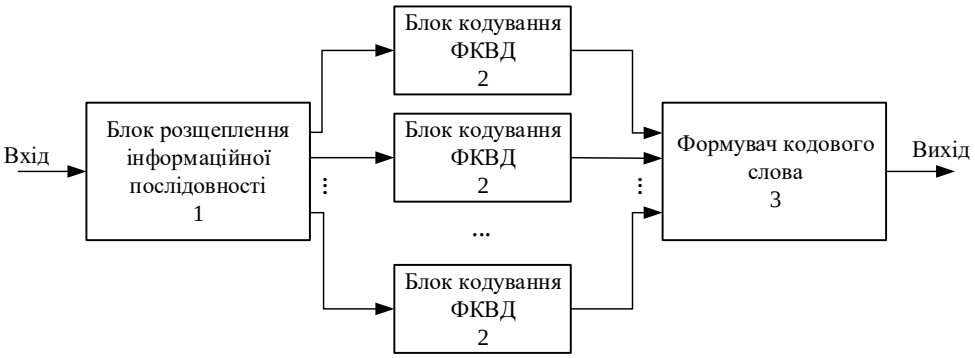


Рис. 3.9. Структурна схема блоку кодування ФКДКСн

Інформаційне повідомлення $A(x)$ з k біт поступає на вхід блоку розщеплення інформаційної послідовності (1), де поділяється на N блоків довжиною $k_{FCDR}(i)$ біт $(1 \le i \le N)$. Правило формування блоків може триматися в таємниці та становити елемент ключа перетворення. Інформаційні блоки з виходу блоку (1) поступають на відповідні входи N блоків кодування ФКВД (2), де для кожного блоку формується перестановка $\pi(i)$ порядку $M(i)$ відповідно до принципів ФКВД. Структура та принцип роботи блоку кодування ФКВД (2) відповідає рис. 3.2. Параметри перетворення можуть триматися в таємниці. Отримані N перестановок $\pi(i)$ $(1 \le i \le N)$ після кодування двійковим кодом поступають на вхід формувача кодового слова ФКДКСн (3), де відбувається їх конкатенація. Вихід формувача кодового слова ФКДКСн (3) є виходом блоку кодування ФКДКСн.

Структурна схема блоку декодування ФКДКСн представлена на рис. 3.10.

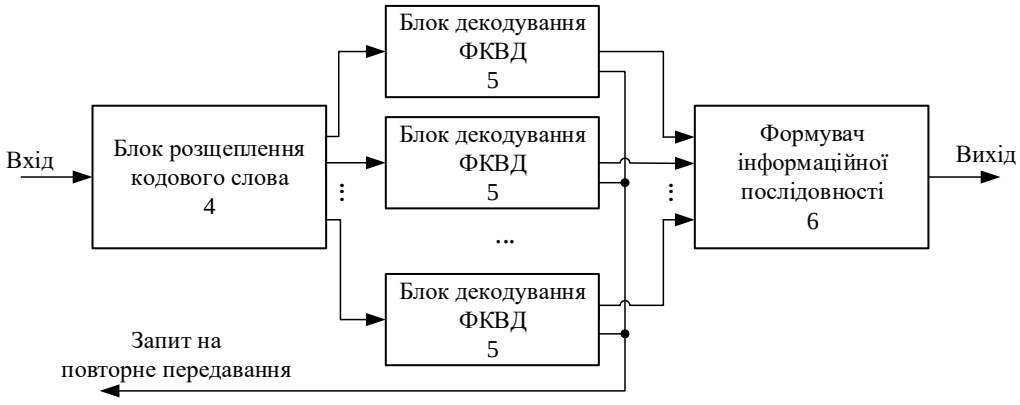


Рис. 3.10. Структурна схема блоку декодування ФКДКСн

Блок декодування складається з послідовно з'єднаних блоку розщеплення кодового слова (4), набору з N паралельно працюючих блоків декодування ФКВД (5) та формувача інформаційної послідовності (6).

Прийнятий з каналу зв'язку блок даних поступає на блок розщеплення кодового слова (4), де виконується виділення N кодових слів ФКВД, які поступають на входи відповідних блоків декодування ФКВД (5). Структура та принцип роботи блоку декодування ФКВД (5) відповідає рис. 3.3. Декодовані перестановки з виходу блоків (5) подаються на вхід формувача інформаційної послідовності (6), де відбувається відновлення інформаційного повідомлення.

3.4.3. Оцінка показників достовірності передавання

Оскільки кодове слово ФКДКСн є конкатенацію N кодових слів ФКВД, не виявлена ним помилка виникає, коли хоча б у одному з N кодових слів ФКВД помилку не виявлено, а решта – помилкою не уражені.

Імовірність не виявленої ФКДКСн помилки дорівнює:

$$P_{ud}\left(FCSCi, p_0\right) = \prod_{i=1}^{N}\left[Q(i) + P_{ud}\left(FCDR(i), p_0\right)\right] - \prod_{i=1}^{N} Q(i) \qquad (3.8)$$

де $Q(i) = q_0^{r_{FCDR}(i)}$ – імовірність прийому без помилок $r_{FCDR}(i)$ біт блоку даних, які відповідають i-му кодовому слову ФКВД;

$P_{ud}\left(FCDR(i), p_0\right)$ – імовірність невиявленої помилки в i-му кодовому слові ФКВД, яка оцінюється за (3.3) або (3.6), де значення r замінюється на $r_{FCDR}(i)$.

Приклад. Нехай $p_0 = 10^{-3}$, $k = 768$, $N = 4$, $k_{FCDR}(i) = 192$, $M(i) = 47$ для $\forall i \in [1; N]$. Тоді $r_{FCDR}(i) = M(i) \cdot \lceil \log_2 M(i) \rceil = 282$, $\forall i \in [1; N]$, $n_{FCSCi} = 1128$, $\nu_{FCSCi} = k \Big/ \sum_{i=1}^{N} r_{FCDR}(i) = 0.68$, а $P_{ud}\left(FCSCi, p_0\right) \le 1.84 \cdot 10^{-4}$, $\Delta P \ge 3.35$ дБ.

На рис. 3.11 показано графіки залежностей (3.8) оцінок $P_{ud}\left(FCSCi, p_0\right)$ від розміру блоку даних на вході кодера для $p_0 = 10^{-3}$ та різних значень N і методів формування блоків ФКВД (ФКВД або ФКВДд).

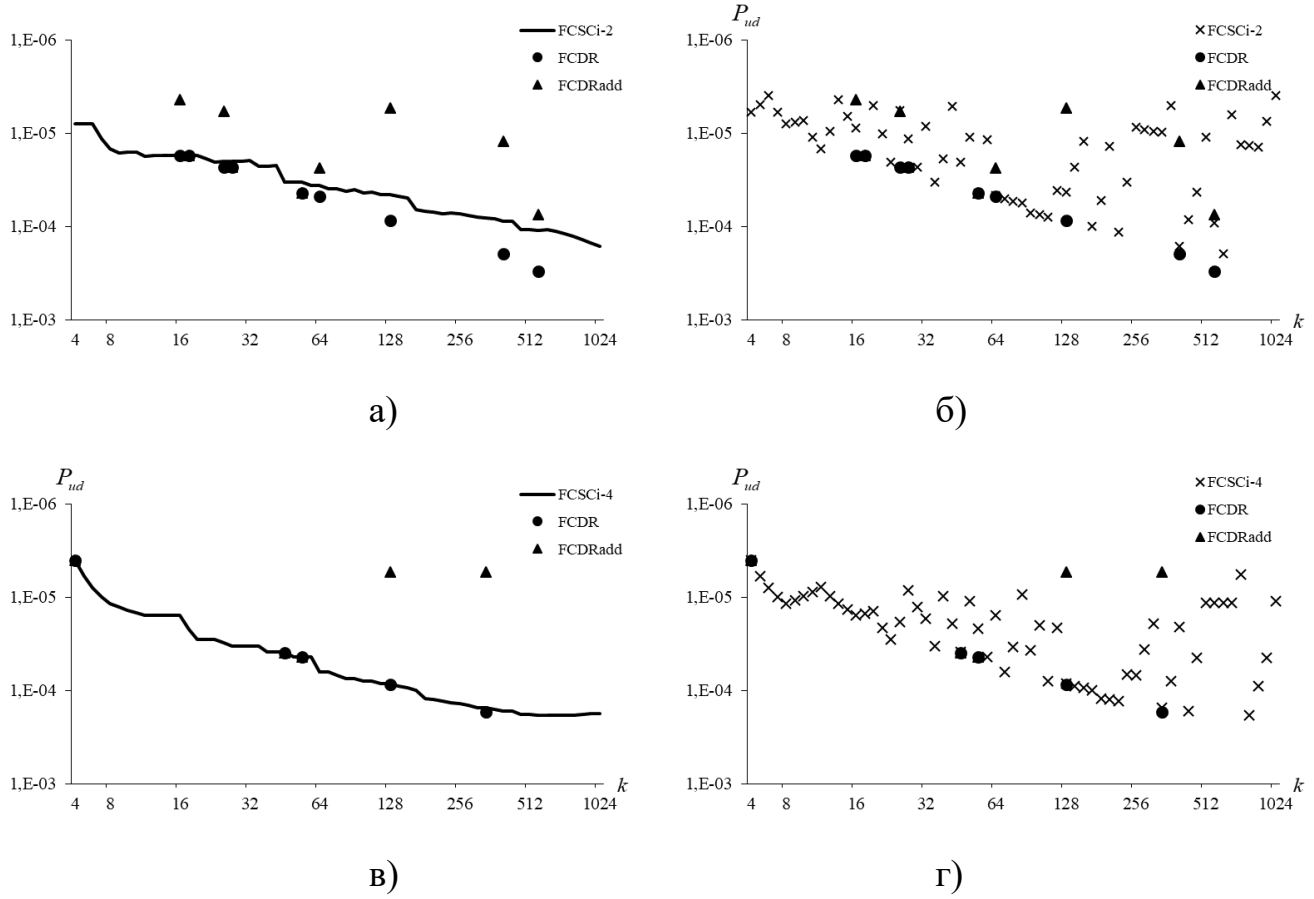


Рис. 3.11. Графіки залежностей оцінок імовірностей невиявленої помилки ФКДКСн від розміру блоку даних на вході кодера для $p_0 = 10^{-3}$ та $N = 2$ блоків ФКВД (а); $N = 2$ блоків ФКВДд (б); $N = 4$ блоків ФКВД (в); $N = 4$ блоків ФКВДд (г)

На рис. 3.12 представлено графіки залежностей енергетичного виграшу за оптимального некогерентного прийому двійкових символів ФКДКСн від розміру блоку даних на вході кодера для $p_0 = 10^{-3}$ та різних значень N і способів формування блоків ФКВД (ФКВД або ФКВДд).

Додатково на графіках рис. 3.11 і 3.12 відображено оцінки ймовірностей невиявленої помилки й енергетичного виграшу, що досягаються в результаті застосування ФКВД і ФКВДд (FCDRadd) для ідентичних ФКДКСн розмірів блоку даних на вході кодера і швидкості коду.

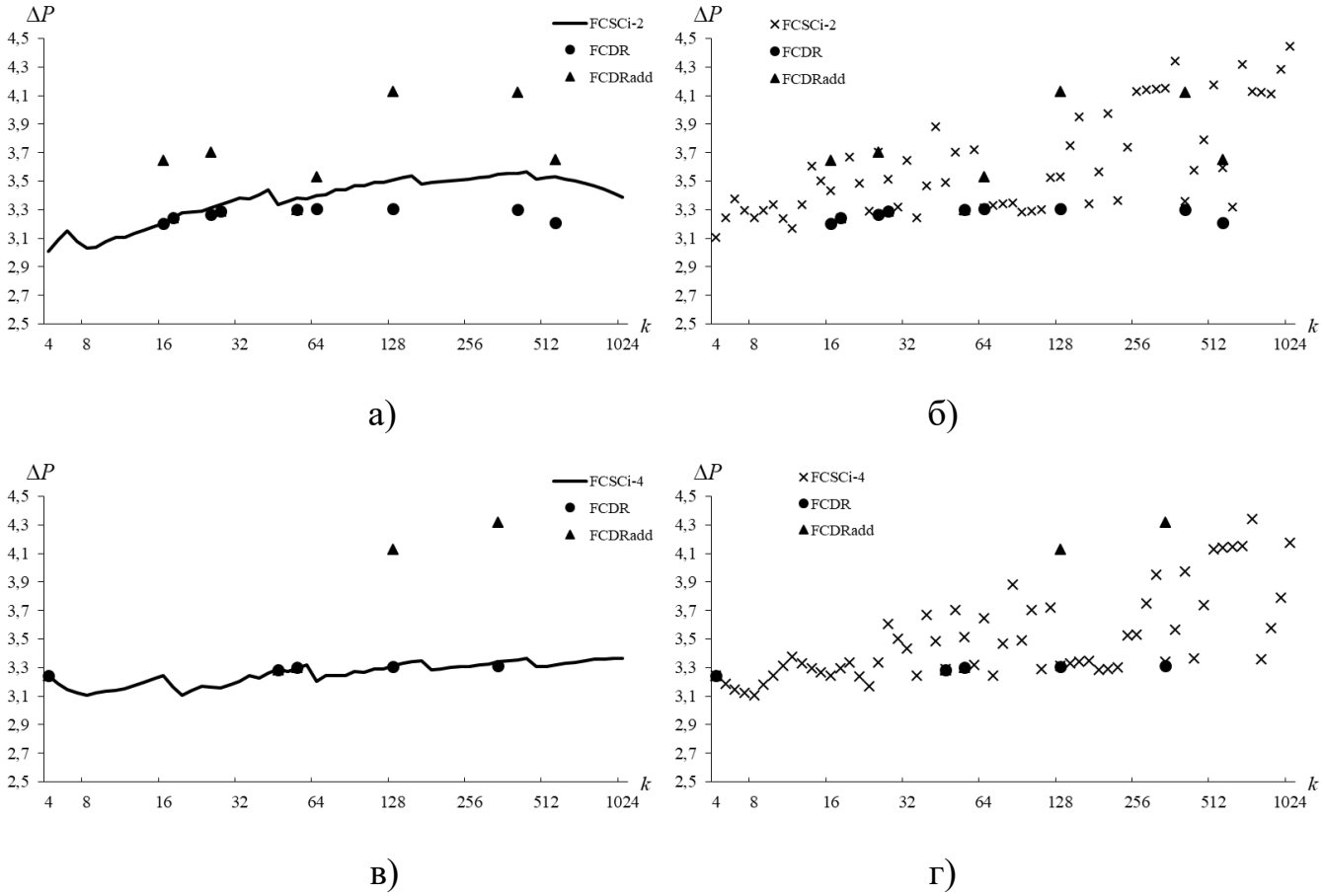


Рис. 3.12. Графіки залежностей оцінок енергетичного виграшу ФКДКСн від розміру блоку даних на вході кодера для $p_0 = 10^{-3}$ та $N = 2$ блоків ФКВД (а); $N = 2$ блоків ФКВДд (б); $N = 4$ блоків ФКВД (в); $N = 4$ блоків ФКВДд (г)

З аналізу представлених графіків випливає, що виявляюча здатність ФКДКСн не поступається виявляючій здатності ФКВД. Ця обставина дозволяє зменшити вимоги до обчислювальних засобів, що реалізують ФКВД, за рахунок використання блоку меншої довжини і конкатенації декількох кодових слів ФКВД у кодове слово ФКДКСн, зберігаючи виявляючу здатність коду і його швидкість. Разом з тим у більшості випадків виявляюча здатність ФКДКСн поступається ФКВДд.

Графіки залежностей (3.7) швидкості ФКДКСн від розміру блоку даних на вході кодера для різних N показано на рис. 3.13.

З графіка на рис. 3.13 випливає, що збільшення кількості N, в цілому, зменшує швидкість коду. Тому швидкість ФКДКСн поступається швидкості ФКВД, хоча за деяких розмірів блоку даних k на вході кодера їх швидкості приблизно

однакові (див., наприклад, швидкості для $k \in [352;448]$). Діапазони значень k, за яких швидкості ФКДКСн і ФКВД збігаються, зменшуються зі збільшенням N.

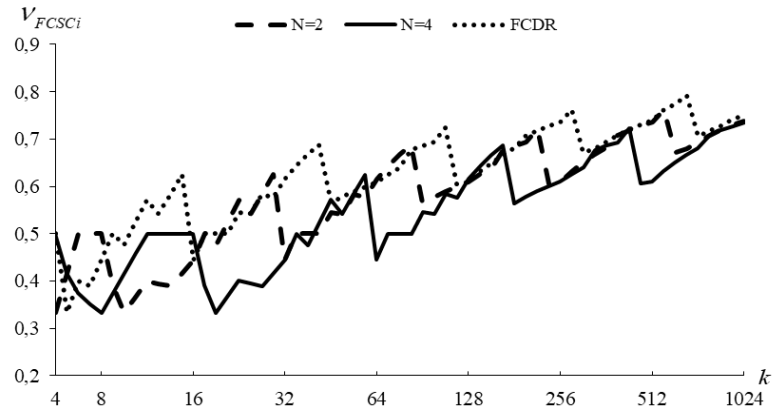


Рис. 3.13. Графік залежності швидкості ФКДКСн від розміру блоку даних

3.4.4. Оцінка стійкості нероздільного факторіального кодування інформації з декількома контрольними сумами

Під час використання ФКДКСн, як і ФКВД, забезпечується криптографічний захист даних і не забезпечується їх імітозахист. Імовірність злому такої системи захисту від несанкціонованого читання методом грубої сили для одноразової спроби підбору ключа $P_{UR}(FCSCi) \le \left(\prod_{i=1}^{N} C_{k-\sum_{j=1}^{i-1} k_{FCDR}(j)}^{k_{FCDR}(i)} \cdot C_{M!}^{2^{k_{FCDR}(i)}} \cdot 2^{k_{FCDR}(i)}! \right)^{-1}$.

3.5. Метод нероздільного факторіального кодування з відновленням даних за перестановкою з заданим числом інверсій

Для ФКВД з (3.2) випливає, що максимальна довжина двійкового інформаційного слова визначається виразом

$$k_{\max} = \lfloor \log_2 M! \rfloor. \qquad (3.9)$$

Вибір значення числа біт інформаційного слова відповідно до (3.9) забезпечує мінімальний показник надлишковості (за потужністю) для заданого M, а

$$1 < \alpha < 2. \qquad (3.10)$$

Факторіальний код, що виявляє помилки та задовольняє умові (3.10), будемо

називати факторіальним кодом з природною надлишковістю. Величина природної надлишковості (за потужністю) $\alpha_{nat} = M!/2^{k_{\max}}$.

Код з $k < k_{\max}$ для заданого M будемо називати факторіальним кодом з внесеною надлишковістю. Величина внесеної надлишковості (за потужністю) $\alpha_{вн} = 2^{\Delta k}$, де $\Delta k = k_{\max} - k$.

Недоліком ФКВД є те, що цей код не виявляє бітові помилки парної кратності, які призводять до перетворення однієї перестановки в іншу.

У цьому підрозділі представимо розроблений і викладений у роботі автора [5] метод факторіального кодування інформації на основі ФКВД, що забезпечує підвищення достовірності передавання інформації за рахунок введення додаткової надлишковості шляхом вибору класу перестановок за заданим критерієм.

3.5.1. Опис методу

Запропонований метод кодування передбачає штучне внесення надлишковості за рахунок зменшення потужності використовуваних перестановок порядку M і, як наслідок, розміру слова джерела: $k = k_{\max} - \Delta k$, $\Delta k > 0$.

Зменшення потужності використовуваних перестановок за умови збереження їх порядку M дозволяє вибрати з $M!$ перестановок тільки такі, які задовольняють наперед заданому набору властивостей. Збільшення надлишковості, за правильного конструювання системи, повинно приводити до збільшення достовірності.

Для розв’язуваної в цьому підрозділі задачі пропонується використовувати число інверсій в перестановці як ознаку її належності до дозволеної множини.

Зокрема, якщо використовувати для перенесення до приймача слів джерела тільки парні (непарні) перестановки, то:

- потужність дозволеної множини слів джерела скоротиться в два рази (одна половина з множини $M!$ перестановок є парною, а інша – непарною);
- декодер виявить усі помилки, що призводять до перетворення перестановки в перестановку і змінюють її парність і не виявить помилки, що призводять до перетворення перестановки в перестановку і не змінюють її парність.

Зауважимо, що перетворення однієї перестановки в іншу еквівалентне перестановці її символів. Скористаємося тим загальновідомим фактом, що перестановка може бути представлена у вигляді добутку транспозицій. Таким чином, перетворення одного кодового слова ФКВД в інше можна представити у вигляді скінченного числа послідовно виконуваних транспозицій. Кожна транспозиція, що застосовується до перестановки, змінює її парність на протилежну. Тому послідовне застосування непарного числа транспозицій змінює парність перестановки, а послідовне застосування парного числа транспозицій не змінює парність перестановки. Це означає, що використання джерелом тільки парних (непарних) перестановок дозволяє виявити помилки, вплив яких призводить до перетворення, еквівалентного непарному числу послідовних транспозицій.

Зауважимо також, що використання джерелом тільки парних (непарних) перестановок призводить до того, що декодером будуть виявлені всі двократні помилки в кодовому слові ФКВД. Це пояснюється тим, що двократна помилка не виявляється ФКВД тоді і тільки тоді, коли вона породжує транспозицію символів у кодовому слові - перестановці. Оскільки транспозиція змінює парність перестановки, це буде виявлено декодером. За цих умов невиявлена помилка декодування може бути оцінена за допомогою виразу (3.3), де замість оцінки $f_{per}(2) \le l_r \cdot M/2$ слід використовувати $f_{per}(2) = 0$.

Таким чином, шляхом скорочення потужності дозволених перестановок і виявлення їх транспозицій у процесі транспортування можна досягти підвищення достовірності передавання систем з ФКВД.

У свою чергу, скорочення потужності множини перестановок – носіїв інформації – в два рази призводить до необхідності зменшення довжини блоку на один біт і, відповідно, до зменшення швидкості коду. Тому використання для перенесення інформації перестановок, число інверсій яких задовольняє певним вимогам, дозволяє виконати обмін швидкості коду на достовірність передавання.

Визначення 3.3. Факторіальним кодом з заданим числом інверсій (ФКЗЧІ) називається ФКВД, множина дозволених кодових слів якого складається з перестановок із заданим числом інверсій.

Визначимо правило вибору дозволеної множини перестановок – носіїв інформації – на основі ознаки числа інверсій, для чого розглянемо теоретичний базис побудови ФКЗЧІ (FCGNI – Factorial Code with a Given Number of Inversions).

Позначимо число інверсій у перестановці π порядку M через $\omega = inv(\pi)$, де $0 \le \omega \le 0{,}5 \cdot M \cdot (M-1)$. Кожному числу ω відповідає частотне число $N_M(\omega)$, яке дорівнює кількості різних перестановок порядку M з числом інверсій, рівним ω.

Виходячи з визначення частотних чисел $N_M(\omega)$, справедливим є вираз $\sum_{\omega=0}^{0,5M(M-1)} N_M(\omega) = M!$, причому $N_M(0) = N_M(0{,}5M(M-1)) = 1$.

Крім того, для $\omega < 0$ і для $\omega > 0{,}5M(M-1)$ частотне число $N_M(\omega) = 0$.

У роботі [277] показано, що розподіл інверсій на всіх перестановках фіксованої довжини збігається з розподілом їх основного індексу. Це означає, що число перестановок порядку M з ω інверсіями збігається з числом перестановок порядку M з основним індексом ω. Ці числа відомі як числа МакМахона (англ. Mahonian numbers). Справедливий і більш сильний результат: число перестановок порядку M з основним індексом k і ω інверсіями збігається з числом перестановок порядку M з основним індексом ω і k інверсіями, тобто дві статистики рівнорозподілені.

Відповідно до [278]–[280], частотні числа $N_M(\omega)$ є коефіцієнтами в розкладанні $\prod_{i=0}^{M-1}(1 + x + \ldots + x^i)$, тобто $\prod_{i=0}^{M-1}(1 + x + \ldots + x^i) = \sum_{\omega=0}^{0.5M(M-1)} N_M(\omega) \cdot x^\omega$.

Згідно [278], [281], для кількості $N_M(\omega)$ перестановок порядку $M \ge 0$ з ω інверсіями справедливим є наступне рекурентне співвідношення:

$$N_{M+1}(\omega) = N_M(\omega - M) + N_M(\omega + 1 - M) + \ldots + N_M(\omega) = \sum_{i=\omega-M}^{\omega} N_M(i), \qquad (3.11)$$

при цьому $N_0(\omega) = 0$ при $\omega \ge 1$.

Наведемо доведення.

Для $\omega < 0$ справедливою є рівність $N_M(\omega) = 0$, тому для $\omega < 0$ також

справедливим є $N_{M+1}(\omega)\equiv 0$. Для $\omega > 0{,}5\cdot(M+1)\cdot M$ виконується нерівність $\omega+1-M > 0{,}5\cdot M\cdot(M-1)$ і $N_M(\omega+1-M)=N_M(\omega+2-M)=\ldots=N_M(\omega)=0$, а значить $N_{M+1}(\omega)=0$, $\omega > 0{,}5\cdot(M+1)\cdot M$. Нехай ω задовольняє умові $0\le\omega\le 0{,}5\cdot(M+1)\cdot M$. Множину перестановок порядку $(M+1)$ позначимо через A, а перестановки порядку M будемо записувати в такий спосіб: $\pi=(\pi_0,\pi_1,\ldots,\pi_{M-1})$, де $\pi_j\in[0,M-1]$, $\pi_j\ne\pi_k$ для $j\ne k$, $j,k\in[0,M-1]$. Розіб'ємо множину перестановок A на $(M+1)$ підмножин A_i, $i\in[0,M]$, наступним чином:

$$\begin{aligned}
&A_0=\{(M,\pi_0,\pi_1,\ldots,\pi_{M-1})\}=\{\Pi_0\},\\
&A_1=\{(\pi_0,M,\pi_1,\ldots,\pi_{M-1})\}=\{\Pi_1\},\\
&\ldots\\
&A_M=\{(\pi_0,\pi_1,\ldots,\pi_{M-1},M)\}=\{\Pi_M\}.
\end{aligned}\tag{3.12}$$

Очевидно, що $A=\bigcup_{i=0}^{M}A_i$. Зауважимо, що число інверсій у кожній перестановці Π_i з підмножини A_i визначається формулою:

$$inv(\Pi_i)=inv(\pi)+M-i.\tag{3.13}$$

Числом $N_{M+1,i}(\omega)$ позначимо кількість різних перестановок Π_i порядку $(M+1)$ у множині A_i з числом інверсій, рівним ω. Легко бачити, що:

$$\begin{aligned}
&N_{M+1,M}(\omega)=N_M(\omega),\\
&N_{M+1,M-1}(\omega)=N_M(\omega-1),\\
&N_{M+1,M-2}(\omega)=N_M(\omega-2),\\
&\ldots\\
&N_{M+1,1}(\omega)=N_M(\omega-M+1),\\
&N_{M+1,0}(\omega)=N_M(\omega-M).
\end{aligned}$$

Звідси слідує що $N_{M+1}(\omega)=\sum_{i=0}^{M}N_{M+1,j}(\omega)=\sum_{i=0}^{M}N_M(\omega-i)=\sum_{j=\omega-M}^{\omega}N_M(j)$. ■

У онлайн-енциклопедії цілочисельних послідовностей (OEIS) [282] представлено послідовність чисел МакМахона $N_M(\omega)$ для $M\in[1,50]$.

Властивості частотних чисел $N_M(\omega)$.

1. Для $M \geq 2$ і $\omega: 2 \leq \omega \leq C_M^2 - 1$ усі частотні числа $N_M(\omega) \geq M - 1$.

2. Частотні числа мають властивість симетрії: для $M \geq 2$ $N_M(\omega) = N_M\left(C_M^2 - \omega\right)$, $N_M(1) = M - 1$.

3. $\sum_{\omega=0}^{0,5M(M-1)} (-1)^{\omega} N_M(\omega) = 0$.

4. $\sum_{\omega=0}^{0,5M(M-1)} \omega N_M(\omega) = \frac{1}{2} C_M^2 M! = \sum_{\pi} inv(\pi)$.

5. Якщо $\omega_1 < \omega_2 \leq \left[0,5 \cdot C_M^2\right]$, то $N_M(\omega_1) < N_M(\omega_2)$.

6. Якщо число C_M^2 парне, тобто $C_M^2 = 2l$, то $\max\limits_{\omega} N_M(\omega) = N_M(l)$. Якщо число C_M^2 непарне, тобто $C_M^2 = 2l + 1$, то $\max\limits_{\omega} N_M(\omega) = N_M(l) = N_M(l+1)$.

7. Рекурентна формула (3.11) може бути приведена до наступної форми:

$$N_{M+1}(\omega) = N_{M+1}(\omega - 1) + N_M(\omega) - N_M(\omega - 1 - M). \qquad (3.14)$$

Зауваження. Для $\omega < M + 1$ формула (3.14) має вигляд $N_{M+1}(\omega) = N_{M+1}(\omega - 1) + N_M(\omega)$, що відповідає (I) з [278, с. 239] і (9) з [230, с. 15].

Визначимо залишок числа інверсій в перестановці порядку M за деяким модулем q: $R = |\omega|_q$, де $2 \leq q \leq 0,5 \cdot M \cdot (M-1)$, а $0 \leq R \leq q - 1$.

Множина різних перестановок π порядку M, число інверсій у яких належить класу лишків $\overline{R}_q$, утворює підмножину (клас) перестановок $B_M(q,R) = \left\{\pi \left| |inv(\pi)|_q = R \right.\right\}$. Потужності $W_M(q,R)$ класів $B_M(q,R)$ у залежності від значень q і R обчислюються наступним чином:

$$W_M(q,R) = \sum_{j=0}^{\left[(0,5 \cdot M \cdot (M-1) - R)/q\right]} N_M(\omega = jq + R). \qquad (3.15)$$

У роботі [230] показано, що для $q \leq M$ потужності класів $B_M(q,R)$ є інваріантними відносно R та дорівнюють

$$W_M(q,R) = M!/q. \qquad (3.16)$$

Зауважимо, що потужності $W_M(q,R)$ класів $B_M(q,R)$ можуть істотно відрізнятися за незмінного значення модуля q. Тому є очевидним, що з метою максимізації швидкості коду для перенесення інформації необхідно використовувати класи перестановок максимальної потужності. Кількість інформації, що переноситься однією перестановкою, дорівнює

$$i_M(q,R) = \log_2\left(W_M(q,R)\right). \tag{3.17}$$

Максимальна довжина двійкового інформаційного слова $k_M(q,R)$, що перетворюється в перестановку порядку M з класу $B(q,R)$, визначається виразом

$$\max\left(k_M(q,R)\right) = \left\lfloor \log_2\left(W_M(q,R)\right)\right\rfloor. \tag{3.18}$$

Однак з цього не випливає, що використання класу перестановок $B_M(q,R)$ максимальної потужності забезпечує найбільшу енергетичну ефективність. Під енергетичною ефективністю будемо розуміти величину різниці рівнів сигналу - переносника перестановок на вході приймача ФКЗЧІ і будь-якого іншого приймача інформації, що забезпечує однакову ймовірність безпомилкового прийому.

Якщо для $q \le M$ всі класи $B_M(q,R)$ рівнопотужні, то для $M < q \le 0{,}5 \cdot M \cdot (M-1)$ потужності класів $B_M(q,R)$ не є однаковими та підлягають експериментальній оцінці.

Для окремого випадку $M = 8$ $(n = 24)$ в таблиці 3.1 наведено результати експериментальної оцінки максимальної потужності $W_{\max}$ класу перестановок $B_M(q,R)$. Крім того, в таблиці наведено:

- значення R, за якого досягається максимальна потужність класу $B_M(q,R)$;
- значення $k_{\max} = \max\left(k_M(q,R)\right)$;
- значення швидкості коду $\nu_{1\max}$, яка відповідає $k_{\max}$.

Якщо врахувати, що для $M = 8$ швидкість ФКВД $\nu_{1\,FCDR} = 0{,}625$, то для ФКЗЧІ вона змінюється від 0,583 (для $q = 2$) до значення 0,458 (для $q = 11\ldots28$).

Таблиця 3.1

Класи $B_M(q,R)$ максимальної потужності для $q \in [2,28]$

q	2	3	4	5	6	7	8	9	10
$W_{\max}$	20160	13440	10080	8064	6720	5760	5040	4522	4184
R	РП	РП	РП	РП	РП	РП	РП	5	4
$k_{\max}$	14	13	13	12	12	12	12	12	12
$\nu_{1\max}$	0,583	0,540	0,540	0,500	0,500	0,500	0,500	0,500	0,500
q	11	12	13	14	15	16	17	18	19
$W_{\max}$	3988	3890	3850	3838	3836	3836	3836	3836	3836
R	3	2	1	0	14	14	14	14	14
$k_{\max}$	11	11	11	11	11	11	11	11	11
$\nu_{1\max}$	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458
q	20	21	22	23	24	25	26	27	28
$W_{\max}$	3836	3836	3836	3836	3836	3836	3836	3836	3836
R	14	14	14	14	14	14	14	14	14
$k_{\max}$	11	11	11	11	11	11	11	11	11
$\nu_{1\max}$	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458

Примітка. Символи РП позначають, що всі класи $B_M(q,R)$ для цього q рівнопотужні, а їх потужність визначено рівністю (3.16).

Виходячи зі сказаного, метод нероздільного факторіального кодування з заданим числом інверсій полягає в наступному:

1) інформаційна послідовність $A(x)$ з k біт перетворюється в перестановку π порядку M;
2) перетворення інформаційного повідомлення в перестановку є бієктивним відображенням $A(x) \leftrightarrow \pi$ рівнопотужних множин інформаційних векторів $A(x)$ і дозволених перестановок π;
3) правило відображення $A(x) \leftrightarrow \pi$ може триматися в таємниці і складати ключ перетворення;
4) множина дозволених перестановок π порядку M належить класу $B_M(q,R) = \left\{ \pi \middle| inv(\pi)\big|_q = R \right\}$ перестановок, число інверсій у яких належить заданому класу лишків $\overline{R}_q$;

5) модуль q класу лишків визначається виходячи з необхідного ступеня підвищення достовірності та допустимої втрати швидкості коду;
6) символи перестановки π кодуються двійковим кодом, після чого вона передається каналом зв'язку одержувачу.

3.5.2. Пристрій кодування і декодування факторіальних кодів з заданим числом інверсій

Кодек ФКЗЧІ містить блок кодування та блок декодування.

Структурна схема блоку кодування ФКЗЧІ представлена на рис. 3.14.

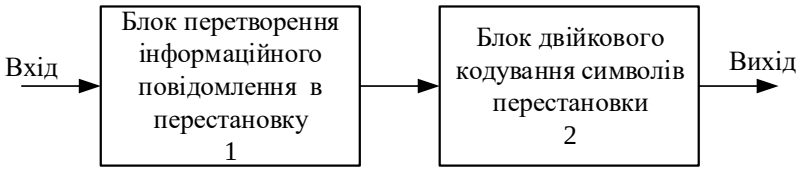


Рис. 3.14. Структурна схема блоку кодування ФКЗЧІ

Інформаційне повідомлення $A(x)$ з k біт, поступає на вхід блоку перетворення інформаційного повідомлення у перестановку (1), де формується перестановка π порядку M заданого класу $B_M(q,R)$. Отримана перестановка після кодування її символів двійковим кодом у блоці (2) передається в канал зв'язку.

Формування перестановки з числом інверсій, що належить заданому класу лишків, може бути виконано, наприклад, табличним способом – створенням таблиці, що має 2^k рядків, у кожний з яких записується одна з перестановок з числом інверсій $\omega : |\omega|_q = R$. Така таблиця створюється під час проектування системи. Число різних таблиць, які можуть бути побудовані, дорівнює

$$\mu(M,q,R,k) = C^{2^k}_{W_M(q,R)} \cdot 2^k!. \qquad (3.19)$$

Одночасно створюється таблиця, що зв'язує перестановки з інформаційним словом для декодера. Якщо ці таблиці тримати в таємниці, то створюються передумови шифрування інформації (за рахунок приховування зв'язку інформаційного слова та відповідної йому перестановки). У цьому випадку вираз

(3.19) визначає потужність ключового простору. Зауважимо, що представлений метод кодування володіє недоліком, властивим усім блоковим шифрам, – однакові блоки відкритого тексту перетворюються в однакові блоки шифртексту. Тому для усунення статистичної надлишковості і зменшення ймовірності появи однакових блоків відкритий текст перед перетворенням доцільно піддати стисненню. Крім того, для вирівнювання статистики повідомлення відкритий текст можна піддати скремблюванню, параметри якого можуть триматися в таємниці.

За такого підходу кодер ФКЗЧІ містить ПЗП, у якому зберігаються таблиці. Вибір таблиці здійснюється сеансовим ключем, а вибір перестановки – k-бітовим словом джерела, що визначає адресу комірки, яка зберігає перестановку.

Структурну схему блоку декодування ФКЗЧІ представлено на рис. 3.15.

Прийнятий з каналу зв’язку блок даних поступає на блок перевірки послідовності (4), де виконується перевірка, чи є отримана послідовність перестановкою. Якщо ця умова не виконується, відбувається формування сигналу запиту на повторне передавання отриманого з помилкою блоку. В іншому випадку прийнята перестановка поступає на вхід блоку оцінки кратності числа інверсій (5).

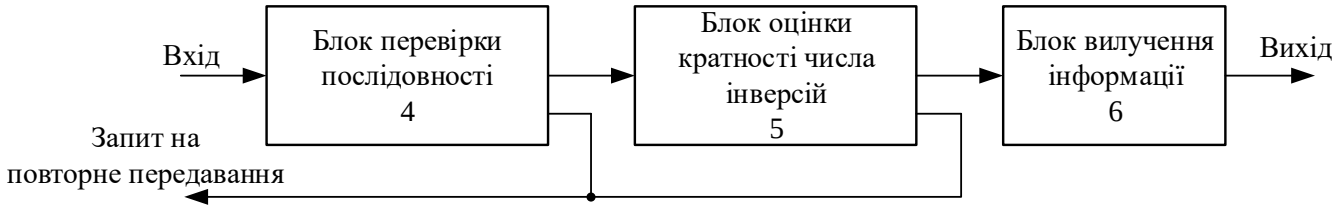


Рис. 3.15. Структурна схема блоку декодування ФКЗЧІ

Якщо число інверсій в прийнятій перестановці не належить заданому класу лишків, то блок оцінки кратності числа інверсій (5) формує сигналу запиту на повторне передавання отриманого з помилкою блоку, при цьому прийнятий блок стирається. Якщо прийнята перестановка зберегла приналежність числа інверсій заданому класу лишків, то блок (5) видає її в блок вилучення інформації (6), який виконує зворотне перетворення перестановки в інформаційне слово. Декодована перестановка з виходу блоку (6) видається споживачеві.

Таким чином, ФКЗЧІ виявляє:

- усі помилки, які породжують перетворення переданої перестановки в «не перестановку»;
- перетворення переданої перестановки в перестановку с числом інверсій, що не належить обраному класу лишків.

3.5.3. Оцінка показників достовірності передавання

Як показано вище, за $q=2$ код виявляє всі помилки кратності $t=2$ і частину помилок більш високої кратності. Вибір модуля q, відмінного від 2 $\left(2<q\le 0{,}5\cdot M\cdot\left(M-1\right)\right)$, призведе до іншого розподілу виявлених і невиявлених помилок, що вимагає обґрунтованого вибору класу $B\left(q,R\right)$. Зазначимо, що за умови вибору $q:\left|q\right|_2=0$ код буде виявляти всі помилки непарної кратності і частину помилок парної кратності.

Приймемо, що 2^K $\left(K=k_M\left(q,R\right)\right)$ перестановок, що утворюють сигнально-кодову конструкцію (СКК), обираються випадково з класу $B_M\left(q,R\right)$. Тоді оцінка ймовірності невиявленої помилки $P_{ud}\left(FCGNI,p_0\right)$ визначається наступним чином:

$$P_{ud}\left(FCGNI,p_0\right)=2^{-K}\sum_{j=1}^{2^K}\sum_{i=2}^{n}f_j\left(i\right)p_0^i\left(1-p_0\right)^{n-i},\qquad(3.20)$$

де $f_j\left(i\right)$ – кількість помилок ваги i, здатних перетворити j-у перестановку обраної СКК у будь-яку іншу перестановку цієї ж СКК, $j\in\left[1;2^K\right]$.

Зазначимо, що оцінка ймовірності невиявленої помилки $P_{ud}\left(FCGNI,p_0\right)$ не є інваріантною відносно вибору СКК. Наступна теорема дозволяє оцінити цю ймовірність на основі аналізу всього класу перестановок $B_M\left(q,R\right)$.

Теорема 3.1. Для ймовірності невиявленої помилки $P_{ud}\left(FCGNI,p_0\right)$ для випадково обраних 2^K перестановок СКК з класу $B_M\left(q,R\right)$ має місце оцінка:

$$P_{ud}\left(FCGNI,p_0\right)=\frac{2^K-1}{W\left(W-1\right)}\sum_{j=1}^{W}\sum_{i=2}^{n}f_j^*\left(i\right)p_0^i\left(1-p_0\right)^{n-i},\qquad(3.21)$$

де $W = W_M(q,R)$;

$f_j^*(i)$ – кількість помилок ваги i, здатних перетворити j-у перестановку класу $B_M(q,R)$ у будь-яку іншу перестановку цього ж класу, $j \in [1;W]$.

Доведення.

Представимо вираз (3.20) у наступному вигляді: $P_{ud}(FCGNI, p_0) = \sum_{i=2}^{n}\left[p_0^i (1-p_0)^{n-i} \frac{1}{2^K} \sum_{j=1}^{2^K} f_j(i) \right]$. Приймемо, що $\overline{f}(i) = \frac{1}{2^K}\sum_{j=1}^{2^K} f_j(i)$ – середня кількість помилок ваги i, здатних перетворити j-у перестановку обраної СКК у будь-яку іншу перестановку цієї ж СКК, $j \in [1;2^K]$. Тоді $P_{ud}(FCGNI, p_0) = \sum_{i=2}^{n} \overline{f}(i)\, p_0^i (1-p_0)^{n-i}$.

Визначимо оцінку ймовірності невиявленої помилки $P_{ud}^*(FCGNI, p_0)$ за умови, що всі перестановки класу $B_M(q,R)$ використовуються в СКК:

$$P_{ud}^*(FCGNI, p_0) = \frac{1}{W}\sum_{j=1}^{W}\sum_{i=2}^{n} f_j^*(i)\, p_0^i (1-p_0)^{n-i}. \qquad (3.22)$$

Аналогічно представимо вираз (3.22) в наступному вигляді: $P_{ud}^*(FCGNI, p_0) = \sum_{i=2}^{n}\left[p_0^i (1-p_0)^{n-i} \frac{1}{W} \sum_{j=1}^{W} f_j^*(i) \right]$. Приймемо також, що $\overline{f^*}(i) = \frac{1}{W}\sum_{j=1}^{W} f_j^*(i)$ – середня кількість помилок ваги i, здатних перетворити j-у перестановку класу $B_M(q,R)$ у будь-яку іншу перестановку цього ж класу, $j \in [1;W]$. Тоді $P_{ud}^*(FCGNI, p_0) = \sum_{i=2}^{n} \overline{f^*}(i)\, p_0^i (1-p_0)^{n-i}$.

У разі випадкового вибору перестановок СКК справедливим є вираз $\frac{\overline{f}(i)}{2^k - 1} = \frac{\overline{f^*}(i)}{W-1}$. Це пояснюється тим, що середня кількість перестановок СКК, до яких відстань Хеммінга від деякої перестановки цієї ж СКК дорівнює значенню i, змінюється прямо пропорційно величині $(W-1)$. Тому

$\frac{P_{ud}\left(FCGNI, p_0\right)}{2^K - 1} = \frac{P^*_{ud}\left(FCGNI, p_0\right)}{W - 1}$, звідки випливає вираз (3.21). ■

Наслідок 3.1. У більш загальному випадку справедливим є вираз $\frac{P_{ud\,1}\left(FCGNI, p_0\right)}{W_1 - 1} = \frac{P_{ud\,2}\left(FCGNI, p_0\right)}{W_2 - 1}$, де $P_{ud\,1}\left(FCGNI, p_0\right)$ і $P_{ud\,2}\left(FCGNI, p_0\right)$ – оцінки ймовірностей невиявленої помилки для потужностей СКК деякого класу $B_M\left(q, R\right)$, рівних W_1 і W_2 відповідно, $W_1, W_2 \le W_M\left(q, R\right)$.

На рис. 3.16 представлено графік залежності оцінки ймовірності не виявленої ФКЗЧІ помилки від модуля q для $M = 8$ $\left(n = 24\right)$ і $p_0 = 10^{-3}$. Значення R обиралися з таблиці 3.1 для забезпечення максимальної потужності класу перестановок $B_M\left(q, R\right)$ для заданих q. Для $q \in \left[2;8\right]$ значення $R = 0$.

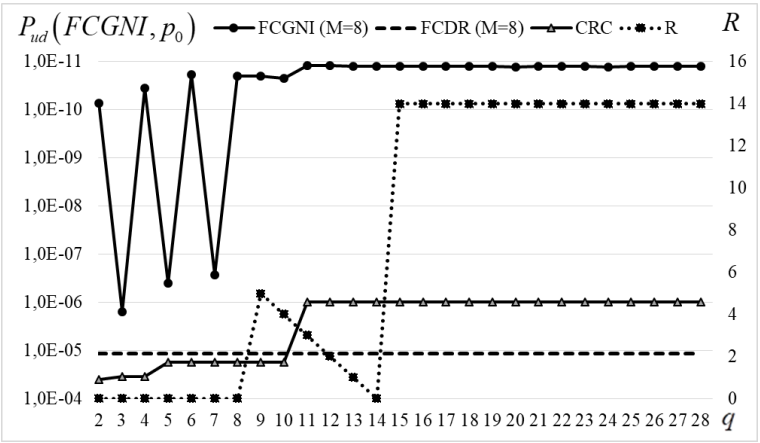


Рис. 3.16. Графік залежності оцінки ймовірності не виявленої ФКЗЧІ помилки від модуля q для $M = 8$ і $p_0 = 10^{-3}$ (максимальна швидкість коду в класі $B_M\left(q, R\right)$)

Пунктирною лінією на графіку позначено оцінку ймовірності не виявленої ФКВД помилки для $M = 8$ – $P_{ud}\left(FCDR, 10^{-3}\right) = 1{,}18 \cdot 10^{-5}$.

Якщо значення R обирати таким чином, щоб забезпечити максимальну достовірність передавання, графік залежності оцінки ймовірності не виявленої ФКЗЧІ помилки від модуля q для $M = 8$ і $p_0 = 10^{-3}$ прийме вигляд, представлений на рис. 3.17. Параметри коду наведено в таблиці 3.2. Символи РД позначають, що всі класи $B_M\left(q, R\right)$ для цього q забезпечують рівну достовірність. Застосування

ФКЗЧІ дозволяє збільшити енергетичний виграш ФКЗЧІ порівняно з CRC-кодом за їх однакових швидкостей – $0.986 дБ \le \Delta P_{FCGNI} - \Delta P_{CRC} \le 3.295 дБ$.

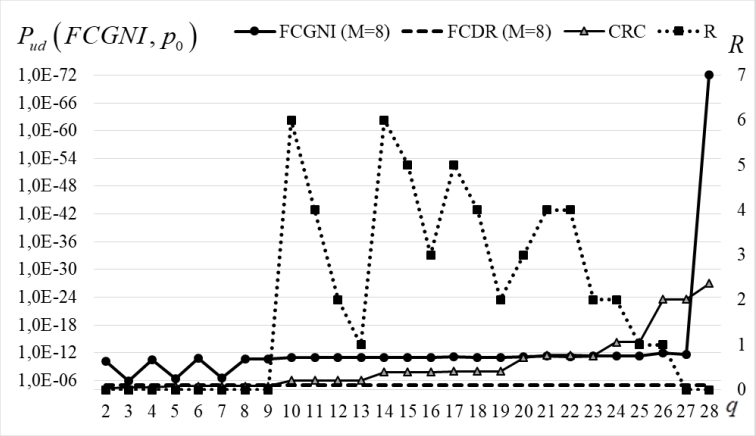


Рис. 3.17. Графік залежності оцінки ймовірності не виявленої ФКЗЧІ помилки від модуля q для $M = 8$ і $p_0 = 10^{-3}$ (максимальна достовірність у класі $B_M(q, R)$)

Таблиця 3.2

Класи $B_M(q, R)$ максимальної достовірності для $q \in [2, 28]$

q	2	3	4	5	6	7	8	9	10
W	20160	13440	10080	8064	6720	5760	5040	4441	4079
R	РД	РД	РД	РД	РД	РД	РД	0	6
k	14	13	13	12	12	12	12	12	11
ν_1	0,583	0,542	0,542	0,500	0,500	0,500	0,500	0,500	0,458
q	11	12	13	14	15	16	17	18	19
W	3937	3890	3850	2017	1758	2016	945	776	988
R	4	2	1	6	5	3	5	4	2
k	11	11	11	10	10	10	9	9	9
ν_1	0,458	0,458	0,458	0,417	0,417	0,417	0,375	0,375	0,375
q	20	21	22	23	24	25	26	27	28
W	419	250	201	103	54	34	14	8	2
R	3	4	4	2	2	1	1	0, 1	0
k	8	7	7	6	5	5	3	3	1
ν_1	0,333	0,292	0,292	0,25	0,208	0,208	0,125	0,125	0,042

Зауважимо, що в загальному випадку для заданого $q \in [2, 28]$ класи з максимальною достовірністю і класи з мінімальною потужністю не збігаються.

Порівняння швидкостей кодів, що забезпечують максимальну потужність СКК і максимальну достовірність залежно від $q \in [2, 28]$, представлено на рис. 3.18.

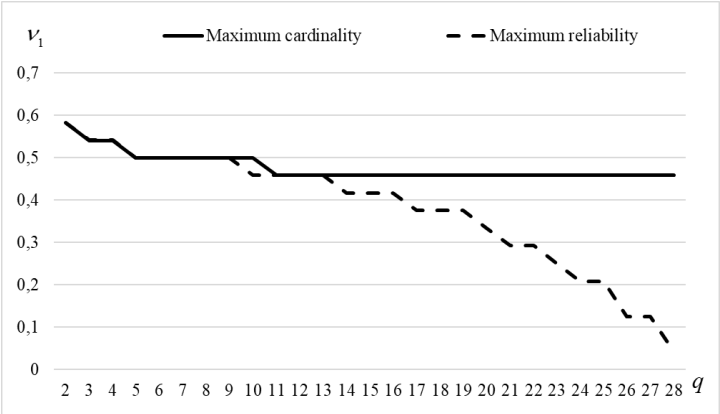


Рис. 3.18. Графіки швидкостей кодів, що забезпечують максимальну потужність СКК і максимальну достовірність залежно від $q \in [2,28]$ для $M = 8$ і $p_0 = 10^{-3}$

Інтегральним показником якості передавання даних є відносна швидкість передавання, обчислювана за (2.39).

Згідно [273], для найпростішої системи з ВЗЗ

$$\nu_2 = Q + P_{ud}\left(FCGNI, p_0\right), \tag{3.23}$$

де $Q = (1 - p_0)^n$ – імовірність прийому кодового слова без помилок.

Графік залежності обчислюваної для ФКЗЧІ за (2.39) з $\nu_2 = Q + P_{ud}\left(FCGNI, p_0\right)$ оцінки відносної швидкості передавання ν_0 від значення q для $M = 8$ і $p_0 = 10^{-3}$ наведено на рис. 3.19. Для кожного $q \in [2,28]$ представлено оцінку максимальної відносної швидкості передавання, а параметри коду наведено в таблиці 3.3.

Штрих-пунктирною лінією на графіку позначена оцінка відносної швидкості передавання ФКВД для $M = 8$ – $\nu_0\left(FCDR, 10^{-3}\right) = 0,610$.

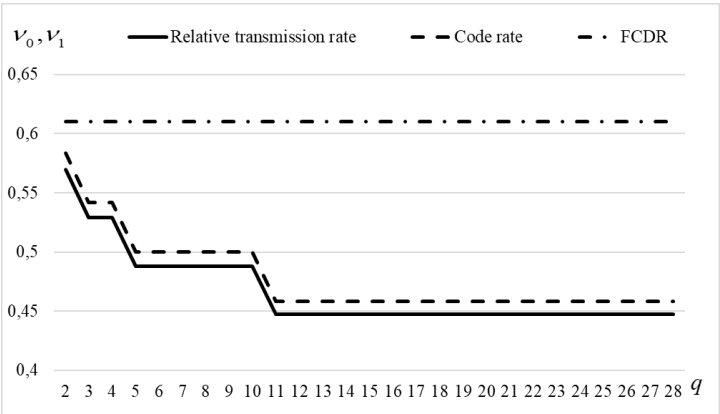


Рис. 3.19. Графік залежності оцінки відносної швидкості передавання для ФКЗЧІ від q для $M = 8$ і $p_0 = 10^{-3}$ (максимальна відносна швидкість передавання в $B_M\left(q, R\right)$)

Графік рис. 3.19 свідчить про те, що для $M=8$ і $p_0=10^{-3}$ відносна швидкість передавання досягає максимальних значень за максимальних значень швидкості коду. Це пояснюється тим, що для заданих параметрів $Q \gg P_{ud}\left(FCGNI, p_0\right)$, звідки для $\nu_2 = Q + P_{ud}\left(FCGNI, p_0\right)$ слідує $\nu_2 \approx Q$.

Таким чином, для $M=8$ і $p_0=10^{-3}$ з метою максимізації відносної швидкості передавання доцільно використовувати класи $B_8\left(2,R\right)$, $R \in \{0;1\}$. За інших M і p_0 значення q і R можуть бути іншими.

Таблиця 3.3

Класи $B_M\left(q,R\right)$ максимальної відносної швидкості передавання для $q \in [2,28]$

q	2	3	4	5	6	7	8	9	10
W	20160	13440	10080	8064	6720	5760	5040	різна	різна
R	РС	РС	РС	РС	РС	РС	РС	РС	3-5
k	14	13	13	12	12	12	12	12	12
ν_1	0,583	0,542	0,542	0,500	0,500	0,500	0,500	0,500	0,500
q	11	12	13	14	15	16	17	18	19
W	різна	різна	різна	різна	різна	різна	різна	різна	різна
R	РС	РС	РС	0-5,9-13	0-4,9-14	0-2,10-15	0,1,10-16	0,10-17	10-18
k	11	11	11	11	11	11	11	11	11
ν_1	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458
q	20	21	22	23	24	25	26	27	28
W	різна	різна	різна	різна	різна	різна	різна	різна	різна
R	10-18	10-18	10-18	10-18	10-18	10-18	10-18	10-18	10-18
k	11	11	11	11	11	11	11	11	11
ν_1	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458	0,458

Примітка. Позначення «різна» означає, що для заданого q потужності класів $B_M\left(q,R\right)$ можуть бути різними.

З рис. 3.19 також випливає, що для $M=8$ і $p_0=10^{-3}$ ФКВД перевершує ФКЗЧІ у відносній швидкості передавання. Разом з тим, графіки рис. 3.16 і 3.17 свідчать, що ФКЗЧІ спрямований на зменшення ймовірності невиявленої помилки (наприклад, для $q=2$ – на більш ніж 5 порядків у порівнянні з ФКВД), що може бути корисним в системах з високими вимогами до ймовірності «хибної тривоги».

3.6. Метод факторіального кодування з відновленням даних і виправленням помилок

Зауважимо, що всі досліджені вище факторіальні коди орієнтовані на застосування в системах з ВЗЗ і не дозволяють реалізувати виправлення помилок.

Разом з тим, надлишковість ФКВД забезпечує можливість збільшення відстані між перестановками – носіями інформації – і створює передумови для створення факторіального коду з виправленням помилок.

У зв'язку з цим у рамках дисертаційного дослідження виконано розробку методу факторіального кодування інформації, який реалізує функцію захисту інформації від несанкціонованого доступу, а також функцію завадостійкого кодування, що поєднує виявлення та виправлення помилок. Викладення та дослідження розробленого методу представлено в роботах автора [54], [52], [48], [283].

3.6.1. Опис методу

Як показано вище, приймач ФКВД містить блок перевірки коректності прийнятої з каналу кодової комбінації і декодер ФКВД.

Коректна послідовність підлягає декодуванню – зворотному перетворенню $f_{FCDR}^{-1}: R_{FCDR}(x) \to A(x)$. Оскільки $M! > 2^k$ для $k > 1$, множина перестановок на вході декодера складається з двох підмножин – дозволеної та забороненої. До дозволеної підмножини відносяться 2^k перестановок (у найпростішому випадку їх синдроми S_F відповідають цілим числам відрізка $\left[0; 2^k - 1\right]$ числової осі), а до забороненої – підмножина з $\left(M! - 2^k\right)$ інших перестановок (синдроми S_F відповідають цілим числам відрізка $\left[2^k; M! - 1\right]$ числової осі). Таким чином, прийом будь-якої перестановки з недозволеної частини множини також ініціює команду перезапиту.

Визначення 3.4. Факторіальним кодом з відновленням даних і виправленням помилок (ФКВДвп) називається нероздільний код, який передбачає заміну інформаційної послідовності з k біт на перестановку чисел порядку M $\left(M! \geq 2^k\right)$,

обчислену за всіма інформаційними бітами, таким чином, що відстань між кодовими словами є достатньою для виправлення виникаючих у каналі зв'язку помилок.

Визначення 3.5. Сигнальними векторами називаються представлені в двійковому вигляді перестановки дозволеної множини, що використовуються для перенесення інформації. Множина сигнальних векторів коду утворює його сигнально-кодову конструкцію (СКК).

Визначення 3.6. Сигнальними точками називаються точки на числовій осі $[0; M!-1]$, які відповідають сигнальним векторам коду.

Множина сигнальних точок коду утворює його сигнальне сузір'я.

Метод факторіального кодування з відновленням даних і виправленням помилок полягає в наступному:

1) інформаційна послідовність $A(x)$ з k біт перетворюється в перестановку π порядку M:
   a) з усієї множини перестановок потужності $M!$ дозволеною є лише підмножина з 2^k перестановок;
   b) показник α визначає відстань між перестановками і залежить від вимог до достовірності передавання і принципів формування СКК;
2) перетворення $A(x) \leftrightarrow \pi$ є бієктивним відображенням рівнопотужних множин інформаційних векторів $A(x)$ і дозволених перестановок π;
3) правило відображення $A(x) \leftrightarrow \pi$ може триматися в таємниці і складати ключ перетворення;
4) символи перестановки π кодуються двійковим кодом, після чого вона передається каналом зв'язку одержувачу.

Реалізації методу ФКВДвп можуть відрізнятися в залежності від того, яким чином досягається збільшення відстані між сигнальними точками сузір'я.

Розглянемо два способи формування СКК для ФКВДвп (FCDRec – FCDR with error correction):

1) СКК на основі мінімальної відстані Евкліда між сигнальними точками. Такі СКК будемо називати СКК першого типу і позначати через СКК-1;

2) СКК на основі мінімальної відстані Хеммінга між сигнальними векторами. Такі СКК будемо називати СКК другого типу і позначати через СКК-2.

3.6.2. Типи сигнально-кодових конструкцій

3.6.2.1. Сигнально-кодова конструкція першого типу

Оскільки потужність множини значень вектора $A(x)$ дорівнює 2^k, мінімальна відстань між сигнальними точками на осі $[0; M!-1]$

$$D_{\min} \le \left\lfloor (M!-1) \big/ (2^k - 1) \right\rfloor. \tag{3.24}$$

У найпростішому випадку 2^k сигнальних точок розташовуються на числовій осі $\left[0; 2^k - 1\right]$ з кроком $D_{\min} = 1$. Такий факторіальний код не призначений для виправлення помилок. Він може бути застосований для виявлення помилок, причому тільки тих, які призводять до перетворення переданої перестановки в «не перестановку» або в перестановку з забороненої множини.

Нагадаємо, що для ФКВД $k \le \lfloor \log_2 M! \rfloor$. Виконаємо оцінку $D_{\min}$ для $k = \lfloor \log_2 M! \rfloor$, для якого досягається максимальна швидкість коду. Оскільки $\log_2 M! - 1 < \lfloor \log_2 M! \rfloor \le \log_2 M!$, має місце $M!/2 < 2^k \le M!$, а $1 \le \dfrac{M!-1}{2^k - 1} < \dfrac{M!-1}{M!/2 - 1} = 2 + \dfrac{2}{M!-2}$. Таким чином, для $k = \lfloor \log_2 M! \rfloor$ мінімальна відстань між сигнальними точками $D_{\min} \le 2$. Такий ФКВД не здатний виправляти помилки, що призводять навіть до мінімального зміщення сигнальних векторів на числовій осі, і тому він може бути застосований лише для виявлення помилок. За цих обставин код також виявляє тільки ті помилки, що призводять до перетворення перестановки в «не перестановку» або в перестановку з забороненої множини.

Для забезпечення можливості виправлення помилок необхідно збільшити мінімальну відстань між сигнальними точками до $D_{\min} \ge 3$.

Для збільшення відстані між сигнальними точками необхідно збільшувати показник надлишковості (за потужністю) α за (3.4). Очевидно, що $\alpha = M!/2^k$ є монотонно зростаючою функцією за M і монотонно спадною за k.

Графічно розташування сигнальних точок на числовій осі представлено на рис. 3.20. Відстань від нуля до сигнальної точки *i* будемо позначати через D_i, а між сигнальними точками i та j – через $D_{i,j} = D_j - D_i$.

Положення сигнальних точок на числовій осі визначається використовуваною СКК. У найпростішому випадку сигнальні точки розташовуються рівномірно з кроком $D_{\min}$, $D_{i,i+1} = D_{\min} = const$ для $i \in \left[0; 2^k - 2\right]$. У більш загальному випадку $D_{i,i+1} \neq const$, а $D_{i,j} \geq D_{\min}$, $i, j \in \left[0; 2^k - 1\right]$, $i \neq j$.

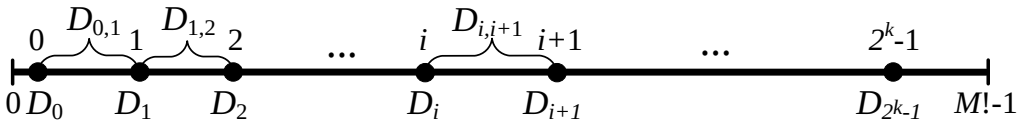


Рис. 3.20. Розташування сигнальних точок на числовій осі

Під час передавання сигнального вектора діюча в каналі зв'язку завада може перетворити передану перестановку в будь-яку іншу перестановку, тим самим змістивши сигнальну точку передавача в будь-яку іншу точку відрізка $\left[0; M!-1\right]$. Ця точка може бути як сигнальною, так і не сигнальною, а прийнята перестановка може належати як до дозволеної, так і до забороненої множин.

Приймач приймає рішення щодо переданого сигнального вектора на підставі критерію максимальної правдоподібності шляхом знаходження сигнальної точки, найближчої (в метриці Евкліда) до точки, що відповідає прийнятому вектору. Для цього декодер обчислює відстані до суміжних сигнальних точок. У разі рівного розподілу цих відстаней формується сигнал перезапиту.

Таким чином, якщо завада змістила сформований передавачем *i*-ий вектор не більше ніж на $-\left\lfloor \left(D_{i-1,i} - 1\right)/2 \right\rfloor$ і $+\left\lfloor \left(D_{i,i+1} - 1\right)/2 \right\rfloor$ точок числової осі, то ця помилка виправляється, а прийнятий вектор коригується приймачем у перестановку, яка відповідає *i*-ій сигнальній точці. Якщо зсув дорівнює $-\left\lfloor D_{i-1,i}/2 \right\rfloor$ (або $+\left\lfloor D_{i,i+1}/2 \right\rfloor$) і $D_{i-1,i}/2 \in \mathbb{Z}$ $\left(D_{i,i+1}/2 \in \mathbb{Z}\right)$, тобто відстань до сусідніх сигнальних точок однакова, помилка виявляється кодом і виправляється шляхом перезапиту. Якщо ж зміщення

перевищує $-\lfloor D_{i-1,i}/2 \rfloor$ (або $+\lfloor D_{i,i+1}/2 \rfloor$), то такі помилки код виправити не може. У цьому випадку, якщо відстані від відповідної прийнятому вектору точки числової осі до сусідніх сигнальних точок однакова, помилка виявляється і виправляється шляхом перезапиту, якщо ж ця відстань різна, має місце помилка декодування (помилкова ідентифікація прийнятого вектора) і не виявлена кодом помилка.

Розглянемо процес декодування, якщо прийнятий вектор відповідає точці з діапазону $[0; D_0 - 1]$ або $\left[D_{2^k-1} + 1; M! - 1 \right]$. Можливі два варіанти:

1) усі точки діапазону $[0; D_0 - 1]$ коригуються в нульову сигнальну точку, а діапазону $\left[D_{2^k-1} + 1; M! - 1 \right]$ – у $\left(2^k - 1\right)$ сигнальну точку;
2) корекція в нульову сигнальну точку виконується для діапазону $\left[D_0 - \lfloor (D_{\min} - 1)/2 \rfloor; D_0 - 1 \right]$, у $\left(2^k - 1\right)$ сигнальну точку – для діапазону $\left[D_{2^k-1} + 1; D_{2^k-1} + \lfloor (D_{\min} - 1)/2 \rfloor \right]$, інші точки крайніх діапазонів є забороненими.

У будь-якому випадку всі помилки, що призводять до зміщення сигнальної точки на відстань $D \le \lfloor (D_{\min} - 1)/2 \rfloor$, виправляються.

Покладемо $D_{i,i+1} = D_{\min}$ для $\forall i \in \left[0; 2^k - 2\right]$, $D_0 = \lfloor (D_{\min} - 1)/2 \rfloor$, а $M! - 1 - D_{2^k-1} \ge \lfloor (D_{\min} - 1)/2 \rfloor$. У цьому випадку має місце оцінка

$$\left(2^k - 1\right) D_{\min} + 2\lfloor (D_{\min} - 1)/2 \rfloor + 1 \le M!. \qquad (3.25)$$

Для заданих k і M мінімальна відстань $D_{\min} \le \max(D) : \left(2^k - 1\right) D + 2\lfloor (D-1)/2 \rfloor + 1 \le M!$. Наприклад, якщо $k = 40$, а $M = 16$, то $D_{\min} \le 19$. Таким чином, вибір параметрів k і M однозначно визначає максимальну виправляючу здатність коду.

Вираз (3.25) також може служити для вибору k або M за інших відомих параметрів коду. Наприклад, якщо $k = 16$, а $D_{\min} = 3$, то $M! \ge 196608$, звідки $M \ge 9$. Якщо ж $M = 8$, а $D_{\min} = 6$, то $k \le 12$.

Крім того, вираз (3.25) для представленого вище другого правила прийняття рішення декодером показує, що всі точки, що лежать правіше граничної точки

$\left(2^k-1\right)D_{\min}+2\left\lfloor\left(D_{\min}-1\right)/2\right\rfloor+1$, відносяться до не використовуваної (забороненої) частини числової множини. Тому всі прийняті з каналу зв'язку кодові комбінації після перевірки коректності проходять порівняння з граничним значенням. Якщо відповідна кодовій комбінації точка числової осі розташована вище граничної точки, проводиться перезапит блоку даних, у іншому випадку виконується пошук найближчої сигнальної точки і ототожнення з нею прийнятої кодової комбінації.

3.6.2.2. Сигнально-кодова конструкція другого типу

Визначена для СКК-1 відстань Евкліда $D_{i,j}$ між сигнальними точками i і j у загальному випадку не дорівнює відстані Хеммінга між кодовими словами, що відповідають цим сигнальним точкам, і не забезпечує такої ж виправляючої здатності коду, яка досягається в метриці Хеммінга. Разом з тим, з теорії коригувальних кодів [68] відомо, що для виправлення помилки в двійкових розрядах кратності t мінімальна відстань Хеммінга $d_{\min}$ між кодовими словами повинна задовольняти умові $d_{\min}\geq 2t+1$.

Відстань Хеммінга між сигнальними точками i і j будемо позначати через $d_{i,j}$. Тоді для ФКВДвп з СКК-2 має виконуватися: $d_{i,j}\geq d_{\min}$, $i,j\in\left[0;2^k-1\right]$, $i\neq j$.

У найпростішому випадку для ФКВД сигнальні вектори відповідають сигнальним точкам з кроком $D_{i,i+1}=D_{\min}=1$ і $D_0=1$. Тоді $d_{\min}=2$, а ФКВД тільки виявляє помилки, що призводять до перетворення переданої перестановки в «не перестановку» або в перестановку з забороненої множини. Визначення зв'язку між M, k і $d_{\min}$ є актуальною задачею, що виходить за рамки цієї роботи.

Очевидно, що для забезпечення можливості виправлення помилок необхідно збільшити мінімальну відстань $d_{\min}$ між сигнальними точками. Для збільшення відстані між сигнальними точками необхідно збільшувати показник надлишковості (за потужністю) α. Помилки можуть бути виправлені для $d_{\min}\geq 3$.

Врахуємо, що відстань Хеммінга між сигнальними векторами парна і, отже, $d_{\min}\vdots 2$. Тому під час передавання i-го сигнального вектора ФКВДвп з СКК-2

справедливі наступні твердження:

1) помилка з вагою $t \le \lfloor (d_{\min} - 1)/2 \rfloor = (d_{\min} - 2)/2 = d_{\min}/2 - 1$ виправляється, а прийнятий вектор коригується приймачем у переданий сигнальний вектор;
2) помилка з вагою $t = d_{\min}/2$ може бути як виправлена (якщо мінімальна відстань $r_{\min}$ відповідає відстані лише до одного i-го сигнального вектора), так і виявлена і виправлена шляхом перезапиту (якщо мінімальна відстань $r_{\min}$ відповідає відстані до двох або більше сигнальних векторів);
3) якщо вага помилки $t > d_{\min}/2$, може мати місце виправлена помилка (якщо $r_{\min}$ відповідає відстані лише до одного i-го сигнального вектора), виявлена помилка (якщо $r_{\min}$ відповідає відстані до двох і більше сигнальних векторів) або невиявлена помилка внаслідок помилкової ідентифікації (якщо $r_{\min}$ відповідає відстані лише до одного сигнального вектора, відмінного від i-го).

Таким чином, такий код дозволяє комбінувати виправлення найбільш частих поєднань помилок і виявлення з подальшим повторенням для більш рідкісних поєднань помилок.

Актуальним питанням, що лежить за рамками цієї роботи, під час вибору СКК другого типу є питання максимальної кількості $N_{sv}(d_{\min}, M)$ сигнальних векторів, що забезпечують задану мінімальну відстань $d_{\min}$ за відомого M (це питання тісно пов'язане з теорією решіток і задачею найкращої упаковки куль у просторах різних розмірностей [12], [284]). Знаючи значення $N_{sv}(d_{\min}, M)$, можна сконструювати ефективний код, що передає за допомогою однієї перестановки $k = \log_2 N_{sv}$ біт інформації і виправляє всі помилки кратності $t \le d_{\min}/2 - 1$. Імовірнісні характеристики такого коду визначаються за представленими нижче виразами, в яких замість значення $2^k - 1$ приймається значення $N_{sv}(d_{\min}, M) - 1$, а $k = \log_2 N_{sv}$.

3.6.3. Пристрій кодування та декодування факторіальних кодів з відновленням даних і виправленням помилок

Пристрій кодування та декодування ФКВДвп містить блок кодування та блок

декодування [49]. Структурна схема блоку кодування зображена на рис. 3.21.

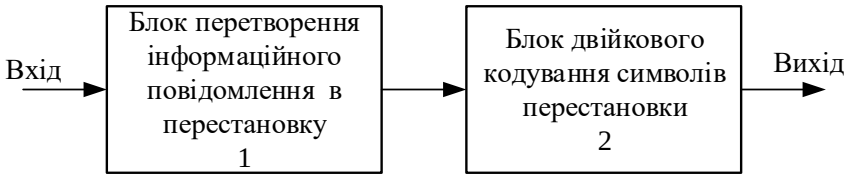


Рис. 3.21. Структурна схема блоку кодування пристрою кодування та декодування ФКВДвп

Інформаційне повідомлення $A(x)$, яке містить k біт, поступає на вхід блоку перетворення інформаційного повідомлення в перестановку (1), де формується перестановка π порядку M. Правило відображення $A(x) \leftrightarrow \pi$ може триматися в таємниці та становити ключ перетворення. Отримана перестановка після кодування її символів двійковим кодом у блоці (2) передається в канал зв'язку.

У найпростішому випадку для СКК-1 сигнальні точки розміщуються рівномірно з кроком $D_{\min}$. Для цього точки відрізку $\left[0; 2^k - 1\right]$ проектуються на відрізок $\left[0; L-1\right]$, де $L = D_{\min} \cdot \left(2^k - 1\right) + 2 \cdot \left\lfloor \left(D_{\min} - 1\right)/2 \right\rfloor$, шляхом перетворення $D = A_{10} \cdot D_{\min} + \left\lfloor \left(D_{\min} - 1\right)/2 \right\rfloor$, де A_{10} – десятковий еквівалент двійкового представлення вектора $A(x)$, $A_{10} \in \left[0; 2^k - 1\right]$, D – значення, що відповідає сигнальній точці вектора $A(x)$. Після цього значення D послідовно перетворюється в число A_F у ФСЧ, синдром перестановки S_F та перестановку порядку M, $M! \geq L$, яка після кодування символів рівномірним двійковим кодом передається каналом.

Узагальнена структурна схема блоку декодування пристрою кодування та декодування ВКВДвп зображена на рис. 3.22.

Прийнятий з каналу зв'язку блок даних поступає на блок обробки прийнятої послідовності (3), де виконується процедура виявлення та виправлення помилок. Якщо помилка виявляється, але не може бути виправлена, формується сигнал запиту на повторення цього блоку. У іншому випадку сформована на виході блоку обробки прийнятої послідовності (3) перестановка потрапляє на вхід блоку вилучення

інформації (4), де з неї відновлюється інформаційний блок.

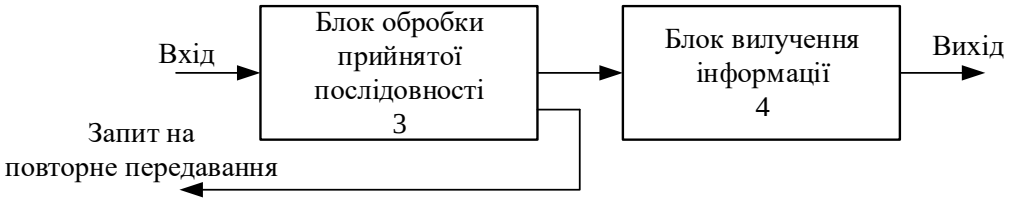


Рис. 3.22. Узагальнена структурна схема блоку декодування пристрою кодування та декодування ФКВДвп

Структура і функції блоку обробки прийнятої послідовності (3) залежить від типу СКК, що використовується.

Структурна схема блоку обробки прийнятої послідовності блоку декодування пристрою кодування та декодування факторіальних кодів з виявленням і виправленням помилок для СКК-1 зображена на рис. 3.23.

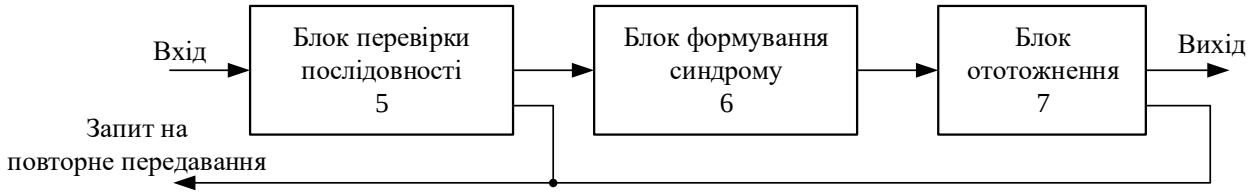


Рис. 3.23. Структурна схема блоку обробки прийнятої послідовності блоку декодування пристрою кодування та декодування ФКВДвп для СКК-1

Прийнятий з каналу зв’язку блок даних поступає на блок перевірки послідовності (5), де виконується перевірка, чи є отримана послідовність перестановкою. Якщо ця умова не виконується, відбувається формування сигналу запиту на повторне передавання отриманого з помилкою блоку. В іншому випадку прийнята перестановка поступає на вхід блоку формування синдрому (6), де послідовно знаходяться синдром перестановки S_F, число A_F та точка D відрізку $[0; M!-1]$, яка відповідає отриманій перестановці. Отримане на виході блоку формування синдрому (6) значення потрапляє на вхід блоку ототожнення (7), де виконується пошук найближчої (в метриці Евкліда) сигнальної точки. У випадку,

якщо існує дві сигнальні точки, відстань до яких однакова і мінімальна, декодер формує сигнал запиту на повторне передавання блоку. Якщо найближча сигнальна точка одна, виконується її зворотне відображення на інтервал $\left[0;2^k-1\right]$. За рівномірного розташування сигнальних точок $A_{10}=\lfloor D/D_{\min}\rfloor$.

Блок обробки прийнятої послідовності для СКК-2 виконує виявлення і виправлення помилок і працює наступник чином. Після отримання з каналу зв'язку блоку даних блок обробки прийнятої послідовності виконує наступні дії:

1) визначає відстань Хеммінга r_i між прийнятим вектором та всіма сигнальними векторами, $i\in\left[0;2^k-1\right]$;
2) знаходить мінімальну відстань $r_{\min}=\min\{r_i\}$;
3) якщо існує єдине $i\in\left[0;2^k-1\right]$: $r_i=r_{\min}$, то прийнятий вектор ототожнюється з i-им сигнальним вектором;
4) якщо існує як мінімум два значення $i,j\in\left[0;2^k-1\right]$: $r_i=r_j=r_{\min}$, то формується сигнал на повторний запит блоку даних.

Таким чином, правила декодування, реалізовані в блоці обробки прийнятої послідовності, базуються на критерії максимальної правдоподібності, а запропонований факторіальний код забезпечує поєднання властивостей кодів з прямим виправленням помилок (ECC) і кодів з виявленням помилок і їх виправленням шляхом перезапиту (EDC).

3.6.4. Оцінка показників достовірності передавання

Помилки, які не виявляються кодом, обумовлені тільки тими перетвореннями, за яких передана перестановка трансформувалася в перестановку, що відповідає будь-якій точці числової осі, найменш віддаленої від іншої сигнальної точки.

Позначимо через $f_{per}^{ud}(i,t)$ кількість помилок ваги t, що призводять до помилкового декодування i-го сигнального вектора. Імовірність не виявленої ФКВД або ФКВДвп помилки

$$P_{ud}\left(FCDRec, p_0\right) = \sum_{i=0}^{2^k-1}\left(P_w\left(i\right) \cdot \sum_{t=1}^{r} f_{per}^{ud}\left(i,t\right) p_0^t q_0^{r-t} \right), \tag{3.26}$$

де $P_w\left(i\right)$ – імовірність застосування джерелом i-го слова, $i \in \left[0, 2^k - 1\right]$.

Визначимо частку φ помилок, що призводять до помилкового декодування:

1) для ФКВД у режимі виявлення помилок: $\varphi = \varphi_{обн} = \left(2^k - 1\right) / M!$;

2) для ФКВДвп у режимі виправлення і виявлення помилок:

$$\varphi = \varphi_{испр} \geq \varphi_{обн} + \frac{2 \cdot \left(2^k - 1\right) \cdot}{M!} = \frac{\left(2^k - 1\right)\left(2\left\lfloor \left(D_{\min} - 1\right)/2 \right\rfloor + 1\right)}{M!}.$$

Оскільки множина помилок, що призводять до помилкового декодування в режимі виправлення і виявлення помилок, містить множину помилок, що призводять до помилкового декодування в режимі виявлення помилок, для $D_{\min} \geq 3$ виконується нерівність $P_{ud}\left(FCDRec, p_0\right) > P_{ud}\left(FCDR, p_0\right)$.

Врахуємо, що для найпростішої системи з ВЗЗ динамічна складова втрати швидкості внаслідок перезапитів $\nu_2 = Q + P_{ud}$. У разі використання коду з виправленням і виявленням помилок справедливим є вираз

$$Q + P_{EC} + P_{det} + P_{ud} = 1, \tag{3.27}$$

де P_{EC} – імовірність, що помилка виправлена;

P_{det} – імовірність виявленої помилки.

Тоді динамічна складова втрати швидкості внаслідок перезапитів для коду з виправленням і виявленням помилок

$$\nu_2 = 1 - P_{det} = Q + P_{EC} + P_{ud}. \tag{3.28}$$

Імовірність виправлення помилок для ФКВДвп:

$$P_{EC}\left(FCDRec, p_0\right) = \sum_{i=0}^{2^k-1}\left(P_w\left(i\right) \cdot \sum_{t=1}^{r} f_{per}^{EC}\left(i,t\right) p_0^t q_0^{r-t} \right), \tag{3.29}$$

де $f_{per}^{EC}\left(i,t\right)$ – кількість помилок ваги t, що виправляються ФКВДвп для i-ої сигнальної точки.

Порівнюючи вираз $\nu_2 = Q + P_{ud}$ для ФКВД і вираз (3.29) для ФКВДвп, можна

бачити, що для режиму виявлення помилок ν_2 і, як наслідок, $\nu_0 = \nu_1 \cdot \nu_2$, нижча, ніж для режиму виправлення і виявлення помилок.

Таким чином, за однакових параметрів і $D_{\min} \geq 3$ ФКВДвп забезпечує більшу відносну швидкість передавання в порівнянні з ФКВД, однак програє в завадостійкості. Енергетичний виграш ΔP для ФКВДвп за оптимального некогерентного прийому двійкових символів обчислюється згідно виразу (2.41).

Відповідно до [273, с. 677],

$$\left(1 - p_{0eq}\right)^N = \left(1 - P_{ud}\right)^{\left\lfloor \frac{N}{k} \right\rfloor \frac{1}{1 - P_{det}}}. \tag{3.30}$$

Вирішуючи рівняння (3.30) відносно p_{0eq} для $p_{0eq}, P_{ud} \ll 1$, можна бачити, що

$$p_{0eq} \approx P_{ud} \Big/ \left(k\left(1 - P_{det}\right)\right). \tag{3.31}$$

Відповідно до (3.27) для системи ФКВД з виправленням і виявленням помилок $1 - P_{det} = Q + P_{EC} + P_{ud}$. Тоді для ФКВДвп вираз (3.31) набуває вигляду:

$$p_{0eq} \approx P_{ud} \Big/ \left(k\left(Q + P_{EC} + P_{ud}\right)\right). \tag{3.32}$$

Залишкова ймовірність помилкового прийому [273, с. 678], під якою розуміється ймовірність того, що комбінація, видана одержувачу, містить хоча б одну помилку, для ФКВДвп дорівнює

$$P_{res} = P_{ud} \Big/ \left(1 - P_{det}\right) = P_{ud} \Big/ \left(Q + P_{EC} + P_{ud}\right). \tag{3.33}$$

У додатку Д розглянуто приклади реалізації ФКВДвп для різних типів СКК, а також виконано їх порівняльну оцінку за наведеними вище показниками.

3.7. Порівняльна оцінка методів нероздільного факторіального кодування інформації

Виконаємо порівняльну оцінку представлених у цьому розділі методів нероздільного факторіального кодування інформації. Для цього перерахуємо їх основні властивості.

Властивості ФКВД:

– забезпечує захист від несанкціонованого читання;

– забезпечує захист від помилок в каналі зв’язку;

– не забезпечує імітозахист;

– має властивість самосинхронізації;

– виключає колізії.

За однакових довжини кодової комбінації і швидкості коду здатність до виявлення помилок у ФКВД для малої довжини блоку даних на вході кодера ($k \le 18$ для $p_0 = 10^{-3}$) вища, ніж у ПФК, однак нижча за CRC-код.

ФКВДд на основі введення додаткових перевірних біт перед перетворенням інформаційного вектора в перестановку, дозволяє підвищити виявляючу здатність ФКВД. Отримані результати для $k \le 1024$ і $p_0 = 10^{-3}$ свідчать про збільшення енергетичного виграшу за оптимального некогерентного прийому двійкових символів у результаті застосування запропонованого методу на величину до 1,6 дБ.

Оскільки кодове слово ФКДКСн складається з кодових слів ФКВД, воно має властивості, характерні для ФКВД. Водночас:

– виявляюча здатність ФКДКСн не поступається ФКВД;

– у більшості випадків виявляюча здатність ФКДКСн поступається ФКВДд.

ФКЗЧІ також має властивості, характерні для ФКВД, однак має більшу виявляючу здатність за рахунок використання для перенесення інформації перестановок, число інверсій в яких належить заданому класу лишків. Таким чином, ФКЗЧІ реалізує обмін швидкості коду на достовірність передавання.

Поєднання функцій прямого виправлення помилок і їх виявлення та виправлення шляхом перезапиту дозволяє підвищити відносну швидкість передавання ФКВД за рахунок зниження завадостійкості коду. Показники завадостійкості ФКВДвп залежать від вибору СКК.

Таким чином, представлені в цьому розділі нероздільні факторіальні коди задовольняють наступним сформульованим у пункті 1.2.6 вимогам,:

1) ФКВД, ФКВДд, ФКДКСн , ФКЗЧІ, ФКВДвп забезпечують виявлення помилок;

2) ФКВДвп забезпечує виправлення помилок;

3) ФКВД, ФКВДд, ФКДКСн ФКЗЧІ, ФКВДвп забезпечують криптографічний захист інформації;

4) ФКВД, ФКВДд, ФКДКСн ФКЗЧІ, ФКВДвп забезпечують циклову синхронізацію без застосування роздільника (прапора) між блоками;

5) ФКВД, ФКВДд, ФКДКСн ФКЗЧІ, ФКВДвп забезпечують організацію замкнутого угруповання абонентів у відкритій мережі.

Властивості всіх розроблених факторіальних кодів наведено в таблиці 3.4.

Таблиця 3.4

Властивості факторіальних кодів

Код	Роздільний	Завадостійкий		Крипто-стійкий	Імітo-стійкий	Само-синхронізується
		виявляє помилки	виправляє помилки			
ПФК	+	+	-	-	+	+
КФК	+	+	-	-	+	-
ФКП	+	+	-	-	-	+
ФКНКСр	+	+	-	-	+	+
ФКВД	-	+	-	+	-	+
ФКВДд	-	+	-	+	-	+
ФКДКСн	-	+	-	+	-	+
ФКЗЧІ	-	+	-	+	-	+
ФКВДвп	-	+	+	+	-	+

За необхідності поєднання властивостей виявлення помилок у каналі зв’язку і захисту інформації від несанкціонованого доступу можна використовувати будь-які модифікації ФКВД. Водночас підвищення достовірності передавання в порівнянні з ФКВД без втрати швидкості коду може бути досягнуто шляхом використання ФКВДд, з втратою швидкості коду – шляхом використання ФКЗЧІ. У разі невисоких вимог до обчислювальних ресурсів кодека може бути використаний ФКДКСн. Достовірність ФКДКСн співвідноситься з ФКВД. Для забезпечення виправлення помилок слід використовувати ФКВДвп.

3.8. Висновки

У третьому розділі дисертації отримано наступні результати:

– вперше розроблено методи нероздільного факторіального кодування

інформації (метод факторіального кодування з відновленням даних за перестановкою, метод факторіального кодування з відновленням даних за перестановкою з доповненням, метод нероздільного факторіального кодування з декількома контрольними сумами, метод факторіального кодування з відновленням даних за перестановкою з заданим числом інверсій, метод факторіального кодування з відновленням даних за перестановкою та виправленням помилок), які за рахунок реалізації єдиної процедури завадостійкого кодування та шифрування шляхом бієктивного перетворення інформаційної послідовності в перестановку чисел заданого порядку, параметри якого тримаються в таємниці, дозволяють забезпечити захист інформації від помилок каналу зв'язку та несанкціонованого доступу, а також підвищити її достовірність під час передавання в телекомунікаційних системах в умовах обмежень пропускної здатності каналів зв'язку;

– розроблено структурні схеми та алгоритми роботи пристроїв кодування та декодування факторіальних кодів (ФКВД(д), ФКЗЧІ, ФКДКСн, ФКВДвп), що надають можливість їх практичної реалізації, дозволяють забезпечити захист інформації від несанкціонованого доступу та помилок каналу зв'язку, а також досягти енергетичний виграш у порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості, зокрема, для ймовірності помилки в каналі зв'язку $p_0 = 10^{-3}$: ФКВД – до 0,821 дБ, ФКЗЧІ – до 3,295 дБ (для порядку перестановки 8).

Розроблені принципи нероздільного факторіального кодування інформації дозволяють розширити науково-технічну базу методів і засобів захисту інформації від несанкціонованого доступу і помилок у каналі зв'язку.

РОЗДІЛ 4. МЕТОД ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ ЛІНІЙНОГО КОНГРУЕНТНОГО МЕТОДУ ТА ЙОГО ЗАСТОСУВАННЯ В КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯХ

4.1. Вступ

У першому розділі детально розглянуто властивості найпростіших ГПВЧ на основі ЛКГ і РЗЛЗЗ. Показано, що недостатньо вивченими є питання, пов’язані з формуванням на основі ЛКГ послідовностей, що складаються з усіх цілих чисел діапазону $[0, M-1]$ (перестановок порядку M), шляхом послідовного обходу вершин графа його станів. Зокрема, в [20], [180] представлено розроблений метод формування ПВП на основі ЛКГ шляхом конкатенації циклів генератора, що дозволило формувати послідовність перестановок. Разом з тим, автором використовуються тільки такі структури графа станів ЛКГ, які містять непересічні цикли. У дисертаційній роботі поставлено задачу розвитку методу побудови ГПВЧ на основі ЛКГ шляхом конкатенації будь-яких зв’язних компонентів графа його станів, для чого необхідно виконати:

1) розширений аналіз топології графів станів ЛКГ;
2) розширений аналіз впливу параметрів ЛКГ на його топологію;
3) удосконалення методу формування ПВП на основі конкатенації зв’язних компонентів графа станів ЛКГ для генерації елементів перетворення інформації в процесі факторіального кодування.

4.2. Моделі формування дискретних випадкових процесів

Визначимо дві моделі формування дискретних випадкових процесів:

1) модель «вилучення без повернення»;
2) модель «вилучення з поверненням».

Для пояснення принципів формування д.в.в. відповідно до цих моделей

розглянемо аналогію з лототроном, у барабан якого поміщені M куль.

Модель «вилучення без повернення» полягає в тому, що з лототрону послідовно витягуються перемішані кулі, витягнута куля в барабан не повертається. Імовірність появи будь-якого з залишених в урні куль залежить від кількості вже витягнутих куль i і дорівнює $p_i = 1/(M-i)$, $i \in [0, M-1]$. Імовірність появи будь-якої з витягнутих куль дорівнює нулю. Після вилучення останньої кулі лототрон заповнюється кулями, процедура перемішування і вилучення куль повторюється.

Модель «вилучення з поверненням» відрізняється від описаної вище тим, що витягнута куля після фіксування її номера поміщається назад у лототрон, а кулі заново перемішуються. Імовірність отримання будь-якої кулі для такої моделі не залежить від кількості вже витягнутих куль і дорівнює $p = 1/M$.

Загалом, модель «вилучення без повернення» реалізують методи і пристрої формування послідовностей випадкових перестановок, а модель «вилучення з поверненням» – методи і пристрої формування послідовностей випадкових чисел з рівномірним законом розподілу.

З урахуванням поставленої задачі, у цьому розділі буде виконано розробку методу формування послідовностей псевдовипадкових чисел за допомогою ЛКГ, який базується на моделі «вилучення без повернення».

У наступному розділі роботи буде виконано аналіз комбінаційного методу формування послідовностей псевдовипадкових чисел за допомогою підсумовування за модулем, який базується на моделі «вилучення з поверненням», а реалізується за допомогою засобів, побудованих на основі моделі «вилучення без повернення».

4.3. Топологія лінійного конгруентного генератора

Дослідимо й узагальнимо структури графа станів ЛКГ. Для цього спочатку проаналізуємо основні підходи до формування графів станів пристроїв формування ПВП.

4.3.1. Графи-цикли

Граф-цикл [285], відомий також як просто n-цикл [286], представляє собою

граф, що містить n вузлів і складається з єдиного циклу, який проходить через усі його вузли. Граф-цикл позначається через C_n. Число вершин у C_n дорівнює числу ребер, кожна вершина має степінь 2 – будь-яка вершина інцидентна двом ребрам.

Графи-цикли використовуються, наприклад, для ілюстрації структури мультиплікативних груп M_n (рис. 4.1). Такі графи формуються шляхом створення пронумерованих вузлів, по одному для кожного елементу α класу лишків, і побудови циклів, отриманих шляхом обчислення α^i для $i = 1, 2, \ldots$. Кожне ребро такого графа має двонаправлений характер [285].

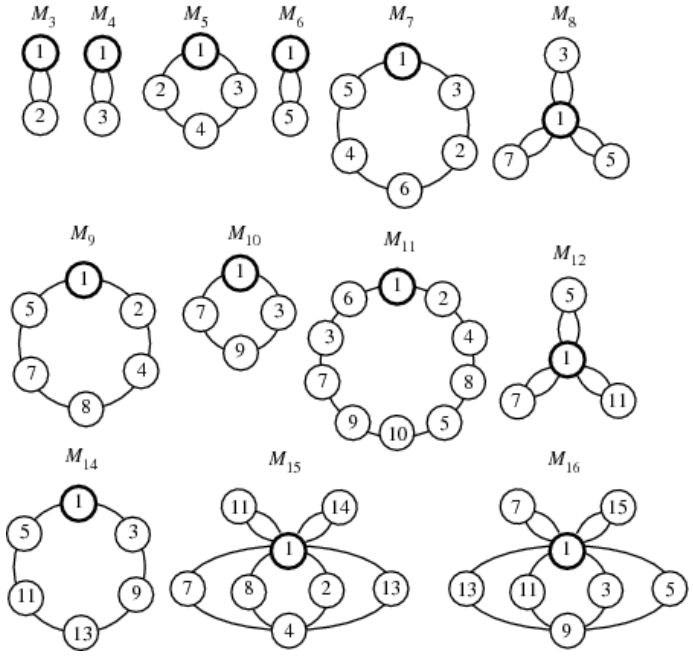


Рис. 4.1. Графи для деяких мультиплікативних груп малого порядку (з [287])

На всіх графах рис. 4.1 вузол з $\alpha = 1$ виділено, оскільки він є нуль-циклом: $\beta_j = \left|\alpha^j\right|_M = \alpha = 1$ за будь-якого j. Далі будемо користуватись таким самим позначенням для відображення нуль-циклів у графі станів ЛКГ.

Зауважимо, що на рис. 4.1 не всі представлені графи є графами-циклами. Це випливає з того, що мультиплікативна група за модулем M може бути ізоморфна добутку декількох циклічних груп (наприклад, $M_8 \leftrightarrow C_2 \times C_2$, а $M_{15} \leftrightarrow C_2 \times C_4$). У цьому випадку граф є об’єднанням декількох графів-циклів.

Зауважимо також, що для візуального відображення структури графа станів

ЛКГ необхідно використовувати орієнтований граф-цикл [51] – орієнтовану версію графа-циклу, в якому всі дуги спрямовані в одному і тому ж напрямку.

4.3.2. Алгебра монад і топологія їх графів

Цей пункт, як і його назва, базується на роботах [288]–[290] В.І. Арнольда.

Визначення 4.1 [288]. Монадою називається відображення скінченної множини в себе. Граф монади має вершинами всі елементи цієї скінченної множини, а орієнтовані ребра з'єднують кожен елемент з його образом.

Іншими словами, граф монади – це довільний скінченний орієнтований граф, з кожної вершини якого виходить рівно одне ребро. Ітерації монади призводять будь-яку вершину до циклу-атрактора, як показує наступна теорема.

Теорема 4.1 [288]. Кожна зв'язна компонента графа монади є лісом з орієнтованих до коріння кореневих дерев, коріння яких з'єднані орієнтованим циклом (топологічно окружністю) з ребер, що з'єднують коріння дерев.

Іншими словами [289], зв'язні компоненти будь-якої монади є циклами-атракторами, оснащеними кореневими деревами, приєднаними своїм корінням до кожної вершини циклу-атрактора. Число вершин циклу може дорівнювати 1. У цьому випадку вся компонента – одне кореневе дерево.

Теорема 4.2 [290]**.** Кожна компонента зв'язності графа будь-якого відображення скінченної множини в себе містить один і тільки один цикл.

Нехай S – скінченна група, а відображення $f : S \to S$ перетворює кожен її елемент $s \in S$ у відповідності до виразу (1.1): $f(s) = |K \cdot s + C|_M$.

Визначення 4.2. Відображення $f : S \to S$ назвемо монадою групи S.

Визначення 4.3 (за [288]). Символами O_n, A_n, T_m, E_n позначимо наступні орієнтовані графи:

O_n = Орієнтований цикл з n вершин;

A_n = Зв'язний граф з $2n$ вершин, що представляє собою цикл довжини n, оснащений n одноребернимі деревами, які входять по одному в кожну з n вершин;

T_{2^n} = Кореневе дерево з $2n$ вершинами і n поверхами крім кореня, яке

розгалужується бінарно на поверхах $1,\ldots,n-1$; корінь вважається нульовим поверхом, і в нього теж входять два ребра: одне – від нього самого і одне – від єдиної вершини першого поверху;

E_n = Кореневе дерево з n вершинами, з кожної з яких ребро веде прямо в корінь (так що $E_2 = A_1 = T_2$);

D_n = $4n$-вершинний граф, що складається з циклу O_n довжини n, оснащеного в кожній своїй вершині трьома вхідними до неї ребрами (утворюють разом з цією належною циклу вершиною кореневе дерево $D_1 = E_4$).

Наприклад, графи монад для адитивних циклічних груп у полі $\mathbb{Z}_n$ мають вигляд, наведений на рис. 4.2.

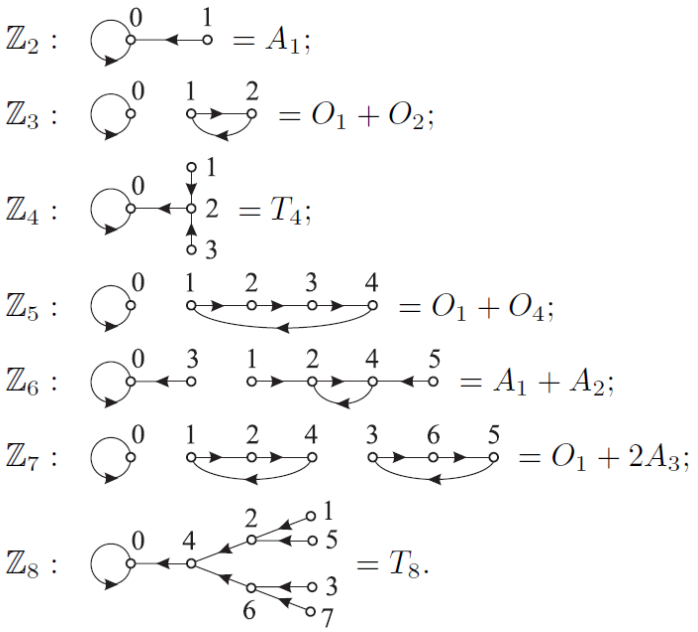


Рис. 4.2. Графи монад деяких найпростіших циклічних адитивних груп (з [288])

Приклади графів монад для мультиплікативних циклічних груп у полі $\mathbb{Z}_n$ мають вигляд, наведений на рис. 4.3.

Визначення 4.4 (за [288]). Добутком $A*B$ монад A і B, які діють на X і Y відповідно, називається монада, яка діє на прямому добутку $X*Y$ покомпонентно: $(A*B)(x,y) = (Ax*By)$. Число елементів монади-добутку дорівнює добутку чисел елементів монад-співмножників.

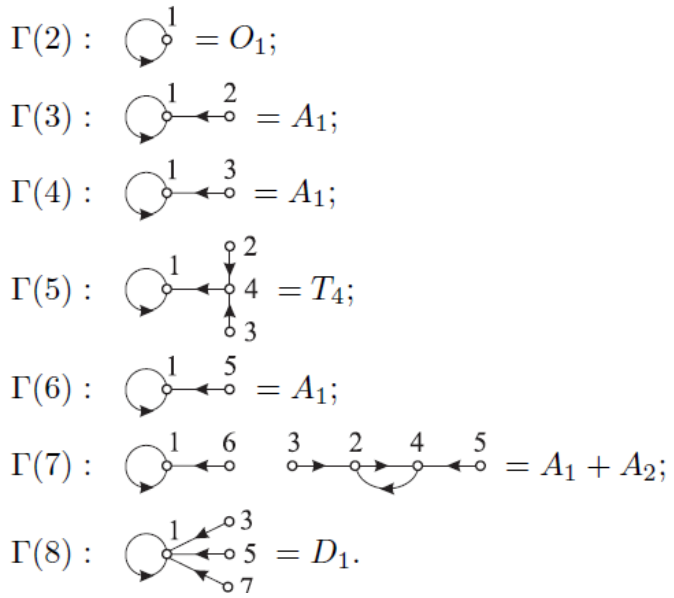


Рис. 4.3. Графи монад деяких найпростіших груп Ейлера (з [288])

Визначення 4.5 (за [288]). Граф монади-добутку є добутком графів співмножників: $\left[граф\left(A*B\right)\right]=\left[граф\left(A\right)\right]*\left[граф\left(B\right)\right]./\ A_n=A_1*O_n,\ D_n=D_1*O_n.$

Множення будь-якого кореневого дерева T на O_n оснащує n-цикл O_n кореневими деревами виду T з корінням в усіх точках циклу.

4.3.3. Графи лінійного конгруентного генератора

Приклади графів монад групи S для деяких параметрів ЛКГ зображено в таблиці Е.1 додатку Е.

Структури графів монад групи S ЛКГ для всіх можливих параметрів за $M \le 20$ представлено в таблиці Е.2 додатку Е.

Узагальнимо проаналізовані структури і представимо в таблиці Е.3 додатку Е деякі типові графи, характерні для ЛКГ. Нуль-циклом будемо називати цикл, що складається з одного елементу, і позначати його через O_1.

Розширюючи наведені в [50], [180] закономірності, наведемо деякі графи станів ЛКГ і параметри, для яких ці графи характерні:

1) O_M – для:

а) $M \ge 2,\ K=1,\ C=1;$

б) $M = 2^p$, $K = 4l + 1$, $C = 2m + 1$, $l, m \in \mathbb{Z} \geq 0$;

в) M – простого, $K = 1$, $C \geq 1$;

2) dO_t – для $M = 2^p$, $K = 4l - 1$, $l \in \mathbb{Z} \geq 1$, і $C = 2m + 1$, $m \in \mathbb{Z} \geq 0$. За цих умов:

а) для $l = 2^{k-2}$ $\left(K = 2^k - 1\right)$, $k \geq 2$, має місце $t = 2M/\left(K + 1\right)$ і $d = \left(K + 1\right)/2$ (або $t = 2^{p-l+1}$, $d = 2^{l-1}$);

б) для $l = 2k - 1$ $\left(K = 8k - 5\right)$, $k \geq 1$, має місце $t = M/2$ і $d = 2$;

в) для $l = 2k$, $k \geq 1$, $K \neq 2^r - 1$, $r \geq 3$ (тобто $k \neq 2^{r-3} : k = 2^{i-4}\left(2j + 1\right)$, а $l = 2^{i-3}\left(2j + 1\right)$ $\left(K = 2^{i-1}\left(2j + 1\right) - 1\right)$ для $j \in \left[1; 2^{p-i} - 1\right]$, $i \in \left[4; p - 1\right]$) має місце $t = M/2^{i-2}$, $d = 2^{i-2}$;

3) $dO_t + O_1$ – для M – простого, $K \geq 2$, $C \in \mathbb{Z}$;

4) дерево з коренем – нуль-циклом – для $M = 2^p$, $K \in \left\{2l : l \in \mathbb{N}, 0 < l < 2^{p-1}\right\}$, $C \in \left\{0, 1, \ldots, 2^p - 1\right\}$, $p \in \mathbb{N}$.

Зауважимо, що наведені в таблиці Е.3 графи можуть також бути представлені у вигляді матриць інцидентності.

4.3.4. Узагальнений граф станів лінійного конгруентного генератора

Аналіз можливих графів станів ЛКГ показує, що всі вони можуть бути зведені до єдиної конфігурації, що містить множину з d циклів однакової або різної довжини, включаючи нуль-цикли, та множину з d' передциклів (дерев), що приводять до циклів. За цих обставин

$$M = \sum_{i=1}^{d} t_i + \sum_{j=1}^{d'} t_j', \tag{4.1}$$

де t_i – довжина i-го циклу;

t_j' – кількість вершин у j-му дереві за винятком кореня.

Узагальнений граф ЛКГ може бути представлений у наступному вигляді:

$$G_{LCG} = \left(V_{LCG}, A_{LCG}\right),$$

де V_{LCG} – множина вершин графа;

A_{LCG} – множина дуг графа.

У свою чергу,

$$V_{LCG} = \{v_k\} \cup \{v_l^{'}\},$$

де $\{v_k\}$ – множина вершин, що належать циклам, $k = 1,2,\ldots,\sum_{i=1}^{d} t_i$;

$\{v_l^{'}\}$ – множина вершин, що належать деревам, за винятком їх коренів, $l = 1,2,\ldots,\sum_{j=1}^{d'} t_j^{'}$;

$$A_{LCG} = \{a_k\} \cup \{a_l^{'}\},$$

де $\{a_k\}$ – множина дуг, що належать циклам, $k = 1,2,\ldots,\sum_{i=1}^{d} t_i$;

$\{a_l^{'}\}$ – множина дуг, що належать деревам, $l = 1,2,\ldots,\sum_{j=1}^{d'} t_j^{'}$.

Відповідно до [179], за простого M справедливі вирази $d' = 0$, $t_i = t$ для $\forall i \in [1, d-1]$ і $t_d = 1$, а вираз (4.1) набуває вигляду: $M = \sum_{i=1}^{d-1} t + 1$.

Представимо узагальнений граф станів ЛКГ в термінах теорії алгебри монад і топології їх графів.

Таблиця Е.3 показує, що ніяких більш складних візерунків, крім добутків дерев і циклів, у графах монад відображення $f : S \to S$ не зустрічається: граф ЛКГ є незв'язне об'єднання циклів, оснащених добутками дерев. Оскільки $E_n = T_{n^1} * O_1, A_t = T_{2^1} * O_t$, $D_t = T_{4^1} * O_t$, кожну зв'язну компоненту графа ЛКГ можна представити у вигляді $T_{a^n} * \left(T_{b^m} * O_t\right)$. Так наприклад, $O_t = T_{a^0} * \left(T_{b^0} * O_t\right)$, а $A_t = T_{a^0} * \left(T_{2^1} * O_t\right) = T_{2^1} * \left(T_{b^0} * O_t\right)$, $E_n = T_{a^0} * \left(T_{n^1} * O_1\right) = T_{n^1} * \left(T_{b^0} * O_1\right)$. Тоді узагальнений граф станів ЛКГ має вигляд:

$$G_{LCG} = \sum_{i=1}^{d} d_i \left(T_{a_i^{n_i}} * \left(T_{b_i^{m_i}} * O_{t_i}\right)\right), \tag{4.2}$$

де d – число різних типів компонент зв'язності графа станів ЛКГ;

d_i – число компонент зв'язності графа станів ЛКГ i-го типу;

a_i, n_i, b_i, m_i, t_i – параметри компонент зв'язності графа станів ЛКГ i-го типу.

У цьому випадку $\sum_{i=1}^{d} d_i a_i^{n_i} b_i^{m_i} t_i = M$.

Визначення правил обчислення числа компонент графа $\sum_{i=1}^{d} d_i$, їх типів d і значень чисел a_i, n_i, b_i, m_i, t_i через параметри ЛКГ виходить за рамки цієї роботи і вимагає подальших досліджень.

Визначимо деякі властивості топології ЛКГ.

4.4. Дослідження впливу параметрів лінійного конгруентного генератора на його топологію

Ядром процедури створення ЛКГ є вибір параметрів K, C, M у залежності від заданих вимог до вихідної послідовності або в залежності від вимог до конкретної конфігурації графа станів кінцевого автомата. Зміна хоча б одного з цих параметрів призводить до зміни конструкції графа станів генератора. Виходячи з цього, визначимо зв'язок параметрів K, C, M з топологією графа станів ЛКГ.

4.4.1. Ізоморфізм графів лінійного конгруентного генератора і циклічної групи для простого M

У роботі [179] показано, що за простого M множина M цілих чисел відрізка $[0, M-1]$ на виході ЛКГ розбивається на d непересічних підмножин: $(d-1)$ підмножин M_j однакової потужності T, причому $M = \bigcup_{j=1}^{d-1} M_j$, $\bigcap_{i \neq j} M_i M_j = \varnothing$, а $M - 1 = (d-1) \cdot T$, і одну підмножину потужності 1.

У термінах алгебри монад і їх топологій це означає, що граф монади $f(s) = |K \cdot s + C|_M$ групи S має d компонент зв'язності: $G_{LCG}\big|_{M-\text{просте}} = (d-1)O_T + O_1$,

$T=(M-1)/(d-1)$.

Крім того, в [179] показано, що розв'язок в цілих числах рівняння

$$q_T M-(K^T-1)s_0=C(K^T-1)/(K-1) \tag{4.3}$$

визначає зв'язок довжини циклів T з параметрами K, C, M. З іншого боку, для заданої довжини циклів T вираз (4.3) дозволяє визначити параметр K і ВПЗ s_0 для формування необхідної конфігурації циклів ЛКГ.

Запропонований спосіб є обчислювально складним, особливо за великих значень параметрів K, C, M.

Спираючись на результати роботи [13], визначимо параметри ЛКГ, що забезпечують формування циклів довжини T з розкладання (1.2).

Зазначимо, що математична модель процесу обчислення конгруентних чисел за рівнянням (1.1) є ітераційним процесом на основі обчислення залишку за заданим модулем M. Аналогічний ітераційний процес має місце під час формування елементів циклічної групи з операцією множення в $\mathbb{Z}_M$:

$$\beta_j=\left|\alpha^j\right|_M=\left|\alpha\cdot\beta_{j-1}\right|_M, \tag{4.4}$$

де β_j – елемент циклічної групи;

α – твірний елемент циклічної групи.

Доведемо ізоморфізм графів циклічної групи (4.4) і ЛКГ.

Теорема 4.3. Кожна відмінна від O_1 компонента зв'язності графа ЛКГ з параметрами K, C і простим модулем M ізоморфна графу циклічної групи $\langle K\rangle$ у $\mathbb{Z}_M$ з операцією множення і твірним елементом K, $1<K<M$.

Доведення.

Кожен елемент циклічної групи $\langle K\rangle$ з твірним елементом K $(1<K<M)$ обчислюється таким чином:

$$\beta_j=\left|K^j\right|_M=\left|K\cdot\beta_{j-1}\right|_M, \tag{4.5}$$

Нехай порядок такої циклічної групи дорівнює T. Тоді $\beta_0=\left|K^0\right|_M=1=\left|K^T\right|_M=\beta_T$, причому для $\forall j:0<j<T$ $\left|K^j\right|_M\neq 1$.

Як показано в [291], M -й елемент конгруентної послідовності

$$s_m = \left| K^m s_0 + C\sum_{i=0}^{m-1} K^i \right|_M = K^m s_0 + C\left(K^m - 1\right)\Big/\left(K-1\right) - q_m M\,, \tag{4.6}$$

де q_m – неповна частка від ділення $K^m s_0 + C\left(K^m - 1\right)\Big/\left(K-1\right)$ на M.

Тоді елемент s_T конгруентної послідовності визначається наступним чином:

$$s_T = \left| K^T s_0 + C\left(K^T - 1\right)\Big/\left(K-1\right)\right|_M. \tag{4.7}$$

З огляду на властивості адитивності та мультиплікативності лишків:

$$s_T = \left| K^T s_0 + C\left(K^T - 1\right)\Big/\left(K-1\right)\right|_M = \left\| K^T s_0 \right|_M + \left| C\left(K^T - 1\right)\Big/\left(K-1\right)\right|_M \Big|_M =$$

$$= \left\| \left\| K^T \right|_M \left| s_0 \right|_M \right|_M + \left\| C \right|_M \left| \left(K^T - 1\right)\Big/\left(K-1\right)\right|_M \Big|_M \Big|_M .$$

В останньому виразі $\left|K^T\right|_M = \beta_T = \beta_0 = 1$, а $\left|s_0\right|_M = s_0$, оскільки $s_0 < M$.

Оскільки $\left|K^T\right|_M = 1$, а $1 < K < M$, справедливо $\left|\left(K^T - 1\right)\Big/\left(K-1\right)\right|_M = 0.$

Тому $s_T = \left\| s_0 \right|_M + \left\| C \right|_M \cdot 0 \Big|_M \Big|_M = s_0$.

Доведемо, що $T = \min\left(t\right)\Big|_{S_t = S_0}$. Нехай існує $T_1 < T$: $s_{T_1} = s_0$.

Скориставшись (4.6), отримаємо: $s_{T_1} = \left| K^{T_1} s_0 + C\left(K^{T_1} - 1\right)\Big/\left(K-1\right)\right|_M = s_0.$

Враховуючи що $s_T = s_0$, маємо

$\left| K^{T_1} s_0 + C\left(K^{T_1} - 1\right)\Big/\left(K-1\right)\right|_M = s_0 = \left| K^T s_0 + C\left(K^T - 1\right)\Big/\left(K-1\right)\right|_M$ або

$\left| K^T s_0 - K^{T_1} s_0 + C\left(K^T - 1\right)\Big/\left(K-1\right) - C\left(K^{T_1} - 1\right)\Big/\left(K-1\right)\right|_M = 0.$ Звідси

$\left| s_0\left(K^T - K^{T_1}\right) + C\left(K^T - K^{T_1}\right)\Big/\left(K-1\right)\right|_M = 0$ або $\left|\left(K^T - K^{T_1}\right)\Big/\left(K-1\right)\left(s_0\left(K-1\right) + C\right)\right|_M = 0.$

Для простого M і $K < M$ остання рівність справедлива за умови $\left|K^T - K^{T_1}\right|_M = 0$ або $\left|s_0\left(K-1\right) + C\right|_M = 0$.

Оскільки $\left|K^T\right|_M = 1$, а $\left|K^{T_1}\right|_M \neq 1$ $\left(T_1 < T\right)$, має місце $\left|K^T - K^{T_1}\right|_M \neq 0$.

Вираз $\left|s_0\left(K-1\right) + C\right|_M = 0$ описує нуль-цикл O_1 ЛКГ.

Дійсно, для нуль-циклу виконується $s_1 = s_0$ або $s_0 = \left|Ks_0 + C\right|_M$. Оскільки $s_0 < M$, $\left|s_0\right|_M = \left|Ks_0 + C\right|_M$, звідки $\left|s_0(K-1) + C\right|_M = 0$ або $s_0(K-1) + C = q_1 M$.

Рівність $s_0 = (Mq_1 - C)/(K-1)$ виконується, якщо чисельник дробу кратний знаменнику, тобто $Mq_1 - C = (K-1)q_2$ або

$$Mq_1 - (K-1)q_2 + C = 0. \tag{4.8}$$

Отримане рівняння (4.8) є рівнянням першої степені з двома невідомими q_1 і q_2. Відповідно до [292], це рівняння розв'язується в цілих числах, якщо M і $(K-1)$ взаємно прості. Оскільки для простого M будь-яке $K < M$ є взаємно простим до нього, які б M і K не були, рівняння (4.8) завжди має розв'язок:

$$\begin{cases} q_1 = (-1)^{n-1} CQ_{n-1} - (K-1)t, \\ q_2 = (-1)^n CP_{n-1} + Mt, \end{cases} \tag{4.9}$$

де $t = 0, \pm 1, \pm 2 \ldots$;

n – порядок ланцюгового дробу розкладання $M/(K-1)$,

P_{n-1} і Q_{n-1} – чисельник і знаменник ланцюгового дробу відповідно.

Крім того, в [179] доведено, що під час розв'язання в цілих числах рівності $s_0 = (Mq_1 - C)/(K-1)$ $s_0 < M$ і q_1 визначаються єдиним чином (нуль-цикл – єдиний).

Таким чином, період відмінного від нуль-циклу циклу ЛКГ з параметрами K, C, M відповідає порядку циклічної групи з твірним елементом K. Тому відмінні від O_1 цикли графа ЛКГ з K, C і простим модулем M ізоморфні циклу графа циклічної групи $\langle K \rangle$ у $\mathbb{Z}_M$ з операцією множення і твірним елементом K. ■

Для спрощення визначення параметрів ЛКГ, які забезпечують формування циклу O_T періоду T, на основі доведеної теореми визначимо деякі залежності порядку циклічної групи від твірного елементу $K \in [2, M-1]$.

Властивість 1. Порядки циклічних груп $\langle K_1 \rangle$ і $\langle K_2 \rangle$ з твірними елементами K_1 і K_2 відповідно, причому $\left|K_1 \cdot K_2\right|_M = 1$, і модулем M рівні між собою, а елементи циклічних груп, що формуються за (4.5), слідують у зворотному порядку.

Доведення.

З умови $\left|K_1 \cdot K_2\right|_M = 1$ випливає, що елементи K_1 і K_2 є прямим і зворотним елементами циклічної групи. Нехай порядок циклічної групи $\langle K_1 \rangle$ з твірним елементом K_1 дорівнює T. Тоді $\beta_T = \left|K_1^T\right|_M = \beta_0 = 1.$ Враховуючи скінченність циклічної групи $\langle K_1 \rangle$, отримаємо: $\beta_j = \left|K_1^j\right|_M = \left|K_1^{T-(T-j)}\right|_M = \left|\left|K_1^T\right|_M \cdot \left(K_1^{-1}\right)^{T-j}\right|_M = \left|\left(\left|K_1^{-1}\right|_M\right)^{T-j}\right|_M = \left|{K_2}^{T-j}\right|_M$. Звідси випливає, що порядки циклічних груп $\langle K_1 \rangle$ і $\langle K_2 \rangle$ з твірними елементами K_1 і K_2 відповідно рівні між собою, а елементи циклічних груп, які формуються згідно з (4.5), слідують у зворотному порядку. ■

Властивість 2. За простого M циклічну групу порядку два завжди породжує тільки елемент $K = M - 1.$

Доведення.

Якщо елемент K є твірним для циклічної групи порядку два, то $\left|K^2\right|_M = 1$ або

$$K^2 = q \cdot M + 1, \tag{4.10}$$

де $q \neq 0.$

Оскільки $K < M$, справедливо $K^2 = q \cdot M + 1 > q \cdot K + 1,$ звідки $q < \left(K^2 - 1\right)/K$ або $q < K - 1/K$. Оскільки $q \in \mathbb{Z},\ q \leq K - 1.$

З виразу (4.10) випливає, що $M = \left(K^2 - 1\right)/q = \left(K - 1\right)\left(K + 1\right)/q$. Якщо M – просте, необхідною умовою виконання цієї тотожності є: $\left|q\right|_{K-1} = 0$ або $\left|q\right|_{K+1} = 0$.

Оскільки $q \leq K - 1,$ рівність $\left|q\right|_{K+1} = 0$ розв'язків не має. Тому єдиним розв'язком рівняння $\left|q\right|_{K-1} = 0$ для $q \leq K - 1$ є $q = K - 1.$ Підставляючи його в вираз (4.10), отримаємо $K^2 = \left(K - 1\right) \cdot M + 1,$ звідки $M = K + 1$ або $K = M - 1.$ ■

Властивість 3. Якщо елемент K є твірним елементом циклічної групи порядку T, то елемент $K_1 = K^i$ є твірним елементом циклічної групи порядку $T_1 = T/НСД\left(T, i\right).$

Доведення.

Якщо $K_1 = K^i$, то $\left|K_1^1\right|_M = \left|K^i\right|_M$, $\left|K_1^2\right|_M = \left|K^{2i}\right|_M$, а $\left|K_1^l\right|_M = \left|K^{li}\right|_M$ – обчислений за (4.5) l-тий елемент циклічної групи $\langle K_1 \rangle$ відповідає обчисленому за (4.5) li-тому елементу циклічної групи $\langle K \rangle$. Тому мінімальне значення T_1, за якого $\left|K_1^{T_1}\right|_M = \left|K^T\right|_M = 1$, дорівнює $T_1 = T / НСД(T,i)$. ■

З властивості 3 слідують два загальновідомих наслідки.

Наслідок 1. У якості твірного елементу для циклічної групи $\langle K \rangle$ порядку T може виступати не тільки K, а й ті його степені K^i, для яких $НСД(T,i) = 1$.

Наслідок 2. Кількість твірних елементів для циклічної групи порядку T дорівнює $\varphi(T)$.

Приклад 1. Визначити порядки всіх утворюючих $\langle K \rangle$ елементів для $M = 17$.

Складемо таблицю з усіх значень K $(0 < K < M)$ і відповідних їм порядків T.

Таблиця 4.1

Твірні елементи циклічної групи та їх порядки для $M = 17$

K	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
T	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

Заповнення таблиці виконується наступним чином.

Оскільки $M = 17$, ненульові елементи поля $\mathbb{Z}_M$ $\{1,2,\ldots,16\}$ утворюють групу відносно множення. Порядок цієї групи дорівнює $M - 1 = 16$.

Порядки циклічних груп можуть набувати значень з розкладання $M - 1 = 16$ на множники, тобто з набору $\{1,2,4,8,16\}$. Це твердження також випливає з прямих наслідків теореми Лагранжа [293]:

- порядок будь-якої підгрупи скінченної групи ділить порядок групи;
- порядок будь-якого елементу скінченної групи ділить порядок групи.

Відповідно до властивості 2, елемент $K = M - 1 = 16$ породжує циклічну групу порядку $T = 2$. З урахуванням властивості 3 і її наслідку 1, порядки елементів $K = 2$, $K = 4$, $K = 8$ дорівнюють $T = 8$, $T = 4$ і $T = 8$ відповідно. Відповідно до властивості 1, однакові порядки мають елементи $K = 2$ і $K = 9$, $K = 3$ і $K = 6$, $K = 4$ і $K = 13$,

$K=5$ і $K=7$, $K=8$ і $K=15$, $K=10$ і $K=12$, $K=11$ і $K=14$. Тому порядки елементів $K=9$, $K=13$, $K=15$ дорівнюють $T=8$, $T=4$, $T=8$ відповідно.

Кількість елементів, що породжують мультиплікативну групу $\mathbb{Z}_M^{\times}$ кільця лишків за модулем M, дорівнює $\varphi(M-1)=\varphi(16)=8$. Тоді порядки всіх елементів з множини $\{3,5,6,7,10,11,12,14\}$ дорівнюють $T=16$.

Таким чином, кількість твірних елементів для циклічних груп порядку $T=1$, $T=2$, $T=4$, $T=8$ і $T=16$ дорівнюють відповідно 1, 1, 2, 4 і 8, що підтверджується наслідком 2 властивості 3.

Приклад 2. Визначити параметри K і C ЛКГ для $M=17$, граф станів якого має два цикли з періодами $T=8$.

Згідно з теоремою 4.3, період відмінного від нуль-циклу циклу ЛКГ відповідає порядку циклічної групи $\langle K\rangle$. Відповідно до таблиці 4.1 порядок $T=8$ мають елементи $K\in\{2,8,9,15\}$. Тому граф станів ЛКГ для $M=17$ має два цикли з періодами $T=8$ для наступних його параметрів: $K\in\{2,8,9,15\}$, $0\le C\le M-1$.

Наприклад, для $K=9$ і $C=4$ стани ЛКГ приймають значення, наведені в таблиці 4.2. Для побудови циклів ЛКГ використано принцип, викладений у [19].

Таблиця 4.2

Стани ЛКГ для $K=9$, $C=4$, $M=17$

ВПЗ	s_i							
$s_0=0$	$s_1=4$	$s_2=6$	$s_3=7$	$s_4=16$	$s_5=12$	$s_6=10$	$s_7=9$	$s_8=0$
$s_0=1$	$s_1=13$	$s_2=2$	$s_3=5$	$s_4=15$	$s_5=3$	$s_6=14$	$s_7=11$	$s_8=1$

Одна з можливих реалізацій надциклу після конкатенації двох представлених циклів, а також нуль-циклу $s_0=8$ набуває вигляду: $(0,4,6,7,16,12,10,9,1,13,2,5,15,3,14,11,8)$.

Таким чином:

– параметри ЛКГ для формування ПВП за простого M можуть бути визначені з використанням формули (4.5) замість (4.3), що є обчислювально більш простою операцією;

– сформульовані властивості, що стосуються залежності порядку циклічної

групи від твірного елементу K, дозволяють істотно (більш, ніж у два рази) скоротити об'єм обчислень у порівнянні з формулою (4.3);

– запропонована процедура вибору параметрів ЛКГ дозволяє визначити всі значення параметра K, за яких генератор породжує циклічну конгруентну послідовність заданої довжини T.

Отримані результати призводять до спрощення процедури вибору параметрів ЛКГ для формування циклів конгруентної послідовності заданої довжини.

4.4.2. Кількість нуль-циклів у графі станів лінійного конгруентного генератора

Оскільки довжина нуль-циклу дорівнює 1, підставивши $T=1$ і $s_T = s_0$ у вираз (4.7), отримаємо рівняння для зв'язку параметрів ЛКГ під час його формування:

$$\left|(K-1)s_0 + C\right|_M = 0. \tag{4.11}$$

Спираючись на [16], [294], сформулюємо твердження, що визначають умови існування і кількість нуль-циклів у графі станів ЛКГ.

Теорема 4.4. Точка $s_0 = 0$ є нуль-циклом у графі станів ЛКГ тоді і тільки тоді, коли $C = 0$.

Доведення.

Поклавши в (4.11) $s_0 = 0$, отримаємо $|C|_M = 0$. Оскільки $C < M$, $C = 0$.

Якщо ж $C = 0$, то $s_0 = 0$ є коренем рівняння (4.11) і породжує нуль-цикл. ■

Зауваження 1. Для $C = 0$ вираз (4.11) має вигляд $\left|(K-1)s_0\right|_M = 0$, звідки $(K-1)s_0 = qM$, де q – частка від ділення $(K-1)s_0$ на M, $q \in \mathbb{Z}$, $q \geq 0$. З умови $K, s_0 < M$ випливає $(K-1)s_0 < M^2 - M$ і, відповідно, $0 \leq q < M-1$.

Зауваження 2. Для простого M і $1 < K < M$ коренем рівняння $\left|(K-1)s_0\right|_M = 0$ є тільки $s_0 = 0$. Таким чином, для простого M і $C = 0$ існує тільки один нуль-цикл, який розташовується в точці $s_0 = 0$.

Зауваження 3. Для складеного M розв'язком рівняння $\left|(K-1)s_0\right|_M = 0$ можуть бути кілька пар чисел (K, s_0), серед яких $s_0 = 0$ для $\forall K$. Якщо $НСД(K-1, M) = 1$, нуль-цикл $s_0 = 0$ єдиний.

Теорема 4.5. Для існування нуль-циклу в графі станів ЛКГ необхідно і достатньо, щоб значення C було кратне $НСД(K-1, M)$.

Доведення.

З виразу (4.11) випливає, що $(K-1)s_0 + C = qM$, де q – неповна частка від ділення $(K-1)s_0 + C$ на M, $q \in \mathbb{Z}$, $q \geq 0$.

Нехай $a = K-1$; $x = s_0$; $b = M$; $y = q$, $c = C$. тоді вираз $(K-1)s_0 + C = qM$ матиме такий вигляд:

$$ax - by + c = 0. \tag{4.12}$$

Нехай $e = НСД(K-1, M) = НСД(a, b)$. Тоді рівняння (4.12) перетворюється до виду: $(a'x - b'y)e + c = 0$, де $a' = a/e$, $b' = b/e$, і згідно з [292], може мати цілі рішення тільки в тому випадку, коли C ділиться на e. ■

Визначимо взаємозв'язок параметрів і ВПЗ для ЛКГ, що призводять до формування нуль-циклу. Будемо вважати, що $e = НСД(K-1, M) = НСД(a, b) = 1$. У іншому випадку рівність (4.12) може бути зведена до вигляду $a'x - b'y + c' = 0$, де $c' = c/e$, а a' і b' взаємно прості: $НСД(a', b') = 1$.

Розглянемо спочатку випадок, коли $c = C = 0$. Тоді $ax - by = 0$, звідки $x = by/a$. Очевидно, що $x \in \mathbb{Z}$ тоді і тільки тоді, коли $\left|y\right|_a = 0$, тобто для $y = ai$, де $i \in \mathbb{Z}$. Тоді $x = bi$. Введемо обмеження для параметрів і невідомих рівняння (4.12):

$$0 \leq a < b-1;\ 0 \leq x < b;\ 0 \leq y < b-1;\ 0 \leq c < b. \tag{4.13}$$

З урахуванням того, що $x = bi$ і $x < b$, єдиним цілим розв'язком рівняння $ax - by = 0$ є $x = 0$, $y = 0$. Виконуючи зворотну заміну, отримаємо $s_0 = 0$.

Таким чином, для $C = 0$ і взаємно простих $a = K-1$ і $b = M$ у графі станів ЛКГ існує тільки один нуль-цикл, який розташовується в точці $s_0 = 0$, що підтверджує положення зауважень до теореми 4.4.

Для $c \neq 0$, відповідно до теореми 1 з [292], усі розв'язки рівняння (4.12) мають вигляд: $x = x_0 + bi$, $y = y_0 + ai$, де x_0, y_0 – будь-який розв'язок рівняння (4.12), $i \in \mathbb{Z}$. Оскільки $0 \le x < b$, єдиним розв'язком залишається $x = x_0$ і, відповідно, $y = y_0$.

Таким чином, для взаємно простих $K-1$ і M нуль-цикл – єдиний. У загальному випадку відповідь на питання про кількість нуль-циклів у структурі графа станів ЛКГ дає наступна теорема.

Теорема 4.6. Кількість нуль-циклів у графі станів ЛКГ дорівнює $e = НСД(K-1, M)$ (для $|C|_e = 0$).

Доведення.

Перетворимо вираз (4.12) до виду $a'x - b'y + c' = 0$, де $a' = a/e, b' = b/e$, $c' = c/e$, $e = НСД(a,b)$. Для того, щоб це рівняння мало розв'язок у цілих числах, необхідно, щоб $c' \in \mathbb{Z}$.

Вираз $a'/b' = a/b = (K-1)/M$ розкладемо в ланцюговий дріб виду $(K-1)/M = P_n/Q_n$, де n – порядок ланцюгового дробу. Відповідно до [292], розв'язок рівняння $a'x - b'y + c' = 0$ має вигляд: $x = (-1)^{n-1} Q_{n-1} c/e + bi/e$, $y = (-1)^{n-1} P_{n-1} c/e + i\,a/e$, $i \in \mathbb{Z}$. З урахуванням зворотної заміни

$$\begin{aligned} s_0 &= (-1)^{n-1} \frac{C}{e} Q_{n-1} + \frac{M}{e} i, \\ q &= (-1)^{n-1} \frac{C}{e} P_{n-1} + \frac{K-1}{e} i. \end{aligned} \tag{4.14}$$

З $s_0 = (-1)^{n-1} Q_{n-1} C/e + iM/e$, а також з обмеження $0 \le s_0 < M$ випливає, що параметр i може приймати рівно e значень, таких що $s_0 \in [0, M-1]$. Тому кількість нуль-циклів у графі станів ЛКГ дорівнює значенню $e = НСД(K-1, M)$. ■

Зауваження 1. Для $K = 1$ і $C \neq 0$ граф станів ЛКГ не містить жодного нуль-циклу. У цьому випадку граф станів ЛКГ буде містити $d = НСД(M, C)$ циклів довжиною $t = M / НСД(M, C)$.

Зауваження 2. Для $K = 1$ і $C = 0$ граф станів ЛКГ завжди містить M нуль-циклів.

Зауваження 3. Для $K>1$ і $C=0$ граф станів ЛКГ завжди містить e нуль-циклів у точках $s_0 = Mi/e$, $i=0,1,\ldots,e-1$.

Зауваження 4. Для $K=2$ граф станів ЛКГ завжди містить один нуль-цикл, який розташовується в точці $s_0 = |M-C|_M$.

Зауваження 5. Якщо $e=K-1$, то $(K-1)/M = 1/\big(M/(K-1)\big) = P_n/Q_n$. У цьому випадку $n=2$, $P_{n-1}=0$, $Q_{n-1}=1$, а $s_0 = -C/e + Mi/e$, де $i=0,1,\ldots,K-2$.

Приклад 1. Нехай $K=11$, $C=5$ і $M=15$. Визначимо, в яких точках розташовуються нуль-цикли ЛКГ з такими параметрами.

Значення $e = НСД(K-1,M)=5$. Зауважимо, що $|C|_e = 0$. Ланцюговий дріб $\dfrac{K-1}{M} = \dfrac{10}{15} = \dfrac{2}{3} = \dfrac{1}{1+\dfrac{1}{2}}$. Тоді відповідно до (4.14) $s_0 = 1+3i$, $q = 1+2i$. Для забезпечення умови $0 \le s_0 < M$ необхідно, щоб $i \in \{0,1,2,3,4\}$. Тоді нуль-цикли ЛКГ з параметрами $K=11$, $C=5$ і $M=15$ розташовуються в точках $s_0 \in \{1,4,7,10,13\}$.

Приклад 2. Нехай $K=6$, $C=5$ і $M=15$. Також визначимо, в яких точках розташовуються нуль-цикли ЛКГ з такими параметрами.

Значення $e = НСД(K-1,M) = НСД(5,15) = 5$. Зауважимо, що $|C|_e = 0$, а $e = K-1$. Згідно з зауваженням 5 до теореми 4.6, нуль-цикли ЛКГ розташовуються в точках $s_0 = -1+3i$, де $i=1,2,\ldots,5$. Тоді $s_0 \in \{2,5,8,11,14\}$.

Теорема 4.7. Максимальна кількість нуль-циклів у графі станів ЛКГ з параметрами M і $K>1$ досягається для $K = Mk/p+1$ і $C = Mc/p$, де p – мінімальний множник в розкладанні числа M на прості множники, k і c – будь-які цілі числа, що задовольняють умовам $1 \le k < p$ і $0 \le c < p$.

Доведення.

Згідно з теоремою 4.6, кількість нуль-циклів у графі станів ЛКГ дорівнює значенню $e = НСД(K-1,M)$.

Представимо число M у вигляді

$$M = p_1^{l_1} p_2^{l_2} \cdot \ldots \cdot p_n^{l_n},$$

де p_i – прості множники, $p_i > 1$, $p_i < p_{i+1}$, $l_i > 0$, $i \le n$.

Оскільки $K < M$, значення $e = НСД(K-1, M)$ досягає свого максимального значення, якщо $K - 1 = Mk / p_1 = kp_1^{l_1 - 1} p_2^{l_2} \cdot \ldots \cdot p_n^{l_n}$, де k – будь-яке ціле число, $1 \le k < p_1$.

Згідно з теоремою 4.5, для існування нуль-циклів необхідно, щоб значення C було кратне $e = НСД(K-1, M)$. Якщо $K - 1 = Mk / p_1$, то $e = НСД(K-1, M) = M / p_1$. З урахуванням теореми 4.5, а також умови $C < M$, параметр $C = Mc / p_1$, де c – будь-яке ціле число, $0 \le c < p_1$. ■

Приклад. Визначимо, за яких параметрів K і C ЛКГ досягається максимальна кількість нуль-циклів у його графі станів для $M = 300$.

Для цього представимо $M = 300$ у вигляді добутку степенів простих чисел: $M = p_1^{l_1} p_2^{l_2} \cdot \ldots \cdot p_n^{l_n} = 2^2 \cdot 3^1 \cdot 5^2$. Мінімальний множник у такому розкладі – $p = p_1 = 2$. Тоді, відповідно до теореми 4.7, для досягнення максимальної кількості нуль-циклів $K = Mk / p + 1 = 150k + 1$, $C = Mc / p = 150c$. Змінні k і c можуть приймати будь-які значення з діапазонів $1 \le k < p$ і $0 \le c < p$ – $1 \le k < 2$ і $0 \le c < 2$, звідки $k = 1$, $c \in \{0,1\}$. Тому $K = 151$, $C \in \{0,150\}$. Кількість нуль-циклів ЛКГ $d = 150$.

Зауваження. За необхідності виконання умови взаємної простоти параметрів K і M у теоремі 4.7 значення p обирається рівним мінімальному множнику в розкладанні числа M на прості множники, для якого $\exists k : НСД(K, M) = 1$.

Теорема 4.8. Граф станів ЛКГ з параметром M не має нуль-циклів тоді і тільки тоді, коли:

1) $C \ne 0$ для $K = 1$;

2) $e = НСД(K-1, M) > 1$ і $|C|_e \ne 0$ для $K > 1$.

Доведення.

Згідно з теоремою 4.5, для існування нуль-циклу необхідно і достатньо, щоб параметр C був кратний $e = НСД(K-1, M)$.

Для того, щоб нуль-циклів у графі станів ГСЧ не існувало, рівняння $ax - by + c = 0$ або $(a'x - b'y)e + c = 0$ (з урахуванням замін, введених під

час доведення теореми 4.5) не повинно мати цілочисельних розв'язків. Це виконується тільки за умов:

1) $c = C \neq 0$ для $a = 0$ $(K = 1)$;

2) $e = НСД(a,b) = НСД(K-1, M) > 1$ і $|c|_e = |C|_e \neq 0$ для $a > 0$ $(K > 1)$.

Якщо для $K = 1$ $C = 0$, рівняння (4.12) зводиться до виду $by = 0$ і, згідно з зауваженням 2 теореми 4.6, граф станів ЛКГ завжди буде мати M нуль-циклів.

Якщо ж $|C|_e = 0$ для $e > 1$ і $K > 1$, то рівняння $a'x + b'y + c' = 0$ (див. теорему 4.6) завжди має цілочисельні розв'язки, кількість яких – $e = НСД(K-1, M)$. ■

Методика вибору параметрів ЛКГ, граф станів якого не має нуль-циклів, полягає в наступному:

1) обирається модуль M, що визначає область визначення д.в.в.;
2) з множини $[1, M-1]$ обирається K: $K = 1$ або $НСД(K-1, M) > 1$;
3) якщо $K = 1$, параметр C обирається довільним чином з множини цілих чисел діапазону $[1, M-1]$. За цих умов, відповідно до зауваження 1 теореми 4.6., граф станів ЛКГ буде містити $d = НСД(M, C)$ циклів довжиною $t = M / НСД(M, C)$;
4) якщо параметр K обраний таким чином, що $K > 1$ і $e = НСД(K-1, M) > 1$, параметр C обирається довільним чином з множини цілих чисел діапазону $[1, M-1]$, які задовольняють умові $|C|_e \neq 0$.

Зауважимо, що для того, щоб граф станів ЛКГ не містив дерев і мав вигляд $G_{LCG} = \sum_{i=1}^{d} d_i O_{t_i}$, відповідно до [150] значення K у пункті 2 наведеної методики необхідно обирати таким чином, щоб $НСД(K, M) = 1$.

Приклад 1. Визначимо для $M = 15$ усі параметри K і C ЛКГ, граф станів якого не містить нуль-циклів.

Перший параметр $K = 1$. Тоді $C \in \{1, 2, \ldots, 14\}$. Оберемо параметри K відповідно до умови $НСД(K-1, 15) > 1$. Цій умові задовольняють значення

$K \in \{4,6,7,10,13\}$. Відповідно до наведеної вище методики визначимо параметри $C : |C|_e \neq 0$ для значень K і зведемо їх у таблицю 4.3.

Таблиця 4.3

Параметри K і C ЛКГ для $M = 15$, граф станів якого не містить нуль-циклів

K	C
$K = 1$	$C \in \{1,2,\ldots,14\}$
$K = 4$	$C \in \{1,2,4,5,7,8,10,11,13,14\}$
$K = 6$	$C \in \{1,2,3,4,6,7,8,9,11,12,13,14\}$
$K = 7$	$C \in \{1,2,4,5,7,8,10,11,13,14\}$
$K = 10$	$C \in \{1,2,3,4,6,7,8,9,11,12,13,14\}$
$K = 13$	$C \in \{1,2,4,5,7,8,10,11,13,14\}$

Виконаємо формування перестановки чисел порядку M за допомогою ЛКГ для $K = 13$ і $C = 2$. Результати формування надциклу зведемо в таблицю 4.4.

Таблиця 4.4

Послідовність циклів на виході ЛКГ з параметрами $K = 13$, $C = 2$, $M = 15$

ВПЗ	s_i										
$s_0 = 0$	$s_1 = 2$	$s_2 = 13$	$s_3 = 6$	$s_4 = 5$	$s_5 = 7$	$s_6 = 3$	$s_7 = 11$	$s_8 = 10$	$s_9 = 12$	$s_{10} = 8$	$s_{11} = 1$
$s_0 = 4$	$s_1 = 9$	$s_2 = 14$									

Як можна бачити з таблиці 4.4, граф станів такого ЛКГ містить два цикли з довжинами 12 і 3. Таким чином, для складених M граф станів ЛКГ не обов'язково складається з циклів однакової довжини.

Приклад 2. Визначимо всі параметри K і C, за яких граф станів ЛКГ з параметром $M = 2^p$ не містить нуль-циклів.

Перший параметр $K = 1$. Тоді $C \in \left[1, 2^p - 1\right]$.

Значення параметра $K > 1$, що задовольняють умові $e = НСД\left(K - 1, 2^p\right) > 1$, складають множину чисел виду $2l + 1$, де $p, l \in \mathbb{N}$, $0 < l < \left(2^p - 1\right)/2$. Тоді $e = 2^m$,

$m \in \mathbb{N}$, $0 < m < p$. Значення параметра C, що задовольняють умові $|C|_e \neq 0$, складають множину чисел виду $en + c = 2^m n + c$, де $c, n \in \mathbb{N}$, $0 < c < e$, $0 \le n < \lfloor 2^{p-m} \rfloor$.

Отримані результати зведемо в таблицю 4.5.

Таблиця 4.5

Параметри K і C ЛКГ для $M = 2^p$, $p \in \mathbb{N}$, граф станів якого не містить нуль-циклів

K	C
$K = 1$	$C \in \{1, 2, \ldots, 2^p - 1\}$
$K = 2l + 1,$ $l \in \mathbb{N},\ 0 < l < \dfrac{2^p - 1}{2}$	$C = 2^m n + c,\ m = \log_2 НСД\left(K - 1, 2^p\right),$ $c, n \in \mathbb{N},\ 0 < c < 2^m,\ 0 \le n < \lfloor 2^{p-m} \rfloor$

Наприклад, для $M = 32 = 2^5$ параметри K і C можуть набувати значень, наведених у таблиці 4.6.

Таблиця 4.6

Параметри K і C ЛКГ для $M = 32$, граф станів якого не містить нуль-циклів

K	C
$K = 1$	$C \in \{1, 2, \ldots, 31\}$
$K \in \{3, 7, 11, 15, 19, 23, 27, 31\}$	$C \in \{1, 3, \ldots, 31\}$
$K \in \{5, 13, 21, 29\}$	$C \in \begin{Bmatrix} 1,2,3,\ 5,6,7,\ 9,10,11, \\ 13,14,15,\ 17,18,19, \\ 21,22,23,\ 25,26,27, \\ 29,30,31 \end{Bmatrix}$
$K \in \{9, 25\}$	$C \in \begin{Bmatrix} 1,2,3,4,5,6,7, \\ 9,10,11,12,13,14,15, \\ 17,18,19,20,21,22,23, \\ 25,26,27,28,29,30,31 \end{Bmatrix}$
$K = 17$	$C \in \begin{Bmatrix} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15, \\ 17,18,19,20,21,22,23,24,25,26,27,28,29,30,31 \end{Bmatrix}$

Теорема 4.9. Граф станів ЛКГ з параметром M має один нуль-цикл тоді і тільки тоді, коли $e = НСД(K-1, M) = 1$.

Доведення.

Граф станів ЛКГ має один нуль-цикл, якщо рівняння $(K-1)s_0 + C = qM$ має один розв'язок. Розв'язком рівняння є $s_0 = (-1)^{n-1} Q_{n-1} C/e + Mi/e$, де $e = НСД(K-1, M)$, $i = 0, \pm 1, \pm 2...$ (див. доведення теореми 4.6). Для того, щоб розв'язок був єдиним $(s_0 \in [0, M-1])$, необхідно, щоб $e = 1$. Тоді $s_0 = (-1)^{n-1} CQ_{n-1} + Mi$, де значення i обирається, щоб $s_0 \in [0, M-1]$.

Якщо ж $e = НСД(K-1, M) > 1$, то відповідно до теорем 4.6 і 4.8, нуль-циклів або не існує, або їх кількість більша одного. ■

Зауваження. Число значень параметра K, за якого для заданого M граф станів ЛКГ містить тільки один нуль-цикл, дорівнює $\varphi(M) - 1$.

Приклад 1. Визначимо всі параметри K і C ЛКГ для $M = 15$, за яких у його графі станів міститься тільки один нуль-цикл.

Виберемо параметри $K < M$ відповідно до умови $e = НСД(K-1, M) = 1$. Цій умові задовольняють значення $K \in \{2, 3, 5, 8, 9, 12, 14\}$. Тоді параметр $C \in \{0, 1, \ldots, 14\}$.

Виконаємо формування перестановки чисел порядку M за допомогою ЛКГ, наприклад, для $K = 8$ і $C = 2$. Результати формування зведемо в таблицю 4.7.

Таблиця 4.7

Послідовність циклів на виході ЛКГ з $K = 8$, $C = 2$, $M = 15$

ВПЗ	$s_0 = 0$	$s_0 = 1$	$s_0 = 4$	$s_0 = 5$	$s_0 = 9$
s_i	$s_1 = 2$	$s_1 = 10$		$s_1 = 12$	$s_1 = 14$
	$s_2 = 3$	$s_2 = 7$		$s_2 = 8$	
	$s_3 = 11$	$s_3 = 13$		$s_3 = 6$	

Як можна бачити з таблиці 4.7, граф станів такого ЛКГ містить три цикли довжиною 4, один цикл довжиною 2 і один нуль-цикл в точці $s_0 = 4$.

Приклад 2. Визначимо всі параметри K і C, за яких граф станів ЛКГ з параметром $M = 2^p$, $p \in \mathbb{N}$, містить один нуль-цикл.

Значення параметра K, що задовольняють умові $e = НСД\left(K-1, 2^p\right) = 1$, складають множину чисел виду $2l$, де $l \in \mathbb{N}$, $0 < l < 2^{p-1}$. Параметр $C \in \left\{0,1,\ldots,2^p-1\right\}$.

Наприклад, для $M = 32 = 2^5$ параметри K і C можуть набувати наступних значень: $K \in \left\{2l : l \in \mathbb{N}, 0 < l < 16\right\}$ (тобто $K \in \left\{2,4,6,\ldots,30\right\}$), $C \in \left\{0,1,\ldots,31\right\}$.

Наведені в цьому пункті теореми дозволяють вибирати параметри ЛКГ з заданою кількістю нуль-циклів у його графі станів. Зауважимо, що найбільш зручними з точки зору конкатенації циклів є структури, які містять нуль-циклів.

4.5. Опис методу формування послідовностей псевдовипадкових чисел на основі лінійного конгруентного методу

Основною ідеєю розробленого методу формування послідовностей псевдовипадкових чисел є послідовний обхід контуру графа станів ЛКГ для отримання послідовності довжиною M чисел, рівномірно розподілених у діапазоні $[0, M-1]$. У результаті такої процедури формується перестановка чисел порядку M.

Згідно з визначенням 1.8, надциклом називається послідовність слів ЛКГ, отримана шляхом конкатенації всіх циклів ЛКГ в єдиний цикл довжиною M. Довизначимо його і сформулюємо наступне визначення.

Визначення 4.1. Надциклом називається послідовність слів ЛКГ, отримана шляхом конкатенації всіх зв’язних компонентів (циклів і передциклів (дерев)) ЛКГ у єдиний цикл довжиною M.

Якщо під час формування ПВП порядок обходу графа станів залишається незмінним протягом усього часу роботи генератора, він буде формувати періодично повторювану перестановку порядку M. У випадку зміни порядку обходу графа станів після формування кожного надциклу буде формуватися ПВП перестановок.

Сутність пропонованого методу полягає в перетворенні будь-якого типу графа ЛКГ до типу 1.1 за рахунок конкатенації всіх зв’язних компонентів – циклів і

передциклів (дерев). Для побудови ГПВЧ з рівномірним розподілом чисел на відрізку $[0, M-1]$ топологія графа ЛКГ принципової ролі не грає, однак для спрощення конструкції ГПВЧ доцільно використовувати графи типу 1.4.

Для графів з непересічними циклами без передциклів (дерев) до початку формування послідовності визначаються представники кожного циклу (ВПЗ) та їх довжини. У процесі формування послідовності по черзі, в певному порядку, в ЛКГ завантажуються ВПЗ і формуються відповідні їм цикли. Після перебору всіх представників циклів утворюється надцикл. Така послідовність є періодичною з періодом $T = M$. Подібні послідовності можуть застосовуватися для формування таблиці перестановки, зокрема, для факторіального кодування, або в задачах, де необхідна довжина послідовності, менша за M, або наявність кореляції допустима.

Для формування гіперциклу порядок чергування циклів змінюється.

Наприклад, для графа типу 1.4 значення d і t є дільниками M. Це означає, що множина цілих чисел відрізка $[0, M-1]$ може бути розділена на d підмножин потужності t слів кожна. Представимо елементи таких d підмножин у вигляді, наведеному на рис. 4.4 [16]. Таку конструкцію будемо називати основною матрицею ЛКГ з непересічними циклами.

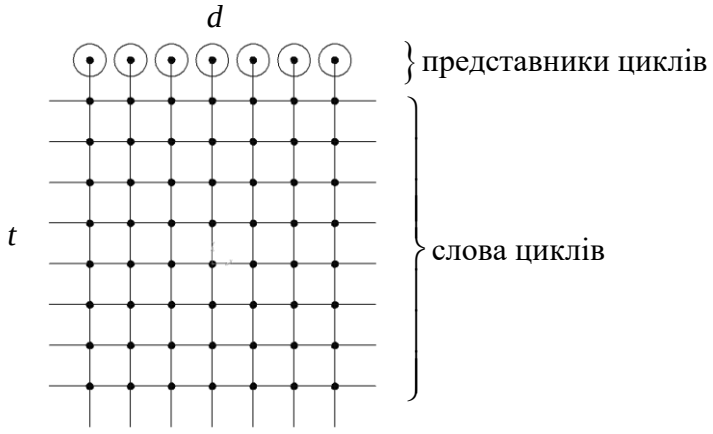


Рис. 4.4. Основна матриця ЛКГ з непересічними циклами

Формування слова основної матриці відбувається наступним чином. Визначаються два випадкових числа d_i і t_i. Перше визначає представника циклів, який завантажується в ЛКГ в якості ВПЗ. Друге число є номером слова в циклі, яке

обчислюється, наприклад, за формулою (4.6), і виводиться на вихід генератора. Так триває доти, поки не будуть перебрані всі d представників циклів і всі t слів.

Для збільшення періоду повторення послідовності в наступних циклах проводиться перестановка стовпців і рядків основної матриці. У цьому випадку зменшується кореляція між словами, інтервал між суміжними однойменними словами стає випадковим із середнім значенням, рівним M , а максимальний період повторення послідовності досягає значення $L_{gc} = M \cdot d! \cdot t^d$.

За умови, якщо граф станів ЛКГ містить як цикли (включаючи нуль-цикли), так і передцикли (дерева), їх конкатенація відбувається таким чином.

Поточний ВПЗ ЛКГ визначається шляхом вибору з множини цілих чисел діапазону $[0, M-1]$. ЛКГ із заданими параметрами формує послідовність псевдовипадкових чисел доти, поки числа на його виході не повторяться. У разі повторної появи будь-якого елементу, не обов'язково рівного ВПЗ, формування послідовності припиняється. За цих умов сформовані числа відповідають усім вузлам деякого циклу ЛКГ і, можливо, всім вузлам або їх частині одного з передциклів (дерева) цього циклу.

Далі визначається новий поточний ВПЗ ЛКГ шляхом його вибору з множини цілих чисел діапазону $[0, M-1]$, за винятком уже сформованих. Після цього ЛКГ з новим ВПЗ знову формує ПВП до повторної появи елементу, однак уже у всій сформованій послідовності. Така процедура триває до тих пір, поки всі елементи множини цілих чисел відрізка $[0, M-1]$ не будуть сформовані.

З урахуванням викладеного, вдосконалений метод формування ПВП на основі використання ЛКГ полягає в наступному:

1) у разі необхідності (наприклад, для підвищення швидкості формування ПВП або виконання вимог щодо просторової складності алгоритму, який реалізує запропонований метод) визначаються тип графа станів ЛКГ, а також умови, яким повинні задовольняти параметри K, C і M ЛКГ для отримання заданого типу структури. Визначення типу графа станів ЛКГ може проводитися відповідно до представлених у таблиці Е.3 типових графів, а

вибір зазначених параметрів – за допомогою теорем і властивостей, сформульованих у підрозділі 4.3 цієї роботи. За цих умов параметр M визначає область визначення псевдовипадкової величини. У разі, якщо вибір типу графа станів не проводиться, параметри ЛКГ визначаються довільним чином з урахуванням пред'явлених до них обмежень;

2) у разі необхідності (наприклад, за непересічних циклів графа станів ЛКГ без передциклів (дерев) для підвищення швидкості формування послідовності псевдовипадкових чисел) визначаються представники кожного циклу генератора (ВПЗ), які записуються в пам'ять;
3) визначається поточний ВПЗ ЛКГ шляхом вибору (випадкового або детермінованого) з множини збережених ВПЗ, якщо цю множину задано, або з множини цілих чисел діапазону $[0, M-1]$;
4) формується послідовність псевдовипадкових чисел за допомогою ЛКГ з заданими параметрами доти, поки генератор формує неповторювані числа. У разі повторної появи будь-якого елементу (не обов'язково рівного ВПЗ (для графа, що містить непересічні цикли без передциклів (дерев) – рівного ВПЗ)) формування поточного відрізка послідовності припиняється;
5) визначається новий поточний ВПЗ ЛКГ шляхом його вибору (випадкового або детермінованого):
   5.1) з множини ще не використаних ВПЗ, якщо цю множину задано;
   5.2) з множини цілих чисел діапазону $[0, M-1]$ за винятком чисел, присутніх у сформованій частини ПВП;
6) формується ПВП для заданого ВПЗ до повторної появи елементу в сформованій послідовності (для графа, що містить непересічні цикли без передциклів (дерев) – рівного поточному ВПЗ);
7) перехід до п.5 до перебору всіх ВПЗ;
8) перехід до п.3 до перебору всіх комбінацій послідовно використовуваних у п.п. 3 і 5 ВПЗ (якщо вони задаються і зберігаються в пам'яті);
9) перехід до п.2 до перебору всіх комбінацій ВПЗ (якщо вони задаються і зберігаються в пам'яті).

Таким чином, запропонований метод дозволяє виконувати конкатенацію не тільки відокремлених і непересічних циклів у графі станів ЛКГ, а й передциклів (дерев), якщо вони в ній містяться.

Крім того, запропоновані підходи можуть бути використані для формування послідовностей псевдовипадкових чисел на основі РЗЛЗЗ з довільним генераторним поліномом. Це пояснюється тим, що використання звідного полінома в якості генераторного для РЗЛЗЗ призводить до збільшення числа і зміни структури зв'язних компонентів у графі станів генератора [45], [295], [296].

4.6. Пристрій формування послідовностей псевдовипадкових чисел

Пристрій формування ПВП на основі ЛКГ поєднує в собі:

- ЛКГ – виконує обчислення за формулою (4.6);
- керуючий автомат – виконує конкатенацію всіх зв'язних компонентів графа станів ЛКГ (циклів і передциклів (дерев)) у один надцикл довжиною M ;
- стохастичний автомат – виконує зміну порядку обходу графа станів ЛКГ.

Для підвищення стійкості породжуваної ПВП алгоритми роботи керуючого і стохастичного автоматів тримаються в секреті. Тоді потужність ключового простору визначається кількістю і структурою зв'язних компонентів графа станів ЛКГ.

Для ЛКГ з графами станів, що належать типам 1.1-1.7, структурна схема пристрою формування ПВП на основі ЛКГ приймає вигляд, показаний на рис. 4.5.

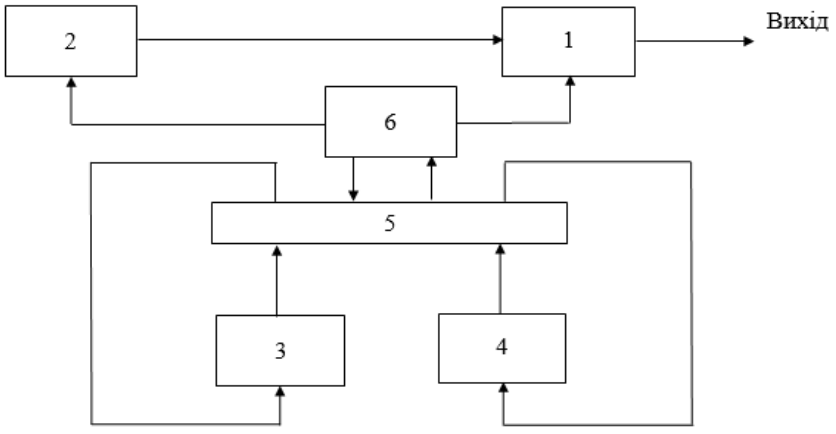


Рис. 4.5. Структурна схема пристрою формування ПВП на основі ЛКГ з непересічними циклами без передциклів (дерев) у його графі станів

Пристрій формування ПВП містить ЛКГ 1, запам’ятовувальні пристрої (ЗП) 2, 3 і 4, блок 5, що слугує для перемішування в кожному з надциклів порядку слів у ЗП 3 і 4, і керуючий пристрій 6. Запам’ятовувальні пристрої ЗП 2, 3 і 4 зберігають:

1) представників циклів;
2) перерахованих у випадковому порядку чисел $\{1,2,\ldots,d\}$, де d – кількість циклів у графі станів ЛКГ;
3) перерахованих у випадковому порядку чисел $\{1,2,\ldots,t\}$.

До початку застосування (наприклад, під час виготовлення) генератора в ЗП 2 вносяться отримані розрахунковим шляхом представники циклів, включаючи представника нуль-циклу. У ЗП 3 вносяться розміщені у випадковому порядку числа $\{1,2,\ldots,d\}$, а в ЗП 4 вносяться розміщені у випадковому порядку числа $\{1,2,\ldots,t\}$.

З початком застосування генератора керуючий пристрій 6 вибирає з ЗП 3 і 4 по одному слову, утворюючи пару $\{d_i,t_i\}$. З ЗП 2 вибирається представник циклу, що знаходиться в комірці d_i. Якщо цей представник не породжує нуль-цикл, то він завантажується в якості ВПЗ в генератор 1, який обчислює слово, віддалене на t_i кроків від ВПЗ, за допомогою виразу (4.6). Отримане слово видається на вихід пристрою, формування першого слову завершено. Якщо число d_i є адресою елементу, що породжує нуль-цикл, то з ЗУ 2 цей елемент видається безпосередньо на вихід генератора. Під час генерації наступних слів процедура повторюється. Керуючий пристрій 6 виконує:

– контроль однократного включення в породжувану на виході генератора послідовність елементу, що породжує нуль-цикл, і блокування спроб його повторного включення в надцикл;
– контроль одноразового застосування кожної з пар $\{d_i,t_i\}$ і блокування спроб введення в генератор однакових пар у межах надциклу.

Після завершення формування надциклу за командою керуючого пристрою 6 пристрій перестановки 5 виконує перестановку слів у ЗП 3 і 4. Далі процес формування випадкової послідовності чисел повторюється. Використання випадкового порядку формування слів у кожному надциклі, а також однократне

застосування пар $\{d_i, t_i\}$ у надциклі гарантують однакову ймовірність появи слів у послідовності на виході генератора.

Структурна схема пристрою формування послідовностей псевдовипадкових чисел на основі ЛКГ з будь-яким графом станів приймає вид, наведений на рис. 4.6.

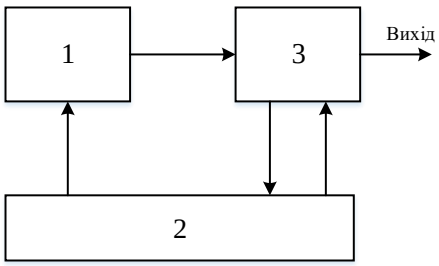


Рис. 4.6. Структурна схема пристрою формування послідовностей псевдовипадкових чисел на основі ЛКГ з будь-яким графом станів

Поточний ВПЗ ЛКГ вибирається з множини цілих чисел діапазону $[0, M-1]$ і завантажується в ЛКГ 1, який формує послідовність чисел і записує їх у ЗП 3. ПВП формується доти, поки генератор формує неповторювані числа. У разі, якщо сформоване ЛКГ число вже міститься в ЗП 3, формування поточного відрізка послідовності припиняється. Визначається новий ВПЗ ЛКГ, що не рівний будь-якому з чисел, що зберігаються в ЗП 3. Формування ПВП триває до повторної появи елементу в ЗП 3, після чого формується новий ВПЗ. Така процедура триває до формування всіх цілих чисел діапазону $[0, M-1]$. ЗП 3 буде містити надцикл ЛКГ.

На вихід пристрою числа можуть надходити двома способами:

1) послідовно після безпосереднього формування елементу послідовності і перевірки його унікальності в ЗП 3;
2) послідовно або паралельно після формування надциклу в ЗП 3.

Після видачі сформованого надциклу на вихід пристрою послідовність ЗП 3, стирається, а процедура формування нового надциклу повторюється.

Крім того, представляється можливим розширити область визначення функції розподілу д.в.в. до множини всіх цілих чисел відрізка $[0, M'-1]$. Для цього необхідно сформувати вектор-рядок додаткових слів множини, що включає слова,

які довизначають функцію розподілу. У цьому випадку формування послідовності включає два незалежних процеси:

- обчислення основних слів за допомогою ЛКГ;
- розстановка додаткових слів (у випадковому порядку).

Порядок розташування основних слів і порядок розстановки додаткових слів змінюються для кожного надциклу.

Сукупність зазначених операцій призводить до формування рівномірно розподіленої послідовності з M' слів.

Запропоновані підходи до побудови пристрою формування ПВП на основі ЛКГ використано для створення програмних реалізацій генераторів [19], [297].

У таблиці 4.8 наведено допустимі значення параметрів генераторів для забезпечення максимального періоду ПВП.

Таблиця 4.8

Параметри ГПВЧ для досягнення максимального періоду ПВП

Метод	Період	Допустимі значення параметрів ГПВЧ	Розмір простору допустимих значень параметрів ГПВЧ
Лінійний конгруентний метод	$T = M$	1) $НСД(C, M) = 1$; 2) $\lvert K-1\rvert_p = 0$ для $\forall$ простого $p : \lvert M\rvert_p = 0$; 3) якщо $\lvert M\rvert_4 = 0 \Rightarrow \lvert K-1\rvert_4 = 0$.	$\varphi(M)\cdot P$, де P – кількість значень K, що задовольняють умовам 2 і 3.
Метод на основі РЗЛЗЗ	$T = 2^n - 1$	Генераторний поліном $G_n(x)$ – примітивний.	Відповідає кількості примітивних поліномів степені n
Метод формування ПВП на основі конкатенації циклів ЛКГ	$T = M$	$НСД(K, M) = 1$.	$\varphi(M)\cdot M$.
Метод формування ПВП на основі конкатенації циклів РЗЛЗЗ	$T = 2^n$	Генераторний поліном $G_n(x)$ породжує циклічну структуру графа станів РЗЛЗЗ.	Відповідає кількості поліномів степені n, які породжують циклічну структуру графа станів РЗЛЗЗ
Запропонований метод	$T = M$	$K, C < M$.	M^2.

Виконаємо дослідження швидкості роботи програмної реалізації генератора перестановок на основі розробленого методу та порівняємо її з швидкістю роботи генератора, що реалізує сучасний алгоритм Фішера-Йєтса. Для об'єктивності оцінки генератори реалізовано на одній платформі та досліджено на одному комп'ютері з фіксованими показниками продуктивності. Результати зведемо в таблицю 4.9.

Швидкість роботи розробленого генератора перевищує швидкість роботи генератора перестановок із застосуванням алгоритму Фішера-Йєтса.

Варто зазначити, що ПВП, яка формується відповідно до запропонованого методу, не є криптографічно стійкою і її не можна застосовувати в «чистому» вигляді в криптографічних перетвореннях, наприклад, у якості гами поточного шифру. Разом з тим, запропоновані підходи до формування ПВП можуть бути використані для реалізації багатоетапної процедури шифрування. Виконаємо розробку такого методу криптографічного перетворення інформації.

Таблиця 4.9

Порівняльний аналіз швидкості формування послідовності перестановок

Метод	Первинний ГПВЧ	Швидкість формування (слів/сек)				
		$M=20$	$M=50$	$M=100$	$M=150$	$M=200$
Фішера-Йєтса	LFIB78	86000	86000	85200	85050	85000
	MarsaLFIB4	73400	73500	73600	73800	73850
	DX-47-3	77300	78600	78500	78400	78300
Метод формування ПВП на основі конкатенації циклів ЛКГ		234373	209190	177012	154609	138816
Запропонований метод		179506	137845	100636	71536	67235

4.7. Метод двоконтурного криптографічного перетворення даних

Відомі методи потокового шифрування [187] передбачають генерацію рівномірно розподіленої послідовності символів (слів) гами. Гаму підсумовують посимвольно з символами відкритого тексту, в результаті отримують шифртекст. Стійкість такої криптосистеми визначається стійкістю гами шифру.

Перш за все, зазначимо, що завдання створення рівномірно розподіленої

послідовності псевдовипадкових чисел на основі ЛКГ з будь-топологією графа станів вирішується шляхом використання запропонованого в підрозділі 4.5 методу. Так, для ЛКГ за фіксованого M і різних значень параметрів K і C шляхом конкатенації циклів і передциклів (дерев) можна отримати різні за структурою надцикли періоду M. Крім того, запропонований у [44], [180] метод дозволяє формувати надцикл для генераторів на основі РЗЛЗЗ. За цих обставин різні генераторні поліноми однієї і тієї ж степені будуть давати різні за структурою послідовності періоду M.

Звернемо увагу на те, що сума слів в надциклі дорівнює

$$\sigma = M\left(M-1\right)/2. \qquad (4.15)$$

З цього випливає, що якщо використовувати ковзне вікно з M слів і порахувати суму слів у цьому вікні, то рівність суми значенню (4.15) з певною ймовірністю свідчить про знаходження меж надциклу. З одного боку, ця обставина може бути використаною для вирішення задачі синхронізації надциклу, а з іншого боку – суттєво полегшує процедуру криптоаналізу.

У цій роботі не ставиться задача розгляду циклової синхронізації або криптостійкості в повному обсязі – це предмет окремого дослідження. Зазначимо лише, що для підвищення криптографічної стійкості послідовності можна скористатися додатковою процедурою формування нелінійної ПВП, наприклад, шляхом композиції послідовності надциклу ЛКГ з М-послідовністю, період T якої дорівнює великому простому числу Мерсенна. У цьому випадку умова (4.15) буде виконуватися не на надциклі, а на відрізку з T надциклів. Суттєвим є те, що для виконання пошуку циклової фази криптоаналітику необхідно проводити пошук циклової фази на відрізку з T надциклів, у той час як законному користувачеві для пошуку циклової фази достатньо 3-5 надциклів (з урахуванням коефіцієнта накопичення за входом). Тому застосування зазначеної композиції в процесі встановлення синхронізації не дозволяє криптоаналітику гарантовано отримати послідовність з T надциклів, оскільки процедура пошуку циклової фази законними користувачами закінчується значно раніше. Законні користувачі виходять з режиму синхронізації і переходять до режиму пересилання даних.

Разом з тим, оскільки ймовірність входження криптоаналітика в синхронізм не дорівнює нулю, для ускладнення процедури криптоанализу доцільно ввести другий контур шифрування. Запропоновані рішення можуть служити підставою для розробки методу двоконтурного шифрування даних, основні принципи якого викладені в роботах автора [22], [23].

4.7.1. Опис методу

Розроблений метод відноситься до обчислювальної техніки і може бути використаний для криптографічного захисту даних у телекомунікаційних системах і мережах. Метод двоконтурного шифрування може бути застосований для обміну конфіденційними даними каналами зв'язку будь-якої фізичної природи, незахищеними від несанкціонованого доступу до циркулюючої в них інформації.

Сутністю пропонованого методу криптографічного перетворення є створення нелінійної гами шляхом композиції генераторів на основі ЛКГ і РЗЛЗЗ у першому контурі шифрування, а також введення другого контуру криптоперетворення на іншому ключі й іншим способом.

Перший контур шифрування включає процедури:

- формування нелінійної гами, шляхом, наприклад, обчислення рівнозначності послідовності на основі ЛКГ та послідовності на основі допоміжного рекурсивного генератора на регістрі зсуву. Така операція забезпечує підвищення рівня приховування закону утворення гами;
- посимвольне додавання нелінійної гами з символами відкритого тексту, утворюючи шифртекст першого контуру.

Другий контур виконує повторне шифрування – кожне слово з виходу першого контуру шифрування розщеплюється на два слова d і t меншої розрядності – n_1 і n_2. Закон розщеплення може триматися в таємниці та представляти собою частину ключа. Отримані значення d і t підсумовуються відповідно за модулем 2^{n_1} і 2^{n_2} зі значеннями, сформованими допоміжним ГПВЧ на основі ЛКГ. Ці значення мають бути рівномірно розподіленими в діапазонах

$\left[0;2^{n_1}-1\right]$ і $\left[0;2^{n_2}-1\right]$. Одне з модифікованих слів d' і t' слугує для вибору стовпця, а інше – рядка основної матриці генератора другого контуру шифрування. Сформовані другим генератором слова формують кінцевий результат криптографічного перетворення. Ці перетворення і визначають сутність методу двоконтурного шифрування і технічний результат, що ним досягається.

Основним блоком розробленої криптосистеми є генератор рівномірно розподіленої ПВП. Для цієї мети можуть бути використані як розроблені генератори на основі ЛКГ, так і РЗЛЗЗ. Тип використовуваного генератора в кожному з контурів, а також їх параметри тримаються в секреті і є частиною ключа. Для генерації послідовності обирається $M = 2^p$, де p – розрядність слова джерела відкритого тексту, а M відповідає потужності алфавіту джерела.

Генератор на основі ЛКГ, що формує послідовність псевдовипадкових чисел, будується на основі розробленого та представленого вище методу.

Для створення генератора на основі РЗЛЗЗ вибирають генераторний поліном степені $p = \log_2 M$. Для незвідних генераторних поліномів породжувана послідовність з ненульовим ВПЗ є М-послідовністю з періодом $T = 2^p - 1$. Для звідних генераторних поліномів, як це показано в [45], [295], граф станів РЗЛЗЗ складається з циклів, що не перетинаються. Таким чином, як для незвідних, так і для звідних генераторних поліномів існує можливість шляхом конкатенації циклів, що не перетинаються, формувати надцикли довжиною M.

Символ (слово) з виходу першого контуру шифрування поступає на вхід генератора другого контуру, де розщеплюється на два слова меншої розрядності. Номери розрядів слова, що входять в кожне з цих слів, тримають у таємниці.

Найбільш зручною структурою графа станів генератора другого контуру шифрування є $dO_t - d$ циклів по t слів у кожному циклі, $d \times t = M$, $M = 2^p$.

Перше слово на вході другого контуру шифрування визначає номер циклу основної матриці генератора та містить $\log_2 d$ двійкових розрядів, де d – загальна кількість циклів у графі станів генератора. Друге слово визначає номер слова в циклі основної матриці генератора та містить $\log_2 t$ двійкових розрядів, де t – загальна

кількість слів у циклі графу станів генератора. Оскільки $M = 2^p$, а $d \times t = M$, то $d = 2^{p_d}$, а $t = 2^{p_t}$, де $p_d + p_t = p$. Таким чином, $\log_2 d \in \mathbb{Z}$ і $\log_2 t \in \mathbb{Z}$.

Таким чином, для другого контуру перетворення найбільш зручно (проте не обов'язково) використовувати генератор на основі конкатенації циклів ЛКГ з графом станів типу 1.4, оскільки він містить *d* циклів довжиною *t* кожен, де $dt = M$. Крім того, цей тип структури ЛКГ характерний для $M = 2^p$, що ідеально відповідає для криптоперетворення двійкових даних.

ЛКГ з $M = 2^p$, граф станів яких відповідає типу 1.1 з одним циклом довжиною M, можуть також бути використані в другому контурі шифрування.

З цією метою розділимо надцикл з $M = 2^p$ слів на d сегментів по t слів кожен (виходячи з умови $dt = M$) і запам'ятаємо перше слово кожного сегмента. Тоді за p-розрядним двійковим числом $x_i \in [0, M-1]$ на виході першого контуру шифрування можна обчислити значення $d_i = \lfloor x_i / t \rfloor$ і $t_i = |x_i|_t$. За отриманим значенням d_i визначається перший представник цього сегмента, який завантажується в ЛКГ в якості ВПЗ s_0. ЛКГ обчислює слово s_x, віддалене на t_i слів від s_0.

Зауважимо, що більш гнучким для застосування в другому контурі шифрування є саме граф станів типу 1.1, оскільки він забезпечує можливість регулювання кількості і довжини використовуваних сегментів у широких межах: $d \in \left\{2^{p_d} : p_d \in \mathbb{N}, p_d < p\right\}$, $t \in \left\{2^{p_t} : p_t \in \mathbb{N}, p_t = p - p_d\right\}$.

Разом із тим, зауважимо, що з урахуванням розробленого методу формування ПВП у другому контурі криптографічного перетворення можна використати ЛКГ з будь-яким типом графа станів. Спосіб формування основної матриці визначається окремо для кожного типу.

Таким чином, метод двоконтурного шифрування полягає в наступному:

1) перший контур передбачає побітове додавання нелінійної гами до символів відкритого тексту. Нелінійна гама формується шляхом, наприклад, нелінійної комбінації послідовності на виході генератора на основі ЛКГ та послідовності РЗЛЗЗ. Тип і параметри генераторів тримаються в секреті та є частиною ключа;

2) кожне слово отриманого шифртексту розщеплюється на два слова меншої розрядності (n_1 і n_2). Номери розрядів слова, що входять в кожне з цих слів, тримаються в секреті та є частиною ключа шифрування;

3) отримані два слова меншої розрядності підсумовуються відповідно за модулем 2^{n_1} і 2^{n_2} з рівномірно розподіленими в діапазонах $\left[0;2^{n_1}-1\right]$ і $\left[0;2^{n_2}-1\right]$ числами, сформованими допоміжним ГПВЧ на основі ЛКГ;

4) отримані в результаті підсумовування слова визначають номер рядка та стовпця основної матриці генератора. Параметри генератора тримаються в секреті та є частиною ключа шифрування. Сформоване генератором значення є символом шифртексту, яке видається у відкритий канал зв'язку одержувачу інформації.

Розроблений метод двоконтурного шифрування може відрізнятися в параметрах перетворення та допускати наступні модифікації:

1) метод двоконтурного шифрування, що використовує операцію додавання за деяким модулем інформаційної послідовності та послідовності гами, сформованої шляхом нелінійної композиції двох псевдовипадкових послідовностей, періоди повторення яких взаємно прості, який відрізняється тим, що в першому контурі шифрування формується нелінійна композиція послідовності рівномірно розподілених на відрізку $\left[0;M-1\right]$ чисел і рівномірно розподіленої псевдовипадкової послідовності, яка формується за допомогою виконання, наприклад, операції обчислення рівнозначності (або її заперечення) символів (слів) однієї й іншої послідовностей, після чого формується вихідна послідовність першого контуру шифрування шляхом складання за деяким модулем інформаційної послідовності і отриманої композитної послідовності, кожне слово отриманого шифртексту розщеплюється на два слова, до кожного з яких додається випадкове число з допоміжного генератора, після чого одне слово слугує для вибору стовпця, а інше – рядка матриці генератора другого контуру шифрування, слова з виходу якого видаються у відкритий канал зв'язку одержувачу інформації;

2) метод за п.1, який відрізняється тим, що матрицю генератора в першому та другому контурі шифрування формують з d стовпців і t рядків, де $dt=M$, $M=2^n$,

$d = t = 2^{0.5n}$, M – потужність алфавіту джерела, n – розрядність слова джерела, при цьому правило формування слів, що є номерами стовпця і рядка матриці генератора другого контуру шифрування, тримається в секреті є ключем шифру;

3) метод за п.1, який відрізняється тим, що після завершення циклу формування послідовності рівномірно розподілених на відрізку $[0; M-1]$ чисел проводиться перестановка символів у масивах, що визначають порядок обходу стовпців і рядків матриці, при цьому таблиця перестановок тримається в секреті і є ключем шифру.

4.7.2. Пристрій двоконтурного криптографічного перетворення даних

Реалізувати метод двоконтурного шифрування можна за допомогою пристрою, узагальнена структурна схема якого показана на рис. 4.7.

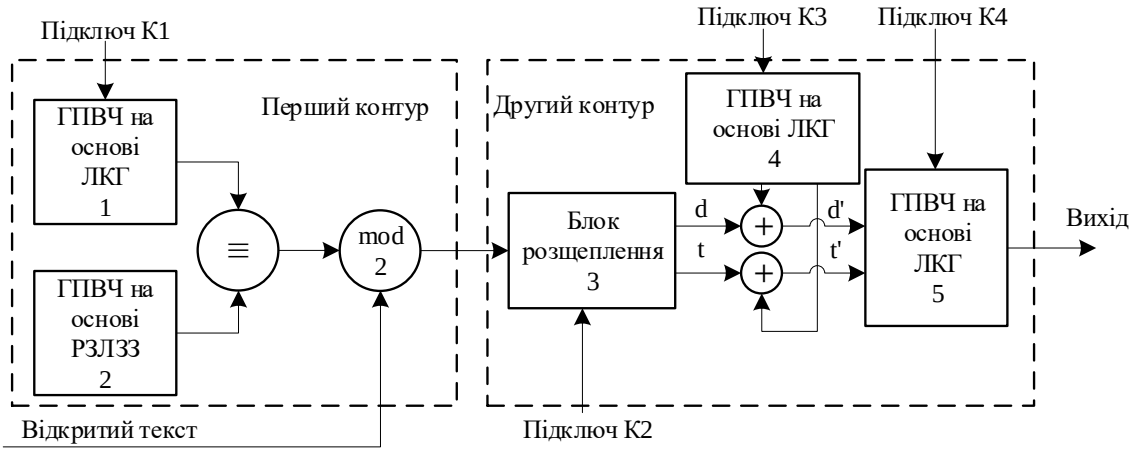


Рис. 4.7. Структурна схема пристрою двоконтурного криптографічного перетворення даних

Перший контур шифрування утворений першим ГПВЧ (1), параметри якого управляються підключем К1, допоміжним ГПВЧ (2), нелінійним елементом, який виконує, наприклад, операцію обчислення рівнозначності над символами, що породжуються першим і другим генераторами. У результаті нелінійного перетворення слів генераторів (1) і (2) утворюється нелінійна гама шифру, яка підсумовується в суматорі за модулем два з символами відкритого тексту.

Другий контур шифрування утворений блоком розщеплення (3) слова першого

контуру шифрування на два слова меншої розмірності. Параметри блоку розщеплення управляються підключем К2. Отримані після розщеплення два слова меншої розрядності підсумовуються з числами, сформованими допоміжним ГПВЧ на основі ЛКГ (4). Отримані слова слугують для керування процесом формування слова генератором (5). Послідовність слів з виходу блоку (5) є повторно зашифрованим текстом і видається для передавання одержувачу інформації.

На відміну від [180], [23], [22], у структурну схему пристрою двоконтурного криптографічного перетворення даних між блоками (3) та (5) введено додаткову операцію підсумовування за модулем з числами від додаткового ГПВЧ.

Наведемо принцип роботи запропонованого пристрою двоконтурного криптографічного перетворення даних для 16-бітового внутрішнього стану.

Блок (1) представляє собою генератор рівномірно розподілених на відрізку $\left[0,2^{16}-1\right]$ чисел на основі ЛКГ. За відсутності циклу максимального періоду відбувається конкатенація зв'язних компонентів графу станів ЛКГ шляхом використання запропонованого вище методу, $M = 2^{16}$. ВПЗ для наступної зв'язної компоненти під час виконання конкатенації обирається шляхом послідовного перебирання значень від 0 до $2^{16}-1$.

Блок (2) є РЗЛЗЗ на основі примітивного генераторного поліному.

Усі параметри блоків (1) і (2) змінюються після досягнення генераторами максимального періоду. Порядок зміни фіксований, зберігається у вигляді константи. Оскільки періоди всіх генераторів системи рівні і складають 2^{16} 16-бітних слів, то зміна параметрів фактично відбувається синхронно. Над отриманими значеннями з виходів блоків (1) і (2) виконується операція «виключаюче АБО-НІ».

Шифрування в першому контурі відбувається за допомогою операції суми за модулем два відкритого тексту та сформованої гами. Оскільки внутрішній стан системи 16-бітний (2 байти), шифрування відбувається блоками по два байти.

Отримане від першого контуру 16-бітне слово в блоці розщеплення (3) розщеплюється на два півслова d і t. Закон розщеплення тримається в таємниці. Отримані значення d і t підсумовуються за модулем 2^8 із значеннями, з ГПВЧ на

основі ЛКГ (4). Результуючі значення d' і t' використовуються в якості вказівників для основної матриці ГПВЧ на основі ЛКГ (5).

4.7.3. Аналіз статистичних властивостей послідовності на виході пристрою двоконтурного криптографічного перетворення даних

Для оцінки кореляційних зв'язків виходів блоків системи двоконтурного шифрування з її вихідним потоком виконаємо аналіз бітової взаємокореляційної функції (ВКФ). Для цього оберемо декілька проміжних станів блоків (1) та (2) першого контуру пристрою потокового шифрування та сформуємо послідовності слів довжиною у повний період $\left(2^{16}\right)$. Для отриманих послідовностей та гами першого контуру побудуємо графіки ВКФ (рис. 4.8 та 4.9).

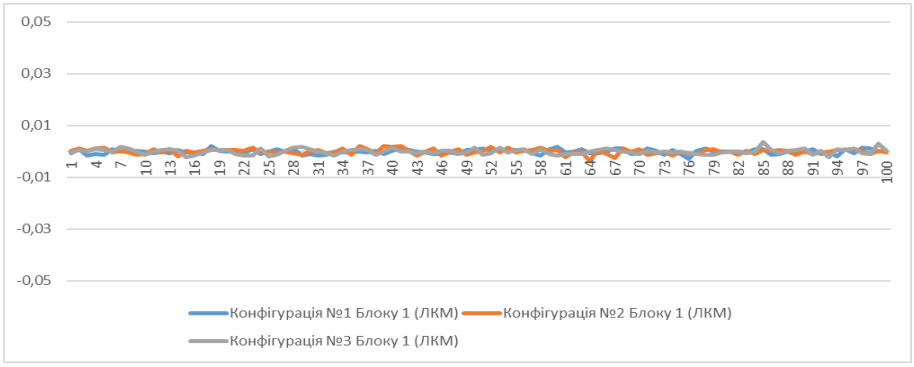


Рис. 4.8. ВКФ послідовностей блоку (1) та гами для трьох різних конфігурацій (параметрів ГПВЧ блоку (1))

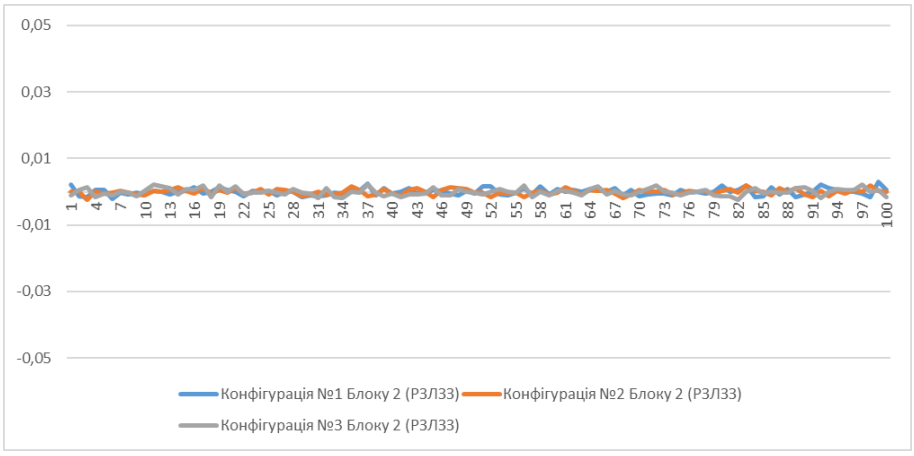


Рис. 4.9. ВКФ послідовностей блоку (2) та гами для трьох різних конфігурацій (параметрів ГПВЧ блоку (2))

На рис. 4.8 і 4.9 відсутні значні сплески кореляції, тому можна вважати, що внутрішній стан пристрою шифрування та гама є некорельованими.

Розглянемо результати тестування зашифрованого тексту на виході запропонованого пристрою шифрування за допомогою пакетів статистичного тестування NIST STS, DIEHARD і TestU01. На рис. 4.10 наведено досягнуті значення *p*-value для пакету статистичного тестування NIST STS. Тести, значення яких нижче 0,96 (вертикальна лінія на рисунку 2) вважаються непройденими.

Як можна бачити з рис. 4.10, декілька тестів мають значення *p*-value, незначно менші за 0,96. Додаткові дослідження застосування пакету статистичного тестування NIST STS до послідовностей на виході запропонованого пристрою шифрування свідчать про те, що представлені на рис. 4.10 відхилення не є статистично значущими. Таким чином, статистичні властивості досліджуваної послідовності успішно проходять тестування NIST STS.

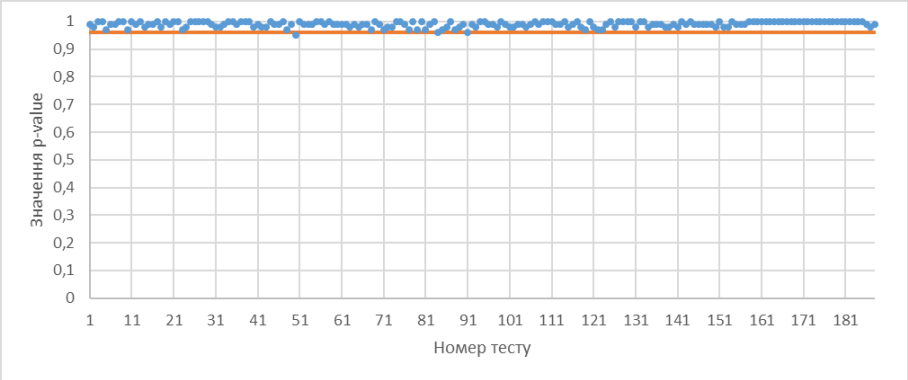


Рис. 4.10. Результати тестування виходу пристрою двоконтурного шифрування за допомогою пакету статистичного тестування NIST STS

Результати тестування за допомогою статистичного пакету тестування DIEHARD свідчать про успішне проходження тестів. Скорочені результати однієї реалізації тестування наведено в таблиці 4.10.

Тестування за допомогою пакету статистичного тестування TestU01 проводились у режимі «Rabbit» (26 тестів, докладний список наведений у [298, с. 152], що дозволяє перевірити довільну кількість випадкових біт. Тестування проводилось для послідовності біт кількістю 104000000 біт. Результати тестування

свідчать про успішне проходження всіх тестів.

Таблиця 4.10

Скорочені результати тестування виходу пристрою двоконтурного шифрування за допомогою пакету статистичного тестування DIEHARD

Назва тесту	Досягнутий рівень значущості
Birthday spacings	0,301001
Overlapping permutations	0,162231 0,015549
Ranks of matrices	0,764176 0,680330 0,585782
Monkey tests	0,35833 0,47361 0,68954 0,77734 0,55913 0,84564 0,56833 0,43015 0,93218 0,88855
	0,99841 0,44580 0,98819 0,05040 0,40371 0,76818 0,75148 0,10984 0,31322 0,29604
Count the 1s	0,956766 0,507801
Parking lot test	0,995047
Minimum distance test	0,945206
Random spheres test	0,299056
The squeeze test	0,892176
Overlapping sums test	0,322803
Runs test	0,557943 0,569683 0,805834 0,640948
The craps test	0,580001 0,864747

Результати статистичного аналізу послідовностей на виході пристрою двоконтурного шифрування свідчить про високий ступінь перемішування та розсіювання символів у шифртексті та його високу якість.

4.7.4. Порівняльний аналіз властивостей методу двоконтурного криптографічного перетворення даних

Виконаємо аналіз властивостей розробленого методу двоконтурного криптографічного перетворення даних та порівняємо їх з властивостями потокових і блокових шифрів. Результати представимо в таблиці 4.11.

Як можна бачити з таблиці 4.11, розроблений метод дозволяє об’єднати переваги потокових і блокових шифрів: довжина ключа скінченна, трек помилки не перевищує довжини блоку, блокування виносу ключа, рандомізація інформаційного масиву не вимагається, а також забезпечує підвищення криптографічної стійкості

перетворення (або полегшує вимоги до генератора гами) в порівнянні з використанням тільки першого контуру криптоперетворення.

Таблиця 4.11

Порівняльний аналіз властивостей шифрів

Тип шифрування	Довжина ключа, біт	Трек помилки, біт	Винос ключа	Рандомізація
Потокове (шифр Вернама)	∞	0	+	+
Блокове	Скінченна	= довжині блоку /∞*	–	– / +*
DES	64 (56)	64 /∞*	–	– / +*
3DES	192 (178)	64 /∞*	–	– / +*
AES	128, 192, 256	128 /∞*	–	– / +*
ГОСТ 28147-89	256	64 /∞*	–	– / +*
Калина	128, 256, 512	128, 256, 512 /∞*	–	– / +*
Двоконтурне шифрування	$\log_2\left(2^{6n}\cdot(n!)^3\cdot\varphi\left(2^n-1\right)/n\right)$	= довжині блоку n	–	+

Примітка: * – за режимів вироблення імітовставки (CBC) та гамування зі зворотним зв’язком (CFB).

Зважаючи на властивості розробленого методу двоконтурного криптографічного перетворення інформації, він може бути застосований для захисту від несанкціонованого доступу інформації з природною надлишковістю (аудіо, відео) у режимі реального масштабу часу.

4.8. Висновки

У четвертому розділі дисертації отримані наступні результати:

- вперше розроблено модель узагальненого графа станів ЛКГ, яка за рахунок представлення кожної зв’язної компоненти графа у вигляді циклів, оснащених добутками дерев, дозволяє виконати класифікацію типів компонент зв’язності графа станів ЛКГ та дослідити вплив параметрів на його топологію;
- удосконалено метод формування ПВП на основі лінійного конгруентного методу, який за рахунок розробленої моделі узагальненого графа станів ЛКГ та

представлення кожної зв'язної компоненти графа у вигляді циклів, оснащених добутками дерев, шляхом конкатенації в графі станів ЛКГ не лише відособлених непересічних циклів, а і передциклів (дерев), якщо вони в ньому містяться, дозволяє формувати ПВП рівномірно розподілених чисел максимального періоду незалежно від топології графа станів ЛКГ, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду в число разів, що дорівнює відношенню потужності алфавіту ЛКГ до її функції Ейлера;

- розроблено структурну схему та алгоритм роботи пристрою формування ПВП перестановок на основі ЛКГ з будь-яким типом графа його станів, що забезпечують можливість його практичної реалізації та дозволяють мінімізувати часові витрати на вибір параметрів ЛКГ і збільшити розмір простору їх допустимих значень для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів. Швидкість роботи розробленого генератора перевищує швидкість роботи генератора перестановок на основі ГПВЧ LFIB78 із застосуванням алгоритму Фішера-Йєтса для $M \le 125$ (зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази);

- удосконалено метод симетричного криптографічного захисту інформації на основі операції гамування, який за рахунок введення другого контуру шифрування та використання в ньому принципів конкатенації зв'язних компонентів у графі станів ЛКГ дозволяє виключити можливість винесення гами, зменшити ймовірність зламу шифру методом повного перебору ключового простору та підвищити стійкість до статистичного криптоаналізу;

- розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації і дозволяють виключити можливість винесення гами, забезпечити скінченний трек помилки та зменшити в порівнянні з використанням тільки першого контуру ймовірність зламу шифру методом повного перебору ключового простору в $2^{4n} \cdot (n!)^2$ разів, де n – розрядність блоку даних.

РОЗДІЛ 5. ДОСЛІДЖЕННЯ КОМБІНАЦІЙНОГО МЕТОДУ ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ ПІДСУМОВУВАННЯ ЗА МОДУЛЕМ

5.1. Вступ

У першому розділі дисертаційної роботи поставлено задачу теоретично обґрунтувати принципи побудови комбінаційного генератора, що використовує підсумовування за модулем, для забезпечення необхідних статистичних властивостей під час вирішення задач захисту інформації на основі факторіального кодування; виконати аналіз якості ПВП залежно від параметрів комбінаційного генератора і властивостей початкових послідовностей. Для цього необхідно:

− дослідити закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем в залежності від параметрів первинних генераторів;

− обґрунтувати загальні вимоги до первинних генераторів для отримання рівномірного закону розподілу д.в.в. на виході комбінаційного генератора;

− виконати аналіз послідовності на виході комбінаційного генератора за допомогою графічних і статистичних методів тестування для різних первинних послідовностей. Крім використання загальновідомих методів тестування, актуальним є виявлення і дослідження нових статистичних властивостей автокореляційних функцій послідовностей випадкових і псевдовипадкових чисел і їх порівняння на основі статистичних критеріїв. Особливий інтерес представляє розподіл коефіцієнтів кореляції ненульового порядку, а також розподіл їх знаків.

5.2. Комбінаційний метод формування послідовностей псевдовипадкових чисел на основі підсумовування за модулем

Опис методу формування ПВП на основі підсумовування за модулем M слів на виході декількох первинних генераторів циклічно повторюваних перестановок представлено в роботах [29], [30], [180].

Його суть полягає в наступному:

1) первинними псевдовипадковими послідовностями є циклічно повторювані перестановки чисел деякого порядку;

2) вихідне значення послідовності, що генерується в поточний момент часу, утворюється шляхом застосування комбінаційної функції до слів з виходів первинних генераторів;

3) комбінаційна функція – підсумовування за модулем M.

Таким чином, як показано в [29], досліджуваний комбінаційний ГПВЧ у якості первинних генераторів використовує генератори перестановок або попередньо сформовані таблиці перестановок (циклічні зсувні регістри, в які попередньо занесені перестановки). У процесі роботи комбінаційного генератора вихідні значення, що підлягають комбінації, циклічно формуються первинними генераторами або зчитуються з таблиць перестановок. Закон розподілу чисел всередині перестановки є рівномірним для всіх значень з області визначення випадкової величини і має нульову помилку відтворення закону розподілу. Помилка відтворення визначається відповідно до методики, викладеної в [17].

Таким чином, до складу розглянутого комбінаційного генератора входять n первинних генераторів перестановок $(n \geq 2)$, а також блок підсумовування за модулем M. Структурну схему генератора представлено на рис. 5.1.

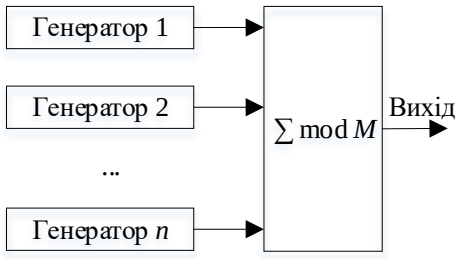


Рис. 5.1. Структурна схема досліджуваного комбінаційного генератора

Нехай первинними генераторами є таблиці перестановок (циклічні зсувні регістри, в які попередньо занесені перестановки). Так, у i-тій вихідній таблиці в довільному порядку без повторів і пропусків записано числа від 0 до $(M_i - 1)$

включно $\left(i \in [1,n]\right)$. Початкове заповнення таблиць перестановок може проводитися як випадковими даними, так і за допомогою детермінованого алгоритму (наприклад, шляхом конкатенації зв'язних компонентів графа станів ЛКГ, генератора М-послідовності або інших відомих алгоритмів [221], [222], [224], [232], [234], [235], [237], [299]). Є доцільним використання різних джерел для заповнення кожної з вихідних таблиць.

Період результуючої послідовності на виході комбінаційного генератора визначається потужностями алфавітів вихідних генераторів (розмірами таблиць перестановок) $M_1, M_2, \ldots, M_n$ і дорівнює

$$T = HCK\left(M_1, M_2, \ldots, M_n\right). \tag{5.1}$$

Для отримання максимального періоду повторення послідовності на виході комбінаційного генератора потужності алфавітів вихідних генераторів повинні бути взаємно простими. Тоді

$$T = \prod_{i=1}^{n} M_i .$$

Принцип функціонування представленого комбінаційного генератора описано в [29] і полягає в наступному. У *i*-у таблицю перестановок завантажується випадкова послідовність чисел від 0 до $\left(M_i - 1\right)$ $\left(i \in [1,n]\right)$ без повторів і пропусків. Для кожної таблиці існує лічильник, який вказує на поточне значення, яке зчитується з таблиці. Початкове значення лічильників може триматися в секреті. Лічильники всіх таблиць працюють синхронно – кожен з лічильників збільшує своє значення на одиницю в однакові моменти часу при появі імпульсу на тактовому вході.

Дані з виходів кожного з лічильників є адресними для зчитування значень з вихідних таблиць перестановок. При цьому на виході кожної з таблиць з'являється значення, що відповідає адресі, на який вказує лічильник. Сформовані n слів одночасно надходять на суматор за модулем M. Вихід суматора є виходом ГПВЧ.

Кожен з лічильників після досягнення значення, рівного розміру відповідної йому таблиці, обнулюється.

Оскільки всі первинні генератори однотипні, є доцільним виділити в структурі пристрою комбінаційного генератора комбінаційну частину та пам’ять [8]–[10], [300]–[302].

Виділення в структурі пристрою комбінаційної частини та пам’яті забезпечує можливість:

− у разі формування первинними генераторами своїх послідовностей в процесі роботи комбінаційного генератора – скорочення апаратних витрат за рахунок того, що в комбінаційному генераторі можна використовувати для всіх первинних генераторів тільки одну комбінаційну структуру, що визначає алгоритм;

− у разі використання таблиць перестановок у якості первинних генераторів – адаптацію для реалізації комбінаційного генератора на однокристальній ЕОМ.

Структурну схему комбінаційного генератора з виділенням комбінаційної частини та пам’яті для використання таблиць перестановок у якості первинних генераторів представлено на рис. 5.2.

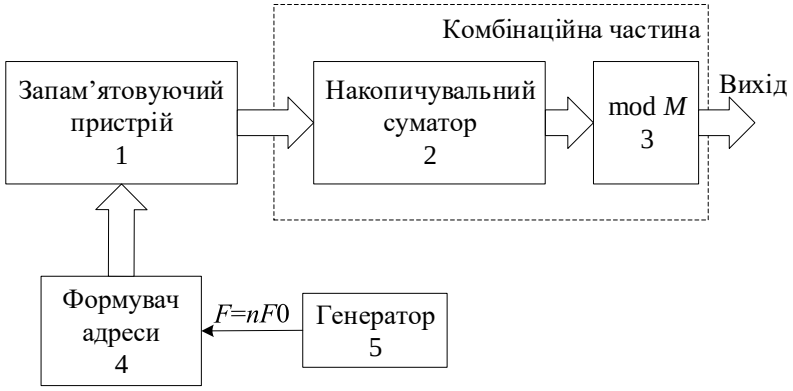


Рис. 5.2. Модифікована структурна схема комбінаційного генератора

Перед початком використання генератора в пристрій (1) завантажуються n таблиць перестановок. У формувачі адреси (4) встановлено адресу першого слова першої таблиці. Накопичувальний суматор (2) обнулений. Після ввімкнення комбінаційного генератора пристрій (1) видає на вхід накопичувального суматора (2) перше слово першої таблиці перестановок. Оскільки накопичувальний суматор (2) обнулений, він запам’ятовує значення, яке надійшло на його вхід. Далі під дією

генератора (5) формувач адреси (4) змінює адресу таким чином, що він вказує на перше слово другої таблиці перестановок. Оперативна пам’ять (1) видає на вхід накопичувального суматора (2) перше слово другої таблиці. Накопичувальний суматор (2) підсумовує значення, яке надійшло на його вхід, зі своїм вмістом. Таким чином, по черзі протягом одного інтервалу формування слова комбінаційного генератора виконуються необхідні дії для даних кожного з первинних генераторів.

Після того, як у накопичувальному суматорі виконано підсумовування всіх слів, що зберігаються в запам’ятовуючому пристрої, сума надходить на вхід блоку обчислення залишку від ділення за модулем M (3), результат надходить на вихід комбінаційного генератора. Накопичувальний суматор (2) обнулюється.

Під час формування наступного слова генератора формувач адреси (4) вказує на наступне слово таблиці перестановок, що зберігається в пам’яті. Після досягнення останнього слова покажчик адреси переходить на початок таблиці.

У [180] показано, що час відтворення повного періоду слів на виході запропонованої конструкції комбінаційного генератора становить 250 і більше років у залежності від кількості первинних таблиць перестановок. Це дозволяє зробити висновки, що процес відтворення повного періоду має високу обчислювальну складність, що робить цей процес практично нездійсненним.

Визначимо закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M.

5.3. Закон розподілу дискретної випадкової величини на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем

Операція підсумовування за модулем використовується практично в усіх методах і алгоритмах криптографічних перетворень інформації. Широко відомий шифр Вернама [266]–[268], що володіє абсолютною криптографічного стійкістю, передбачає використання операції підсумовування за модулем два над відкритим текстом і ключем. За цих обставин, якщо символи ключа обираються випадковим

чином і ймовірності появи нуля й одиниці в ключовому потоці однакові і дорівнюють $P(0)=P(1)=0.5$, символи шифртексту також є випадковими, а ймовірності появи в ньому нуля й одиниці однакові і дорівнюють $P(0)=P(1)=0.5$. Це твердження можна поширити на алфавіти довільної потужності M.

Разом з тим невивченим є питання закону розподілу результату підсумовування за модулем M д.в.в., рівномірно розподілених на множинах цілих чисел з потужностями, що відрізняються від M. Крім того, також становить інтерес закон розподілу результату підсумовування за модулем $M=2$ двійкових випадкових величин, що мають відхилення від рівномірного розподілу. Ці питання є значущими для побудови комбінаційного генератора, що породжує рівномірно розподілену на множині потужності M послідовність випадкових чисел, під час вирішення задач криптографічного захисту інформації.

Розглянемо спочатку статистичні особливості комбінацій випадкових двійкових процесів на основі найпростіших булевих перетворень двох змінних. Оскільки основним призначенням комбінаційного генератора є формування випадкової двійкової послідовності з рівномірним законом розподілу в ній нулів і одиниць, виділимо ті булеві функції, які дозволяють отримати бажаний результат для заданих ймовірностей появи нулів і одиниць у первинних потоках. З індукції очевидно, що якщо двійкова послідовність, сформована в результаті комбінації двох рівномірно розподілених первинних випадкових двійкових послідовностей, є рівномірно розподіленою, то і результат комбінації більшої кількості таких первинних послідовностей також буде рівномірно розподіленим.

Результати дослідження представлено в додатку Ж.

Представимо результати дослідження закону розподілу д.в.в. на виході комбінаційного генератора, комбінаційною функцією якого є операція підсумовування за деяким модулем M, а також умов, за яких цей закон розподілу є строго рівномірним. Основні результати цього дослідження відображено в [55], [303].

Нехай у загальному випадку кількість первинних генераторів випадкових чисел в комбінаційному генераторі дорівнює n. Приймемо спочатку $n=2$. У цьому

випадку є два незалежних первинні генератори рівномірно розподілених випадкових величин X і Y з потужностями алфавітів M_x і M_y. Області визначення цих д.в.в. – $X \in [0, M_x - 1]$ і $Y \in [0, M_y - 1]$. Оскільки комбінаційною функцією генератора є підсумовування за модулем *M*, то розглянутий комбінаційний генератор виконує операцію $Z = |X + Y|_M$ ($|A|_B$ позначає лишок числа A за модулем B).

Задача дослідження зводиться до знаходження ймовірностей $P(Z = z_i)$ для $\forall z_i \in [0, M - 1]$, а також визначення умов, за яких отриманий закон розподілу д.в.в. Z буде строго рівномірним, тобто $P(Z = z_i) = 1/M$ для $\forall z_i \in [0, M - 1]$.

Розглянемо функцію $Z' = X + Y$ з множиною значень $Z' \in [0, M_x + M_y - 2]$. Визначимо функцію розподілу $F(z')$ і закон розподілу $f(z')$ д.в.в. Z'.

Для цього знайдемо функцію розподілу $G(x, y)$ і закон розподілу $g(x, y)$ системи випадкових величин (X, Y). Скористаємося рис. 5.3.

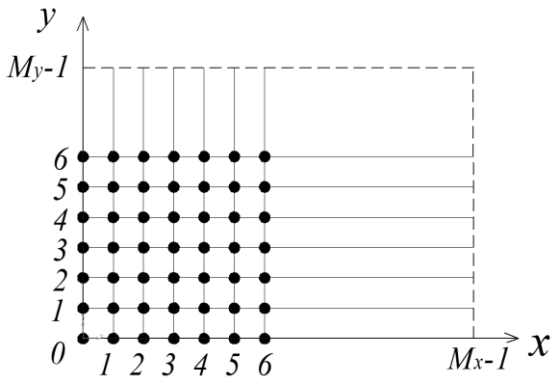


Рис. 5.3. Розташування системи випадкових величин X і Y на числовій осі

Зазначимо, що функцією розподілу системи двох д.в.в. (X, Y) називається функція двох аргументів $G(x, y)$, що дорівнює ймовірності спільного виконання двох нерівностей $X < x$, $Y < y$.

Через рівномірний розподіл д.в.в. *X* і *Y*, а також їх незалежність справедливі вирази $G(0,0) = 0/M_x \cdot 0/M_y = 0$, $G(0,1) = 0/M_x \cdot 1/M_y = 0$, $G(1,0) = 1/M_x \cdot 0/M_y = 0$, $G(1,1) = 1/M_x \cdot 1/M_y = 1/M_x M_y$, $G(1,2) = 1/M_x \cdot 2/M_y = 2/M_x M_y$, тощо. У загальному

вигляді $G(x,y)=P(X<x,Y<y)=xy/M_xM_y$, $x\in[0,M_x]$, $y\in[0,M_y]$.

Закон розподілу системи д.в.в. (X,Y)

$$g(x,y)=G(x+1,y+1)-G(x+1,y)-G(x,y+1)+G(x,y)=$$
$$=\frac{(x+1)(y+1)}{M_xM_y}-\frac{(x+1)y}{M_xM_y}-\frac{x(y+1)}{M_xM_y}-\frac{xy}{M_xM_y}$$

або

$$g(x,y)=1/M_xM_y. \tag{5.2}$$

Закон розподілу системи д.в.в. (X,Y) $g(x,y)=1/M_xM_y$ означає, що ймовірність події, яка відповідає кожній із точок на рис. 5.3, однакова і дорівнює $1/M_xM_y$.

Для знаходження закону розподілу д.в.в. $Z'=X+Y$ побудуємо на площині $x0y$ пряму $z'=x+y$ (рис. 5.4).

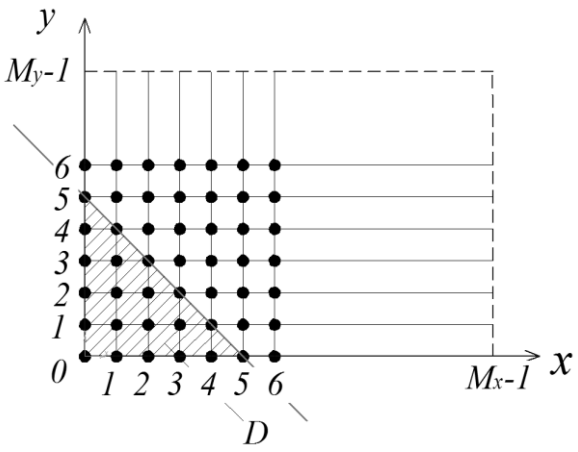


Рис. 5.4. Область D

Позначимо через D область, для якої висота поверхні $z'=x+y$ над площиною $x0y$ менша за z'. Для виконання нерівності $F(z')=P(Z'<z')$, випадкова точка (x,y) повинна потрапити в область D. Отже, функція розподілу величини $Z'=X+Y$ має вигляд $F(z')=P((X',Y')\subset D)=\sum_{(x',y')\subset D} g(x,y)$ або

$$F(z')=\begin{cases}\dfrac{1}{M_xM_y}\left(\dfrac{z'(z'+1)}{2}\right) \text{ при } z'\in\left[0,\min\left(M_x,M_y\right)\right];\\ F\left(\min\left(M_x,M_y\right)\right)+\dfrac{1}{M_xM_y}\left(z'-\min\left(M_x,M_y\right)\right)\cdot\min\left(M_x,M_y\right)\\ \qquad\qquad \text{при } z'\in\left[\min\left(M_x,M_y\right),\max\left(M_x,M_y\right)\right];\\ 1-\dfrac{1}{M_xM_y}\cdot\dfrac{\left(M_x+M_y-z'-1\right)\left(M_x+M_y-z'\right)}{2}\\ \qquad\qquad \text{при } z'\in\left[\max\left(M_x,M_y\right),M_x+M_y-1\right].\end{cases}$$

Закон розподілу величини $Z'=X+Y$ $P\left(Z'=z_i'\right)=F\left(z_i'+1\right)-F\left(z_i'\right)$ або

$$P\left(Z'=z_i'\right)=\begin{cases}\dfrac{z'+1}{M_xM_y} \text{ при } z'\in\left[0,\min\left(M_x,M_y\right)-1\right];\\ \dfrac{1}{\max\left(M_x,M_y\right)} \text{ при } z'\in\left[\min\left(M_x,M_y\right)-1,\max\left(M_x,M_y\right)-1\right];\\ \dfrac{M_x+M_y-z'-1}{M_xM_y} \text{ при } z'\in\left[\max\left(M_x,M_y\right)-1,M_x+M_y-2\right].\end{cases} \quad (5.3)$$

Графічне представлення закону розподілу випадкової величини $Z'=X+Y$ показано на рис. 5.5.

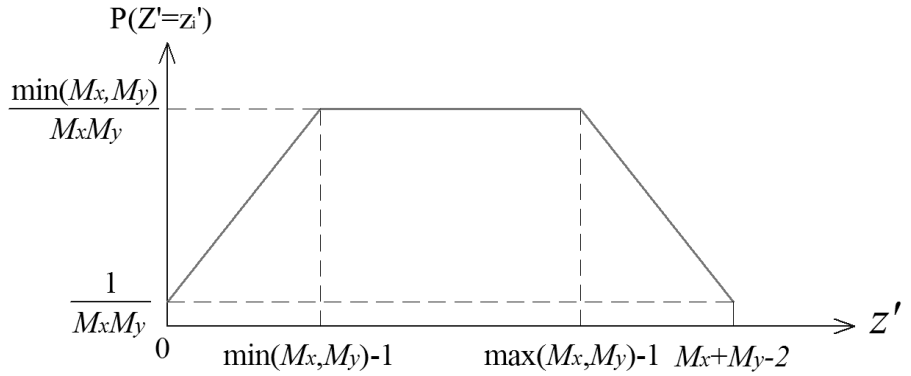


Рис. 5.5. Закон розподілу випадкової величини $Z'=X+Y$

За рівності M_x і M_y закон розподілу випадкової величини $Z'=X+Y$ вироджується в закон Сімпсона, а графік закону розподілу, відповідно, – в трикутник Сімпсона.

Розглянемо тепер функцію $Z = |X + Y|_M = |Z'|_M$ з множиною значень $Z \in [0, M-1]$. Закон розподілу функції Z має вигляд:

$$P(Z = z_i) = \sum_{k=0}^{K_i} P(Z' = kM + z_i),$$

де K_i – максимальне число, за якого $K_i M + z_i \le M_x + M_y - 2$.

Таким чином,

$$P(Z = z_i) = \sum_{k=0}^{\left\lfloor \frac{M_x + M_y - 2 - z_i}{M} \right\rfloor} P(Z' = kM + z_i),$$

де $\lfloor A \rfloor$ – ціла частина (функція «підлога») від числа A.

Визначимо умови, за яких $P(Z = z_i) = 1/M$ для $\forall z_i \in [0, M-1]$:

1) очевидно, що за $M > \max(M_x, M_y)$ закон розподілу д.в.в. Z не є рівномірним;

2) за $M = \max(M_x, M_y)$ для всіх $z_i \in \left[0, \min(M_x, M_y) - 1\right]$

$$P(Z = z_i) = \frac{z_i + 1}{M_x M_y} + \frac{M_x + M_y - \max(M_x, M_y) - z_i - 1}{M_x M_y} = \frac{1}{\max(M_x, M_y)}$$ і закон розподілу д.в.в. Z є рівномірним з $P(Z = z_i) = 1/M$ для всіх $z_i \in [0, M-1]$;

3) за $M = \max(M_x, M_y)/n$ закон розподілу д.в.в. Z також є рівномірним з $P(Z = z_i) = n/\max(M_x, M_y) = 1/M$ для всіх $z_i \in [0, M-1]$;

4) для $M = \min(M_x, M_y)$ скористаємося рис. 5.6.

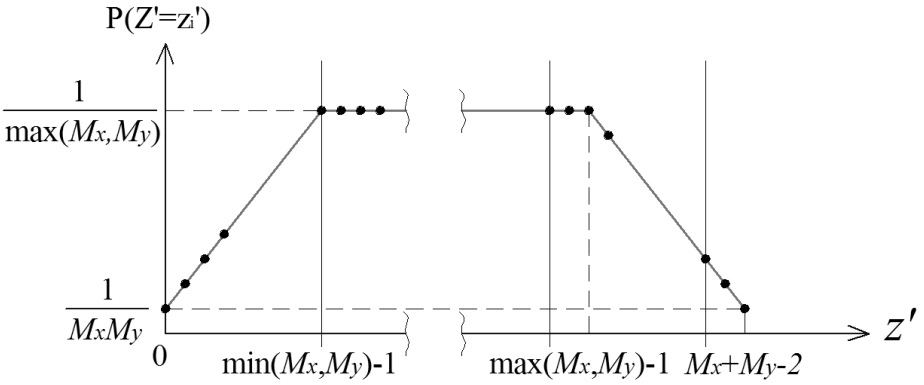


Рис. 5.6. Закон розподілу д.в.в. $Z' = X + Y$ для $M = \min(M_x, M_y)$

За $m=\left\lfloor \dfrac{\max\left(M_x,M_y\right)-\min\left(M_x,M_y\right)}{M} \right\rfloor$ для всіх $z_i\in\left[0,\left|M_x+M_y-2\right|_M+1\right]$

справедливо

$$P\left(Z=z_i\right)=\frac{z_i+1}{M_xM_y}+m\frac{1}{\max\left(M_x,M_y\right)}+\frac{M_x+M_y-\left(m+1\right)M-z_i-1}{M_xM_y}=\frac{1}{\min\left(M_x,M_y\right)}.$$

Для всіх $z_i\in\left[\left|M_x+M_y-2\right|_M+2,M-1\right]$ справедливо

$$P\left(Z=z_i\right)=\frac{z_i+1}{M_xM_y}+\left(m-1\right)\frac{1}{\max\left(M_x,M_y\right)}+\frac{M_x+M_y-mM-z_i-1}{M_xM_y}=\frac{1}{\min\left(M_x,M_y\right)}.$$

Таким чином, за $M=\min\left(M_x,M_y\right)$ для всіх $z_i\in\left[0,M-1\right]$

$P\left(Z=z_i\right)=\dfrac{1}{\min\left(M_x,M_y\right)}=\dfrac{1}{M}$ і закон розподілу д.в.в. Z є рівномірним;

5) за $M=\min\left(M_x,M_y\right)/n$ закон розподілу д.в.в. Z також є рівномірним з $P\left(Z=z_i\right)=n/\min\left(M_x,M_y\right)=1/M$ для всіх $z_i\in\left[0,M-1\right]$.

Таким чином, для д.в.в. $Z=\left|X+Y\right|_M$ можна сформулювати наступну теорему.

Теорема 5.1. Для рівномірного розподілу на множині цілих чисел потужності M д.в.в., отриманої в результаті підсумовування за модулем M двох незалежних первинних випадкових величин, рівномірно розподілених на множинах цілих чисел з діапазонів $\left[0,M_x-1\right]$ і $\left[0,M_y-1\right]$, достатньо, щоб хоча б одне зі значень M_x або M_y було кратне M.

Наслідок 5.1. Для рівномірного розподілу на множині цілих чисел потужності M д.в.в., отриманої в результаті підсумовування за модулем M деякої кількості n незалежних первинних випадкових величин, рівномірно розподілених на множинах цілих чисел з діапазонів $\left[0,M_i-1\right]$, $i=1,2,\ldots n$, достатньо, щоб хоча б одне зі значень M_i було кратне M.

Дійсно, якщо існує деяке значення $M_j:\left|M_j\right|_M=0$, то, згідно теореми 5.1, комбінація j-го генератора і будь-якого іншого i-го генератора породжує

рівномірно розподілену на множині $[0, M-1]$ послідовність. Виконуючи таким чином послідовну комбінацію з рештою генераторів, легко показати справедливість сформульованого наслідку. Математично наведений доказ можна відобразити за допомогою перетворення

$$Z = \left|\sum_j X_j\right|_M = \Big|\Big(\Big(\Big(\big(X_j + X_1\big) + X_2\Big) + \ldots + X_{j-1}\Big) + X_{j+1}\Big) + \ldots + X_n\Big|_M =$$

$$= \Big|\Big|\Big|\big|X_j + X_1\big|_M + X_2\Big|_M + \ldots + X_{j-1}\Big|_M + X_{j+1}\Big|_M + \ldots + X_n\Big|_M,$$

де X_i – незалежні первинні випадкові величини, $i = 1, 2, \ldots n$;

X_j – первинна випадкова величина, для якої справедливо $\left|M_j\right|_M = 0$.

Зауважимо, що доведена теорема справедлива для істинно випадкових первинних величин, які є реалізаціями природного «білого» шуму, з нескінченними періодами повторення. Якщо ж первинні послідовності рівномірно розподілених випадкових чисел X і Y періодичні з періодами T_x і T_y, то період повторення послідовності випадкових чисел на виході комбінаційного генератора залежить від періодів повторення первинних послідовностей і дорівнює $T = НСК\left(T_x, T_y\right)$.

Наслідок 5.2. Достатньою умовою справедливості теореми 5.1 для первинних випадкових величин X і Y з періодами T_x і T_y $\left(\left|T_x\right|_{M_x} = 0,\ \left|T_y\right|_{M_y} = 0\right)$ є умова взаємної простоти періодів T_x і T_y $\left(НСД\left(T_x, T_y\right) = 1\right)$.

Це пояснюється тим, що за такої умови події, які відповідають будь-якій з точок на рис. 5.3, зустрічаються однакову кількість $\left(n = \dfrac{НСК\left(T_x, T_y\right)}{M_x \cdot M_y} \in Z\right)$ разів на всьому періоді послідовності і, відповідно, закон розподілу системи д.в.в. (X, Y) $g(x, y) = 1/M_x M_y$.

Якщо ж $\left|T_x\right|_{M_x} \neq 0$, $\left|T_y\right|_{M_y} \neq 0$ або $НСД\left(T_x, T_y\right) \neq 1$ то потрібні додаткові дослідження з урахуванням принципів формування X і Y.

Наслідок 5.3. Достатньою умовою справедливості наслідку 5.1 теореми 5.1 для n первинних д.в.в. X_i, $i=1,2,\ldots n$, з періодами T_i $\left(\left|T_i\right|_{M_i}=0\right)$ є умова попарної взаємної простоти періодів T_i, тобто $НСД\left(T_i,T_j\right)=1$ для $\forall T_i,T_j$, $i\neq j$.

В окремому випадку в якості первинних генераторів можуть використовуватися генератори перестановок (підстановок), кожен з яких циклічно формує деяку перестановку, або таблиці перестановок, реалізовані за допомогою циклічних зсувних регістрів, що містять попередньо сформовані різні послідовності перестановок. У процесі роботи комбінаційного генератора вихідні значення, що підлягають композиції, формуються циклічно генераторами перестановок або зчитуються з виходів циклічних зсувних регістрів. Звідси $T_x=M_x$, а $T_y=M_y$.

У такому випадку закон розподілу системи д.в.в. $\left(X,Y\right)$ має вигляд $g\left(x,y\right)=1/M_xM_y$, а закон розподілу д.в.в. $Z'=X+Y$ визначається виразом (5.3), за умови, що M_x і M_y взаємно прості. Це пояснюється тим, що умова взаємної простоти значень M_x і M_y є необхідною і достатньою для того, щоб період формованої композиції був максимальним і дорівнював $T_{\max}=M_x\cdot M_y$, а події, що відповідають будь-якій з точок на рис. 5.3, зустрічалися рівно один раз на всьому періоді послідовності. В інших випадках період послідовності буде меншим $T_{\max}=M_x\cdot M_y$ і як наслідок, $g\left(x,y\right)\neq 1/M_xM_y$.

Якщо ж $НСД\left(T_x,T_y\right)\neq 1$, то потрібні додаткові дослідження з урахуванням принципів формування первинних послідовностей перестановок X і Y. У будь-якому випадку період $T=НСК\left(T_x,T_y\right)=НСК\left(M_x,M_y\right)$ повинен бути кратний M.

У силу сказаного, сформулюємо наступну теорему.

Теорема 5.2. Для рівномірного розподілу д.в.в. на множині цілих чисел потужності M на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів від двох первинних генераторів, що циклічно формують перестановки на множинах цілих чисел з діапазонів $\left[0,M_x-1\right]$ і

$\left[0, M_y - 1\right]$ для першого і другого генератора, відповідно, достатньо, щоб M_x і M_y були взаємно прості і одне зі значень M_x або M_y було кратне *M*.

Експериментальні дослідження показують, що якщо M_x і M_y взаємно прості, то для рівномірного розподілу д.в.в. на множині цілих чисел потужності M на виході комбінаційного генератора умова кратності значенню M одного зі значень M_x або M_y є обов'язковим (випадків рівномірного розподілу д.в.в. на виході генератора, коли $НСД\left(M_x, M_y\right) = 1$, $\left|M_x\right|_M \neq 0$, $\left|M_y\right|_M \neq 0$, а $\left|НСК\left(M_x, M_y\right)\right|_M = 0$ (наприклад, $M_x = 9$, $M_y = 16$, $M = 6$), не спостерігалося).

Наслідок 5.4. Для рівномірного розподілу д.в.в. на множині цілих чисел потужності M на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів від деякої кількості n незалежних первинних генераторів, кожний з яких циклічно формує перестановку на множині цілих чисел $\left[0, M_i - 1\right]$, $i = 1, 2, \ldots n$, достатньо, щоб $НСД\left(M_i, M_j\right) = 1$ для $\forall M_i, M_j$, $i \neq j$, і одне зі значень M_i було кратне M $\left(\exists M_j : \left|M_j\right|_M = 0\right)$.

Цей наслідок доводиться подібно до того, як доведено наслідок 5.1.

У загальному випадку, коли не потрібно строгої відповідності закону розподілу д.в.в. рівномірному закону розподілу (не потрібно строго однакової кількості всіх значень д.в.в. *Z* з області її визначення на весь період композиції), однак слід дотримуватися статистичної гіпотези про її рівномірний розподіл на всьому періоді генерованої послідовності, можна скористатися критерієм Пірсона. Для цього для двох первинних генераторів слід обчислити значення

$$\chi^2 = V \sum_{z_i=0}^{M-1} \frac{\left(P\left(Z = z_i\right) - p_0\left(z\right)\right)^2}{p_0\left(z\right)} = V \sum_{z_i=0}^{M-1} \frac{\left(\sum_{k=0}^{\left\lfloor \frac{M_x + M_y - 2 - z_i}{M} \right\rfloor} P\left(Z' = kM + z_i\right) - p_0\left(z\right) \right)^2}{p_0\left(z\right)},$$

де $p_0\left(z\right) = 1/M$ відповідає гіпотетичному (теоретичному) закону розподілу рівномірно розподіленої д.в.в. Z у області її визначення $\left(Z \in \left[0, M - 1\right]\right)$;

$V = T = НСК\left(M_x, M_y\right)$ – об'єм вибірки, що дорівнює періоду послідовності.

Далі розраховане значення потрібно порівняти з квантилем закону розподілу χ^2 заданого рівня значущості і зробити висновок про відповідність або невідповідність цього закону розподілу рівномірному закону.

Для визначення величини помилки відтворення закону розподілу д.в.в. як числа символів помилкового потоку, що припадає на одиницю об'єму вибірки, скористаємося формулою з роботи [17], де помилка відтворення закону розподілу визначається за допомогою виразу

$$\xi = \frac{1}{2}\sum_{z_i=0}^{M-1}\left|P\left(Z = z_i\right) - p_0\left(z\right)\right|.$$

Якщо первинні послідовності рівномірно розподілених д.в.в. X і Y періодичні з періодами T_x і T_y, $\left|T_x\right|_{M_x} = 0$, $\left|T_y\right|_{M_y} = 0$, $НСД\left(T_x, T_y\right) = 1$ і хоча б одне зі значень M_x або M_y кратне M, то $g\left(x, y\right) = 1/M_x M_y$, $\left|T\right|_M = 0$, а $P\left(Z = z_i\right) = 1/M$. Це свідчить про нульову помилку відтворення рівномірного закону розподілу символів на виході комбінаційного генератора: $\xi = \frac{1}{2}\sum_{z_i=0}^{M-1}\left|P\left(Z = z_i\right) - p_0\left(z\right)\right| = 0$.

Зауважимо, що для будь-якої підстановки на деякій множині потужності M помилка відтворення рівномірного закону розподілу також дорівнює нулю: $\xi = 0$.

Методика вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем M полягає в наступному:

1) перед визначенням значень M_i, $i = 1, 2, \ldots n$, n – число первинних генераторів, попередньо слід визначити необхідні значення модуля M і періоду T;
2) у разі використання таблиць перестановок з метою мінімізації об'єму пам'яті, що відводиться під їх зберігання, слід вибирати значення M_i, максимально близькі одне до одного, а також максимально близькі до значення $\sqrt[n]{T}$;
3) одне зі значень M_i повинно бути кратне M.

Таким чином, проведене дослідження дозволило отримати наступні

результати:

- визначено закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів, отриманих від n первинних генераторів рівномірно розподілених випадкових чисел;
- визначено умови, за яких закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M є строго рівномірним. У якості вихідних первинних послідовностей випадкових чисел розглянуто послідовності істинно випадкових чисел як з необмеженими, так і з обмеженими періодами, а також послідовності, що представляють собою циклічно повторювані перестановки.

5.4. Оцінка статистичних властивостей послідовності псевдовипадкових чисел на виході комбінаційного генератора

У цьому підрозділі наведемо результати перевірки випадковості послідовностей чисел, сформованих за допомогою комбінаційного генератора. Для цього будемо використовувати такі тести та критерії:

- графічні тести (гістограма розподілу, розподіл на площині, автокореляційна функція, профіль лінійної складності тощо);
- критерій рівномірності розподілу в k-вимірному просторі (критерій серій [156]);
- непараметричні критерії знаків і серій;
- статистичні пакети тестування NIST STS [248], Diehard [247], TestU01 [249];
- статистичні критерії перевірки кореляційних зв’язків послідовності.

5.4.1. Графічні тести

У роботі [29] наведено результати тестування послідовностей на виході комбінаційного генератора за допомогою графічних тестів.

Отримані результати показують, що послідовності, породжені комбінаційним генератором, мають великий період повторення, успішно проходять графічні тести:

гістограма розподілу слів послідовності підтверджує рівномірний розподіл слів послідовності, що формується генератором; аналіз тесту розподілу на площині не показав будь-яких візерунків на отриманому зображенні; відсутні сплески бічних пелюсток на автокореляційній функції, що свідчить про відсутність кореляції між символами послідовності; графічний спектральний тест показує відсутність значних сплесків гармонік; профіль лінійної складності показує лінійне збільшення складності послідовностей по мірі збільшення розміру вибірки.

5.4.2. Критерій рівномірності розподілу в *k*-вимірному просторі

У [156] показано, що випадкова послідовність повинна мати рівномірний розподіл *k*-грам. Іншими словами, послідовність має бути рівномірно розподілена у *k*-вимірному просторі, а символи алфавіту потужності 2^k мають бути рівномірно розподілені у такій послідовності.

Нехай первинні генератори є циклічними регістрами зсуву довжини M_i, де i – порядковий номер генератора, $1 \le i \le n$. У i-ий первинний генератор у процесі його ініціалізації записуються всі числа діапазону $[0; M_i - 1]$ без повторів і пропусків – одна з можливих $M_i!$ варіантів перестановок. Таким чином, періоди первинних генераторів дорівнюють потужності їх алфавітів: $T_i = M_i$.

Однією з основних вимог, що пред'являються до ПВП, є їх складна передбачуваність: виявлення закону залежності наступних елементів послідовності від попередніх має бути максимально важкою задачею.

Найочевиднішою вимогою ускладнення передбачуваності послідовності є рівна ймовірність появи кожного символу алфавіту послідовності. Це означає, що якщо $A_M = \{a_1, a_2, ..., a_M\}$ – алфавіт послідовності потужності M, а $S_{A_M,N} = (s_1, s_2, ..., s_N)$ – деяка послідовність довжини N символів алфавіту A_M $(s_i \in A_M)$, то $P\left(s_{N+1} = a_j \middle| S_{A_M,N}\right) = \frac{1}{M}$ для $\forall a_j \in A_M$.

За умови рівномірного розподілу символів алфавіту ентропія повідомлення H є максимальною: $H = H_{\max} = \log_{M_1} M$, де M_1 – потужність вторинного алфавіту, за

яким визначається ентропія.

Уведемо поняття питомої ентропії $H_{пит}$ – ентропії, що приходиться на один символ первинного алфавіту. Тоді, якщо потужність первинного алфавіту – M_1, а вторинного – M_2, то питома ентропія

$$H_{пит} = \frac{H}{L_{сер}}, \tag{5.4}$$

де $L_{сер}$ – середня довжина кодової комбінації (середня кількість символів первинного алфавіту, необхідних для кодування символів вторинного алфавіту).

Якщо символи вторинного алфавіту розподілені рівномірно, то код є теж рівномірним, $H = H_{\max}$, $L_{сер} = \lceil \log_{M_1} M_2 \rceil$, а $H_{пит} = H_{пит\,\max} = \frac{H_{\max}}{L_{сер}}$ або

$$H_{пит} = \frac{\log_{M_1} M_2}{\lceil \log_{M_1} M_2 \rceil}. \tag{5.5}$$

Надалі будемо розглядати ситуацію, коли символи вторинного алфавіту формуються з символів первинного алфавіту за допомогою рівномірного кодування.

Під час перетворення послідовності символів більш потужного вторинного алфавіту A_{M_2} у послідовність символів менш потужного первинного алфавіту A_{M_1}, $M_2 > M_1$ (кодування символів вторинного алфавіту A_{M_2} символами первинного алфавіту A_{M_1} – «укрупнення» символів), справедливі наступні твердження.

Лема 5.1. Якщо символи вторинного алфавіту A_{M_2}, з яких складається деяка послідовність, рівномірно в ній розподілені і $\log_{M_1} M_2 \in \mathbb{Z}$, то символи первинного алфавіту A_{M_1}, з яких складається закодована послідовність, також рівномірно розподілені.

Справедливість сформульованого твердження дозволяють підтвердити наступні перетворення:

$$\{0,1,2,3\}_{A_{M_2=4}=\{0,1,2,3\}} \to \{00,01,10,11\}_{A_{M_1=2}=\{0,1\}},$$

$$\{0,1,2,3,4,5,6,7,8,9\}_{A_{M_2=9}=\{0,1,2,3,4,5,6,7,8,9\}} \to \{00,01,02,10,11,12,20,21,22\}_{A_{M_1=3}=\{0,1,2\}}.$$

Теорема 5.3. Якщо питома ентропія, визначена за деякою послідовністю символів вторинного алфавіту A_{M_2}, дорівнює одиниці $\left(H_{пит} = \frac{\log_{M_1} M_2}{\lceil \log_{M_1} M_2 \rceil} = 1 \right)$, то символи первинного алфавіту A_{M_1} у закодованій послідовності є рівномірно розподіленими.

Доведення.

Дійсно, якщо $H_{пит} = \frac{H}{L_{сер}} = 1$, то $H = \lceil \log_{M_1} M_2 \rceil$. Через те, що $H \le H_{\max} = \log_{M_1} M_2$, а $\lceil \log_{M_1} M_2 \rceil \ge \log_{M_1} M_2$, рівняння $H = \lceil \log_{M_1} M_2 \rceil$ має розв'язок тоді і тільки тоді, коли $H = H_{\max} = \log_{M_1} M_2$ (що свідчить про рівномірний розподіл символів вторинного алфавіту в послідовності) та $\log_{M_1} M_2 \in \mathbb{Z}$ (що може мати місце тільки за умови $M_2 \ge M_1$). Відповідно до леми 5.1 символи первинного алфавіту в послідовності також рівномірно розподілені. Теорему доведено. ■

Зазначимо, під час перетворення послідовності із рівномірним розподілом символів менш потужного первинного алфавіту A_{M_1} у послідовність із більш потужним вторинним алфавітом A_{M_2} $(M_2 > M_1)$ символи вторинного алфавіту не завжди будуть рівномірно розподілені. Наприклад (використано відповідність символів із попереднього прикладу):

$$(0,1,0,1,0,1,0,1)_{A_{M_1=2}=\{0,1\}} \to (1,1,1,1)_{A_{M_2=4}=\{0,1,2,3\}}.$$

Очевидно, що оригінальна послідовність (із алфавітом $A_{M_1=2} = \{0,1\}$) має рівномірний закон розподілу символів, проте нова послідовність (із алфавітом $A_{M_2=4} = \{0,1,2,3\}$) не відповідає умові рівномірного закону розподілу символів.

Наслідок 5.5. Таким чином, під час перетворення послідовності із деякою потужністю алфавіту M_1 до послідовності із більшою потужністю алфавіту M_2, символи якого складаються з символів первинного алфавіту і утворюють з них повну множину кортежів, і якщо символи нової послідовності рівномірно розподілені, символи оригінальної послідовності також рівномірно розподілені.

Перетворення послідовностей із меншою потужністю алфавіту до послідовностей із більшою потужністю можна розглядати як основну ідею аналізу розподілу *k*-грам: оригінальна послідовність зводиться (назвемо цей процес *k*-перетворенням) до послідовності *k*-грам (яку назвемо *k*-послідовністю).

Алфавітом *k*-послідовності є сукупність усіх варіантів *k*-грам – множина всіх кортежів символів первинного алфавіту оригінальної послідовності.

Таким чином, у результаті *k*-перетворення отримуємо нову послідовність із потужністю алфавіту $M_2 = M_1^k$.

У роботах автора [25], [26] викладено результати дослідження закону розподілу *k*-грам на виході комбінаційного генератора. Отримані результати показують, що послідовність на виході розглянутого комбінаційного генератора рівномірно розподілена у *k*-вимірному просторі для всіх досліджених $k \le 21$.

5.4.3. Непараметричні критерії знаків і серій

Коротко викладемо основні результати, представлені в роботі автора [38].

Дослідженню піддавався комбінаційний генератор з різною кількістю вихідних генераторів (від 2 до 8), що представляють собою циклічні зсувні регістри (таблиці) із записаними в них перестановками, сформованими за допомогою ЛКГ (на основі запропонованого в розділі 2 методу), адитивного генератора [304] або генератора випадкових чисел (використовується квантовий ГВЧ [305]). Потужність алфавіту M обрано рівною 256, що дозволяє без додаткових перетворень формувати двійковий файл зі слів на виході комбінаційного генератора, придатний для подальшого використання статистичними пакетами тестування.

Оцінка послідовності на виході досліджуваного генератора проводилася за допомогою непараметричних критеріїв знаків [258, с. 254–260], [261, с. 89–91] і серій [261, с. 91–93]. Зауважимо, що непараметричні критерії використовують не чисельні значення вибірки, а її структурні властивості, що дозволяє провести оцінку послідовності незалежно від передбачуваного закону розподілу.

Так, критерій знаків дозволяє визначити однорідність двох розглянутих вибірок. Однорідними називаються вибірки, які мають однакові функції розподілу.

Розглядалося порівняння різних реалізацій комбінаційного генератора з випадковою послідовністю чисел [306], що утворена шляхом оцифрування радіошумів і прийнятої в якості еталонної.

Критерій серій, у свою чергу, дозволяє визначити, що слова на виході досліджуваного генератора є випадковими і незалежними.

Розглянемо результати дослідження послідовностей, породжених комбінаційним генератором, за допомогою критерію знаків.

У якості нульової гіпотези H_0 прийнято твердження, що досліджувані послідовність комбінаційного генератора і еталонна послідовність є однорідними, тобто ймовірності відхилення різниці між словами досліджуваної і випадкової послідовностей в ту або іншу сторону рівні між собою. Тоді $H_0 : p = 0.5$. Як альтернативні висувалися гіпотези:

– гіпотеза $H_1 : p > 0.5$ – імовірність відхилення різниці між словами досліджуваної і випадкової послідовностей у позитивну сторону більше, ніж у негативну;

– гіпотеза $H_2 : p < 0.5$ – імовірність відхилення різниці між словами досліджуваної і випадкової послідовностей у негативну сторону більше, ніж у позитивну.

Рівень значущості $\alpha = 0.05$. Відповідно до рекомендацій, викладених в [258, с. 257–258], число випробувань для застосування критерію знаків повинно бути досить великим для значень p, близьких до 0,5 і конкуруючих з $p = 0.5$. Наприклад, для того, щоб критерій знаків в 95% випадків відкидав гіпотезу $H_0 : p = 0.5$, коли насправді $p = 0.45$ з рівнем значущості 5%, необхідно провести не менше 1297 спостережень [258, с. 258]. Мінімально необхідний обсяг вибірки монотонно збільшується при наближенні значення p до 0,5 і при зменшенні рівня значущості. Виходячи з цього, в якості вихідних даних для застосування критерію знаків розглядалися перші 4096 слів кожної з послідовностей комбінаційного генератора в залежності від різної кількості вихідних таблиць і різного їх заповнення.

Результати дослідження наведено в таблицях 5.1-5.3.

Таблиця 5.1

Результати тесту критерію знаків для заповнення вихідних таблиць за допомогою адитивного генератора

Кількість первинних генераторів	$H_1: p > \frac{1}{2}$				$H_2: p < \frac{1}{2}$			
	k_1	k_2	F_B	$F_{1-\alpha}(k_1,k_2)$	k_1	k_2	F_B	$F_{1-\alpha}(k_1,k_2)$
2	4004	4158	1,03846	1,052845729	4160	4002	0,96202	1,052877192
3	4120	4030	0,97816	1,052903529	4032	4118	1,02133	1,052885731
4	4048	4118	1,01729	1,052833121	4120	4046	0,98204	1,052847624
5	4064	4092	1,00689	1,052868834	4094	4062	0,99218	1,052874892
6	4086	4072	0,99657	1,052866114	4074	4084	1,00245	1,052863692
7	4150	4006	0,9653	1,052894063	4008	4148	1,03493	1,052865383
8	4170	4004	0,96019	1,052839127	4006	4168	1,04044	1,052806147

Таблиця 5.2

Результати тесту критерію знаків для заповнення вихідних таблиць за допомогою ЛКГ

Кількість первинних генераторів	$H_1: p > \frac{1}{2}$				$H_2: p < \frac{1}{2}$			
	k_1	k_2	F_B	$F_{1-\alpha}(k_1,k_2)$	k_1	k_2	F_B	$F_{1-\alpha}(k_1,k_2)$
2	4032	4126	1,02331	1,052858914	4128	4030	0,97626	1,05287829
3	4144	4012	0,96815	1,052891519	4014	4142	1,03189	1,052865263
4	4042	4110	1,01682	1,052879733	4112	4040	0,98249	1,052893882
5	4104	4058	0,98879	1,052856773	4060	4102	1,01034	1,052847902
6	4106	4050	0,98636	1,052878137	4052	4104	1,01283	1,052867234
7	4136	4018	0,97147	1,052895362	4020	4134	1,02836	1,052871924
8	4136	4032	0,97485	1,052846122	4034	4134	1,02479	1,052825585

Таблиця 5.3

Результати тесту критерію знаків для заповнення вихідних таблиць за допомогою квантового ГВЧ

Кількість первинних генераторів	$H_1: p > \frac{1}{2}$				$H_2: p < \frac{1}{2}$			
	k_1	k_2	F_B	$F_{1-\alpha}(k_1,k_2)$	k_1	k_2	F_B	$F_{1-\alpha}(k_1,k_2)$
2	4178	3990	0,955	1,052864423	3992	4176	1,04609	1,052826959
3	4112	4060	0,98735	1,052824398	4062	4110	1,01182	1,052814342
4	4030	4108	1,01935	1,052925982	4110	4028	0,98005	1,052942209
5	4144	4010	0,96766	1,0528986	4012	4142	1,0324	1,052871927
6	4120	4044	0,98155	1,05285459	4046	4118	1,0178	1,052839677
7	4150	4006	0,9653	1,052894063	4008	4148	1,03493	1,052865383
8	4000	4166	1,0415	1,052832819	4168	3998	0,95921	1,052866671

Отримані результати показують однорідність послідовності, отриманої за допомогою комбінаційного генератора (для всіх досліджених варіантів заповнення первинних таблиць), і еталонної послідовності випадкових чисел. Таким чином, функції розподілу досліджуваних випадкових величин збігаються.

Результати дослідження послідовностей комбінаційного генератора за допомогою критерію серій наведено в таблиці 5.4. Успішним проходженням тесту є знаходження результату розрахунку статистики критерію z_B в межах критичних значень, які для рівня значущості $\alpha = 0.01$ приймають значення: $-2.576 < z_B < 2.576$.

Таблиця 5.4

Результати тесту критерію серій

Кількість первинних генераторів	z_B		
	заповнення вихідних таблиць за допомогою адитивного генератора	заповнення вихідних таблиць за допомогою лінійного конгруентного методу	заповнення вихідних таблиць за допомогою квантового генератора випадкових чисел
2	-0,43836	-0,56361	-0,56266
3	0,688852	2,191802	-2,0657
4	0,698043	0,815126	-0,05872
5	-2,06656	0,188859	-0,68042
6	0,313115	-0,8141	-0,06262
7	-0,93934	-0,1869	1,565573
8	-1,31418	-0,1869	-0,68885

Результати застосування критерію серій підтверджують гіпотезу про випадковість слів на виході комбінаційного генератора.

5.4.4. Статистичні пакети тестування NIST STS, Diehard, TestU01

Результати тестування послідовностей комбінаційного генератора за допомогою пакетів тестування NIST STS [248] викладені в роботах автора [38], [307], а також у роботі [180], виконаній під його керівництвом.

Для аналізу статистичних характеристик послідовностей комбінаційного генератора за допомогою пакета тестування NIST STS використовувалася вибірка розміром 2^{25} байт. Відповідно до рекомендацій NIST [248], [308], кожен з 188 тестів пакету проводився $N = 10^3$ раз над послідовністю довжиною $V = 10^6$ біт. Нульова гіпотеза H_0 = {послідовність, що перевіряється, є випадковою}. Результати

перевірки рівномірності розподілу значень *p-value*, отриманих в результаті тестування, наведені в таблиці 5.5.

Таблиця 5.5

Кількість непройдених тестів за критерієм рівномірності розподілу значень *p-value*

Заповнення таблиць	Кількість вихідних таблиць						
	2	3	4	5	6	7	8
ЛКГ	148/188	1/188	0/188	0/188	0/188	0/188	0/188
Адитивний генератор	147/188	0/188	0/188	0/188	0/188	0/188	0/188
Квантовий генератор	149/188	0/188	0/188	0/188	0/188	0/188	0/188

Відповідно до рекомендацій NIST [248], [308], відношення кількості значень *p-value*, які більші за довірчу ймовірність, до загальної кількості результатів тесту повинно бути не меншим 96%.

Результати тестування відповідно до цього критерію наведено в таблиці 5.6.

Таблиця 5.6

Кількість непройдених тестів за критерієм потрапляння значень *p-value* в критичну область за довірчої ймовірності $\alpha = 0.01$

Заповнення таблиць	Кількість вихідних таблиць						
	2	3	4	5	6	7	8
ЛКГ	11/188	1/188	2/188	1/188	3/188	1/188	3/188
Адитивний генератор	17/188	3/188	2/188	0/188	0/188	0/188	0/188
Квантовий генератор	20/188	1/188	1/188	0/188	0/188	0/188	0/188

Результати, представлені в таблицях 5.5 і 5.6, свідчать про те, що:

− використання двох первинних генераторів незалежно від способу їх побудови призводить до непроходження великої частини тестів згідно таблиці 5.5 і значної частини тестів згідно таблиці 5.6. Причиною цьому послужив малий період послідовності і зациклення генератора;

− використання трьох і більше первинних генераторів призводить до того, що всі варіанти комбінаційного генератора задовольняють вимогам рівномірності розподілу значень *p-value* (таблиця 5.5). Однак додаткова оцінка кількості послідовностей, які успішно пройшли тести з імовірністю не нижче 96% (таблиця 5.6), показує незначні відхилення для послідовностей, що використовують ЛКГ. Тому подібну конструкцію комбінаційного генератора не рекомендується

використовувати в задачах, що потребують високої якості ПВП, зокрема, в криптографічних задачах. Для інших варіантів формування первинних генераторів (за їх кількості 5 і більше) послідовності повністю проходять усі тести пакету тестування NIST.

Отримані в [180] результати тестування послідовностей комбінаційного генератора за допомогою статистичного пакета Diehard [247] свідчать про успішне проходження тестів для 3 і більше первинних генераторів.

Результати тестування послідовностей комбінаційного генератора за допомогою статистичного пакета TestU01 [249] представлені в [180] і також свідчать про успішне проходження тестів. Результати тестування, запозичені з [180], наведено в таблиці 5.7.

Таблиця 5.7

Результати тестування ГПВЧ за допомогою пакета TestU01 (з [180])

ГПВЧ	Режим		
	SmallCrush	Crush	BigCrush
ЛКМ, $M=2^{32}$, K=69069, C=1	11	106	-
ЛКМ, $M=2^{32}$, K=1099087573, C=0	13	110	-
ЛКМ, $M=2^{63}$, $K=5^{19}$, C=1	+	5	8
ЛКМ, $M=2^{61}-1$, $K=2^{30}-2^{19}$, C=0	+	1	3
CLCG4	+	+	+
Вихор Мерсенна	+	2	2
РЗЛЗЗ (LFSR113)	+	6	6
Комбінаційний ГПВЧ на основі підсумовування за модулем *M* 4 первинних ГПВЧ на основі ЛКМ	+	+	+

Таким чином, результати тестування послідовностей комбінаційного генератора за допомогою пакетів тестування NIST STS, Diehard і TestU01 показують, що успішне проходження тестів спостерігається для наступних конфігурацій генератора: кількість вихідних генераторів (таблиць перестановок) – 5 і більше; заповнення вихідних таблиць – адитивний генератор, квантовий ГВЧ. Отримані результати свідчать про те, що запропонований комбінаційний генератор може бути використаний в задачах, що потребують високої якості ПВП, в тому числі для криптографічних перетворень.

5.4.5. Кореляційні властивості

Викладемо основні результати, представлені в роботі автора [37].

У цій роботі вирішено наступні задачі:

− дослідження і аналіз кореляційних зв’язків випадкових і псевдовипадкових послідовностей чисел за допомогою оцінок коефіцієнтів автокореляції і АКФ. Визначення значущості оцінок коефіцієнтів автокореляції. У якості джерела ПВЧ використовувалися генератор типу «Вихор Мерсенна» [133] і комбінаційний генератор з комбінаційною функцією підсумовування за модулем [30];

− дослідження і аналіз розподілу бічних пелюсток оцінки АКФ випадкової послідовності чисел і статистична перевірка гіпотез відповідності з цим розподілом бічних пелюсток оцінок АКФ ПВП. Бічними пелюстками АКФ названі точки на графіку АКФ (коррелограммі), що відповідають коефіцієнтам кореляції ненульового порядку;

− дослідження розподілу знаків бічних пелюсток оцінок АКФ випадкових і псевдовипадкових послідовностей чисел за допомогою статистичних критеріїв, а також дослідження розподілу *k*-грам для знаків оцінок АКФ.

Оцінка кореляційних властивостей послідовностей випадкових чисел проводилася за фіксованою вибіркою обсягом $V = 2^{16}$ значень алфавіту потужності $M = 256$. Позначимо елемент послідовності випадкових чисел в дискретний момент часу t у вигляді x_t, $t \in [0, V-1]$. Оцінка нормованої АКФ для послідовності випадкових чисел розраховувалася відповідно до [258, с. 460], [259, с. 402] таким чином:

$$r_x(\tau) = \frac{\sum_{i=0}^{V-1-\tau} \left[\left(x_i - \bar{x} \right) \cdot \left(x_{i+\tau} - \bar{x} \right) \right]}{\sqrt{\sum_{i=0}^{V-1-\tau} \left(x_i - \bar{x} \right)^2 \cdot \sum_{i=0}^{V-1-\tau} \left(x_{i+\tau} - \bar{x} \right)^2}}, \qquad (5.6)$$

де $\bar{x} = \frac{1}{V} \sum_{i=0}^{V-1} x_i$ – статистична оцінка математичного сподівання.

Обчислено оцінки нормованих АКФ за $\tau \in \left[1, \frac{V}{4} \right]$ для різних послідовностей:

– випадкової послідовності чисел (оцифрованих радіошумів [306] і квантового ГВЧ [305]);

– послідовності чисел генератора типу «Вихор Мерсенна» [133] MT19937;

– послідовності комбінаційного генератора [30] з різними його параметрами (кількість вихідних циклічних зсувних регістрів – від 4 до 8, різне їх заповнення: за допомогою ЛКГ, адитивного генератора [304] і ГВЧ [305]).

Виконано аналіз значущості оцінок коефіцієнтів автокореляції у відповідності до *t*-критерію Стьюдента [261, с. 26]. Незважаючи на те, що досліджувані випадкові вектори не належать двовимірному нормальному розподілу, така перевірка є правомірною. Це пояснюється тим, що згідно [309], [310], розподіли статистик критеріїв, використовуваних під час перевірки гіпотези про рівність нулю для парних, часткових і множинних коефіцієнтів кореляції (в тому числі і *t*-критерія Стьюдента), стійкі до відхилень спостережуваного багатовимірного закону від нормального.

Проведене дослідження відносних частот потрапляння статистики *t*-критерію Стьюдента в критичну область, а також розподілу максимальних абсолютних значень нормованих коефіцієнтів автокореляції $r_x^*(\tau)=\left[r_x(\tau)-M_r(\tau)\right]/\sigma_r(\tau)$ на 1000 вибірок кожного генератора свідчить про відсутність значущих кореляційних сплесків для всіх оцінок АКФ, а також показує однорідність статистик для всіх розглянутих джерел. При цьому використовувалися значення початкових моментів розподілу нормованих коефіцієнтів автокореляції (5.6) відповідно з виразами, представленими нижче в розділі 4: $M_r(\tau)=-(n-1)^{-1}$, $\sigma_r(\tau)\approx\sqrt{1/(n-\tau)}$.

5.4.5.1. Розподіл нормованих коефіцієнтів автокореляції

Бічними пелюстками АКФ будемо називати точки на коррелограмі для $\tau\neq 0$.

Побудуємо гістограму розподілу нормованих значень $r_x^*(\tau)$ бічних пелюсток оцінки нормованої АКФ випадкової послідовності чисел. Аналогічні гістограми побудуємо і для інших оцінок. Оскільки експериментально отримано $\max\left|r_x^*(\tau)\right|<4.8$, розділимо діапазон значень $(-4.8,4.8)$ на піддіапазони з кроком

$\Delta = 0,2$. Визначимо для кожної оцінки АКФ статистику розподілу амплітуди нормованих бічних пелюсток за піддіапазонами. Гістограми розподілу нормованих значень бічних пелюсток деяких оцінок нормованих АКФ показано на рис. 5.7.

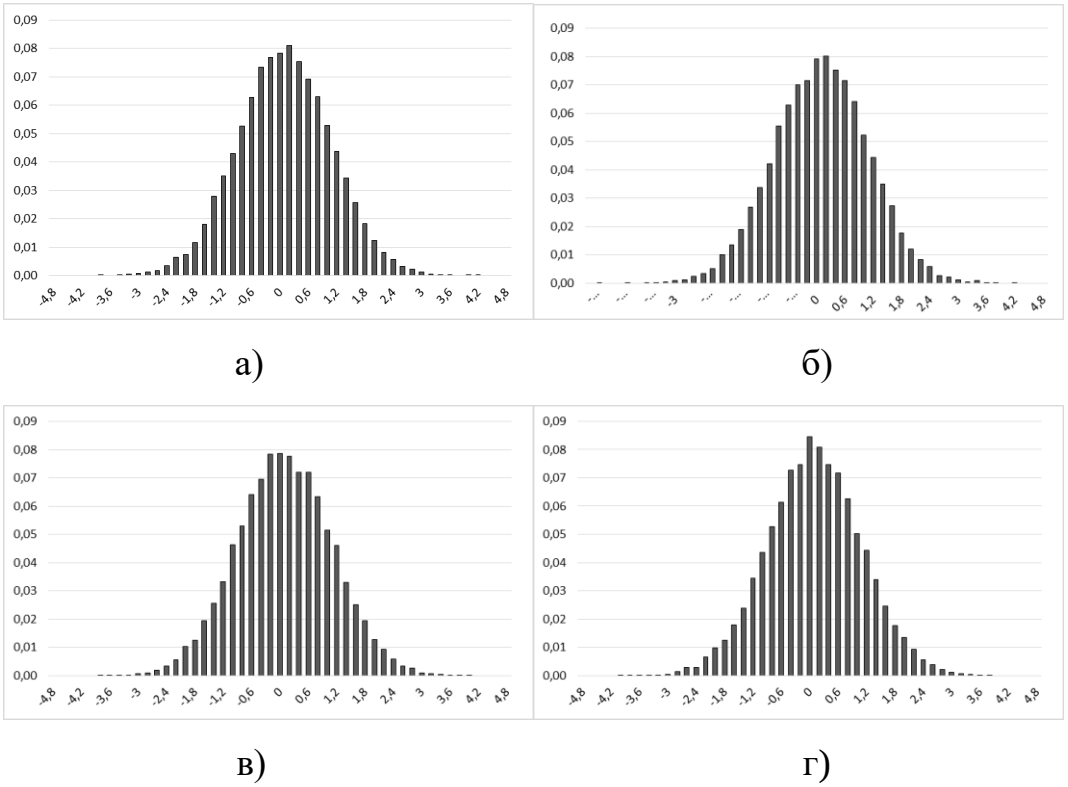


Рис. 5.7. Гістограми розподілу нормованих значень бічних пелюсток оцінок нормованих АКФ для: а – оцифрованих радіошумів; б – вихору Мерсенна; в – комбінаційного генератора з використанням чотирьох циклічних регістрів зсуву і їх заповненням з допомогою ЛКГ; г – комбінаційного генератора з використанням восьми циклічних регістрів зсуву і їх заповненням за допомогою квантового ГВЧ.

Візуальний аналіз гістограм розподілу нормованих значень бічних пелюсток отриманих оцінок нормованих АКФ показує, що розподіли схожі між собою і мають форму нормального закону розподілу.

У таблиці 5.8 відображено результати перевірки узгодженості емпіричного розподілу нормованих значень бічних пелюсток оцінки нормованої АКФ оцифрованих радіошумів з теоретичним граничним (стандартним нормальним) за критеріями Колмогорова [261, с. 80–82], Смірнова [261, с. 80–82], ω^2 Крамера-

Мізеса-Смірнова [258, с. 277–281], [261, с. 83], Ω^2 Андерсона-Дарлінга [261, с. 83], [311] і χ^2 Пірсона [258, с. 267–275].

Таблиця 5.8

Результати перевірки гіпотези нормальності розподілу нормованих значень бічних пелюсток оцінки нормованої АКФ оцифрованих радіошумів

Критерій	Розрахункове значення статистики S^*	Критична область	Досягнутий рівень значущості $P\left(S > S^*\right)$
Колмогорова	0,7082	$S_K > 1{,}3581$	0,6976
Смірнова	2,0059	$S_m > 5{,}9915$	0,3668
ω^2 Крамера-Мізеса-Смірнова	0,0820	$n\omega^2 > 0{,}4614$	0,6807
Ω^2 Андерсона-Дарлінга	0,5694	$n\Omega^2 > 2{,}4924$	0,6773
χ^2 Пірсона	21,14	$\chi^2 > 47{,}40$	0,9451

Для кожного з критеріїв наведено розрахункове значення статистики, критична область за рівня значущості $\alpha = 0.05$, а також досягнутий рівень значущості $P\left(S > S^*\right) = 1 - G\left(S \middle| H_0\right)$, де $G\left(S \middle| H_0\right)$ – граничний розподіл статистики S відповідного критерію узгодженості за справедливості гіпотези H_0, що перевіряється, S^* – розрахункове значення статистики критерію.

Досягнуті рівні значущості статистик критеріїв свідчать про узгодженість емпіричного розподілу нормованих значень бічних пелюсток оцінки нормованої АКФ оцифрованих радіошумів зі стандартним нормальним законом.

Відповідно до критерію χ^2 [258, с. 267–275] виконаємо перевірку гіпотези однорідності розподілу нормованих значень бічних пелюсток кожної з оцінок нормованих АКФ розглянутих послідовностей ПВЧ і розподілу нормованих значень бічних пелюсток оцінки нормованої АКФ послідовності випадкових чисел оцифрованих радіошумів. Розрахункові значення статистик розглянутого критерію, їх критичні області для рівня значущості $\alpha = 0.05$, а також досягнуті рівні значущості наведено в таблиці 5.9.

Таблиця 5.9

Результати перевірки гіпотези однорідності розподілу нормованих значень бічних пелюсток оцінок нормованих АКФ

		Заповнення первинних циклічних зсувних регістрів	Кількість первинних циклічних зсувних регістрів	Розрахункове значення статистики χ^2	Досягнутий рівень значущості $P\left(S > S^*\right)$
Джерело ПВЧ	Комбінаційний генератор	Лінійний конгруентний генератор	4	28,20	0,71
			6	34,36	0,40
			8	25,49	0,82
		Адитивний генератор	4	22,44	0,92
			6	29,21	0,66
			8	18,70	0,98
		Квантовий ГВЧ	4	27,94	0,72
			6	19,63	0,97
			8	29,82	0,63
	Вихор Мерсенна			25,90	0,81
Квантовий ГВЧ				22,83	0,91
Критична область статистики критерію при $\alpha = 0.05$				$\chi^2 > 47,40$	

Наведені результати аналізу (таблиця 5.9) показують, що розрахункові значення статистик не потрапляють у критичні області (досягнуті рівні значущості істотно перевищують $\alpha = 0.05$), тому гіпотезу однорідності розподілів нормованих значень бічних пелюсток оцінок нормованих АКФ слід прийняти.

Також з метою перевірки статистичної гіпотези про однорідність розподілів бічних пелюсток оцінок нормованих АКФ послідовностей ПВЧ розподілу бічних пелюсток оцінки нормованої АКФ послідовності випадкових чисел оцифрованих радіошумів скористаємося статистичними критеріями знаків [258, с. 254–260], [261, с. 89–91] і серій [261, с. 91–93], а також ранговими критеріями Смірнова [261, с. 81], Вілкоксона [261, с. 93–95] і типу омега-квадрат Лемана-Розенблатта [261, с. 86]. Врахуємо, що відповідно до рекомендацій, викладених у [312], [313], під час перевірки гіпотези абсолютної однорідності двох незалежних вибірок спроможними (рос. состоятельными) критеріями (статистичними критеріями, що достовірно відрізняють перевірювану гіпотезу від альтернатив за необмеженого збільшення кількості спостережень) є тільки критерії Смірнова та Лемана-Розенблатта.

Розрахункові значення статистик усіх розглянутих критеріїв, а також їх критичні області для рівня значущості $\alpha = 0.05$ наведено в таблиці 5.10.

Таблиця 5.10

Розрахункові і критичні значення статистик критеріїв знаків, серій, Смірнова, Вілкоксона і Лемана-Розенблатта в результаті перевірки гіпотези про однорідність розподілів бічних пелюсток оцінок нормованих АКФ

		Заповнення первинних циклічних зсувних регістрів	Кількість первинних циклічних зсувних регістрів	Розрахункові значення статистик				
				$F_{в1}$, $F_{в2}$ критерію знаків	$s_в$ критерію серій	$D_{m,n}$ критерію Смірнова	$z_в$ критерію Вілкоксона	t критерію Лемана-Розенблатта
Джерело ПВЧ	Комбінаційний генератор	ЛКГ	4	$F_{в1}$=1,0093 $F_{в2}$=0,9905	0,5262	0,0054	-0,1175	0,0457
			6	$F_{в1}$=1,0098 $F_{в2}$=0,9900	-1,9267	0,0052	-0,0313	0,0451
			8	$F_{в1}$=1,0113 $F_{в2}$=0,9886	1,9651	0,0080	-1,0645	0,1349
		Адитивний генератор	4	$F_{в1}$=1,0066 $F_{в2}$=0,9932	-1,1627	0,0079	-0,3760	0,0739
			6	$F_{в1}$=0,9956 $F_{в2}$=1,0042	0,0241	0,0099	-0,0865	0,1779
			8	$F_{в1}$=1,0034 $F_{в2}$=0,9963	0,3051	0,0070	-0,3205	0,0547
		Квантовий ГВЧ	4	$F_{в1}$=1,0088 $F_{в2}$=0,9910	0,9635	0,0078	-0,5695	0,0807
			6	$F_{в1}$=1,0150 $F_{в2}$=0,9850	-0,0632	0,0063	-0,3159	0,0338
			8	$F_{в1}$=1,0103 $F_{в2}$=0,9896	-2,5046	0,0075	-0,3828	0,0512
	Вихор Мерсенна			$F_{в1}$=0,9912 $F_{в2}$=1,0086	0,7447	0,0064	-0,1831	0,0759
Квантовий ГВЧ				$F_{в1}$=1,0093 $F_{в2}$=0,9905	0,2762	0,0048	-0,2634	0,0262
Критична область статистики критерію				$F_в$>1,0311	$\lvert s_в \rvert$>2,576	$D_{m,n} \geq 0,015$	$\lvert z_в \rvert$>1,96	t > 0,461

Розрахункові значення статистик (таблиця 5.10) не потрапляють у критичні області, тому гіпотезу однорідності розподілів бічних пелюсток оцінок нормованих АКФ послідовностей ПВЧ розподілу бічних пелюсток оцінки нормованої АКФ послідовності випадкових чисел оцифрованих радіошумів слід прийняти.

Отримані результати підтверджують, що запропонований комбінаційний генератор може бути використаний у задачах, що потребують високої якості ПВП, в тому числі для криптографічних перетворень.

5.4.5.2. Розподіл знаків бічних пелюсток АКФ

У роботі [37] виконано також аналіз розподілу знаків у отриманих послідовностях за допомогою статистичних критеріїв знаків [258, с. 254–260], [261, с. 89–91] і серій [261, с. 91–93]. Результати перевірки підтверджують гіпотезу про рівну ймовірності позитивного і негативного знаку оцінок АКФ для критерію знаків і гіпотезу про випадковість розташування позитивних і негативних знаків оцінок АКФ для критерію серій.

Виконано перевірку рівномірного розподілу знаків бічних пелюсток оцінок АКФ в k-вимірному просторі $(1 \le k \le 8)$ за допомогою критерію χ^2 [258, с. 267–275]. Оскільки значна кількість статистик потрапляє в критичну область, в тому числі і для оцифрованих радіошумів, отримані результати не можуть свідчити про те, що розподіли k-грам для знаків оцінок нормованих АКФ при $k \ge 2$ для досліджуваних послідовностей чисел є рівномірними.

Разом з тим, запропонований у роботі [37] підхід до аналізу знаків бічних пелюсток оцінок АКФ в k-вимірному просторі є новим у кореляційному аналізі та знаходить своє продовження в наступному розділі цієї роботи.

Отримані результати підтверджують, що запропонований комбінаційний метод формування ПВП може бути використаний у задачах, що потребують високої якості ПВП, у тому числі для криптографічних перетворень.

Зокрема, наведені вище методи формування ПВП можуть бути успішно застосовані для створення прихованого каналу передавання даних [14], [15], [314], [315], організації ключового обміну [11], [18], стеганографічних додатків [316], підвищення стійкості електронних кодових замків [24], [317]. Крім того, комбінаційний метод формування ПВП є основою для синтезу ПВП на основі додавання за модулем M результатів n операцій криптографічного перетворення інформації [31]–[33], [318], що є окремим напрямом досліджень.

5.5. Висновки

У п’ятому розділі дисертаційної роботи отримано наступні результати:

− вперше теоретично обґрунтовано принципи побудови комбінаційного генератора з комбінаційною функцією підсумовування за модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел як з необмеженими, так і з обмеженими періодами, а також перестановок, які циклічно повторюються, за рахунок визначення закону розподілу д.в.в. на виході такого комбінаційного генератора, що дозволило сформувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення необхідних статистичних властивостей послідовності чисел, зокрема, в реалізаціях запропонованого методу формування перестановок на основі ФСЧ;

− розроблено методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем M, що дозволяє забезпечити рівномірний розподіл сформованої д.в.в. на множині цілих чисел потужності M та проходження пакетів статистичного тестування ПВП NIST STS, Diehard, TestU01.

РОЗДІЛ 6. МЕТОД І КРИТЕРІЇ ОЦІНЮВАННЯ ПОСЛІДОВНОСТЕЙ ВИПАДКОВИХ ЧИСЕЛ. МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

6.1. Вступ

Оскільки випадкові послідовності чисел є багатопараметричними процесами, для оцінки їх якості використовують різні методи та критерії. Ці методи та критерії розглядають випадкові процеси з різних позицій, використовуючи для цього різні статистичні оцінки.

У першому розділі дисертації показано, що питання оцінки коефіцієнтів автокореляції випадкових і псевдовипадкових послідовностей чисел є недостатньо вивченим. У цьому розділі вирішується задача розробки методу та критерію оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що дозволяє виявити в них не виявлені до теперішнього часу статистичні нерегулярності. Крім того, актуальними є питання кількісної оцінки помилки відтворення закону розподілу д.в.в. в результаті зміни її області визначення, що також знаходить відображення в цьому розділі.

Разом з тим, для вирішення поставлених задач попередньо оцінимо статистичні властивості нормованих коефіцієнтів автокореляції дискретного випадкового процесу, які обчислюються відповідно до різних підходів. Ця оцінка необхідна для побудови статистичних критеріїв перевірки гіпотези відповідності АКФ досліджуваної послідовності кореляційним властивостями білого шуму, АКФ якого математично описується дельта-функцією Дірака [260, с. 84]. Зауважимо, що ця перевірка є інтегральною і враховує коефіцієнти автокореляції всіх порядків (подібно критеріям Бокса-Пірса [262], Льюнга-Бокса [263]), на відміну від перевірки згідно з t-критерієм Стьюдента [261].

У шостому розділі вирішується також підсумкова задача дисертаційної роботи, що полягає в розробці методології захисту інформації на основі факторіального кодування даних.

6.2. Критерій оцінювання послідовностей рівномірно розподілених випадкових чисел

6.2.1. Інтегральна оцінка коефіцієнтів автокореляції

Згідно [319, с. 247], у загальному вигляді нормований коефіцієнт автокореляції $\rho_x(t',t")$ випадкового процесу $X(t)$ обчислюється відповідно до виразу:

$$\rho_X(t',t") = \frac{K_X(t',t")}{\sqrt{D_X(t')}\cdot\sqrt{D_X(t")}} = \\ = \frac{M\left[\left(X(t')-M\left[X(t')\right]\right)\cdot\left(X(t")-M\left[X(t")\right]\right)\right]}{\sqrt{D_X(t')}\cdot\sqrt{D_X(t")}}, \tag{6.1}$$

де $X(t'),\ X(t")$ – перетини випадкового процесу в моменти часу t' і $t" = t'+\tau$. Ці перетини $X(t')$ і $X(t")$ будемо представляти як випадкові величини X' і $X"$;

$M\left[X(t')\right] = M(X'),\ M\left[X(t")\right] = M(X")$ – математичні сподівання перетинів випадкового процесу $X(t'),\ X(t")$ (випадкових величин X' і $X"$);

$D_X(t') = D(X'),\ D_X(t") = D(X")$ – дисперсії перетинів випадкового процесу $X(t'),\ X(t")$ (випадкових величин X' і $X"$);

$K_X(t',t")$ – кореляційний момент (коефіцієнт коваріації) перетинів випадкового процесу $X(t'),\ X(t")$ (випадкових величин X' і $X"$).

Покладемо, що процес на виході ГВЧ (ГПВЧ) є стаціонарним випадковим процесом. Для такого процесу $M\left[X(t')\right] = M\left[X(t")\right] = m_X = const$, $D_X(t') = D_X(t") = \sigma_X^2 = const$, а коефіцієнт автокореляції залежить тільки від величини зсуву $\tau = t"-t'$: $K_X(t',t") = k_X(\tau)$.

Нехай $\overset{\circ}{X}' = X' - M(X'),\ \overset{\circ}{X}" = X" - M(X")$ – центровані випадкові величини з математичними сподіваннями $M\left(\overset{\circ}{X}'\right) = M\left(\overset{\circ}{X}"\right) = 0$ і дисперсіями $D\left(\overset{\circ}{X}'\right) = D\left(\overset{\circ}{X}"\right) = \sigma_X^2$. Тоді кореляційний момент

$$k_X(\tau) = M\left(\overset{\circ}{X}' \cdot \overset{\circ}{X}''\right),$$

а нормований коефіцієнт автокореляції

$$\rho_X(\tau) = \frac{k_X(\tau)}{\sqrt{D(X')} \cdot \sqrt{D(X'')}} = \frac{M\left(\overset{\circ}{X}' \cdot \overset{\circ}{X}''\right)}{\sigma_X^2}. \qquad (6.2)$$

Нехай випадкові величини $\overset{\circ}{X}'$ і $\overset{\circ}{X}''$ є некорельованими, що відповідає властивостям перетинів білого шуму, і незалежними. Тоді величина $\rho_X(\tau)$ інваріантна по відношенню до величини $\tau \neq 0$ і $\rho_X(\tau \neq 0) \equiv 0$ [258, с. 170].

Зазначимо, що добуток випадкових величин $\xi = \overset{\circ}{X}' \cdot \overset{\circ}{X}''$ може сам розглядатися як випадкова величина з параметрами: $M(\xi) = M\left(\overset{\circ}{X}'\right) \cdot M\left(\overset{\circ}{X}''\right) = 0$ і

$$D(\xi) = M(\xi^2) - M^2(\xi) = M\left[\left(\overset{\circ}{X}' \cdot \overset{\circ}{X}''\right)^2\right] = M\left(\overset{\circ}{X}'^2\right) \cdot M\left(\overset{\circ}{X}''^2\right) = D\left(\overset{\circ}{X}'\right) \cdot D\left(\overset{\circ}{X}''\right) = \sigma_X^4,$$

а $\sigma_\xi = \sigma_X^2$. У такому випадку $\rho_X(\tau) = \dfrac{M(\xi)}{\sigma_\xi}$.

Зауважимо, що для значень дискретного випадкового процесу $\xi(t)$, що утворюють зліченну множину незалежних значень $\xi_1, \xi_2, \ldots, \xi_n, \ldots$, $M(\xi) = \lim\limits_{n\to\infty}\left(\dfrac{1}{n}\sum\limits_{i=1}^{n}\xi_i\right)$.

Відповідно до теореми Ліндеберга-Леві [319, с. 206], якщо взаємно незалежні випадкові величини $\xi_1, \xi_2, \ldots, \xi_n, \ldots$ однаково розподілені і мають математичне сподівання $M(\xi) = a$ і дисперсію σ_ξ^2, то для $n \to \infty$ величина $\dfrac{\sum\limits_{i=1}^{n}\xi_i - na}{\sigma_\xi\sqrt{n}}$ має стандартний нормальний розподіл:

$$\frac{\sum\limits_{i=1}^{n}\xi_i - na}{\sigma_\xi\sqrt{n}} \to N(0;1).$$

З урахуванням того, що $M(\xi)=a=0$,

$$\frac{\sum_{i=1}^{n}\xi_i - na}{\sigma_\xi\sqrt{n}} = \frac{\sqrt{n}\frac{1}{n}\sum_{i=1}^{n}\xi_i}{\sigma_\xi} = \sqrt{n}\frac{M(\xi)}{\sigma_\xi} = \sqrt{n}\rho_X(\tau) \to N(0;1).$$

Іншими словами, граничний розподіл нормованого коефіцієнта автокореляції $\rho_X(\tau)$ випадкового процесу, перетини якого є незалежними випадковими величинами, є нормальним розподілом з математичним сподіванням $M\left(\rho_X(\tau)\right)=0$ і дисперсією $D\left(\rho_X(\tau)\right)=\frac{1}{n}$.

Врахуємо, що $D\left(\rho_X(\tau)\right)=M\left(\rho_X^2(\tau)\right)-\left(M\left(\rho_X(\tau)\right)\right)^2=\lim_{\mathrm{T}\to\infty}\left(\frac{1}{\mathrm{T}}\sum_{\tau=1}^{\mathrm{T}}\rho_X^2(\tau)\right)$. Звідси слідує що

$$\lim_{\substack{n\to\infty\\ \mathrm{T}\to\infty}}\left(\sum_{\tau=1}^{\mathrm{T}}\rho_X^2(\tau)\right)=\frac{\mathrm{T}}{n}. \qquad (6.3)$$

Вираз (6.3) визначає граничне значення потужності бічних пелюсток АКФ $W(\mathrm{T})=\sum_{\tau=1}^{\mathrm{T}}\rho_x^2(\tau)$: $\lim_{\substack{n\to\infty\\ \mathrm{T}\to\infty}}\left(W(\mathrm{T})\right)=\frac{\mathrm{T}}{n}$.

Крім того, оскільки для $n\to\infty$ $\rho_X(\tau)\to N\left(0;\frac{1}{n}\right)$, випадкова величина $\sum_{\tau=1}^{\mathrm{T}}n\rho_X^2(\tau)$ для $n\to\infty$ має розподіл χ^2_{T} з T ступенями вільності:

$$n\sum_{\tau=1}^{\mathrm{T}}\rho_X^2(\tau)\to\chi^2_{\mathrm{T}}. \qquad (6.4)$$

Для потужності бічних пелюсток:

$$nW(\mathrm{T})\to\chi^2_{\mathrm{T}}.$$

Таким чином, вираз (6.4) представляє собою інтегральну оцінку коефіцієнтів автокореляції і створює передумови до побудови статистичних критеріїв перевірки кореляційних властивостей досліджуваних послідовностей випадкових і псевдовипадкових чисел за їх емпіричним оцінками.

Незважаючи на те, що нормовані коефіцієнти автокореляції строго визначені теоретичним виразом (6.1), оцінка кореляційних властивостей емпіричної послідовності чисел може істотно залежати від властивостей досліджуваної послідовності й умов експерименту. Зокрема, оцінка кореляційних властивостей послідовності може бути проведена:

- на періоді послідовності в разі її періодичності – шляхом аналізу періодичної АКФ (ПАКФ);
- на деякій непоповнюваній вибірці фіксованого розміру;
- у реальному масштабі часу, коли елементи послідовності почергово надходять на аналізатор.

Крім того, оцінка кореляційних властивостей (псевдо) випадкових послідовностей чисел може проводитися в умовах, коли закон розподілу д.в.в. та його параметри є повністю відомими або визначаються емпіричним шляхом.

У всіх перерахованих випадках для реалізації інтегральної оцінки коефіцієнтів автокореляції необхідно знати перший і другий початкові моменти нормованих коефіцієнтів автокореляції як випадкових величин.

Виконаємо оцінку цих статистичних властивостей нормованих коефіцієнтів автокореляції дискретного випадкового процесу, які обчислюються відповідно до визначених вище підходів.

6.2.2 Оцінка статистичних властивостей нормованих коефіцієнтів автокореляції

6.2.2.1. Оцінка періодичної автокореляційної функції

АКФ є періодичною, якщо вихідна послідовність є також періодичною. Причому, як показано в [320], для періодичних сигналів доцільно оцінювати ймовірнісні моменти на мінімальному періоді, а з урахуванням властивості симетрії графіка ПАКФ відносно осі, віддаленої від осі ординат на половину періоду, допускається скорочення кількості обчислюваних значень у 2 рази.

Нехай існує періодично повторювана з періодом n послідовність чисел $\left(x_0, x_1, \cdots, x_{n-1}\right)$. У такому випадку, як показано в [156, с. 72] і [187, с. 127–131],

оцінка нормованого коефіцієнта автокореляції обчислюється відповідно до виразу:

$$r_{ПАКФ\ x}(\tau)=\frac{\sum_{i=0}^{n-1}\left[\left(x_i-\bar{x}\right)\cdot\left(x_{(i+\tau)\bmod n}-\bar{x}\right)\right]}{\sum_{i=0}^{n-1}\left(x_i-\bar{x}\right)^2}=\frac{n\sum_{i=0}^{n-1}x_i x_{(i+\tau)\bmod n}-\left(\sum_{i=0}^{n-1}x_i\right)^2}{n\sum_{i=0}^{n-1}x_i^2-\left(\sum_{i=0}^{n-1}x_i\right)^2},\qquad(6.5)$$

де $\bar{x}=\frac{1}{n}\sum_{i=0}^{n-1}x_i$ – статистична оцінка математичного сподівання д.в.в. X.

Зауважимо, що оцінка (6.5) виконується на всьому періоді послідовності. Тому оцінка математичного сподівання д.в.в. X збігається з математичним сподіванням: $\bar{x}=\frac{1}{n}\sum_{i=0}^{n-1}x_i=\lim_{m\to\infty}\left(\frac{1}{m}\sum_{i=0}^{m}x_i\right)=M(X)$. Виходячи з подібних міркувань, оцінка дисперсії на всьому періоді послідовності також збігається з дисперсією д.в.в.: $\sigma_x^2=\frac{1}{n}\sum_{i=0}^{n-1}\left(x_i-\bar{x}\right)^2=\lim_{m\to\infty}\left(\frac{1}{m}\sum_{i=0}^{m}\left(x_i-M(X)\right)^2\right)=D(X)=\sigma_X^2$. Тоді вираз (6.5) можна представити у вигляді:

$$r_{ПАКФ\ x}(\tau)=\frac{\frac{1}{n}\sum_{i=0}^{n-1}\left[\left(x_i-M(X)\right)\cdot\left(x_{(i+\tau)\bmod n}-M(X)\right)\right]}{\sigma_X^2}.\qquad(6.6)$$

Очевидно, що з урахуванням властивості симетрії графіка ПАКФ відносно осі, віддаленої від осі ординат на половину періоду, аналіз оцінок коефіцієнтів автокореляції доцільно проводити для $\tau\in\left(0;\left[n/2\right]+1\right)$.

Відповідно до [156, с. 73], $M\left(r_{ПАКФ\ x}(\tau)\right)=-\frac{1}{n-1}$, а оцінка зверху дисперсії величини $r_{ПАКФ\ x}(\tau)$, обчисленої за (6.5) для довільних незалежних змінних, має вигляд: $D\left(r_{ПАКФ\ x}(\tau)\right)\le\frac{n^2}{(n-1)^2(n-2)}$. Разом з тим, за нормального розподілу вихідних величин $D_{норм}\left(r_{ПАКФ\ x}(\tau)\right)=\frac{n(n-3)}{(n+1)(n-1)^2}$ [321], а за їх рівномірного розподілу – $D_{равн}\left(r_{ПАКФ\ x}(\tau)\right)=\frac{24}{5}n^{-2}+O\left(n^{-7/3}\log(n)\right)$ [156, с. 73]. Крім того, як

показано в [322], величина $r_{ПАКФ\,x}(\tau)$ розподілена асимптотично нормально навіть для досить малих об'ємах вибірок $(n>10)$, а в [156, с. 73] надано рекомендацію, що для некорельованих величин оцінка (6.5) повинна знаходитися між значеннями $M\left(r_{ПАКФ\,x}(\tau)\right)-2\sqrt{D\left(r_{ПАКФ\,x}(\tau)\right)}$ і $M\left(r_{ПАКФ\,x}(\tau)\right)+2\sqrt{D\left(r_{ПАКФ\,x}(\tau)\right)}$.

6.2.2.2. Оцінка АКФ за вибіркою фіксованого розміру

Зазначимо, що оцінка АКФ за деякою непоповнюваною вибіркою $(x_0, x_1, \cdots, x_{n-1})$ фіксованого розміру n широко використовується в econometриці для побудови регресійних моделей [262], [263]. Крім того, подібна оцінка АКФ використовується для дослідження властивостей послідовностей в аперіодичному режимі, характерному для передавання інформації в системах зв'язку [323, с. 62]. У цьому випадку оцінка нормованої АКФ розраховується відповідно до виразу [324]:

$$r_x^*(\tau)=\frac{C_\tau^*}{C_0^*}=\frac{\frac{1}{n-\tau}\sum_{i=0}^{n-1-\tau}\left[\left(x_i-M(X)\right)\cdot\left(x_{i+\tau}-M(X)\right)\right]}{\frac{1}{n}\sum_{i=0}^{n-1}\left(x_i-M(X)\right)^2} \tag{6.7}$$

за відомого апріорно значення $M(X)$ або виразом [324]:

$$r_x^{**}(\tau)=\frac{C_\tau^{**}}{C_0^{**}}=\frac{\frac{1}{n-\tau}\sum_{i=0}^{n-1-\tau}\left[\left(x_i-\bar{x}\right)\cdot\left(x_{i+\tau}-\bar{x}\right)\right]}{\frac{1}{n}\sum_{i=0}^{n-1}\left(x_i-\bar{x}\right)^2}, \tag{6.8}$$

де $\bar{x}=\frac{1}{n}\sum_{i=0}^{n-1}x_i$ – статистична оцінка математичного сподівання $M(X)$.

У роботі [324] показано, що якщо випадкові вектори $(x_i, x_{i+\tau})$ є незалежними і однаково розподіленими, то закон розподілу величини $r_x^*(\tau)$ (а також і $r_x^{**}(\tau)$) має асимптотичний нормальний розподіл.

Різні автори використовують або рекомендують використовувати для оцінки (6.8) значення нуля в якості наближеної оцінки її математичного сподівання і значення $n^{-1/2}$ [262] або $\left(n(n+2)/(n-\tau)\right)^{-1/2}$ [263] як наближену оцінку її

середньоквадратичного відхилення. Разом з тим, точне значення математичного сподівання оцінки (6.8) визначено в [325] і дорівнює $M\left(r_x^{**}(\tau)\right)=-(n-1)^{-1}$. Верхню межу дисперсії оцінки (6.8) для будь-якого закону розподілу вихідних значень $\{x_i\}$ визначено в [326]: $D\left(r_x^{**}(\tau)\right)\le\dfrac{n^4-(\tau+7)n^3+(7\tau+16)n^2+2(\tau^2-9\tau-6)n-4\tau(\tau-4)}{n(n-1)^2(n-2)(n-3)}$. Крім того, в [326] також показано, що для нормально розподілених випадкових величин $D_{норм}\left(r_x^{**}(\tau)\right)=\dfrac{n^4-(\tau+3)n^3+3\tau n^2+2\tau(\tau+1)n-4\tau^2}{(n+1)n^2(n-1)^2}$, а вираз $D\left(r_x^{**}(\tau)\right)=(n-\tau)/(n(n+2))$ з [263] справедливий у разі відомого математичного сподівання $M(X)$, тобто для величини $r_x^{*}(\tau)$ за (6.7).

Розглянемо вираз для оцінки нормованої АКФ, що приводиться, наприклад, у [258, с. 460] або [259, с. 402]:

$$r_x^{***}(\tau)=\frac{\sum_{i=0}^{n-1-\tau}\left[\left(x_i-\bar{x}\right)\cdot\left(x_{i+\tau}-\bar{x}\right)\right]}{\sqrt{\sum_{i=0}^{n-1-\tau}\left(x_i-\bar{x}\right)^2\cdot\sum_{i=0}^{n-1-\tau}\left(x_{i+\tau}-\bar{x}\right)^2}},\qquad(6.9)$$

де $\bar{x}=\dfrac{1}{n}\sum_{i=0}^{n-1}x_i$.

Закон розподілу величини $r_x^{***}(\tau)$ для незалежних і однаково розподілених випадкових векторів $(x_i,x_{i+\tau})$ має асимптотичний нормальний розподіл [327, розд. 3.2.1]. Це твердження також підтверджується роботами [309], [310], де показано, що розподіли статистик кореляційного аналізу стійкі до відхилень спостережуваного багатовимірного закону від нормального, а емпіричні розподіли цих статистик добре описуються граничними законами, отриманими в припущенні про нормальність спостережуваних величин.

Для знаходження математичного сподівання $M\left(r_x^{***}(\tau)\right)$ скористаємося методикою, викладеною в [325].

Нехай $z_i = x_i - \bar{x}$, тоді $\sum_{i=0}^{n-1} z_i = \sum_{i=0}^{n-1}\left(x_i - \bar{x}\right) = \sum_{i=0}^{n-1} x_i - n\bar{x} = 0.$

$$M\left(r_x^{***}(\tau)\right) = M\left(\frac{\sum_{i=0}^{n-1-\tau} z_i \cdot z_{i+\tau}}{\sqrt{\sum_{i=0}^{n-1-\tau} z_i^2 \cdot \sum_{i=0}^{n-1-\tau} z_{i+\tau}^2}}\right) = M\left(\frac{(n-\tau)\cdot z_i \cdot z_{i+\tau}}{\sum_{i=0}^{n-1-\tau} z_i^2}\right) = n \cdot M\left(\frac{z_i \cdot z_{i+\tau}}{\sum_{i=0}^{n-1} z_i^2}\right) =$$

$$= \frac{1}{n-1} \cdot M\left(\frac{\sum_{i\neq j}\left(z_i \cdot z_j\right)}{\sum_{i=0}^{n-1} z_i^2}\right) = \frac{1}{n-1} \cdot M\left(\frac{\left(\sum_{i=0}^{n-1} z_i\right)^2 - \sum_{i=0}^{n-1} z_i^2}{\sum_{i=0}^{n-1} z_i^2}\right) = -(n-1)^{-1}.$$

Дисперсія $D\left(r_x^{***}(\tau)\right)$ може бути обчислена згідно з загальновідомим виразом:

$$D\left(r_x^{***}(\tau)\right) = M\left(\left(r_x^{***}(\tau)\right)^2\right) - M^2\left(r_x^{***}(\tau)\right).$$

Як показано в [326], $\left(\sum_{i=0}^{n-1-\tau} z_i z_{i+\tau}\right)^2 = \sum_{i=0}^{n-1-\tau} z_i^2 z_{i+\tau}^2 + 2\sum_{i=0}^{n-1-2\tau} z_i\, z_{i+\tau}^2 z_{i+2\tau} + \sum_{*} z_i z_{i+\tau} z_j z_{j+\tau}$, де $\sum_{*}$ означає підсумовування за $i, j = 1,\ldots,n-\tau$, причому $i, i+\tau, j, j+\tau$ – різні. Крім того, за умови симетричного спільного розподілу величин $z_0,\ldots,z_{n-1}$,

$$M\left(\left(r_x^{***}(\tau)\right)^2\right) = M\left[\left(\sum_{i=0}^{n-1-\tau} z_i^2 \cdot \sum_{i=0}^{n-1-\tau} z_{i+\tau}^2\right)^{-1} \left\{\begin{array}{l}(n-\tau)z_1^2 z_2^2 + 2(n-\tau)z_1^2 z_2 z_3 + \\ +\left((n-\tau)^2 - 2(n-2\tau) - (n-\tau)\right) z_1 z_2 z_3 z_4\end{array}\right\}\right] =$$

$$= M\left[\left(\frac{n-\tau}{n}\sum_{i=0}^{n-1} z_i^2\right)^{-2} \left\{\begin{array}{l}\dfrac{n-\tau}{n(n-1)}\sum^{*} z_i^2 z_j^2 + \dfrac{2(n-2\tau)}{n(n-1)(n-2)}\sum^{*} z_i^2 z_j z_k + \\ +\dfrac{(n-\tau)^2 - 2(n-2\tau) - (n-\tau)}{n(n-1)(n-2)(n-3)}\sum^{*} z_i z_j z_k z_l\end{array}\right\}\right],$$

де $\sum^{*}$ позначає підсумовування за всіма різними індексами від 0 до $n-1$.

Використовуючи для $r \geq 1$ рівність $S_r = \sum_{i=0}^{n-1} z_i^r$, а також $\sum^{*} z_i^2 z_j^2 = S_2^2 - S_4$, $\sum^{*} z_i^2 z_j z_k = 2S_4 - S_2^2$ і $\sum^{*} z_i z_j z_k z_l = 3S_2^2 - 6S_4$ з [328, с. 708], за аналогією з [326]

отримаємо:

$$M\left(\left(r_x^{***}(\tau)\right)^2\right)=\frac{n}{(n-1)(n-2)(n-3)(n-\tau)^2}\left[\begin{array}{l}\left(-n^3+(\tau+3)n^2-\tau(n+6\tau)\right)M\left[S_4/S_2^2\right]+\\+\left(n^2(n-\tau-4)+3(n-\tau)+3\tau(n+\tau)\right)\end{array}\right].$$

Як показано в [326], [329], $1/n\le S_4/S_2^2\le 1$ для будь-якого закону розподілу випадкових величин z_i. Тоді, за аналогією з [326], Можна отримати верхню межу дисперсії оцінки коефіцієнта кореляції за (6.9). Для цього, замінюючи $M\left[S_4/S_2^2\right]$ на $1/n$, отримаємо:

$$M\left(\left(r_x^{***}(\tau)\right)^2\right)\le\frac{n^4-n^3(\tau+5)+n^2(4\tau+6)+n\left(3\tau^2-4\tau\right)-6\tau^2}{(n-1)(n-2)(n-3)(n-\tau)^2}.$$

Тоді

$$D\left(r_x^{***}(\tau)\right)\le\frac{n^5-n^4(\tau+7)+n^3(7\tau+16)+n^2\left(2\tau^2-18\tau-12\right)-n\left(4\tau^2-16\tau\right)}{(n-1)^2(n-2)(n-3)(n-\tau)^2}. \quad (6.10)$$

Відповідно до [325], для нормально розподілених випадкових величин x_i виконується $M\left[S_4/S_2^2\right]=\frac{3(n-1)}{n(n+1)}$, а

$$D_{норм}\left(r_x^{***}(\tau)\right)=\frac{n^4-(\tau+3)n^3+3\tau n^2+2\tau(\tau+1)n-4\tau^2}{(n+1)(n-1)^2(n-\tau)^2}. \quad (6.11)$$

Варто зазначити, що

$$D_{норм}\left(r_x^{***}(\tau)\right)=\frac{1-\frac{3}{n}+\frac{2\tau}{n^3}+\frac{2\tau^2(n-1)}{n^3(n-\tau)}}{\left(1+\frac{1}{n}\right)\left(1-\frac{1}{n}\right)^2(n-\tau)}\xrightarrow[n\gg\tau]{n\to\infty}\frac{1}{n-\tau}.$$

Крім того, в загальному випадку

$$D\left(r_x^{***}(\tau)\right)\le\frac{1-\frac{7}{n}+\frac{16}{n^2}-\frac{12}{n^3}+\frac{2\tau(\tau-1)(n-2)}{n^3(n-\tau)}}{\left(1-\frac{1}{n}\right)^2\left(1-\frac{2}{n}\right)\left(1-\frac{3}{n}\right)(n-\tau)}\xrightarrow[n\gg\tau]{n\to\infty}\frac{1}{n-\tau}.$$

Таким чином, отримані результати повністю узгоджуються з [259, с. 412], де

показано, що дисперсія оцінки за (6.9) асимптотично дорівнює $\frac{1}{n-\tau}$ за умови, що значення n велике. Разом з тим, отримані оцінки (6.10) і (6.11) є більш точними. Основні результати представленого дослідження відображені в роботі автора [59].

6.2.2.3. Оцінка АКФ для послідовностей великого періоду

Під час аналізу кореляційних властивостей послідовності випадкових чисел, породжених стаціонарним дискретним випадковим процесом $X(t)$, множиною $\{x_i(t)\}$ реалізацій цього випадкового процесу можуть бути будь-які з зсувів аналізованої послідовності (іншими словами, «нульова» точка відліку початку реалізації може бути довільною). У такому випадку можна розглядати множину реалізацій $\{x_i(t): x_i(t) = x_{i-j}(t+j)\}$. Для забезпечення можливості практичного аналізу коефіцієнтів автокореляції реалізаціями випадкового процесу $X(t)$ вважатимемо послідовності з n чисел, перші з яких формуються в моменти часу $t = 0,1,2,\ldots$. Такий підхід є найбільш ефективним у разі, коли кореляційні властивості послідовності випадкових чисел аналізуються не за деякою непоповнюваною вибіркою фіксованого розміру, а розраховуються в реальному масштабі часу, в той час як елементи послідовності записуються в буфер обмеженого об'єму (такий підхід нагадує метод «ковзного вікна»).

Позначимо елемент послідовності випадкових чисел у дискретний момент часу t у вигляді x_t. Тоді оцінка нормованого коефіцієнта автокореляції порядку τ знаходиться таким чином:

$$r_x(\tau) = \frac{\sum_{i=0}^{n-1}\left[\left(x_{t+i} - \overline{x(t)}\right)\cdot\left(x_{t+\tau+i} - \overline{x(t+\tau)}\right)\right]}{\sqrt{\sum_{i=0}^{n-1}\left(x_{t+i} - \overline{x(t)}\right)^2 \cdot \sum_{i=0}^{n-1}\left(x_{t+\tau+i} - \overline{x(t+\tau)}\right)^2}}, \qquad (6.12)$$

де $\overline{x(t)} = \frac{1}{n}\sum_{i=0}^{n-1} x_{t+i}$, $\overline{x(t+\tau)} = \frac{1}{n}\sum_{i=0}^{n-1} x_{t+\tau+i}$ – середні вибіркові значення перетинів випадкового процесу $X(t)$, $X(t+\tau)$. Зауважимо, що для стаціонарного випадкового

процесу для наскільки завгодно малих значень $\varepsilon > 0$ виконується рівність $\lim\limits_{n\to\infty}\left(P\left(\left|\overline{x(t)} - \overline{x(t+\tau)}\right| < \varepsilon\right)\right) = 1.$

Закон розподілу оцінки $r_x(\tau)$ за (6.12) для незалежних і однаково розподілених випадкових векторів $(x_{t+i}, x_{t+\tau+i})$ є асимптотично нормальним [327, розд. 3.2.1] з математичним сподіванням $\rho_x(\tau)$ і дисперсією [330, с. 393]

$$D\left(r_x(\tau)\right) = \frac{\rho^2}{4n}\left(\frac{\mu_{40}}{\mu_{20}^2} + \frac{\mu_{04}}{\mu_{02}^2} + \frac{2\mu_{22}}{\mu_{20}\mu_{02}} + \frac{4\mu_{22}}{\mu_{11}^2} - \frac{4\mu_{31}}{\mu_{11}\mu_{20}} - \frac{4\mu_{13}}{\mu_{11}\mu_{02}}\right),$$

де під μ_{km} розуміються теоретичні центральні моменти порядку k і m: $\mu_{km} = \left(x_{t+i} - M\left(x_{t+i}\right)\right)^k \left(x_{t+\tau+i} - M\left(x_{t+\tau+i}\right)\right)^m$. Згідно з [330, с. 393], у разі нормально розподіленої сукупності $D\left(r_x(\tau)\right) = \frac{\left(1-\rho^2\right)^2}{n}$.

Разом з тим, як показано в [330, с. 436, 506], внаслідок застосування логарифмічного перетворення Фішера [331] до вибіркових коефіцієнтів кореляції r, величину $z = \frac{1}{2}\ln\left(\frac{1+r}{1-r}\right)$ слід вважати розподіленої нормально, із середнім значенням $\frac{1}{2}\ln\left(\frac{1+\rho}{1-\rho}\right) + \frac{\rho}{2(n-1)}$ і дисперсією $\frac{1}{n-3}$, так що величина $\lambda = \sqrt{n-3}\left(\frac{1}{2}\ln\left(\frac{1+r}{1-r}\right) - \left(\frac{1}{2}\ln\left(\frac{1+\rho}{1-\rho}\right) + \frac{\rho}{2(n-1)}\right)\right)$ нормальна: $\lambda \sim N(0;1)$.

Таким чином, для незалежних і однаково розподілених випадкових векторів $(x_{t+i}, x_{t+\tau+i})$ $\rho_X(\tau) \equiv 0$, величина $\lambda_x(\tau) = \frac{\sqrt{n-3}}{2}\ln\left(\frac{1+r_x(\tau)}{1-r_x(\tau)}\right)$ має стандартний нормальний розподіл, а

$$\sum_{\tau=1}^{\mathrm{T}}\left(\lambda_x(\tau)\right)^2 \to \chi^2_{\mathrm{T}}. \qquad (6.13)$$

6.2.2.4. Оцінка АКФ послідовностей рівномірно розподілених випадкових/псевдовипадкових чисел з відомими параметрами

За умови, якщо виконується перевірка статистичних властивостей послідовності на виході генератора рівномірно розподілених випадкових або псевдовипадкових чисел у деякому діапазоні $[a,b]$ (подібні генератори найбільш широко застосовуються для задач забезпечення інформаційної безпеки в якості генераторів ключових послідовностей з максимальною ентропією), найпростіший аналіз досліджуваної послідовності дозволяє визначити множину значень д.в.в. на виході генератора. Так, якщо в розпорядженні є послідовність чисел $\{x_i \in A\}$, що належать алфавіту A, то його потужність $N = \max\{x_i\} - \min\{x_i\} + 1$, діапазон значень д.в.в. $X \in [\min\{x_i\}; \max\{x_i\}]$, її математичне сподівання $M(X) = \frac{\min\{x_i\} + \max\{x_i\}}{2}$, а дисперсія $D(X) = \frac{N^2 - 1}{12}$.

Зауважимо, що подібна оцінка може бути проведена, якщо об'єм аналізованої послідовності чисел істотно перевершує потужність алфавіту. В іншому випадку існує ймовірність невірно визначити нижню або верхню межу множини значень д.в.в. X. Так, імовірність того, що мінімальне або максимальне значення алфавіту потужності N не буде присутнє в послідовності об'єму V, дорівнює

$$P_{пом} = 2\left(\frac{N-1}{N}\right)^V.$$

Таким чином, для заданих значень потужності алфавіту N і ймовірності $P_{пом}$ можна обчислити необхідний об'єм вибірки, який дозволяє проводити зазначену оцінку:

$$V \geq \log_{\frac{N-1}{N}} \frac{P_{пом}}{2}.$$

Наприклад, для $N = 256$ і $P_{gjv} = 10^{-10}$ отримаємо: $V \geq \log_{1-\frac{1}{256}} \frac{10^{-10}}{2} = 6061$.

За відомих параметрів (математичне сподівання $M(X)$ і дисперсії $D(X)$) випадкового процесу $X(t)$ оцінка нормованої АКФ може бути обчислена за

допомогою виразу

$$r_x'(\tau)=\frac{\frac{1}{n}\sum_{i=0}^{n-1}\left[\left(x_{t+i}-M(X)\right)\cdot\left(x_{t+\tau+i}-M(X)\right)\right]}{D(X)}. \quad (6.14)$$

У такому випадку для незалежних значень x_i, а також відповідно до закономірностей, викладених під час виведення виразів (6.3) і (6.4), і $n\to\infty$ $r_x'(\tau)\to N\left(0;\frac{1}{n}\right)$,

$$\lim_{\substack{n\to\infty\\ \mathrm{T}\to\infty}}\left(\sum_{\tau=1}^{\mathrm{T}}\left(r_x'(\tau)\right)^2\right)=\frac{\mathrm{T}}{n}, \quad (6.15)$$

а

$$n\sum_{\tau=1}^{\mathrm{T}}\left(r_x'(\tau)\right)^2\to\chi^2_{\mathrm{T}}. \quad (6.16)$$

Вирази (6.15) і (6.16) для потужності бічних пелюсток $W'(\mathrm{T})=\sum_{\tau=1}^{\mathrm{T}}\left(r_x'(\tau)\right)^2$ оцінки АКФ (6.14) можна переписати таким чином:

$$\lim_{\substack{n\to\infty\\ \mathrm{T}\to\infty}}\left(W'(\mathrm{T})\right)=\frac{\mathrm{T}}{n}, \quad (6.17)$$

$$nW'(\mathrm{T})\to\chi^2_{\mathrm{T}}. \quad (6.18)$$

У цьому випадку статистичний критерій відповідності АКФ досліджуваної послідовності рівномірно розподілених (псевдо) випадкових чисел АКФ білого шуму полягає в обчисленні оцінок нормованих коефіцієнтів автокореляції за (6.14), формуванні оцінки потужності бічних пелюсток $W'(\mathrm{T})$ з подальшим її оцінюванням за (6.18).

6.2.3. Опис критерію оцінювання послідовностей рівномірно розподілених випадкових чисел

З урахуванням описаного вище критерію критерій оцінювання послідовностей рівномірно розподілених випадкових чисел полягає в наступному:

1) у разі невідомої області визначення д.в.в. вона визначається емпіричним

шляхом;

2) обчислюються математичне сподівання та дисперсія д.в.в.;

3) за допомогою виразу (6.14) обчислюється послідовність оцінок $r_x'(\tau)$ нормованих коефіцієнтів автокореляції для $\tau \in [1;\mathrm{T}]$;

4) обчислюється потужність бічних пелюсток оцінки АКФ $W'(\mathrm{T}) = \sum_{\tau=1}^{\mathrm{T}} \left(r_x'(\tau)\right)^2$;

5) якщо величина $nW'(\mathrm{T})$ для обраного рівня значущості α не перевищує квантиль $\chi^2_{1-\alpha,\mathrm{T}}$ розподілу хі-квадрат з T ступенями вільності, нульова гіпотеза, яка полягає в тому, що числа аналізованої послідовності випадкові, приймається. У іншому випадку нульова гіпотеза відкидається.

Виконаємо застосування цього критерію для деяких відомих генераторів рівномірно розподілених випадкових чисел.

6.2.4. Застосування критерію оцінювання послідовностей рівномірно розподілених випадкових чисел

Виконаємо застосування розробленого методу для відомих ГПВЧ, які проходять усі тести пакету тестування TestU01 [249]. Для цього проведемо $N = 1000$ незалежних випробувань, де визначимо значення $nW'(\mathrm{T})$. Після цього підрахуємо відносну частоту події $A = \left\{nW'(\mathrm{T}) \le \chi^2_{1-\alpha,\mathrm{T}}\right\}$.

Позначимо через Q величину, яка в кожному конкретному випробуванні приймає значення 1, якщо подія A виконується, і 0, якщо подія A не виконується. Тоді відносна частота події $A = \left\{nW'(\mathrm{T}) \le \chi^2_{1-\alpha,\mathrm{T}}\right\}$ в N незалежних випробуваннях $p^* = \sum_{i=1}^{N} Q_i \Big/ N$. Математичне сподівання відносної частоти $M(p^*) = 1-\alpha$, дисперсія $D(p^*) = \alpha(1-\alpha)/N$. Тоді з імовірністю γ виконується нерівність $\left|p^* - (1-\alpha)\right| < t_\gamma \sqrt{\alpha(1-\alpha)/N}$, де t_γ – квантиль стандартного нормального розподілу з рівнем γ. Іншими словами, обчислювана відносна частота p^* з імовірністю γ має

потрапляти в довірчий інтервал $\left(1-\alpha-t_\gamma\sqrt{\alpha(1-\alpha)/N};1-\alpha+t_\gamma\sqrt{\alpha(1-\alpha)/N}\right)$.

Для проведення тестування оберемо $\alpha=\gamma=0.05$. Тоді довірчий інтервал для p^* – $(0.9365;0.9635)$.

Результати тестування зведено в таблицю 6.1.

Таблиця 6.1

Результати застосування критерію оцінювання рівномірно розподілених ПВП

Генератор	Результати тестування автокореляціними тестами TestU01 (4 smallCrush + 4 bigCrush), пройдено/всього тестів	Результати тестування розробленим критерієм
LCG(2^{24}, 16598013, 12820163)	2/8	не пройдено
LCG(2^{31}, 65539, 0)	6/8	не пройдено
LCG(2^{32}, 69069, 1)	5/8	не пройдено
LCG(2^{32}, 1099087573, 0)	5/8	не пройдено
LCG(2^{46},5^{13}, 0)	7/8	не пройдено
LCG(2^{48}, 25214903917, 11)	7/8	не пройдено
LCG(2^{48},5^{19}, 0)	7/8	не пройдено
LCG(2^{48}, 33952834046453, 0)	7/8	не пройдено
LCG(2^{48}, 44485709377909, 0)	7/8	не пройдено
LCG(2^{59},3^{13}, 0)	8/8	не пройдено
LCG(2^{63},5^{19}, 1)	8/8	не пройдено
LCG(2^{63}, 9219741426499971445, 1)	8/8	не пройдено
LCG($2^{31}-1$, $2^{31}-2^{10}$, 0)	6/8	пройдено
LCG($2^{31}-1$, 16807, 0)	7/8	пройдено
LCG($2^{61}-1$, $2^{30}-2^{19}$, 0)	8/8	пройдено
LCG($10^{12}-11$,427419669081, 0)	8/8	пройдено

Отримані результати застосування розробленого методу свідчать про те, що деякі з генераторів, що успішно проходять усі автокореляційні тести пакету TestU01, не задовольняють розробленому критерію.

Таким чином, проведене дослідження дозволило отримати наступні результати:

- теоретично отримана інтегральна оцінка нормованих коефіцієнтів автокореляції (бічних пелюсток АКФ), що створює основу для побудови статистичних критеріїв перевірки кореляційних властивостей досліджуваних послідовностей випадкових і псевдовипадкових чисел за їх емпіричним оцінками;
- представлено перший і другий початкові моменти оцінок нормованих коефіцієнтів автокореляції для:
  - ПАКФ;
  - АКФ непоповнюваної вибірки фіксованого розміру, що обчислюється відповідно до різних підходів (наприклад, представлених у [324], [258, с. 460] або [259, с. 402];
  - АКФ «ковзного вікна» для послідовностей великого періоду;
- уточнено верхню межу дисперсії оцінок нормованих коефіцієнтів автокореляції, що обчислюються за [258, с. 460] або [259, с. 402], що дозволяє підвищити точність інтегральної оцінки бічних пелюсток АКФ;
- отримав подальший розвиток метод оцінювання автокореляції часових рядів на основі одночасного аналізу декількох коефіцієнтів автокореляції (подібно критеріям Бокса-Пірса [262], Льюнга-Бокса [263]), шляхом його адаптації для рівномірно розподілених випадкових величин, що дозволило виконати комплексну кількісну оцінку АКФ для послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел;
- застосування критерію дозволило виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01.

6.3. Метод оцінювання послідовностей випадкових чисел на основі критерію бар'єрної функції

6.3.1. Теоретичне обґрунтування

У попередньому розділі представлено результати виконаного в роботі автора [37] порівняльного аналізу оцінок АКФ послідовностей псевдовипадкових чисел комбінаційного генератора з комбінуючою функцією підсумовування за модулем M і генератора типу «Вихор Мерсенна» [133] MT19937 з оцінками АКФ випадкових послідовностей чисел оцифрованих радіошумів [306] і квантового ГВЧ [305]. Для формування оцінок АКФ використано підхід, викладений у [258, с. 460], [259, с. 402]. Отримані результати свідчать про однорідність оцінок АКФ для всіх розглянутих послідовностей. Разом з тим, у цьому дослідженні вперше запропоновано досліджувати не тільки абсолютні значення бічних пелюсток оцінок АКФ, а й їх знаки. Проте застосування цього підходу не дозволило виявити відмінності між розглянутими послідовностями випадкових і псевдовипадкових чисел. Водночас отримані результати аналізу розподілу k-грам для знаків оцінок АКФ не підтверджують їх рівномірний розподіл для $k \geq 2$ для всіх досліджуваних послідовностей чисел.

У цьому підрозділі представимо розроблений і викладений у [4] метод оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що дозволяє виявити в них не виявлені до теперішнього часу статистичні нерегулярності. Для цього продовжимо розпочате в [37] дослідження знаків бічних пелюсток емпіричної АКФ.

У якості вихідних послідовностей для порівняльного аналізу будемо використовувати послідовності чисел, отримані за допомогою:

- оцифрованих радіошумів [306] (обрана в якості еталонної);
- квантового ГВЧ [305];
- генератора типу «Вихор Мерсенна» [133] MT19937.

Кореляційний аналіз досліджуваних послідовностей будемо проводити на основі обчислення оцінок коефіцієнтів кореляції між послідовними блоками

фіксованої довжини. Для цього досліджувана послідовність (вибірка) довжини $L_{посл}$ розбивається на блоки довжини $L_{блок}$, які можуть перекривати один одного (на кількість символів, що не перевищує значення $L_{блок}-1$) або відставати один від одного на деяку кількість символів. Відстань між сусідніми блоками послідовності позначимо символом τ. Негативне значення величини τ характеризуватиме перекриття (накладення, зачеплення) блоків на величину абсолютного значення τ. Таким чином, $\tau \geq 1-L_{блок}$ і може приймати будь-які цілі значення з цієї області.

Номер блоку визначається зміщенням відносно початку вибірки і збігається з позицією першого символу блоку.

Описана схема розбиття вибірки на блоки представлена на рис. 6.1.

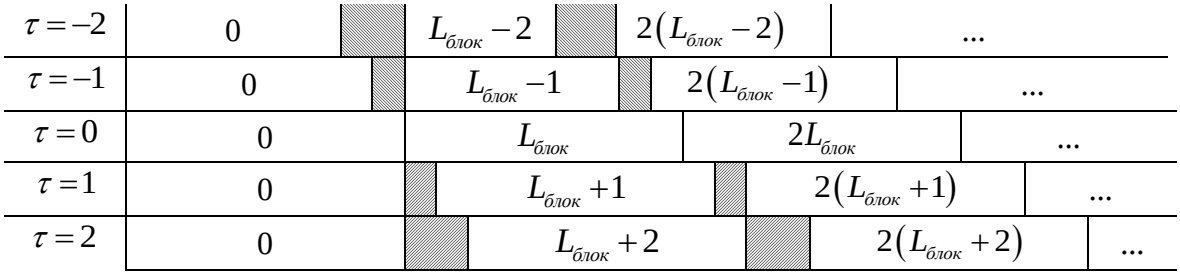


Рис. 6.1. Схема розбиття вибірки на блоки з «перекриттям» і «розтягуванням»

На схемі діагональним штрихуванням зліва направо зверху вниз позначені області перекриття двох сусідніх блоків, а діагональним штрихуванням зліва направо знизу догори – області між двома сусідніми блоками.

Оцінка нормованого коефіцієнта кореляції $r_i(\tau)$ обчислюється для пари блоків з номерами $i\cdot(L_{блок}+\tau)$ і $(i+1)\cdot(L_{блок}+\tau)$ наступним чином:

$$r_i(\tau)=\frac{\frac{1}{L_{блок}}\sum_{l=0}^{L_{блок}-1}\left(\overset{o}{x}\left(i\cdot(L_{блок}+\tau)+l\right)\cdot\overset{o}{x}\left((i+1)\cdot(L_{блок}+\tau)+l\right)\right)}{\sqrt{D\left(X\left(i\cdot(L_{блок}+\tau)\right)\right)}\cdot\sqrt{D\left(X\left((i+1)\cdot(L_{блок}+\tau)\right)\right)}}, \qquad (6.19)$$

де $\overset{o}{x}(j+l)=x(j+l)-M\left(X(j)\right)$ – реалізація центрованої випадкової величини, яка знаходиться на позиції з номером $(j+l)$, $0\leq l\leq L_{блок}-1$;

$x(j+l)$ – елемент вибірки, що знаходиться на позиції з номером $(j+l)$,

$0 \le (j+l) \le L_{посл} - 1;$

$M(X(j))$ і $D(X(j))$ – математичне сподівання і дисперсія д.в.в. $X(j)$, реалізаціями якої є $L_{блок}$ елементів j-ого блоку.

Оскільки в цьому дослідженні аналізу підлягають послідовності випадкових і псевдовипадкових чисел з рівномірним законом розподілу (а нульовою гіпотезою для розроблюваного критерію є твердження про приналежність аналізованої послідовності до категорії послідовностей випадкових рівномірно розподілених чисел), для будь-якого $j \in [0, L_{посл} - L_{блок} + 1]$: $M(X(j)) = \dfrac{\min\{x(p)\} + \max\{x(p)\}}{2}$, $0 \le p \le L_{посл} - 1$, а $D(X(j)) = \dfrac{M^2 - 1}{12}$, де $M = \max\{x(p)\} - \min\{x(p)\} + 1$ – потужність алфавіту.

Таким чином, для будь-якої вибірки довжини $L_{посл}$ можна обчислити $i_{\max}(\tau) = \left\lfloor \dfrac{L_{посл} + \tau}{L_{блок} + \tau} \right\rfloor - 1$ оцінок нормованих коефіцієнтів кореляції $r_i(\tau)$ відповідно до (6.19), а $i \in [0, i_{\max}(\tau) - 1]$.

Нехай потужність алфавіту для всіх використовуваних джерел дорівнює $M = 256$, а елементи послідовностей можуть приймати будь-які цілі значення з діапазону $[0, 255]$. Довжину кожної послідовності виберемо рівною $L_{посл} = 256256$ слів (символів), а довжину блоку – $L_{блок} = 256$ слів. Такий вибір для $\tau = 0$ дозволяє обчислити $i_{\max}(0) = 1000$ оцінок $r_i(0)$ за (6.19). Зауважимо, що за визначених параметрів для будь-якого значення j з діапазону $[0, 256001]$ $M(X(j)) = \dfrac{0 + 255}{2} = 127{,}5$, $D(X(j)) = \dfrac{256^2 - 1}{12} = 5461{,}25$.

Для аналізу послідовності знаків $\{z_i(\tau)\}$ оцінок нормованих коефіцієнтів кореляції $r_i(\tau)$ виконаємо наступне перетворення: $\{z_i(\tau)\} = sign(sign\{r_i(\tau)\} + 0.5)$. Таке перетворення дозволяє отримати множину значень результату, що містить два елементи: -1 і +1.

З огляду на те, що знаменник у виразі (6.19) позитивний, для спрощення процесу обчислення замість оцінки нормованого коефіцієнта кореляції $r_i(\tau)$ можна використовувати оцінку коефіцієнта коваріації $\mathrm{cov}_i(\tau)$ або величину $C_i(\tau) = L_{блок} \cdot \mathrm{cov}_i(\tau)$:

$$C_i(\tau) = \sum_{l=0}^{L_{блок}-1} \left[\overset{o}{x}\left(i \cdot \left(L_{блок} + \tau\right) + l\right) \cdot \overset{o}{x}\left(\left(i+1\right) \cdot \left(L_{блок} + \tau\right) + l\right) \right]. \qquad (6.20)$$

Тоді послідовність знаків

$$\left\{z_i(\tau)\right\} = sign\left(sign\left\{C_i(\tau)\right\} + 0.5\right) = sign\left(sign\left\{r_i(\tau)\right\} + 0.5\right). \qquad (6.21)$$

Для розроблювального критерію відстань між сусідніми блоками послідовності обмежимо зверху нульовим значенням і розглянемо статистичні особливості для перекриття блоків. Тому під час аналізу кожної послідовності отримаємо множину значень $\left\{z_i(\tau)\right\}$, де $i \in \left[0, i_{\max}(\tau) - 1\right]$, $i_{\max}(\tau) = \left\lfloor \dfrac{L_{посл} + \tau}{L_{блок} + \tau} \right\rfloor - 1$, $\tau \in \left[1 - L_{блок}, -1\right]$.

Фіксуючи кожне значення $\tau \in \left[1 - L_{блок}, -1\right]$, отримаємо $\left(L_{блок} - 1\right)$ послідовностей знаків $\left\{z_i(\tau)\right\}$ довжини $i_{\max}(\tau)$.

Далі для кожної послідовності $\left\{z_i(\tau)\right\}$ з зафіксованим τ виконаємо аналіз рівномірності розподілу k-грам знаків (-1 і +1) для $k \geq 1$ за допомогою статистичного критерію χ^2 [258, с. 267–275]. Зауважимо, що відповідно до рекомендацій, викладених у [156, с. 62], такий аналіз вимагає розбиття послідовності $\left\{z_i(\tau)\right\}$ на непересічні блоки (слова) з k знаків (k-грами) виду $\left(z_{kj}(\tau), z_{kj+1}(\tau), \ldots, z_{kj+k-1}(\tau)\right)$.

У результаті аналізу рівномірності розподілу k-грам знаків отримаємо множину значень статистики $\left\{\chi^2(k,\tau)\right\}$, де $k \in \left[1, K\right]$.

Подібний аналіз виконується для великої кількості N вибірок генератора (псевдо) випадкових чисел, у результаті чого формується набір значень $\left\{\chi_n^2(k,\tau)\right\}$, де $n \in \left[1, N\right]$.

Для кожної пари значень (k,τ), де $k\in[1,K]$ і $\tau\in[1-L_{блок},-1]$, обчислюється відносна частота попадання значень $\chi_n^2(k,\tau)$ у критичну область $\left(\chi^2_{1-\alpha,m};\infty\right)$ за заданого рівня значущості α і $m=2^k-1$:

$$W(k,\tau,\alpha)=N_B(k,\tau,\alpha)/N\,, \tag{6.22}$$

де $N_B(k,\tau,\alpha)$ – число появ події $B=\left\{\chi_n^2(k,\tau)>\chi^2_{1-\alpha,m}\right\}$ у N випробуваннях за фіксованих значень k, τ і α.

Зауважимо, що величина $N_B(k,\tau,\alpha)$ і, відповідно, $W(k,\tau,\alpha)$ є випадковими. Визначимо інтервал $\left(W_{\min}(\alpha,\gamma),W_{\max}(\alpha,\gamma)\right)$, симетричний відносно математичного сподівання випадкової величини $W(k,\tau,\alpha)$, у який вона потрапляє з імовірністю γ:

$$\mathrm{P}\left\{W_{\min}(\alpha,\gamma)<W(k,\tau,\alpha)<W_{\max}(\alpha,\gamma)\right\}=\gamma\,. \tag{6.23}$$

Для вирішення цієї задачі визначимо вид розподілу відносної частоти потрапляння значень $\chi_n^2(k,\tau)$ у критичну область $\left(\chi^2_{1-\alpha,m};\infty\right)$. Для цього обчислимо значення $W(k,\tau,\alpha)$ при розтягуванні блоків $(0\le\tau\le 255)$ для $N=1000$ послідовностей оцифрованих радіошумів. Зауважимо, що за $\tau\ge 0$ розподіл $W(k,\tau,\alpha)$ через відсутність кореляції між непересічними блоками білого шуму інваріантний відносно величини τ. Графіки полігонів частот значень $W(k,\tau,\alpha)$, обчислених для $\tau\in[0,255]$, у залежності від деяких параметрів k і α представлені на рис. 6.2. Пунктирною лінією на рис. 6.2 позначено графіки полігонів частот за нормального закону розподілу з математичним сподіванням α і дисперсією $\sigma^2=\alpha(1-\alpha)/N$.

У таблиці 6.2 показано результати перевірки узгодженості емпіричних розподілів значень $W(k,\tau,\alpha)$ з теоретичним граничним (нормальним) за критерієм χ^2 Пірсона [258, с. 267–275]. Наведено досягнуті рівні значущості $P\left(S>S^*\right)=1-G\left(S\middle|H_0\right)$, де $G\left(S\middle|H_0\right)$ – граничний розподіл статистики S критерію χ^2 за умови справедливості нульової гіпотези H_0, S^* – розрахункове значення статистики критерію.

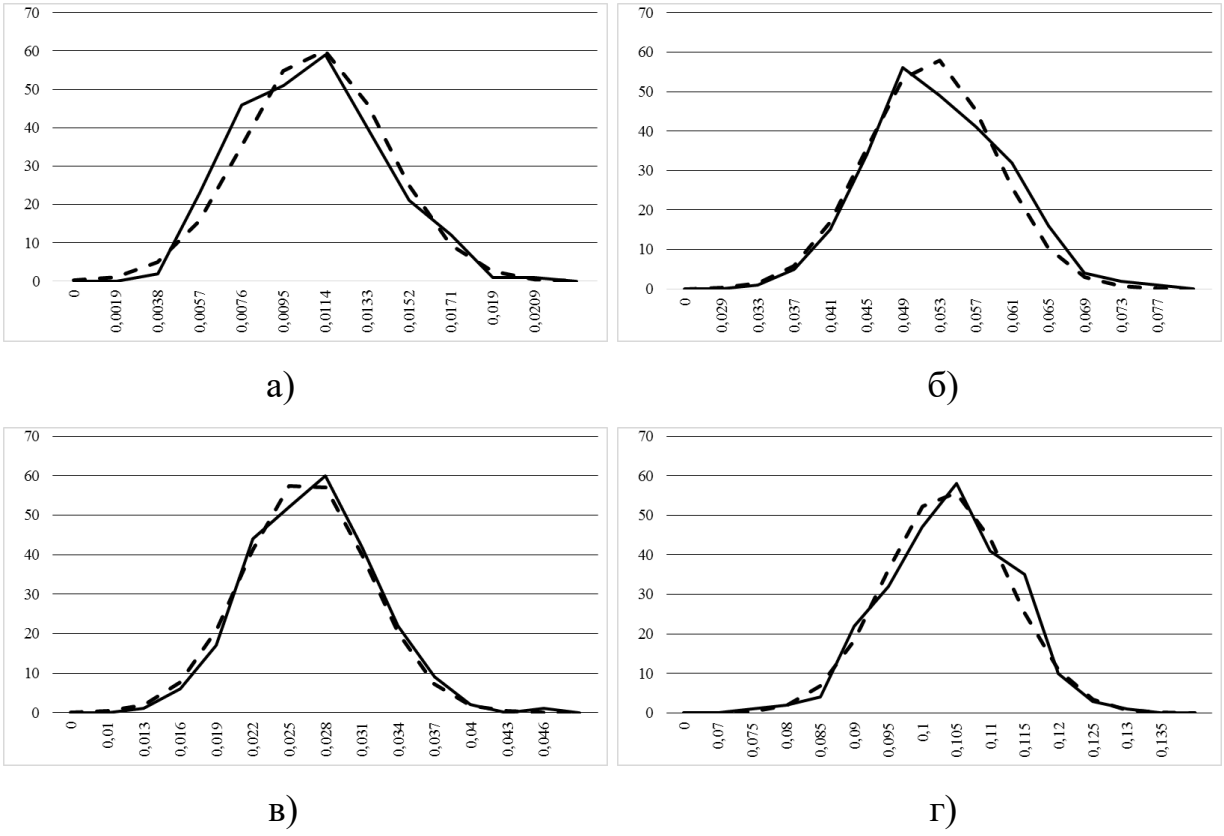


Рис. 6.2. Полігони частот потрапляння статистики $\chi^2(k,\tau)$ у критичну область для: а) $k=1$ і $\alpha=0.01$; б) $k=1$ і $\alpha=0.05$; в) $k=2$ і $\alpha=0.025$; г) $k=2$ і $\alpha=0.1$.

Таблиця 6.2

Результати перевірки гіпотези нормальності розподілу відносної частоти потрапляння значень $\chi_n^2(k,\tau)$ у критичну область

Критерій	Досягнутий рівень значущості $P(S>S^*)$							
	$\alpha=0.01$		$\alpha=0.025$		$\alpha=0.05$		$\alpha=0.1$	
	$k=1$	$k=2$	$k=1$	$k=2$	$k=1$	$k=2$	$k=1$	$k=2$
χ^2 Пірсона	0,4454	0,4952	0,6756	0,7976	0,2867	0,8076	0,3914	0,4505

Досягнуті рівні значущості статистик критерію свідчать про узгодженість емпіричного розподілу $W(k,\tau,\alpha)$ за $\tau\geq 0$ для оцифрованих радіошумів з нормальним законом розподілу з математичним сподіванням α і дисперсією $\sigma^2=\alpha(1-\alpha)/N$.

Перевірка відповідності емпіричного розподілу значень функції $W(k,\tau,\alpha)$ (за фіксованих α і k і $\tau\geq 0$) нормальному закону з математичним сподіванням α і

дисперсією $\sigma^2=\alpha(1-\alpha)/N$ є одним з етапів розроблюваного методу тестування. Невідповідність емпіричного розподілу значень функції $W(k,\tau,\alpha)$ нормальному закону є ознакою непроходження всього тесту. Зазначимо, що дослідження статистики $W(k,\tau,\alpha)$ за $\tau\geq 0$ для квантового ГВЧ і генератора типу «Вихор Мерсенна» MT19937 свідчать про її узгодженість з нормальним законом розподілу з математичним сподіванням α і дисперсією $\sigma^2=\alpha(1-\alpha)/N$.

Оскільки для білого шуму випадкова величина $W(k,\tau,\alpha)$ є нормально розподіленою, ймовірність її попадання в інтервал $\left(W_{\min}(\alpha,\gamma),W_{\max}(\alpha,\gamma)\right)$ визначається виразом $\Phi\left(\frac{P_{\max}(\alpha,\gamma)-\alpha}{\sigma}\right)-\Phi\left(\frac{P_{\min}(\alpha,\gamma)-\alpha}{\sigma}\right)$, де $\Phi(x)$ – функція Лапласа. Тоді нижня $W_{\min}(\alpha,\gamma)$ та верхня $W_{\max}(\alpha,\gamma)$ межі інтервалу $\left(W_{\min}(\alpha,\gamma),W_{\max}(\alpha,\gamma)\right)$, симетричного відносно математичного сподівання α випадкової величини $W(k,\tau,\alpha)$, в який вона потрапляє з імовірністю γ, розраховуються наступним чином:

$$\begin{aligned} W_{\min}(\alpha,\gamma)&=\alpha-t_{\frac{1+\gamma}{2}}\sqrt{\frac{\alpha(1-\alpha)}{N}},\\ W_{\max}(\alpha,\gamma)&=\alpha+t_{\frac{1+\gamma}{2}}\sqrt{\frac{\alpha(1-\alpha)}{N}}, \end{aligned} \tag{6.24}$$

де $t_{\frac{1+\gamma}{2}}$ – квантиль стандартного нормального розподілу з рівнем $\frac{1+\gamma}{2}$.

Визначення 6.1. Бар'єрної функцією $\tau_{\min}(k,\alpha,\gamma)$ будемо називати випадкову функцію параметра α, яка дорівнює мінімальному значенню $-\tau,\tau<0$, за якого відносна частота $W(k,\tau,\alpha)$ потрапляння значень $\chi_n^2(k,\tau)$ у критичну область $\left(\chi^2_{1-\alpha,m};\infty\right)$ перевищує верхню межу $W_{\max}(\alpha,\gamma)$:

$$\tau_{\min}(k,\alpha,\gamma)=\min\left(-\tau>0:W(k,\tau,\alpha)>W_{\max}(\alpha,\gamma)\right). \tag{6.25}$$

Статистичний сенс бар'єрної функції $\tau_{\min}(k,\alpha,\gamma)$ полягає в тому, що за фіксованих значень (k,α,γ) вона вказує «поріг» $-\tau_{\min}$, вище якого: $\tau>-\tau_{\min}$,

спостерігається рівномірний розподіл k-грам знаків емпіричної кореляційної функції (6.19) досліджуваної послідовності випадкових чисел.

Зауважимо, що для нормально розподіленої випадкової величини $W(k,\tau,\alpha)$ справедливі наступні твердження.

Якщо $\alpha' < \alpha'' < 0.5$:

1) $\chi^2_{1-\alpha',\mathrm{m}} > \chi^2_{1-\alpha'',\mathrm{m}}$, тому $W(k,\tau,\alpha') \le W(k,\tau,\alpha'')$;

2) $\alpha'(1-\alpha') < \alpha''(1-\alpha'')$ і як наслідок, $W_{\max}(\alpha',\gamma) < W_{\max}(\alpha'',\gamma)$, а $W_{\max}(\alpha',\gamma) - W_{\min}(\alpha',\gamma) < W_{\max}(\alpha'',\gamma) - W_{\min}(\alpha'',\gamma)$.

Іншими словами, внаслідок збільшення рівня значущості α критична область $\left(\chi^2_{1-\alpha,\mathrm{m}};\infty\right)$ розширюється. Відповідно, відносна частота потрапляння значень $\chi^2_n(k,\tau)$ у критичну область не зменшується (в силу обмеженої кількості вибірок N нерівність нечітка, за необмеженого зростання кількості вибірок відносна частота прямує до ймовірності і нерівність набуває строгого виду). Крім того, внаслідок збільшення рівня значущості розширюється також інтервал $\left(W_{\min}(\alpha,\gamma), W_{\max}(\alpha,\gamma)\right)$.

Таким чином, обидві частини нерівності $W(k,\tau,\alpha) > W_{\max}(\alpha,\gamma)$ з формули (6.25) є монотонно зростаючими функціями по α. Однак, у той же час, бар'єрна функція $\tau_{\min}(k,\alpha,\gamma)$ може не бути монотонною по α.

Дослідимо поведінку бар'єрної функції $\tau_{\min}(k,\alpha,\gamma)$ в залежності від рівня значущості α. Для цього обчислимо послідовність значень $\tau_{\min}(k,\alpha,\gamma)$ для $\alpha \in [\alpha_1,\alpha_2]$ з кроком $\Delta\alpha = \dfrac{\alpha_2 - \alpha_1}{N_\alpha}$ ($N_\alpha + 1$ – кількість значень α) за фіксованого значення γ і $k \in [1,K]$ для $N = 1000$ послідовностей чисел, отриманих за допомогою оцифрованих радіошумів [306], квантового ГВЧ [305], «Вихора Мерсенна» [133] MT19937. Покладемо $\alpha \in [0.01, 0.1]$, $N_\alpha = \{20, 30, 45, 90\}$, $\gamma = 0.95$, а $K = 2$. Графіки залежностей функції $\tau_{\min}(k,\alpha,\gamma)$ від $\alpha \in [0.01, 0.1]$ для $N_\alpha = \{20, 45\}$ і $k = 1$представлено на рис. 6.3.

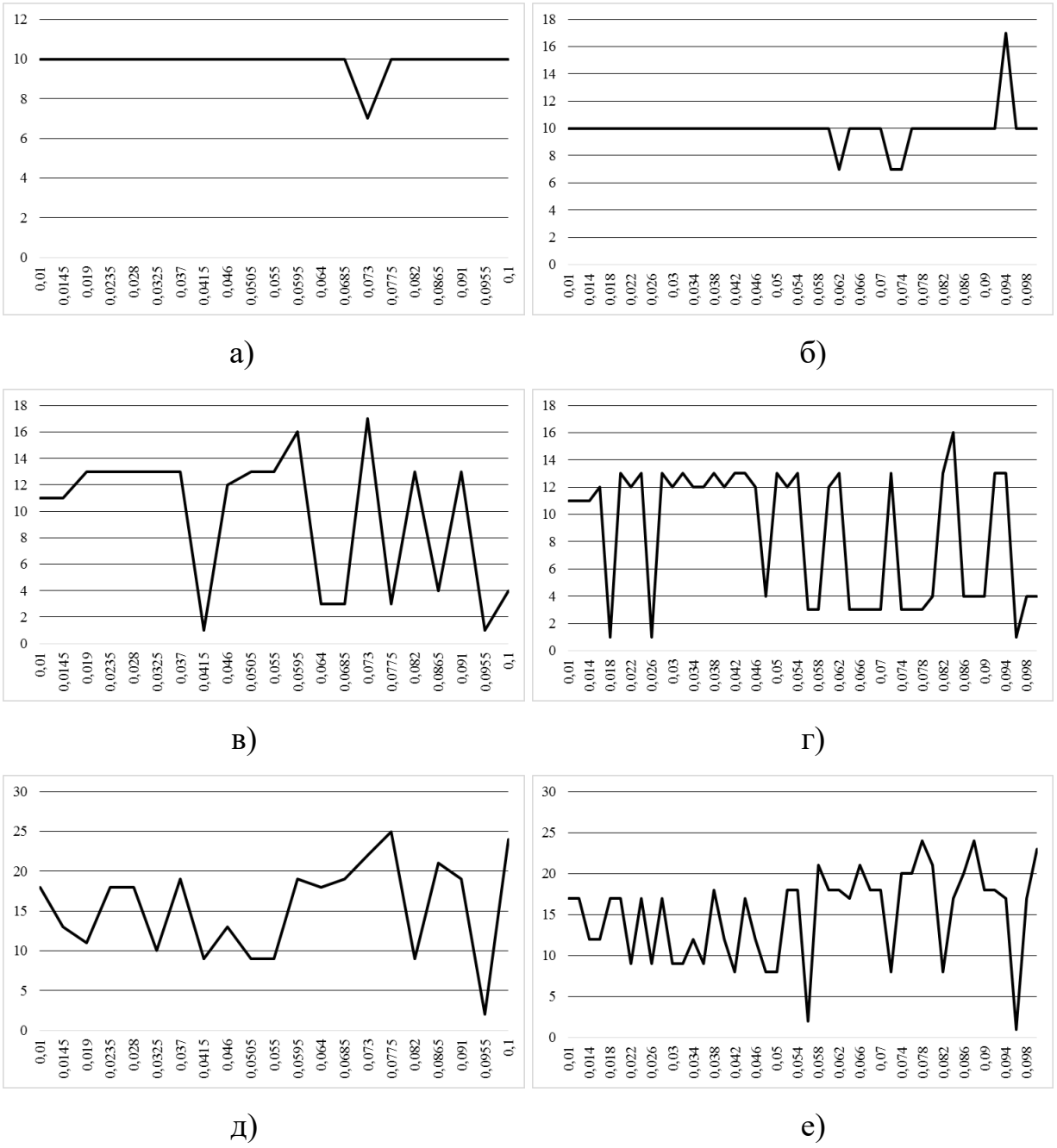


Рис. 6.3. Графіки залежностей $\tau_{\min}(k,\alpha,\gamma)$ від $\alpha \in [0.01, 0.1]$ при $k=1$ для: а) оцифрованих радіошумів, $N_\alpha = 20$; б) оцифрованих радіошумів, $N_\alpha = 45$; в) квантового ГВЧ, $N_\alpha = 20$; г) квантового ГВЧ, $N_\alpha = 45$; д) «Вихора Мерсенна», $N_\alpha = 20$; е) «Вихора Мерсенна», $N_\alpha = 45$.

Як видно з рис. 6.3, графіки для оцифрованих радіошумів істотно відрізняються від інших. Покладемо точки на графіках реалізаціями деяких випадкових величин і обчислимо для них вибіркові дисперсії. Результати зведемо в таблицю 6.3.

Таблиця 6.3

Вибіркові дисперсії $\tau_{min}(k,\alpha,\gamma)$ для $\alpha \in [0.01,0.1]$ і $\gamma = 0.95$ залежно від N_α і k

Джерело	$N_\alpha = 20$		$N_\alpha = 30$		$N_\alpha = 45$		$N_\alpha = 90$	
	$k=1$	$k=2$	$k=1$	$k=2$	$k=1$	$k=2$	$k=1$	$k=2$
Оцифровані радіошуми	0,43	2,03	2,77	2,48	1,69	1,99	1,48	2,03
Квантовий ГВЧ	27,53	3,73	25,10	5,91	23,35	5,91	25,63	5,86
MT19937	36,16	9,23	26,12	9,21	30,42	9,42	30,06	9,13

Отримані результати показують, що дисперсія значень бар'єрної функції $\tau_{\min}(k,\alpha,\gamma)$ мінімальна для оцифрованих радіошумів і є значно меншою, ніж у інших джерел. Однак обчислені емпіричні значення дисперсій не можуть служити в якості статистичного критерію, що виявляє відмінності між послідовностями, породженими природними джерелами випадкових чисел, і штучно згенерованими.

6.3.2. Критерій бар'єрної функції

Для розробки критерію, що характеризує сталість бар'єрної функції, сформулюємо новий підхід до інтерпретації отриманих залежностей $\tau_{\min}(k,\alpha,\gamma)$, графіки яких наведені на рис. 6.3.

Цей підхід базується на використанні ідеології критерія χ^2 Пірсона і полягає в тому, що для кількісної оцінки спостережуваних статистичних нерегулярностей отримані послідовності значень бар'єрної функції $\tau_{\min}(k,\alpha,\gamma)$ для $\alpha \in [\alpha_1,\alpha_2]$ з кроком $\Delta\alpha$ і фіксованих γ і k розглядаються як частоти в результаті реалізації статистичного експерименту з $N_\alpha + 1$ можливими наслідками. Таким чином, представлені на рис. 6.3 графіки залежностей $\tau_{\min}(k,\alpha,\gamma)$ для $\alpha \in [\alpha_1,\alpha_2]$ з кроком $\Delta\alpha$ і фіксованих γ і k розглядаються як полігони частот д.в.в.

Виходячи з того, що в якості еталонного джерела білого шуму обрано джерело оцифрованих радіошумів [306], а також відповідно до виду відповідних йому на рис. 6.3 полігонів частот, теоретичним граничним законом розподілу є рівномірний закон.

6.3.3. Опис методу оцінювання якості послідовностей випадкових чисел

Таким чином, метод оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел базується на дослідженні закону розподілу знаків емпіричної автокореляційної функції (6.19) відносно кількості символів у перекритих частинах відрізків, на які розбивається послідовність чисел, і визначенні допустимого «порогу» перекриття, нижче якого спостерігається рівномірний розподіл знаків автокореляційної функції.

Метод полягає в наступному:

1) досліджувані послідовності генератора розбиваються на блоки, що перекриваються на величину $(-\tau)$;

2) для кожної послідовності обчислюється множина оцінок нормованих коефіцієнтів кореляції відповідно до виразу (6.19), яка перетворюється в множину знаків оцінок нормованих коефіцієнтів кореляції;

3) для кожної отриманої послідовності перевіряється статистична гіпотеза про відповідність розподілу k-грам знаків рівномірному закону;

4) перевіряється статистична гіпотеза про відповідність нормальному закону емпіричного розподілу значень функції відносної частоти випадків невідповідності розподілу k-грам знаків рівномірному закону;

5) відповідно до (6.25) обчислюються значення бар'єрної функції;

6) виконується оцінка обчислених значень бар'єрної функції відповідно до критерію бар'єрної функції.

6.3.4. Реалізація критерію бар'єрної функції

Виконаємо перевірку узгодженості отриманих емпіричних розподілів з відносними частотами $\varphi_{k,\gamma}(\alpha)=\tau_{\min}(k,\alpha,\gamma)\Big/\sum_{\alpha=\alpha_1}^{\alpha_2}\tau_{\min}(k,\alpha,\gamma)$ з теоретичним граничним (рівномірним) за критерієм χ^2 Пірсона [258, с. 267–275]. Досягнуті рівні значущості $P\left(S>S^*\right)=1-G\left(S\middle|H_0\right)$, де $G\left(S\middle|H_0\right)$ – граничний розподіл статистики

S критерію χ^2 за умови справедливості нульової гіпотези H_0 : $\{\varphi_{k,\gamma}(\alpha)=1/(N_\alpha+1)\}$, S^* – розрахункове значення статистики критерію, наведені в таблиці 6.4.

Таблиця 6.4

Результати перевірки гіпотези рівномірності емпіричного розподілу з частотами $\tau_{min}(k,\alpha,\gamma)$ для $\alpha\in[0.01,0.1]$ і $\gamma=0.95$ залежно від N_α і k за критерієм χ^2 Пірсона

Джерело	Досягнутий рівень значущості $P(S>S^*)$							
	$N_\alpha=20$		$N_\alpha=30$		$N_\alpha=45$		$N_\alpha=90$	
	$k=1$	$k=2$	$k=1$	$k=2$	$k=1$	$k=2$	$k=1$	$k=2$
Оцифровані радіошуми	1,0000	0,9977	0,9999	0,9989	1,0000	1,0000	1,0000	1,0000
Квантовий ГВЧ	0,0000	0,7538	0,0000	0,4915	0,0000	0,4446	0,0000	0,4744
«Вихор Мерсенна»	0,0004	0,0109	0,0164	0,0037	0,0000	0,0005	0,0000	0,0000

Отримані результати свідчать про те, що рівномірному закону відповідає розподіл з абсолютними частотами $\tau_{\min}(k,\alpha,\gamma)$ тільки для послідовностей оцифрованих радіошумів. Квантовий ГВЧ і генератор типу «Вихор Мерсенна» MT19937 не задовольняють розробленому критерію. Непроходження тесту квантовим ГВЧ може бути наслідком використання неоптимального перетворення квантових явищ у послідовність випадкових чисел.

Вибір N_α не впливає суттєво на результати експерименту. Тому значення N_α можна обирати як мінімальне значення, за якого правомірно використання статистичного критерію χ^2 Пірсона для перевірки рівномірності дискретного розподілу: $\sum_\alpha \tau_{\min}(k,\alpha,\gamma)>100$ або $N_\alpha=\min(N_\alpha):(N_\alpha+1)\cdot\overline{\tau_{\min}(k,\alpha,\gamma)}>100$, де $\overline{\tau_{\min}(k,\alpha,\gamma)}=\sum_\alpha \tau_{\min}(k,\alpha,\gamma)\Big/(N_\alpha+1)$ – вибіркове середнє.

6.3.5. Опис методики застосування критерію оцінювання послідовностей випадкових чисел

Методика застосування розробленого критерію для перевірки послідовностей випадкових і псевдовипадкових чисел включає в себе наступні етапи:

1) генератором формуються N послідовностей довжини $L_{посл}$ (рекомендується $N \geq 1000$);

2) кожна послідовність розбивається на перекриті на величину $(-\tau)$ блоки довжини $L_{бл}$, $\tau \in [1-L_{бл}, -1]$, кількість блоків дорівнює $i_{\max}(\tau)+1 = \lfloor (L_{посл}+\tau)/(L_{блок}+\tau) \rfloor$ (довжина блоку обирається рівною потужності алфавіту: $L_{посл} = M = 256$, а $L_{посл} = 256256$, щоб $i_{\max}(0) = 1000$);

3) для кожної послідовності відповідно до виразу (6.19) обчислюється множина оцінок нормованих коефіцієнтів кореляції між сусідніми блоками $r_i(\tau)$, $i \in [0, i_{\max}(\tau)-1]$, $i_{\max}(\tau) = \lfloor (L_{посл}+\tau)/(L_{блок}+\tau) \rfloor - 1$;

4) відповідно до формули (6.21) множина оцінок нормованих коефіцієнтів кореляції $\{r_i(\tau)\}$ перетворюється в множину знаків $\{z_i(\tau)\}$;

5) послідовності знаків $\{z_i(\tau)\}$ за фіксованого значення $\tau \in [1-L_{бл}, -1]$ піддаються аналізу на рівномірність розподілу k-грам знаків для ○○⋯○ за допомогою статистичного критерію χ^2, у результаті чого формується множина значень статистики $\{\chi^2(k,\tau)\}$ для однієї послідовності і ○⋯○ $(n \in [1, N])$ – для N послідовностей;

6) для кожної пари значень $k \in [1, K]$ і ○⋯○ відповідно до (6.22) обчислюється статистика $W(k,\tau,\alpha)$ – відносна частота потрапляння значень $\chi_n^2(k,\tau)$ у критичну область $(\chi^2_{1-\alpha,m}; \infty)$ за заданого рівня значущості α і $m = 2^k - 1$. Рівень значущості α приймає послідовно всі значення з діапазону $\alpha \in [\alpha_1, \alpha_2]$ з кроком $\Delta\alpha = (\alpha_2 - \alpha_1)/N_\alpha$ ($\alpha_1 = 0.01$, $\alpha_2 = 0.1$, $N_\alpha \geq 20$);

7) відповідно до критерію χ^2 виконується перевірка відповідності емпіричного розподілу значень функції $W(k,\tau,\alpha)$ (за фіксованих α і k і $\tau \geq 0$) нормальному закону з математичним сподіванням α і дисперсією $\sigma^2 = \alpha(1-\alpha)/N$. Непроходження цього етапу призводить до непроходження всього тесту;

8) для кожного рівня значущості α за (6.24) визначається інтервал $\left(W_{\min}(\alpha,\gamma),W_{\max}(\alpha,\gamma)\right)$, у який випадкова величина $W(k,\tau,\alpha)$ потрапляє з імовірністю γ ($\gamma=0.95$);

9) для відомих значень $W(k,\tau,\alpha)$ відповідно до (6.25) обчислюються значення бар'єрної функції $\tau_{\min}(k,\alpha,\gamma)$;

10) для обчислених значень $\tau_{\min}(k,\alpha,\gamma)$ застосовується критерій бар'єрної функції: виконується перевірка узгодженості емпіричних розподілів з відносними частотами $\varphi_{k,\gamma}(\alpha)$ для $\alpha\in[\alpha_1,\alpha_2]$ з теоретичним граничним (рівномірним) за критерієм χ^2 Пірсона;

11) тест вважається пройденим, якщо для всіх $k\in[1,K]$ отримані статистики не потрапляють у критичну область критерію χ^2 за заданого рівня значущості β.

У результаті проведеного дослідження розроблено метод оцінювання якості послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел на основі кореляційного аналізу шляхом дослідження закону розподілу знаків емпіричної автокореляційної функції щодо кількості символів у перекритих частинах відрізків, на які розбивається послідовність чисел, і визначення допустимого «порогу» перекриття, нижче якого спостерігається рівномірний розподіл знаків автокореляційної функції. Це дозволило виявити статистичні особливості, властиві послідовностям, породженим природними джерелами дискретного білого шуму, і не властиві штучно згенерованим послідовностям псевдовипадкових чисел.

Розроблений метод дозволив виявити невиявлені до теперішнього часу статистичні нерегулярності. Зокрема, серед досліджених у цій роботі джерел рівномірно розподілених (псевдо) випадкових чисел тільки обране в якості еталону джерело випадкових чисел, отриманих шляхом оцифрування радіошумів [306], відповідає розробленому критерію, в той час як квантовий ГВЧ [305] і генератор типу «Вихор Мерсенна» [133] MT19937 не задовольняють пред'явленим вимогам.

Отримані результати мають теоретичне і практичне значення під час оцінювання якості штучно згенерованих послідовностей псевдовипадкових чисел, ступеня близькості їх статистичних властивостей до властивостей послідовностей випадкових чисел і можуть бути використані в спеціалізованих прикладних пакетах тестування технічних засобів формування послідовностей випадкових і псевдовипадкових чисел.

6.4. Критерій оцінювання точності відтворення закону розподілу д.в.в.

6.4.1. Опис критерію

Генератор послідовностей рівномірно розподілених випадкових чисел формує випадкові цілі числа на відрізку $x \in [0, N_1 - 1]$, при цьому величина N_1 визначається розрядністю процесора. Для основної маси нині використовуваних комерційних ПЕОМ $N_1 = 2^n$, де $n = \{32, 64\}$. Під час практичного використання ГВЧ область визначення рівномірно розподіленої випадкової величини визначається конкретною задачею і може відрізнятися від множини цілих чисел відрізка $[0, N_1 - 1]$ – наприклад, включати всі цілі числа відрізка $[0, N_2 - 1]$, де $N_2 < N_1$. У цьому випадку програма обробки чисел на виході ГВЧ спочатку перетворює область визначення д.в.в. з множини цілих чисел відрізка $[0, N_1 - 1]$ до множини раціональних чисел напівінтервалу $[0;1)$ шляхом виконання операції $x^{\wedge} = x / N_1$, а потім обчислює $y = \lfloor x^{\wedge} N_2 \rfloor = \lfloor x N_2 / N_1 \rfloor$, при цьому $0 \le x^{\wedge} < 1$. Така практика обчислень використовується повсюдно, хоча питання точності відтворення випадкових величин залишається невивченим і, як наслідок, питання точності кінцевого результату, обумовлене наявністю помилки відтворення закону розподілу, залишається відкритим.

Для оцінки точності відтворення законів розподілу д.в.в. математична статистика використовує функцію помилки

$$\xi(x) = p_0(x) - p^{\wedge}(x), \tag{6.26}$$

де $p_0(x)=1/N_1$ – гіпотетична (теоретична) ймовірність появи числа $x\in[0,N_1-1]$, що відповідає рівномірному закону розподілу;

$p^{\wedge}(x)=n(x)/V$ – відносна частота появи значення $x\in[0,N_1-1]$ на виході генератора, $n(x)$ – число випадків появи числа x у вибірці об'єму V.

Зауважимо, що функція (6.26) лежить в основі критеріїв Колмогорова [261, с. 80–82], Смірнова [261, с. 80–82], χ^2 Пірсона [258, с. 267–275].

Зазначені критерії слугують для перевірки статистичної гіпотези про відповідність закону розподілу чисел в аналізованої вибірці деякому теоретичному закону і не дають відповіді про кількісний показник відхилення від цього закону.

Представимо розроблений в рамках дисертаційного дослідження і викладений у [17] критерій оцінювання точності відтворення закону розподілу д.в.в.

Для цього визначимо величину помилки відтворення д.в.в. під час зміни області її визначення з множини цілих чисел відрізка $[0,N_1-1]$ в множину цілих чисел відрізка $[0,N_2-1]$, $N_2<N_1$.

Покладемо, що вибірка об'єму V належить генеральній сукупності рівномірно розподіленої д.в.в.

Для встановлення ступеня відповідності емпіричного закону теоретичному розглянемо більш детально вираз (6.26). Представимо його в наступному вигляді:

$$\xi(x)=p_0(x)-p^{\wedge}(x)=\frac{n_0(x)}{V}-\frac{n(x)}{V}=\frac{\Delta n(x)}{V}, \qquad (6.27)$$

де $n_0(x)$ – кількість повторень символу x у теоретичному потоці;

$n(x)$ – кількість повторень символу x у емпіричному потоці;

$\Delta n(x)=n_0(x)-n(x)$.

Отриманий вираз (6.27) допускає наступне трактування процесу: дискретний випадковий процес, що породжується реальним ГВЧ, представляє композицію двох дискретних випадкових процесів. Перший з них – це потік символів з теоретичним законом розподілу, а другий – це потік заважаючих символів з невідомим законом розподілу. Відповідно, кожен з потоків породжується своїм генератором. Генератор

заважаючих символів може вставляти породжувані ним символи в загальний потік і може подавляти (видаляти) символи теоретичного потоку. Вставка/видалення символів трансформує теоретичний розподіл у емпіричний. Тоді помилка відтворення закону розподілу випадкової величини (6.27) є число символів заважаючого потоку, що вразили деякий символ, на одиницю об'єму вибірки. З урахуванням сказаного, сформулюємо критерій оцінювання точності відтворення закону розподілу д.в.в. реальним ГВЧ:

$$\xi = \frac{1}{2}\sum_{x=0}^{N_1-1}\left|\xi(x)\right| = \frac{1}{2}\sum_{x=0}^{N_1-1}\frac{\left|\Delta n(x)\right|}{V} = \frac{1}{2V}\sum_{x=0}^{N_1-1}\left|\Delta n(x)\right|. \qquad (6.28)$$

Значення 2 додатково вводиться в знаменник, оскільки один символ заважаючого потоку змінює статистику повторень відразу для двох символів алфавіту.

Вираз (6.28) означає, що точність відтворення закону розподілу д.в.в. реальним генератором визначається числом символів помилкового потоку, що припадає на одиницю об'єму вибірки.

Звернемо увагу на те, що якщо об'єм вибірки не кратний N_1, то з'являється додатково статистична складова помилки відтворення закону розподілу д.в.в. Це обумовлено тим, що значення $n_0 = V/N_1$ є цілим у тому і тільки в тому випадку, якщо $V = kN_1$, а статистична помилка – помилка, яка визначається ступенем відхилення об'єму вибірки від величини $V = kN_1$, – дорівнює нулю.

Нерівність нулю виразу (6.28) на проміжку, кратному періоду послідовності, характеризує конструктивну помилку відтворення закону розподілу д.в.в. випадкового процесу, породженого реальним ГВЧ (або перетворювачем) – помилку, обумовлену принципом побудови (конструкцією) ГВЧ або перетворювача.

Визначимо величину статистичної похибки, обумовленої некратністю об'єму вибірки довжині циклу ГВЧ.

Нехай послідовність на виході ГВЧ складається з циклів довжини N_1, які у випадковому порядку містять всі значення випадкової величини з області визначення, а порядок проходження символів у циклах може відрізнятися. Об'єм

вибірки $V = kN_1 + m$, де $0 \le m < N_1$ – число символів останнього (неповного) циклу.

Тоді $n_0 = \dfrac{kN_1 + m}{N_1} = k + \varepsilon$, де $\varepsilon = \dfrac{m}{N_1}$. Врахуємо, що для $\forall V \quad p_0(x) = \dfrac{1}{N_1}$, тому $\xi(x) = p_0(x) - p^{\wedge}(x) = \dfrac{n_0(x)}{V} - \dfrac{n(x)}{V} = \dfrac{1}{N_1} - \dfrac{n(x)}{V}$. Значення статистичної помилки відтворення $\xi = \dfrac{1}{2}\sum_{x=0}^{N_1-1}\left|\xi(x)\right| = \dfrac{1}{2}\left((N_1 - m)\left|\dfrac{1}{N_1} - \dfrac{k}{V}\right| + m\left|\dfrac{1}{N_1} - \dfrac{k+1}{V}\right|\right) = \dfrac{m(N_1 - m)}{N_1 V}$ або

$$\xi = \varepsilon(1-\varepsilon)/(k+\varepsilon). \qquad (6.29)$$

З графіка залежності величини помилки відтворення від об’єму вибірки (рис. 6.4) видно, що за умови рівномірного розподілу слів з усієї області визначення випадкової величини в кожному з циклів статистична помилка відтворення закону розподілу д.в.в. має нульове значення для $\varepsilon = 0$ (у точках $V = kN_1$) і зменшується зі збільшенням об’єму вибірки.

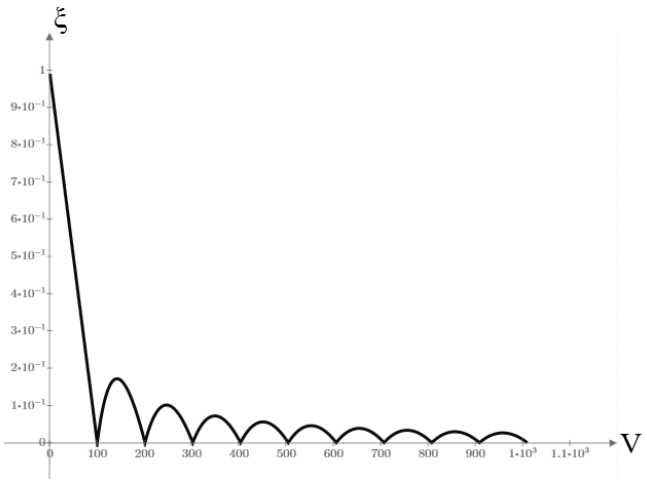


Рис. 6.4. Графік залежності величини помилки відтворення від об’єму вибірки для $N_1 = 101$

6.4.2. Застосування критерію оцінювання точності відтворення закону розподілу д.в.в. для найпростіших генераторів

За допомогою запропонованого критерію (6.28) розглянемо властивості послідовностей і оцінимо помилку відтворення закону розподілу для двох найбільш поширених типів ГПВЧ:

– генератора М-послідовності;

– ЛКГ.

Генератори М-послідовностей породжують періодично повторювану псевдовипадкову послідовність чисел довжиною $N_1 = 2^n - 1$, де n – порядок генераторного полінома. Послідовність на виході такого генератора містить всі числа відрізка $[1, N_1 - 1]$. Звідси випливає, що для області визначення випадкової величини $[1, N_1 - 1]$ генератор М-послідовності породжує рівномірно розподілену випадкову послідовність чисел. Для $x \in [0, N_1 - 1]$ цей же генератор породжує випадкову величину з помилкою, обумовленою відсутністю в послідовності символу «0». Теоретичний і емпіричний розподіл такого генератора на об'ємі вибірки $V = N_1$, а також його помилка відтворення показані на рис. 6.5.

Покладемо, що в деякій конкретній задачі умовою придатності ГВЧ є $\xi \le 10^{-3}$.

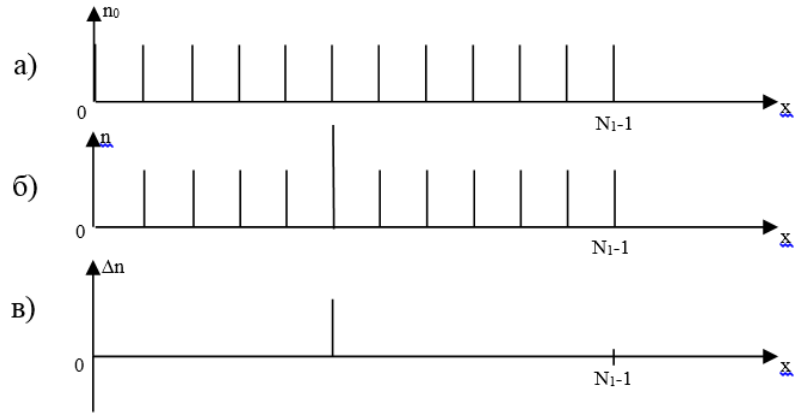


Рис. 6.5. Закони розподілу складових повного потоку символів на виході генератора М-послідовності: а) теоретичного потоку; б) емпіричного потоку; в) помилки відтворення.

Для генератора М-послідовності з $V = N_1$ помилка, обумовлена конструкцією генератора, дорівнює $\xi = 1/N_1$.

З цього випливає, що для $N_1 > 1000$ (порядок генераторного полінома $n \ge 10$) генератор М-послідовності задовольняє наведеній вимозі $\xi \le 10^{-3}$. Граф станів цього

генератора містить один цикл довжиною $N_1 - 1$ і один нуль-цикл, розташований у точці $x = 0$.

Якщо, наприклад, виконати конкатенацію циклів генератора М-послідовності, то період послідовності на виході генератора стане рівним N_1, а помилка відтворення – $\xi = 0$.

Для ЛГК величина помилки визначається конструкцією графа станів. Так, наприклад, для конструкції графа типу 1.1 $\left(O_{N_1}\right)$ (див. таблицю А.3) величина помилки відтворення буде дорівнювати нулю. Однак у цьому випадку символи послідовності мають найбільший ступінь взаємної кореляції, тому що порядок чергування слів у послідовності є детермінованим. Для конструкції графа ЛГК типу 1.3 $\left(O_{N_1-1} + O_1\right)$ (що збігається з конструкцією графа станів генератора М-послідовності) величина помилки ЛГК збігаються з величиною помилки М-послідовності. Відмінність полягає лише в тому, що у генератора М-послідовності відсутнім символом завжди є символ «0», а у ЛГК нуль-цикл може розташовуватися в довільній точці відрізка $[0, N_1 - 1]$. Значення цього символу визначається параметрами ЛГК, тобто його конструкцією.

Для ЛГК з графом станів типу 1.5 $\left(dO_t + O_1\right)$ величина помилки відтворення може бути дуже великою і визначається довжиною циклу t. Так, для $N_1 = 101$ і конструкції графа $5O_{20} + O_1$ число різних символів у послідовності довжини $V = N_1$, що складається з символів довільного циклу, відмінного від нуль-циклу, буде дорівнювати 20, а $\xi \approx 0.8$. Такий генератор навряд чи можна назвати генератором рівномірно розподілених на відрізку $[0, N_1 - 1]$ випадкових послідовностей чисел. Однак ситуація змінюється, якщо виконати конкатенацію циклів графа. У цьому випадку помилка відтворення $\xi = 0$, а кореляція між символами буде нижчою.

6.4.3. Застосування критерію оцінювання точності відтворення закону розподілу дискретної випадкової величини при її перетворенні

Далі будемо виходити з тієї ситуації, що первинний ГВЧ породжує

послідовність випадкових чисел відрізка $[0, N_1 - 1]$, а помилка відтворення рівномірного закону розподілу випадкової величини $\xi = 0$.

Покладемо, що необхідно сформувати рівномірно розподілену випадкову послідовність чисел відрізка $[0, N_2 - 1]$, де $N_1 > N_2$, Причому всі значення з області визначення випадкової величини в сформованій послідовності повинні зустрічатися один раз. Покладемо також, що

$$1 \le (N_1 - 1)/(N_2 - 1) < 2. \qquad (6.30)$$

Зазначимо, що якщо $(N_1 - 1)/(N_2 - 1) \ge 2$, то виконується процедура проріджування стільки раз, скільки потрібно для отримання співвідношення (6.30). Проріджування включає наступні операції:

– з ряду згенерованих чисел видаляються непарні числа (залишаються тільки парні – це, власне, і є проріджування);

– розділивши залишені парні числа на два, формується натуральна послідовність чисел, рівномірно розподілених на відрізку $[0,(N_1 - 1)/2]$ для N_1 – непарного і $[0,(N_1 - 2)/2]$ для N_1 – парного.

Зауважимо, що для $N_1 - 1 = 2^k (N_2 - 1) + l$, $l \in [0, 2^k - 1]$, і виконанні операції проріджування розподіл д.в.в. на відрізку $[0, N_2 - 1]$ буде рівномірним.

Розглянемо два способи зміни області визначення випадкової величини:

1) $y = \lfloor x N_2 / N_1 \rfloor$;

2) $y = |x|_{N_2}$.

Знайдемо величину помилки відтворення закону розподілу д.в.в. y для першого і другого способу її формування, для чого розглянемо фрагмент вихідної послідовності (в якості якої використовуємо натуральну послідовність чисел 0,1,2,3 ...., починаючи з числа 143) і вихідну послідовність для кожного із способів перетворення. Результати зведемо в таблицю 6.5. При цьому $N_1 = 256$, $N_2 = 151$.

З таблиці 6.5 видно, що для першого способу перетворення деякі слова внаслідок виникнення ситуацій $\lfloor x N_2 / N_1 \rfloor = \lfloor (x+1) N_2 / N_1 \rfloor$ з'являються на виході

перетворювача двічі. Число слів-двійників на виході перетворювача після надходження на його вхід N_1 символів первинного генератора дорівнює $\Delta n = N_1 - N_2$.

Таблиця 6.5

Фрагменти вихідної і перетвореної послідовностей

x	143	144	145	146	147	148	149	150	151	152	153
$y = \lfloor x N_2 / N_1 \rfloor = \lfloor x151/256 \rfloor$	84	84	85	86	86	87	87	88	89	89	90
$y = \lvert x \rvert_{N_2} = \lvert x \rvert_{151}$	143	144	145	146	147	148	149	150	0	1	2

Помилка відтворення закону розподілу д.в.в. на виході перетворювача $\xi = \frac{1}{2}\sum_{x=0}^{N_2-1}\left|\xi(x)\right| = \frac{1}{2}\left((N_1 - N_2)\left|\frac{1}{N_2} - \frac{2}{N_1}\right| + (2N_2 - N_1)\left|\frac{1}{N_2} - \frac{1}{N_1}\right|\right)$ або

$$\xi = (N_1 - N_2)(2N_2 - N_1)/N_1N_2. \qquad (6.31)$$

Для розглянутого прикладу $\xi \approx 0.12$, що ставить під сумнів доцільність цього перетворення. З отриманого результату також випливає, що число помилкових символів на інтервалі з N_1N_2 слів дорівнює $(N_1 - N_2)(2N_2 - N_1)$.

Слід зазначити, що оскільки первинний ГВЧ циклічно повторює послідовність чисел відрізка $[0, N_1 - 1]$, то і перетворювач $y = \lfloor x N_2 / N_1 \rfloor$ буде циклічно повторювати вихідну послідовність з однаковою кількістю слів-двійників у кожному циклі. Звідси випливає, що помилка $\xi = \frac{1}{2}\sum_{x=0}^{N_2-1}\left|\xi(x)\right| = \frac{1}{2}\left((N_1 - N_2)\left|\frac{1}{N_2} - \frac{2k}{kN_1}\right| + (2N_2 - N_1)\left|\frac{1}{N_2} - \frac{k1}{kN_1}\right|\right) = \frac{(N_1 - N_2)(2N_2 - N_1)}{N_1N_2}$ зберігається за будь-яких обсягів вибірки $V = kN_1$ і визначає конструктивну помилку перетворювача $y = \lfloor x N_2 / N_1 \rfloor$. Для $V = kN_1 + m$, крім конструктивної складової похибки, виникає статистична складова похибки.

Для другого способу перетворення $y = \lvert x \rvert_{N_2}$. Таким чином, $y = x$ за $x < N_2$ і $y = x - N_2$ за $x \geq N_2$.

Оскільки числа x і $x+N_2$ мають рівні залишки від ділення на N_2, кількість слів, що дорівнює $\Delta n = N_1 - N_2$, у послідовності буде зустрічатися двічі. Внаслідок цього, помилка відтворення перетворювача буде також визначатися виразом (6.31).

Звідси випливає висновок, що жоден з розглянутих способів перетворення не задовольняє поставленим вимогам і, загалом, у чистому вигляді непридатний для практичного використання.

Процедура зміни області визначення д.в.в., що забезпечує нульову помилку відтворення рівномірного закону розподілу, може включати такі операції:

– виконання процедури проріджування вихідної послідовності, щоб виконувалася умова (6.30) $1 \le (N_1 - 1)/(N_2 - 1) < 2$;

– виконання перетворення $y = f(x)$ відповідно до будь-якого зі способів;

– за необхідності проріджування отриманого потоку (видалення слів-двійників).

Пояснимо сенс операції проріджування. Оскільки первинний генератор чисел x породжує слова відрізка $[0, N_1 - 1]$, а вторинний генератор слів y повинен формувати слова відрізка $[0, N_2 - 1]$, то $\Delta n = N_1 - N_2$ слів з N_1 слів на виході вторинного ГВЧ є надлишковими і підлягають видаленню. Ця операція досить просто виконується для $y = |x|_{N_2}$. У цьому випадку підлягають видаленню з входу перетворювача всі слова $x \ge N_2$, які і породжують слова-двійники.

Для $y = \lfloor x N_2 / N_1 \rfloor$ підлягають видаленню по одному з пари слів, які відповідають умові $y(x+1) - y(x) = 0$. Ця операція легко здійсненна, якщо слова $y(x)$ і $y(x+1)$ слідують одне за іншим. У загальному випадку, якщо первинний ГВЧ видає некорельовану послідовність чисел, ця умова не виконується, що призводить до практичної неефективності цього способу для вирішення поставленої задачі.

Таким чином, перетворення області визначення д.в.в. з множини цілих чисел відрізка $[0, N_1 - 1]$ в множину цілих чисел відрізка $[0, N_2 - 1]$ за об'єму вихідної вибірки, кратного N_1, $1 \le (N_1 - 1)/(N_2 - 1) < 2$, шляхом обчислення $y = \lfloor x N_2 / N_1 \rfloor$ або шляхом обчислення функції $y = |x|_{N_2}$ призводить до появи конструктивної помилки

перетворення (6.31). Для $N_1 - 1 = 2^k (N_2 - 1) + l$, $l \in \left[0, 2^k - 1\right]$, і виконанні операції проріджування розподіл д.в.в. на відрізку $\left[0, N_2 - 1\right]$ буде рівномірним з нульовою конструктивної помилкою відтворення.

Величина статистичної помилки, обумовленої некратними об'єму вибірки циклу ГВЧ довжини N_1, визначається виразом (6.29).

6.5. Методологія захисту інформації на основі факторіального кодування даних

Створення методології захисту інформації на основі факторіального кодування даних дозволить отримати єдину стратегію розробки та використання методів факторіального кодування для інтегрованого захисту інформації від помилок каналу зв'язку, а також несанкціонованого доступу та/або модифікації.

Розроблена в рамках дисертаційного дослідження і викладена в [53] методологія (рис. 6.6) базується на методах роздільного та нероздільного факторіального кодування інформації та містить наступні етапи:

1) формування множини загроз під час передавання інформації каналами зв'язку;
2) формування вимог до параметрів кодування та кількісних показників захищеності інформації;
3) вибір методу факторіального кодування інформації;
4) вибір параметрів і розрахунок показників факторіального кодування інформації;
5) вибір методу формування ключових послідовностей;
6) реалізація методу формування ключових послідовностей для факторіального кодування інформації;
7) реалізація методу факторіального кодування інформації.

Опишемо більш детально кожен з етапів запропонованої методології.

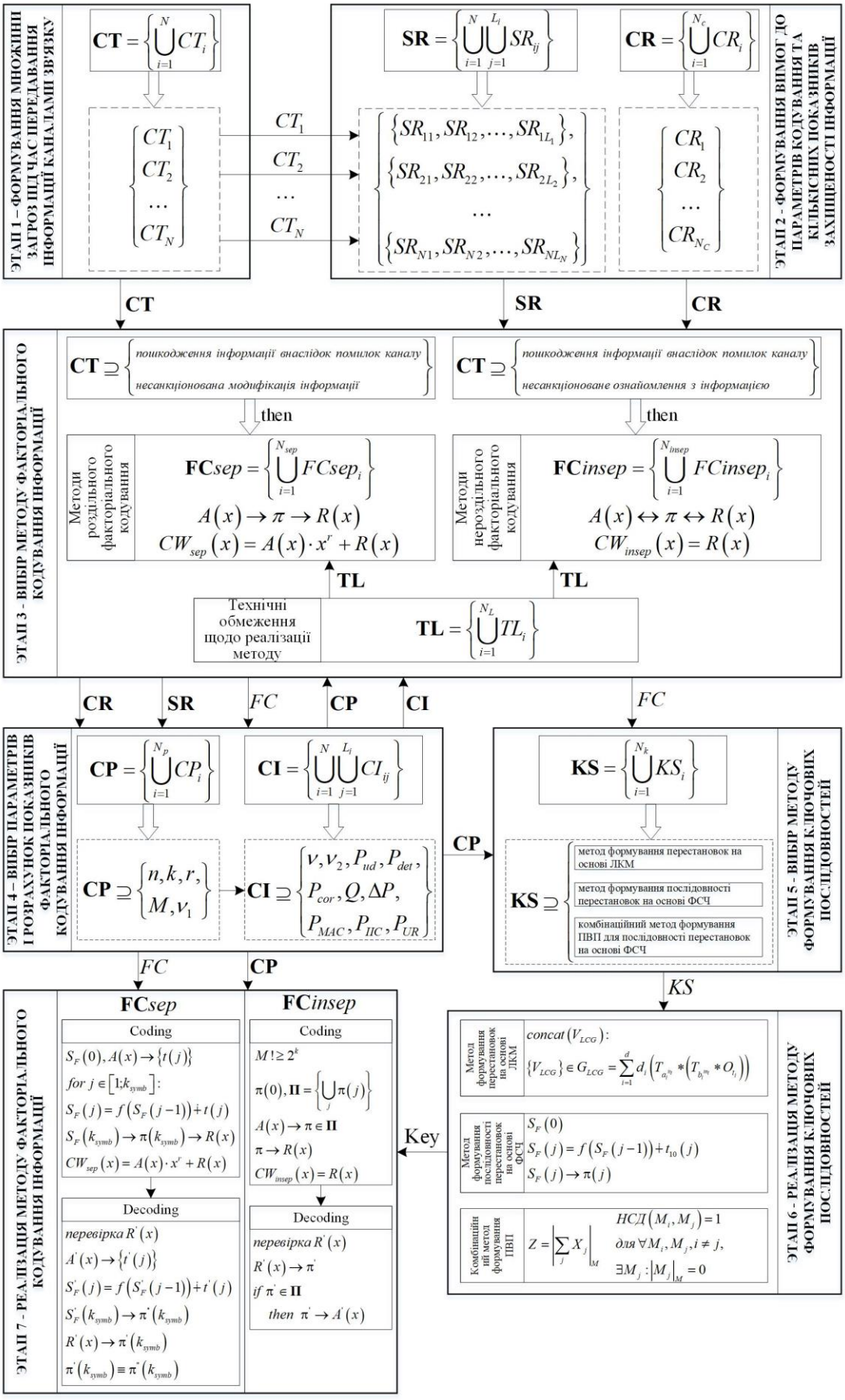


Рис. 6.6. Структурно-аналітичне відображення методології захисту інформації на основі факторіального кодування даних

Етап 1. Формування множини загроз під час передавання інформації каналами зв'язку.

На першому етапі реалізації запропонованої методології користувачу необхідно визначити всі можливі загрози, які виникають під час транспортування інформації каналами зв'язку в телекомунікаційних системах і мережах. У результаті реалізації цього етапу формується множина загроз $\mathbf{CT} = \left\{ \bigcup_{i=1}^{N} CT_i \right\} = \{CT_1, CT_2, \ldots, CT_N\}$, де N – кількість можливих загроз, визначених користувачем. Прикладом загроз можуть бути наступні: $CT_1 =$«*Пошкодження інформації внаслідок помилок каналу*», $CT_2 =$«*Несанкціонована модифікація (НСМ) інформації криптоаналітиком*», $CT_3 =$«*Несанкціоноване ознайомлення з інформацією*» (несанкціонований доступ (НСД) до інформації), $CT_4 =$«*Витік інформації відхідними ланцюгами*» тощо.

Етап 2. Формування вимог до параметрів кодування та кількісних показників захищеності інформації.

На другому етапі на основі сформованої множини загроз **CT** визначаються вимоги до параметрів кодування **CR** та гранично допустимі кількісні показники захищеності інформації **SR**. До множини параметрів коду можуть входити наступні: довжина кодового слова – n, довжина інформаційної частини кодового слова – k, довжина перевірної частини кодового слова – r, швидкість коду – $\nu_1 = k/n$ тощо. Для кожної можливої загрози CT_i, $i \in [1, N]$, може формуватися множина показників захищеності $\mathbf{SR}_i = \left\{ \bigcup_{j=1}^{L_i} SR_{ij} \right\} = \left\{ SR_{i1}, SR_{i2}, \ldots, SR_{iL_i} \right\}$, де L_i – кількість можливих показників для i-ї загрози. Наприклад, для загрози $CT_1 =$«*Пошкодження інформації внаслідок помилок каналу*» множина вимог може мати вигляд: $SR_{11} =$«$\nu \geq 0.85$», $SR_{12} =$«$P_{ud} \leq 10^{-7}$», $SR_{13} =$«$p_{0eq} \leq 10^{-9}$», $SR_{14} =$«$\Delta P \geq 5 дБ$» тощо. У результаті реалізації другого етапу запропонованої

методології формується множина вимог до параметрів кодування $\mathbf{CR} = \left\{ \bigcup_{i=1}^{N_c} CR_i \right\}$ і множина кількісних показників захищеності інформації $\mathbf{SR} = \left\{ \bigcup_{i=1}^{N} \bigcup_{j=1}^{L_i} SR_{ij} \right\}$.

Етап 3. Вибір методу факторіального кодування інформації.

На третьому етапі методології на основі сформованій на першому етапі множині загроз **CT** користувачем обирається метод факторіального кодування інформації. Якщо множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*» і $CT_j =$«*НСМ інформації криптоаналітиком*», метод факторіального кодування обирається з групи з N_{sep} роздільних методів $\mathbf{FC}sep = \left\{ \bigcup_{i=1}^{N_{sep}} FCsep_i \right\}$. Якщо множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*» і $CT_j =$«*Несанкціоноване ознайомлення з інформацією*», метод факторіального кодування обирається з групи з N_{insep} нероздільних методів $\mathbf{FC}insep = \left\{ \bigcup_{i=1}^{N_{insep}} FCinsep_i \right\}$. Якщо ж множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*», $CT_j =$«*НСМ інформації криптоаналітиком*» і $CT_l =$«*Несанкціоноване ознайомлення з інформацією*», користувач може як комбінувати роздільні та нероздільні методи факторіального кодування, так і використовувати метод роздільного факторіального кодування з поєднанням з іншим методом криптографічного закриття інформації, наприклад, методом двоконтурного криптографічного перетворення.

Методи роздільного факторіального кодування інформації **FC***sep* передбачають перетворення інформаційної частини $A(x)$, що поступає на вхід кодера, в перестановку чисел π, яка після кодування двійковим кодом $\left(R(x)\right)$ додається до інформаційної частини, формуючи кодове слово $CW_{sep}(x) = A(x) \cdot x^r + R(x)$, де r – кількість двійкових розрядів у $R(x)$.

Методи нероздільного факторіального кодування інформації **FC***insep* передбачають бієктивне перетворення інформаційної послідовності $A(x)$, що поступає на вхід кодера, в перестановку чисел π, яка після кодування двійковим кодом $\left(R(x)\right)$ передається каналом зв'язку. Таким чином, кодове слово для методів нероздільного факторіального кодування $CW_{insep}(x) = R(x)$.

Порядок перестановки M визначається сформованими на другому етапі вимогами. У будь-якому разі для методів нероздільного факторіального кодування $M! \geq 2^k$, де k – кількість біт у інформаційній послідовності на вході кодера.

Вибір методу факторіального кодування базується також на аналізі множини технічних обмежень $\mathbf{TL} = \left\{ \bigcup_{i=1}^{N_L} TL_i \right\} = \left\{ TL_1, TL_2, \ldots, TL_{N_L} \right\}$, а також на порівнянні сформованих на другому етапі методології вимог до параметрів кодування **CR** та кількісних показників **SR** захищеності інформації з параметрами та показниками факторіального кодування, розрахованими на четвертому етапі.

Множина технічних обмежень, наприклад, може містити наступні елементи: $TL_1 =$«*Неможливість використання вирішального зворотного зв'язку*», $TL_2 =$«*Неможливість видалення прапору циклової синхронізації (delimiter) зі структури кадру*», $TL_3 =$«*Обмеження в продуктивності засобів кодування*», $TL_4 =$«*Обмеження обсязі пам'яті під час операцій кодування/декодування*» тощо.

Етап 4. Вибір параметрів і розрахунок показників факторіального кодування інформації.

Для обґрунтованого вибору та реалізації методів факторіального кодування інформації на цьому етапі на основі характеристик каналу передавання даних визначаються основні параметри $\mathbf{CP} = \left\{ \bigcup_{i=1}^{N_c} CP_i \right\}$ та кількісні показники $\mathbf{CI} = \left\{ \bigcup_{i=1}^{N} \bigcup_{j=1}^{L_i} CI_{ij} \right\}$ досліджуваного факторіального коду з метою їх задоволення, відповідно, множині **CR** вимог до параметрів кодування та множині вимог **SR** до

кількісних показників захищеності інформації, сформованих на другому етапі.

Етап 5. Вибір методу формування ключових послідовностей.

Для обраного на третьому етапі методології методу факторіального кодування інформації, за визначених на четвертому етапі параметрів коду, на п'ятому етапі обирається метод формування ключових послідовностей з множини з N_K можливих методів $\mathbf{KS} = \left\{ \bigcup_{i=1}^{N_K} KS_i \right\}$. Ця множина включає:

1) $KS_1 =$«метод формування псевдовипадкової послідовності (ПВП) чисел на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел (перестановку) незалежно від топології графа станів ЛКГ»;

2) $KS_2 =$«метод формування послідовностей перестановок на основі використання ФСЧ, який забезпечує формування непередбачуваної послідовності перестановок без необхідності приведення випадкового числа додаткового генератора до потрібного діапазону зі змінною верхньою межею, дозволяє уникнути порушення рівномірності розподілу перестановок та підвищити швидкість їх формування»;

3) $KS_3 =$«комбінаційний метод формування ПВП з комбінаційною функцією підсумовування за модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел як з необмеженими, так і з обмеженими періодами, а також перестановок, які циклічно повторюються».

Крім вибору самого методу формування ключової послідовності, в залежності від визначеної множини **CP** обираються параметри для його реалізації.

Етап 6. Реалізація методу формування ключових послідовностей для факторіального кодування інформації.

Цей етап передбачає реалізацію обраного на попередньому етапі методу формування ключових послідовностей з визначеними параметрами.

Зазначимо, що метод формування ПВП на основі використання ЛКГ з будь-якою топологією обумовлює конкатенацію всіх вершин з множини $\{V_{LCG}\}$, що належать графу станів ЛКГ, який узагальнено може бути описаний виразом (4.2).

У методі формування послідовностей перестановок на основі ФСЧ для представлення синдрому перестановки S_F формування наступної перестановки зводиться до модифікації її синдрому згідно з ітераційним виразом (2.6).

Для рівномірного розподілу дискретної випадкової величини на множині цілих чисел потужності M на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем M слів від n незалежних первинних генераторів, кожний з яких циклічно формує перестановку на множині цілих чисел $[0, M_i - 1]$, $i = 1, 2, \ldots, n$, достатньо, щоб значення M_i були попарно взаємно прості ($НСД(M_i, M_j) = 1$ для $\forall M_i, M_j$, $i \neq j$) і одне зі значень M_i було кратне M $\left(\exists M_j : |M_j|_M = 0\right)$.

Етап 7. Реалізація методу факторіального кодування інформації.

Сьомий етап передбачає реалізацію обраного на етапі 3 методу факторіального кодування інформації на основі визначених параметрів (етап 4), а також вибору методу формування ключових послідовностей (етап 5) і його реалізації (етап 6).

Ядро процедури реалізації будь-якого методу роздільного факторіального кодування інформації **FC***sep* включає наступні етапи:

1) інформаційна послідовність $A(x)$, що надходить на вхід кодера, розбивається на укрупнені символи множини $\{t(j)\}$, $j \in [1; k_{symb}]$, де k_{symb} – кількість укрупнених символів;

2) отримана послідовність символів $\{t(j)\}$ прихованим чином на основі перетворення $S_F(j) = f(S_F(j-1)) \dot{+} t(j)$ за заданого $S_F(0)$ визначає $S_F(k_{symb})$;

3) отриманий синдром $S_F(k_{symb})$ перетворюється в перестановку $\pi(k_{symb})$, яка після кодування її символів двійковим кодом формує перевірну частину $R(x)$;

4) формується кодове слово $CW_{sep}(x) = A(x) \cdot x^r + R(x)$.

Процес декодування роздільного факторіального коду містить етапи:

1) перевірна частина $R^{'}(x)$ отриманого з каналу кодового слова перевіряється на відповідність перестановці. Якщо ця перевірка не проходить, формується сигнал перезапиту спотвореного блоку. В іншому випадку:

2) за інформаційною частиною отриманого з каналу кодового слова $A^{'}(x)$ за тими ж етапами, які реалізуються під час кодування, визначається перевірна перестановка $\pi^{''}(k_{symb})$. Якщо обчислена $\pi^{''}(k_{symb})$ та прийнята $\pi^{'}(k_{symb})$ перестановки співпадають, блок даних видається користувачу.

Методи нероздільного факторіального кодування **FC***insep* бієктивно перетворюють інформаційну послідовність $A(x)$, що надходить на вхід кодера, в перестановку π, що належить множині дозволених перестановок $\mathbf{\Pi} = \left\{ \bigcup_j \pi(j) \right\}$ з заданими властивостями. Після кодування символів перестановки двійковим кодом вона видається в канал: $CW_{insep}(x) = R(x)$.

Декодування нероздільного факторіального коду передбачає перевірку отриманого з каналу зв'язку кодового слова $\pi^{'}$ на належність до множини $\mathbf{\Pi}$ та наступне зворотне перетворення в інформаційну послідовність $\pi^{'} \to A^{'}(x)$.

Розроблена методологія захисту інформації на основі факторіального кодування даних дозволяє формалізувати процес створення ефективних засобів забезпечення захисту інформації під час її зберігання та передавання в телекомунікаційних системах і мережах за рахунок інтеграції методів канального кодування та криптографії, що реалізують сумісний захист переданих даних від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу.

6.6. Висновки

У шостому розділі дисертації отримані наступні результати:

- вперше розроблено метод оцінювання послідовностей рівномірно

розподілених випадкових і псевдовипадкових чисел, який за рахунок дослідження закону розподілу знаків емпіричної автокореляційної функції відносно кількості символів в перекритих частинах відрізків, на які розбивається послідовність чисел, і визначення допустимого «порогу» перекриття, нижче якого спостерігається рівномірний розподіл знаків автокореляційної функції, дозволяє виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами дискретного білого шуму, і не притаманні штучно згенерованим ПВП;

– розроблено критерії та методики перевірки послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що можуть бути використані під час оцінювання випадкових послідовностей, у тому числі сумісно з пакетами статистичного тестування. Застосування розроблених критеріїв дозволило виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ;

– вперше розроблено методологію захисту інформації на основі факторіального кодування даних, яка за рахунок формалізованого механізму використання розроблених методів і моделей роздільного та нероздільного факторіального кодування, а також методів і моделей формування ключових послідовностей для факторіального кодування дозволяє забезпечити підтримку процесів створення систем інтегрованого захисту інформації від помилок каналу зв’язку, несанкціонованої модифікації та/або несанкціонованого доступу.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-технічну проблему, яка полягає в створенні методології захисту інформації на основі факторіального кодування даних із необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу із забезпеченням підвищення достовірності передавання інформації за однакових обсягів введеної надлишковості.

Найбільш значущі результати роботи полягають у наступному.

1. Удосконалено метод формування випадкової послідовності перестановок порядку M, який унаслідок виключення необхідності приведення випадкового числа до потрібного діапазону зі змінною верхньою межею дозволив уникнути порушення рівномірності розподілу перестановок та зменшити обсяг пам'яті додаткового ГПВЧ не менш ніж на $\log_2 M$ біт. Вивільнений ресурс може бути направлений на реалізацію додаткових сервісних функцій, наприклад, таких, як контроль і діагностика. Реалізація алгоритму формування послідовності перестановок дозволила підвищити швидкість роботи генератора порівняно з генератором перестановок із застосуванням алгоритму Фішера-Йєтса для $M = 5$ – у 2,1 рази; $M = 10$ – у 2,6 рази; $M = 20$ – у 2,8 рази.

2. Розроблено методи роздільного факторіального кодування інформації (ПФК, КФК, ФКП, ФКДКСр), які за рахунок використання множини змінних констант в якості ключа дозволяють забезпечити захист інформації від модифікації внаслідок випадкових і умисних деструктивних дій, забезпечити властивість самосинхронізації коду та підвищити достовірність інформації в умовах обмежень пропускної здатності каналів зв'язку.

3. Розроблено методи нероздільного факторіального кодування інформації (ФКВД, ФКВДд, ФКЗЧІ, ФКДКСн, ФКВДвп), які дозволяють забезпечити її захист від несанкціонованого читання та помилок каналу зв'язку, забезпечити властивість самосинхронізації коду та підвищити достовірність інформації в умовах обмежень

пропускної здатності каналів зв’язку.

4. Розроблено математичну модель процесу декодування факторіальних кодів, яка дозволяє оцінити достовірність передавання інформації в результаті застосування факторіального кодування. Показано, що в порівнянні з використанням циклічного надлишкового коду за однакових обсягів введеної надлишковості для ймовірності помилки в каналі зв’язку $p_0 = 10^{-3}$ ПФК дозволяє досягти енергетичного виграшу до 2,7 дБ для довжини інформаційної частини $k = 1024$ біти та довжини перевірної частини $r = 64$ біти, КФК – до 1,6 дБ для $k = 1024$ біти та $r = 16$ біт, ФКВД – до 0,821 дБ, ФКЗЧІ – до 3,295 дБ (для порядку перестановки 8).

5. Розроблено модель узагальненого графа станів ЛКГ, яка дозволяє виконати класифікацію типів компонент зв’язності графа станів ЛКГ та дослідити вплив параметрів на його топологію. Розроблена модель надала можливість удосконалити метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів ЛКГ та, як наслідок, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення періоду ПВП $T = M$ у $M/\varphi(M)$ разів. Реалізація алгоритму формування псевдовипадкової послідовності перестановок на основі ЛКГ з будь-яким типом графа його станів дозволила підвищити швидкість роботи генератора порівняно з генератором перестановок на основі ГПВЧ LFIB78 із застосуванням алгоритму Фішера-Йєтса для порядку перестановки $M \le 125$: зокрема, для $M = 20$ – у 2,1 рази; $M = 50$ – у 1,6 рази; $M = 100$ – у 1,2 рази.

6. Удосконалено метод симетричного криптографічного захисту інформації, який дозволяє блокувати можливість винесення гами та зменшити ймовірність зламу шифру методом повного перебору ключового простору в $2^{4n} \cdot (n!)^2$ разів, де n – розрядність блоку даних. Розроблено структурну схему та алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечують можливість його практичної реалізації. Реалізація алгоритму в режимі формування

ПВП дозволяє отримати послідовність, яка успішно проходить тести NIST STS, Diehard, TestU01.

7. Теоретично обґрунтовано принципи побудови комбінаційного генератора, який використовує підсумовування за модулем M в якості комбінаційної функції. Для цього визначено закон розподілу д.в.в. на виході комбінаційного генератора, що містить n первинних генераторів випадкових чисел як із необмеженими, так і з обмеженими періодами, а також перестановок, що циклічно повторюються. Це дало змогу обґрунтувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення рівномірного розподілу чисел у заданому діапазоні, а також розробити методику вибору параметрів первинних генераторів для забезпечення необхідних статистичних властивостей формованої послідовності чисел і її використання в реалізаціях запропонованого методу формування перестановок на основі ФСЧ. Виконана оцінка статистичних властивостей ПВП на виході комбінаційного генератора підтверджує, що запропонований комбінаційний метод формування ПВП може бути використаний у задачах, що потребують їх високої якості, зокрема, для формування псевдовипадкової послідовності перестановок на основі ФСЧ.

8. Розроблено метод, критерії та методики оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, які дозволяють виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами випадкових чисел, і не притаманні штучно згенерованим ПВП. Застосування розробленого інструментарію дало змогу виявити статистичні відхилення для деяких генераторів ПВП, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ.

9. Розроблено методологію захисту інформації на основі факторіального кодування даних, яка дозволяє забезпечити підтримку процесів створення систем захисту інформації від помилок каналу зв’язку, несанкціонованої модифікації та/або несанкціонованого доступу. Застосування цієї методології дає можливість використовувати розроблені методи та моделі в єдиній стратегії досліджень у галузі інтегрованого захисту інформації в телекомунікаційних системах і мережах та

ефективно будувати відповідні системи захисту з заданими властивостями.

10. Результати дисертаційної роботи впроваджено на ДП «НДІ «Акорд», у ТОВ «Діджитал Мастер», у Департаменті освіти та гуманітарної політики Черкаської міської ради та в освітньому процесі Черкаського державного технологічного університету, Черкаського інституту пожежної безпеки імені Героїв Чорнобиля та Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Э. В. Фауре, В. В. Швыдкий и В. А. Щерба, "Комбинированное факториальное кодирование и его свойства", *Радіоелектроніка, інформатика, управління*, № 3, с. 80–86, 2016.

[2] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб комбінованого кодування інформації", патент України №107657, 24.06.2016.

[3] Э. В. Фауре и А. В. Магуров, "Исследование способности обнаружения ошибок комбинированным факториальным кодом", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 13.

[4] E. V. Faure, A. I. Shcherba, and V. M. Rudnytskyi, "The Method and Criterion for Quality Assessment of Random Number Sequences", *Cybernetics and Systems Analysis*, vol. 52, no. 2, pp. 277–284, 2016.

[5] E. V. Faure, A. I. Shcherba, and A. A. Kharin, "Factorial code with a given number of inversions", *Radio Electronics, Computer Science, Control*, no. 2, pp. 143–153, 2018.

[6] N. Alishov, E. Faure, D. Faure, and V. Shadkhin, "Method of linear formation of pseudorandom processes", *Journal of Qafqaz University. Mathematics and computer science*, no. 30, pp. 17–24, 2010.

[7] Э. В. Фауре, Е. В. Ланских, Д. А. Коляда и Ю. И. Черевко, "Преобразование процессов на выходе генераторов М-последовательности и конгруэнц-генераторов", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 17–21, 2012.

[8] Р. О. Бивзюк, Д. В. Фауре и Э. В. Фауре, "Устройство формирования остатков в многоканальных помехоустойчивых кодеках", *Вісник Хмельницького національного університету*, № 4, с. 75–78, 2010.

[9] Э. В. Фауре, Д. В. Фауре, М. В. Сторчак и В. А. Кучеренко, "Исследование и оптимизация методов формирования контрольной суммы помехоустойчивых

кодов", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 63–67, 2011.

[10] Е. В. Фауре, Д. В. Фауре і Р. О. Бівзюк, "Пристрій формування залишків у багатоканальних завадостійких кодеках", патент України №55711, 27.12.2010.

[11] Є. В. Ланських, Е. В. Фауре і А. В. Очеретяна, "Метод організації ключового обміну з використанням прихованого каналу в телефонних мережах загального користування", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 18–21, 2010.

[12] Е. С. Лисицына, В. В. Швыдкий, А. И. Щерба и Э. В. Фауре, "Разделение векторной смеси сигнала и помехи по методу максимального правдоподобия", *Системи обробки інформації*, № 8(89), с. 62–67, 2010.

[13] Э. В. Фауре, Д. В. Фауре и И. Н. Коротеев, "Выбор параметров генератора конгруэнтных чисел", *Сучасна спеціальна техніка*, № 1(20), с. 30–35, 2010.

[14] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Прихована передача інформації у полосі звукових частот", *Сучасний захист інформації*, № 2, с. 22–30, 2011.

[15] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Ансамбль ортогональних шумоподібних сигналів для скритних систем з обмеженим спектром", *Наукові записки УНДІЗ*, № 1(21), с. 33–38, 2012.

[16] А. С. Береза, А. А. Лавданский, В. В. Швыдкий и Э. В. Фауре, "Генерация конгруэнтных последовательностей чисел с заданными свойствами", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 2, с. 3–8, 2012.

[17] Э. В. Фауре, А. С. Береза и Е. А. Ярославская, "Оценка точности воспроизведения закона распределения дискретной случайной величины при ее преобразовании", *Вестник Хмельницкого национального университета*, № 5, с. 176–182, 2012.

[18] В. Ю. Шадхін, Е. В. Фауре і О. В. Костомаров, "Криптографічні засоби захисту інформації в автоматизованих системах дистанційного навчання", *Вісник Хмельницького національного університету*, № 1, с. 126–130, 2012.

[19] В. В. Швыдкий, Э. В. Фауре, В. В. Веретельник и В. А. Щерба, "Генерация стохастической последовательности генератором конгруэнтных чисел", *Системи обробки інформації*, № 3, с. 74–80, 2012.

[20] В. В. Швидкий, А. І. Щерба, Е. В. Фауре і В. В. Веретельник, "Спосіб формування некорельованої послідовності рівномірно розподілених чисел", патент України №74628, 12.11.2012.

[21] Ю. Г. Лега, Э. В. Фауре и А. А. Лавданский, "Технология генерации случайных последовательностей с большой разрядностью чисел", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 3, с. 3–8, 2012.

[22] А. А. Лавданский, В. В. Швыдкий и Э. В. Фауре, "Метод формирования последовательностей случайных чисел и его использование в системах потокового шифрования", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 5–10, 2013.

[23] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, А. І. Щерба і А. О. Лавданський, "Спосіб двоконтурного поточного шифрування", патент України №82044, 25.07.2013.

[24] Э. В. Фауре, Е. С. Лисицына и Д. Ю. Нестеренко, "Метод повышения стойкости электронных кодовых замков", *Вісник Інженерної академії України*, № 2, с. 137–141, 2013.

[25] Е. В. Фауре, М. І. Вишня і В. А. Чорнобай, "Оцінка закону розподілу випадкових чисел комбінаційного генератора у k-вимірному просторі", *Вісник Херсонського національного технічного університету*, №4, с. 169–173, 2014.

[26] E. Faure, V. Chornobai, and M. Vyshnia, "Some statistical properties of pseudorandom number sequences formed by combination generator", in *Современные достижения в науке и образовании : сб. тр. IX междунар. науч. конф., 22-29 сентября 2014 г., Нетания (Израиль)*, Хмельницкий, 2014, pp. 56–58.

[27] Э. В. Фауре, В. В. Швыдкий и А. И. Щерба, "Метод формирования воспроизводимой непредсказуемой последовательности перестановок",

Безпека інформації, т. 20, № 3, с. 253–258, 2014.

[28] Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування випадкової послідовності перестановок", патент України №106668, 10.05.2016.

[29] А. А. Лавданский и Э. В. Фауре, "Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов", *Системні дослідження та інформаційні технології*, № 2, с. 39–50, 2015.

[30] А. А. Лавданский и Э. В. Фауре, "Комбинационный метод формирования последовательности псевдослучайных чисел", в *Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014 р.*, К., 2014, с. 403–404.

[31] Е. В. Фауре, С. В. Сисоєнко і Т. В. Миронюк, "Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення", *Системи управління, навігації та зв'язку*, № 4, с. 85–87, 2015.

[32] В. М. Рудницький, Е. В. Фауре і С. В. Сисоєнко, "Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем", *Вісник Інженерної академії України*, № 3, с. 219–221, 2016.

[33] Е. В. Фауре і С. В. Сисоєнко, "Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу", в *The scientific potential of the present [text]: Proceedings of the International Scientific Conference, St. Andrews, Scotland, UK, December 1, 2016*, Vinnytsia, 2016, с. 119–122.

[34] Э. В. Фауре, В. В. Швыдкий и В. А. Щерба, "Метод формирования имитовставки на основе перестановок", *Захист інформації*, т. 16, № 4, с. 340, 2015.

[35] Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування імітовставки", патент України №106669, 10.05.2016.

[36] Э. В. Фауре и В. В. Швыдкий, "Формирование имитовставки на основе перестановок", в *Проблеми інформатизації: Матеріали другої міжнародної науково-технічної конференції, Черкаси, 25-26 листопада 2014 р.*, Черкаси, 2014, с. 12.

[37] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Анализ корреляционных свойств последовательностей (псевдо) случайных чисел", *Наука і техніка Повітряних Сил Збройних Сил України*, № 1(18), с. 142–150, 2015.

[38] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором", *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, № 18, с. 165–171, 2015.

[39] Э.В. Фауре, В.В. Швыдкий и А.И. Щерба, "Контроль целостности информации на основе факториальной системы счисления", *Journal of Baku Engineering University. Mathematics and computer science*, т. 1, № 1, с. 3–13, 2017.

[40] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб контролю цілісності інформації", патент України №107655, 24.06.2016.

[41] Е. В. Фауре і А. М. Ткаченко, "Дослідження здатності виявлення помилок завадостійким кодом на основі перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 17.

[42] Э. В. Фауре и Р. К. Еременко, "Исследование способности обнаружения ошибок полным факториальным кодом", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 12.

[43] Е. В. Фауре, О. О. Харін і М. О. Качалова, "Дослідження процедури формування контрольної суми повного факторіального коду на основі ітераційного перетворення", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 17.

[44] А. О. Лавданський, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування послідовності рівномірно розподілених випадкових чисел", патент

України №86718, 10.01.2014.

[45] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, О. С. Лісіцина і А. О. Лавданський, "Спосіб формування послідовності випадкових чисел", патент України №86705, 10.01.2014.

[46] Е. В. Фауре, О. О. Харін, В. В. Швидкий і А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", патент України №117004, 12.06.2017.

[47] Е. В. Фауре і О. О. Харін, "Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних", в *Актуальні задачі та досягнення у галузі кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції, Кропивницький, 23-25 листопада 2016 р.*, Кропивницький, 2016, с. 178–179.

[48] Е. В. Фауре, О. О. Харін, В. В. Швидкий і А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", патент України №121361, 11.12.2017.

[49] Е. В. Фауре і О. О. Харін, "Пристрій кодування та декодування факторіальних кодів з виявленням і виправленням помилок", патент України №123640, 12.03.2018.

[50] Э. В. Фауре и А. А. Лавданский, "Способ определения структуры графа состояний линейного конгруэнтного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 18-22 березня 2013 р.*, Черкаси, 2013, с. 110–112.

[51] Е. В. Фауре і В. С. Рузальонок, "Дослідження структури графа станів лінійного конгруентного генератора", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 15–16.

[52] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в *Наукоемкие технологии*

в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография, В. М. Безрук и В. В. Баранник, Ред. Харьков: Лидер, 2017, с. 291–323.

[53] Е. В. Фауре, "Методологія захисту інформації на основі факторіального кодування даних", в *Криптографічне кодування: обробка та захист інформації: колективна монографія*, В. М. Рудницький, Ed Харків: Щедра садиба плюс, 2018, с. 85–95.

[54] Е. В. Фауре, "Факториальное кодирование с исправлением ошибок", *Радіоелектроніка, інформатика, управління*, № 3, с. 130–138, 2017.

[55] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе комбинационного генератора", *Безпека інформації*, т. 20, № 2, с. 153–158, 2014.

[56] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 2, с. 33–39, 2016.

[57] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 57–61, 2016.

[58] Э. В. Фауре, "Факториальное кодирование с несколькими контрольными суммами", *Вісник Житомирського державного технологічного університету. Серія: Технічні науки*, № 3 (78), с. 104–113, 2016.

[59] Э. В. Фауре, "Статистические характеристики оценок нормированных коэффициентов автокорреляции последовательностей (псевдо) случайных чисел", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 16-20 березня 2015 р.*, Черкаси, 2015, с. 46–47.

[60] Э. В. Фауре, "Методика оценки вероятности преобразования перестановки чисел в перестановку при ее передаче по каналу связи", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-*

практичної Internet-конференції, Черкаси, 14-20 березня 2016 р., Черкаси, 2016, с. 78–80.

[61] P. L'Ecuyer, "Random Number Generation", in *Handbook of Computational Statistics*, J. E. Gentle, W. K. Härdle, and Y. Mori, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 35–71.

[62] М. А. Иванов, "Разработка и исследование стохастических методов и средств защиты программных систем ответственного назначения", дис. ... докт. техн. наук : 05.13.11, 05.13.19, Национальный исследовательский ядерный университет «МИФИ», М., 2005.

[63] С. А. Осмоловский, *Стохастическая информатика: инновации в информационных системах*. М.: Горячая линия-Телеком, 2012.

[64] С. А. Осмоловский, *Стохастические методы передачи данных*. М.: Радио и связь, 1991.

[65] С. А. Осмоловский, *Стохастические методы защиты информации*. М.: Радио и связь, 2003.

[66] C. E. Shannon, "A Mathematical Theory of Communication", *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[67] Д. А. Мельников, *Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели*. М.: КУДИЦ-Образ, 2001.

[68] W. W. Peterson and E. J. Weldon, *Error-correcting codes*, 2d ed. Cambridge: MIT Press, 1972.

[69] R. H. Morelos-Zaragoza, *The art of error correcting coding*, 2nd ed. Chichester ; Hoboken, NJ: John Wiley, 2006.

[70] E. R. Berlekamp, *Algebraic coding theory*, Revised edition. New Jersey: World Scientific, 2015.

[71] C. E. Shannon, "Communication theory of secrecy systems", *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1948.

[72] *Data Encryption Standard (DES)*, US standard FIPS PUB 46-3, 25.10.1999.

[73] *Advanced Encryption Standard (AES)*, US standard FIPS PUB 197, 10-Nov-2012.

[74] *Інформаційні технології. Криптографічний захист інформації. Алгоритм*

симетричного блокового перетворення, стандарт України ДСТУ 7624:2014, 07.01.2015.

[75] *Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования*, стандарт СССР ГОСТ 28147-89, 07.01.1990.

[76] *Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования*, стандарт України ДСТУ ГОСТ 28147:2009, 02.01.2009.

[77] R. L. Rivest, A. Shamir, and L. M. Adleman, "Cryptographic communications system and method", USA patent US4405829A, 20-Sep-1983.

[78] Б. Шнайер, *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*. Триумф, 2012.

[79] А. А. Молдовян, Н. А. Молдовян и Б. Я. Советов, *Криптография*. СПб.: Лань, 2001.

[80] *RSA Cryptography Standard,* RSA Laboratories standard PKCS #1 v2.2, 27.10.2012.

[81] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[82] *Digital Signature Standard (DSS)*, US standard FIPS PUB 186-4, Jul-2013.

[83] *Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка*, стандарт України ДСТУ 4145-2002, 07.01.2003.

[84] R. J. McEliece, "A Public-Key Criptosystem Based on Algebraic Theory", Pasadena, CA, The Deep Space Network Progress Report 42–44, 1978.

[85] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory", *Prob. Control and Inf. Theory*, vol. 15, no. 2, pp. 159–166, 1986.

[86] В. М. Сидельников, "Открытое шифрование на основе двоичных кодов Рида-Маллера", *Дискретная математика*, т. 6, № 2, с. 3–20, 1994.

[87] Ю. В. Стасев и А. А. Кузнецов, "Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов", *Кибернетика и системный*

анализ, № 3, с. 47–57, 2005.

[88] В. П. Семеренко, "Интегрированная защита информации: криптография плюс помехоустойчивое кодирование", *Захист інформації*, т. 13, № 3, с. 1–9, 2011.

[89] В. С. Василенко, А. В. Чунарьова, М. Ю. Василенко і А. В. Чунарьов, "Спосіб забезпечення цілісності інформації на базі коду умовних лишків", патент України №75935, 25.12.2012.

[90] В. С. Василенко, А. В. Чунарьова, М. Ю. Василенко і А. В. Чунарьов, "Спосіб забезпечення цілісності інформації на базі лишково-хеммінгового коду", патент України №75938, 25.12.2012.

[91] М. Ю. Василенко, В. С. Василенко і А. В. Чунарьов, "Спосіб забезпечення цілісності інформації на базі завадостійкого коду умовних лишків", патент України №67988, 12.03.2012.

[92] С. А. Осмоловский, "Способ комплексной защиты информации", патент РФ №RU 2292122 C9, 27.07.2007.

[93] С. А. Осмоловский, "Способ передачи и комплексной защиты информации", патент РФ №RU 2367007 C2.

[94] A. P. Stakhov, V. Massingue, and A. Sluchenkova, "Introduction into Fibonacci coding and cryptography", *Osnova, Kharkov,* 1999.

[95] A. P. Stakhov, "Fibonacci matrices, a generalization of the “Cassini formula”, and a new coding theory", *Chaos, Solitons & Fractals,* vol. 30, no. 1, pp. 56–66, 2006.

[96] A. P. Stakhov, "The “golden” matrices and a new kind of cryptography", *Chaos, Solitons & Fractals*, vol. 32, no. 3, pp. 1138–1146, 2007.

[97] А. П. Стахов, "Компьютеры Фибоначчи и новая теория кодирования: история, теория, перспективы", *Известия Южного федерального университета. Технические науки*, т. 38, № 3, с. 205–213, 2004.

[98] А. П. Стахов, "«Золотые» матрицы и новый метод криптографии", в *Современные методы кодирования в электронных системах [Текст] : тезисы докладов третьей международной научной конференции*, Сумы, 24-25 октября 2006 года, с. 41–42.

[99] A. P. Stakhov, "Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas

functions, and the improved method of the “golden” cryptography". Academy of Trinitarizam, Moscow, 2006.

[100] A. P. Stakhov, "The golden section, Fibonacci numbers, mathematics of harmony and “golden” scientific revolution", *Computer science and cybersecurity*, no. 2 (2), pp. 31–68, 2016.

[101] В. Я. Чечельницький, "Методологія підвищення ефективності телекомунікаційних систем на основі інтеграції канального кодування та шифрування даних", дис... д-ра техн. наук: 05.12.13, Нац. авіац. ун-т, К., 2013.

[102] М. И. Мазурков, В. Я. Чечельницкий, П. Е. Баранов, А. Н. Мелешкевич, С. Н. Кропачев и Н. И. Кушниренко, "Методы повышения защиты информации путем объединения операций уплотнения, шифрования и канального кодирования", *Известия вузов. Радиоэлектроника*, т. 54, № 5, с. 3–16, 2011.

[103] М. И. Мазурков, В. Я. Чечельницкий и П. Мурр, "Метод защиты информации на основе совершенных двоичных решеток", *Известия вузов. Радиоэлектроника*, т. 51, № 11, с. 53–57, 2008.

[104] М. И. Мазурков, "Класс минимаксных корректирующих кодов на основе совершенных двоичных решеток", *Известия вузов. Радиоэлектроника*, т. 54, № 9, с. 24–39, 2011.

[105] М. И. Мазурков, "Композиционный матричный шифр на базе совершенных двоичных решеток", *Известия вузов. Радиоэлектроника*, т. 56, № 3, с. 36–44, 2013.

[106] Н. И. Кушниренко и В. Я. Чечельницкий, "Метод криптографической передачи информации на базе эквивалентного класса совершенных двоичных решеток", *Інформатика та математичні методи в моделюванні*, № 4, № 3, с. 210–218, 2014.

[107] В. Я. Чечельницкий, "Классы сигналов на основе совершенных двоичных решеток", дис... канд. техн. наук: 05.12.13, Одесский национальный политехнический ун-т, Одесса, 2002.

[108] P. E. Baranov, M. I. Mazurkov, V. Y. Chechelnytskyi, and A. A. Yakovenko, "Family of two-dimensional correcting codes on a basis of perfect binary array",

Radioelectronics and Communications Systems, vol. 52, no. 9, pp. 501–506, Sep. 2009.

[109] M. I. Mazurkov, V. Y. Chechel'nitskii, and P. Murr, "Information security method based on perfect binary arrays", *Radioelectronics and Communications Systems*, vol. 51, no. 11, pp. 612–614, 2008.

[110] M. I. Mazurkov, V. Y. Chechelnytskyi, and K. K. Nekrasov, "Three-level cryptographic system for block data encryption", *Radioelectronics and Communications Systems*, vol. 53, no. 7, pp. 376–379, 2010.

[111] А. Е. Горячев, "Обнаружение ошибок в перестановках", *Вісник Сумського державного університету. Серія Технічні науки*, № 3, с. 126–134, 2009.

[112] О. А. Борисенко, А. Е. Горячев, Б. К. Лопатченко и А. Н. Кобяков, "Перестановки в телекоммуникационных сетях", *Перестановки в телекомунікаційних мережах*, № 2, с. 15–22, 2013.

[113] О. О. Борисенко и О. Є. Горячев, "Помехоустойчивая передача экономической информации на основе перестановок", *Актуальні проблеми економіки*, № 3, с. 156–163, 2013.

[114] А. А. Борисенко и А. Е. Горячев, "Исправление ошибок в перестановках", *Системи обробки інформації*, № 2 (109), с. 171–173, 2013.

[115] В. И. Коржик, С. А. Осмоловский и Л. М. Финк, "Универсальное стохастическое кодирование в системах с решающей обратной связью", *Проблемы передачи информации*, т. 10, № 4, с. 25–29, 1974.

[116] А. А. Борисенко, С. М. Маценко, С. М. Мальченков и О. И. Ямник, "О помехоустойчивости фибоначчиевых чисел", *Системи обробки інформації*, № 4, с. 84–87, 2015.

[117] А. П. Стахов и В. А. Лужецкий, *Машинная арифметика ЦВМ в кодах Фибоначчи и «золотой» пропорции*. М.: Издательство АН СССР, 1981.

[118] А. П. Стахов, "Помехоустойчивые коды: Компьютер Фибоначчи", *Москва, Знание, серия «Радиоэлектроника и связь*, № 6, с. 64, 1989.

[119] P. Wild, "Infinite families of perfect binary arrays", *Electronics Letters*, vol. 24, no. 14, p. 845, 1988.

[120]И. А. Гепко, "Синтез совершенных двоичных решеток", *Известия вузов. Радиоэлектроника*, т. 41, № 6, с. 13–21, 1998.

[121]В. Я. Чечельницкий, "Метод построения полного класса совершенных двоичных решеток порядка N = 2k", *Известия вузов. Радиоэлектроника*, vol. 49, no. 9, pp. 44–53, 2006.

[122]М. И. Мазурков и В. Я. Чечельницкий, "Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA-технологий", *Известия вузов. Радиоэлектроника*, т. 46, № 5, с. 54–63, 2003.

[123]T. K. Moon, *Error correction coding: mathematical methods and algorithms*. Hoboken, N.J: Wiley-Interscience, 2005.

[124]*3GPP*, US standard Technical Specification 36.212 V14.3.0, Jun-2017.

[125]S. Dolev, L. Lahiani, and Y. Haviv, "Unique permutation hashing", *Theoretical Computer Science*, vol. 475, pp. 59–65, Mar. 2013.

[126]K. E. Iverson, *A Programming Language*. New York, NY, USA: John Wiley & Sons, Inc., 1962.

[127]R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics: a foundation for computer science*, 2nd ed. Reading, Mass: Addison-Wesley, 1994.

[128]D. E. Knuth, *The Art of Computer Programming : Fundamental Algorithms*, 3rd ed., vol. 1. Reading, Mass: Addison-Wesley, 1997.

[129]P. L'Ecuyer, "Efficient and Portable Combined Random Number Generators", *Commun. ACM*, vol. 31, no. 6, pp. 742–751, 1988.

[130]R. R. Coveyou and R. D. Macpherson, "Fourier Analysis of Uniform Random Number Generators", *Journal of the ACM*, vol. 14, no. 1, pp. 100–119, Jan. 1967.

[131]D. H. Lehmer, "Mathematical methods in large-scale computing units", in *Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery*, Cambridge, Mass., 1949, pp. 141–146.

[132]G. Marsaglia and L.-H. Tsay, "Matrices and the structure of random number sequences", *Linear Algebra and its Applications*, vol. 67, pp. 147–156, 1985.

[133]M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator", *ACM Transactions on*

Modeling and Computer Simulation (TOMACS), vol. 8, no. 1, pp. 3–30, 1998.

[134] G. Marsaglia and A. Zaman, "Monkey tests for random number generators", *Computers & Mathematics with Applications*, vol. 26, no. 9, pp. 1–10, 1993.

[135] G. Marsaglia, "Random Number Generation", in *Encyclopedia of Computer Science*, Chichester, UK: John Wiley and Sons Ltd., 2003, pp. 1499–1503.

[136] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*. Society for Industrial and Applied Mathematics, 1992.

[137] R. R. Coveyou, "Random Number Generation is too important to be left to Chance", *Studies in Applied Mathematics (SIAM)*, vol. 3, pp. 70–111, 1969.

[138] S. K. Park and K. W. Miller, "Random Number Generators: Good Ones Are Hard to Find", *Commun. ACM*, vol. 31, no. 10, pp. 1192–1201, 1988.

[139] P. L'Ecuyer and P. Hellekalek, "Random Number Generators: Selection Criteria and Testing", in *Random and Quasi-Random Point Sets*, vol. 138, P. Hellekalek and G. Larcher, Eds. New York, NY: Springer New York, 1998, pp. 223–265.

[140] R. C. Tausworthe, "Random Numbers Generated by Linear Recurrence Modulo Two", *Mathematics of Computation*, vol. 19, no. 90, p. 201, 1965.

[141] H. Niederreiter and I. E. Shparlinski, "Recent Advances in the Theory of Nonlinear Pseudorandom Number Generators", in *Monte Carlo and Quasi-Monte Carlo Methods 2000*, K.-T. Fang, H. Niederreiter, and F. J. Hickernell, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 86–102.

[142] G. Marsaglia, "Regularities in Congruential Random Number Generators", *Numer. Math.*, vol. 16, no. 1, pp. 8–10, 1970.

[143] G. Marsaglia, "Seeds for Random Number Generators", *Commun. ACM*, vol. 46, no. 5, pp. 90–93, 2003.

[144] R. R. Coveyou, "Serial Correlation in the Generation of Pseudo-Random Numbers", *Journal of the ACM*, vol. 7, no. 1, pp. 72–74, Jan. 1960.

[145] G. Marsaglia and A. Zaman, "Some portable very-long-period random number generators", *Computers in Physics*, vol. 8, no. 1, p. 117, 1994.

[146] T. Nishimura, "Tables of 64-bit Mersenne twisters", *ACM Transactions on Modeling and Computer Simulation*, vol. 10, no. 4, pp. 348–357, 2000.

[147]P. L’Ecuyer, "Tables of linear congruential generators of different sizes and good lattice structure", *Mathematics of Computation*, vol. 68, no. 225, pp. 249–261, 1999.

[148]G. Marsaglia and W. W. Tsang, "The 64-bit universal RNG", *Statistics & Probability Letters*, vol. 66, no. 2, pp. 183–187, 2004.

[149]H. Niederreiter, "The Multiple-Recursive Matrix Method for Pseudorandom Number Generation", *Finite Fields and Their Applications*, vol. 1, no. 1, pp. 3–30, 1995.

[150]G. Marsaglia, "The Structure of Linear Congruential Sequences", in *Applications of Number Theory to Numerical Analysis*, S. K. Zaremba, Ed. Academic Press, 1972, pp. 249–285.

[151]M. Matsumoto and Y. Kurita, "Twisted GFSR generators", *ACM Transactions on Modeling and Computer Simulation*, vol. 2, no. 3, pp. 179–194, 1992.

[152]S. Tezuka, *Uniform Random Numbers*. Boston, MA: Springer US, 1995.

[153]P. L’Ecuyer, "Uniform random number generation", *Annals of Operations Research*, vol. 53, no. 1, pp. 77–120, 1994.

[154]P. L’Ecuyer, "History of uniform random number generation", in *Proceedings of the 2017 Winter Simulation Conference*, Las Vegas, Nevada, 2017, p. 28.

[155]P. L’Ecuyer, "Uniform Random Number Generators: A Review", in *Proceedings of the 29th Conference on Winter Simulation*, Washington, DC, USA, 1997, p.127–134.

[156]D. E. Knuth, *The Art of Computer Programming : Seminumerical Algorithms*, 3rd Ed., vol.2. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1997.

[157]W. Freiberger and U. Grenander, *A Short Course in Computational Probability and Statistics*. New York: Springer, 1971.

[158]M. Greenberger, "An A Priori Determination of Serial Correlation in Computer Generated Random Numbers", *Mathematics of Computation*, vol. 15, no. 76, p. 383, 1961.

[159]T. E. Hull and A. R. Dobell, "Random Number Generators", *SIAM Review*, vol. 4, no. 3, pp. 230–254, 1962.

[160]C. F. Gauss, J. Brinkhuis, and C. Greiter, *Disquisitiones Arithmeticae*, Reissue edition. New York: Springer, 1986.

[161]B. D. Ripley, "Thoughts on pseudorandom number generators", *Journal of*

Computational and Applied Mathematics, vol. 31, no. 1, pp. 153–163, 1990.

[162] A. C. Atkinson, "Tests of Pseudo-Random Numbers", *Applied Statistics*, vol. 29, no. 2, p. 164, 1980.

[163] E. J. Dudewicz and T. G. Ralley, *The handbook of random number generation and testing with TESTRAND computer code*. American Sciences Press, 1981.

[164] J. Dagpunar, *Principles of random variate generation*. Clarendon Press, 1988.

[165] L. T. Bernhofen, E. J. Dudewicz, J. Levendovszky, and E. C. van der Meulen, "Ranking of the Best Random Number Generators via Entropy-Uniformity Theory", *American Journal of Mathematical and Management Sciences*, vol. 16, no. 1–2, pp. 49–88, Jan. 1996.

[166] S. L. Anderson, "Random Number Generators on Vector Supercomputers and Other Advanced Architectures", *SIAM Review*, vol. 32, no. 2, pp. 221–251, Jun. 1990.

[167] Z. A. Karian and E. J. Dudewicz, *Modern Statistical Systems and GPSS Simulation: The First Course*, 2nd ed. Boca Raton, FL, USA: CRC Press, Inc., 1998.

[168] L. P. Jennergren, "Another method for random number generation on microcomputers", *SIMULATION*, vol. 41, no. 2, p. 79, 1983.

[169] G. Fishman, *Monte Carlo: Concepts, Algorithms, and Applications*, Corrected edition. New York: Springer, 2003.

[170] G. Fishman and I. Moore L., "An Exhaustive Analysis of Multiplicative Congruential Random Number Generators with Modulus $2^{31} - 1$", *SIAM J. Sci. and Stat. Comput.*, vol. 7, no. 1, pp. 24–45, Jan. 1986.

[171] G. Ugrin-Šparac, "Stochastic investigations of pseudo-random number generators", *Computing*, vol. 46, no. 1, pp. 53–65, 1991.

[172] J. T. Smith, *C++ Toolkit for Engineers and Scientists*, 2nd edition. Springer, 1999.

[173] J. P. C. Kleijnen and N. Adams, "Pseudorandom number generation on supercomputers", Research Memorandum FEW 378, 1989.

[174] P. L'Ecuyer, "Random numbers for simulation", *Communications of the ACM*, vol. 33, no. 10, pp. 85–97, 1990.

[175] G. Marsaglia and A. Zaman, "A New Class of Random Number Generators", *The Annals of Applied Probability*, vol. 1, no. 3, pp. 462–480, 1991.

[176] I. Borosh and H. Niederreiter, "Optimal multipliers for pseudo-random number generation by the linear congruential method", *BIT*, vol. 23, no. 1, pp. 65–74, 1983.

[177] И. А. Кулаков и Ю. В. Москвин, "Способ формирования регулярных последовательностей с элементами, составленными из двоичных сигналов", патент РФ №RU2469382C1, 10.12.2012.

[178] И. А. Кулаков, "Способ формирования нерегулярных последовательностей с элементами, составленными из двоичных сигналов", патент РФ №RU2467378, 20.11.2012.

[179] Т. В. Митянкина, В. В. Швыдкий и А. И. Щерба, "Рандомизация последовательности конгруэнтных чисел", *Вісник Інженерної академії України*, № 2, с. 107–111, 2008.

[180] А. А. Лавданский, "Методи та засоби формування псевдовипадкових послідовностей для комп'ютерної криптографії", Черкаський державний технологічний університет, Черкаси, 2017.

[181] S. W. Golomb, *Sequences with randomness properties*. Baltimore, MD. : : Glenn L. Martin Co, 1955.

[182] N. Zierler, "Linear Recurring Sequences", *Journal of the Society for Industrial and Applied Mathematics*, vol. 7, no. 1, pp. 31–48, 1959.

[183] Е. С. Лисицына, Э. В. Фауре, В. В. Швыдкий и А. И. Щерба, "Некоторые свойства многочленов и их использование в задачах связи", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 134–140, 2006.

[184] H. Fredricksen, "A class of nonlinear de Bruijn cycles", *Journal of Combinatorial Theory, Series A*, vol. 19, no. 2, pp. 192–199, 1975.

[185] J. Havel, A. N. Morozevich, и V. N. Yarmolik, "Генератор рандомизированных псевдослучайных чисел", *Kybernetika*, т. 19, № 1, с. 58–65, 1983.

[186] А. А. Семенов и Д. О. Усанов, "Цифровой генератор хаотического сигнала", патент РФ №2472286, 10.01.2013.

[187] Иванов М.А. и Чугунков И.В., *Теория, применение и оценка качества генераторов псевдослучайных последовательностей*. Москва: Кудиц - Образ,

2003.

[188] P. R. Geffe, "How to Protect Data With Ciphers That are Really Hard to Break", *Electronics*, vol. v. 46, no. n. I, pp. 99–101, 1973.

[189] T. Beth and F. C. Piper, "The Stop-and-Go-Generator", in *Advances in Cryptology*, vol. 209, T. Beth, N. Cot, and I. Ingemarsson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 88–92.

[190] R. A. Rueppel, "When Shift Registers Clock Themselves", in *Advances in Cryptology - EUROCRYPT'87*, vol. 304, D. Chaum and W. L. Price, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 53–64.

[191] J. Reeds, "“Cracking” a random number generator", *Cryptologia*, vol. 1, pp. 20–26, 1977.

[192] J. A. Reeds, "Cracking a Multiplicative Congruential Encryption Algorithm", presented at the *Information Linkage Between Applied Mathematics and Industry*, 1979, pp. 467–472.

[193] J. Reeds, "Solution of Challenge Cipher", *Cryptologia*, vol. 3, pp. 83–95, 1979.

[194] J. B. Plumstead, "Inferring a Sequence Generated by a Linear Congruence", in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Springer US, 1983, pp. 317–319.

[195] J. C. Lagarias and J. A. Reeds, "Unique Extrapolation of Polynomial Recurrences", *SIAM Journal on Computing*, vol. 17, no. 2, pp. 342–362, 1988.

[196] H. Krawczyk, "How to predict congruential generators", *Journal of Algorithms*, vol. 13, no. 4, pp. 527–545, 1992.

[197] H. Krawczyk, "How to Predict Congruential Generators", in *Advances in Cryptology ? CRYPTO? 89 Proceedings*, vol. 435, G. Brassard, Ed. New York, NY: Springer New York, 1990, pp. 138–153.

[198] A. M. Frieze, R. Kannan, and J. C. Lagarias, "Linear Congruential Generators Do Not Produce Random Sequences", presented at the *25th Annual Symposium on Foundations of Computer Science*, 1984, pp. 480–484.

[199] A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and A. Shamir, "Reconstructing Truncated Integer Variables Satisfying Linear Congruences", *SIAM Journal on*

Computing, vol. 17, no. 2, pp. 262–280, 1988.

[200] J. Hastad and A. Shamir, "The cryptographic security of truncated linearly related variables", 1985, pp. 356–362.

[201] J. Stern, "Secret linear congruential generators are not cryptographically secure", 1987, pp. 421–426.

[202] J. Boyar, "Inferring sequences produced by a linear congruential generator missing low-order bits", *Journal of Cryptology*, vol. 1, no. 3, pp. 177–184, Oct. 1989.

[203] B. A. Wichman and l. D. Hill, "An Efficient and Portable Pseudo-Random Number Generator", *Applied Statistics*, vol. 31, pp. 188–190, 1982.

[204] J. Bubicz and J. Stokłosa, "Compound inversive congruential generator design algorithm", in *Proceedings of the 4th International Multiconference on Computer Science and Information Technology*, Amman, 2006, vol. 1, pp. 1–6.

[205] J. Eichenauer and J. Lehn, "A non-linear congruential pseudo random number generator", *Statistische Hefte*, vol. 27, no. 1, pp. 315–326, Dec. 1986.

[206] S. M. Jennings, "A Special Class of Binary Sequences", Westfield College. London University, 1980.

[207] S. M. Jennings, "Multiplexed Sequences: Some Properties of the Minimum Polynomial", in *Cryptography*, vol. 149, T. Beth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1983, pp. 189–206.

[208] C. G. Gunther, "Alternating Step Generators Controlled by De Bruijn Sequences", in *Advances in Cryptology - EUROCRYPT' 87*, vol. 304, D. Chaum and W. L. Price, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 5–14.

[209] K. Zeng, C. H. Yang, and T. R. N. Rao, "On the Linear Consistency Test (LCT) in Cryptanalysis with Applications", in *Advances in Cryptology - CRYPTO'89 Proceedings*, vol. 435, G. Brassard, Ed. New York, NY: Springer New York, 1990, pp. 164–174.

[210] J. O. Bruer, "On Pseudo Random Sequences as Crypto Generators", in *Proceedings of the International Zurich Seminar on Digital Communication*, Switzerland, 1984.

[211] W. G. Chambers and D. Gollmann, "Technical memorandum. Generators for sequences with near-maximal linear equivalence", *IEE Proceedings E Computers*

and Digital Techniques, vol. 135, no. 1, pp. 67–69, 1988.

[212] R. A. Rueppel, "Correlation Immunity and the Summation Combiner", in *Advances in Cryptology-EUROCRYPT ’85*, 1986, pp. 260–272.

[213] W. G. Chambers and D. Gollmann, "Lock-in Effect in Cascades of Clock-Controlled Shift-Registers", in *Advances in Cryptology ? EUROCRYPT ?88*, vol. 330, D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmuller, J. Stoer, N. Wirth, and C. G. G?nther, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 331–343.

[214] M. D. MacLaren and G. Marsaglia, "Uniform Random Number Generators", *Journal of the ACM*, vol. 12, no. 1, pp. 83–89, 1965.

[215] G. Marsaglia and T. A. Bray, "One-line random number generators and their use in combinations", *Communications of the ACM*, vol. 11, no. 11, pp. 757–759, 1968.

[216] F. Gebhardt, "Generating pseudo-random numbers by shuffling a Fibonacci sequence", *Mathematics of Computation*, vol. 21, no. 100, pp. 708–708, 1967.

[217] C. Bays and S. D. Durham, "Improving a Poor Random Number Generator", *ACM Transactions on Mathematical Software*, vol. 2, no. 1, pp. 59–64, Jan. 1976.

[218] C. G. Günther, "On some properties of the sum of two pseudorandom sequences", presented at the *Eurocrypt’86*, Linkoping, Sweden, 1986.

[219] R. A. Rueppel, *Analysis and design of stream ciphers*. Place of publication not identified: Springer-Verlag Berlin An, 2012.

[220] J. D. Golic, "On the linear complexity of functions of periodic GF(q) sequences", *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 69–75, 1989.

[221] D. E. Knuth, *The Art of Computer Programming : Generating All Tuples and Permutations*, 1 edition., vol. Volume 4, Fascicle 2. Upper Saddle River, NJ: Addison-Wesley Professional, 2005.

[222] Э. Рейнгольд, Ю. Нивергельт и Н. Део, *Комбинаторные алгоритмы. Теория и практика*. М.: Мир, 1980.

[223] А. А. Борисенко и В. Б. Чередниченко, "Системы счисления в вычислительной технике", *Вісник СумДУ. Серія Технічні науки*, № 4, с. 162–177, 2009.

[224] А. А. Борисенко, И. А. Кулик и А. Е. Горячев, "Электронная система генерации

перестановок на базе факториальных чисел", *Вісник СумДУ. Серія Технічні науки*, № 1, с. 183–188, 2007.

[225] А. Е. Горячев, "Построение факториальных чисел на основе двоичных счетчиков", *Вісник СумДУ. Серія Технічні науки*, № 4, с. 16–23, 2008.

[226] А. Е. Горячев, "Электронное устройство получения факториальных чисел", *Вісник СумДУ. Серія Технічні науки*, № 2, с. 169–174, 2009.

[227] А. Е. Горячев, "Оценка быстродействия алгоритмов генерации перестановок на основе факториальных чисел", *Вісник СумДУ. Серія Технічні науки*, № 1, с. 62–67, 2010.

[228] А. Е. Горячев и С. А. Дегтяр, "Метод генерации перестановок на основе факториальных чисел с использованием дополняющего массива", *Вісник СумДУ. Серія Технічні науки*, № 3, с. 86–93, 2012.

[229] D. H. Lehmer, "Teaching combinatorial tricks to a computer", in *Proc. Sympos. Appl. Math.*, Providence, R.I., 1960, vol. 10, pp. 179–193.

[230] D. E. Knuth, *The Art of Computer Programming : Sorting and Searching*, 2Nd Ed., vol. 3. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1998.

[231] H. A. Rothe, "Sammlung combinatorisch-analytischer Abhandlungen", in *Sammlung combinatorisch-analytischer Abhandlungen*, Leipzig, 1800, pp. 263–305.

[232] R. Sedgewick, "Permutation Generation Methods", *ACM Computing Surveys*, vol. 9, no. 2, pp. 137–164, 1977.

[233] А. Е. Горячев, "Метод перебора перестановок на основе факториальных чисел", *Вісник СумДУ. Серія Технічні науки*, т. 2, № 3, с. 171–177, 2010.

[234] О. А. Борисенко і О. Є. Горячев, "Пристрій для перебору перестановок", патент України №59628, 25.05.2011.

[235] B. R. Heap, "Permutations by Interchanges", *The Computer Journal*, vol. 6, no. 3, pp. 293–294, Jan. 1963.

[236] A. T. Alexiou, M. M. Psiha, and P. M. Vlamos, "Combinatorial permutation based algorithm for representation of closed RNA secondary structures", *Bioinformation*, vol. 7, no. 1, pp. 91–95, Jun. 2011.

[237] R. A. Fisher and F. Yates, *Statistical Tables for Biological Agricultural and Medical Research*, 3rd ed. London: Oliver & Boyd, 1948.

[238] R. Durstenfeld, "Algorithm 235: Random permutation", *Communications of the ACM*, vol. 7, no. 7, p. 420, Jan. 1964.

[239] S. Sattolo, "An algorithm to generate a random cyclic permutation", *Information Processing Letters*, vol. 22, no. 6, pp. 315–317, 1986.

[240] S. W. Golomb, *Shift register sequences*, Rev. ed. Laguna Hills, Calif: Aegean Park Press, 1982.

[241] *Поточные шифры. Результаты зарубежной открытой криптологии*. М, 1997.

[242] *Інформаційні технології. Методи захисту. Генерування випадкових бітів*, стандарт України ДСТУ ISO/IEC 18031:2015, 18.12.2015.

[243] E. B. Barker and J. M. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", NIST SP 800-90Ar1, Jun. 2015.

[244] M. J. B. Robshaw, "Stream Ciphers. Technical Report TR-701", V. 2.0, 1995.

[245] R. G. Brown, *Introduction to Random Signal Analysis and Kalman Filtering*, Edition Unstated edition. New York: John Wiley & Sons Inc, 1983.

[246] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*, 4th ed. Boston: McGraw-Hill, 2002.

[247] G. Marsaglia, "DIEHARD Battery of Tests of Randomness". [Online]. Available at: http://www.stat.fsu.edu/pub/diehard.

[248] L. E. Bassham III *et al.*, "SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Gaithersburg, MD, United States, 2010.

[249] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators", *ACM Transactions on Mathematical Software*, vol. 33, no. 4, pp. 22-es, 2007.

[250] W. Caelli, E. Dawson, L. Nielsen, and H. Gustafson, *CRYPT–X Statistical Package Manual, Measuring the strength of Stream and Block Ciphers*. Queensland University of Technology, 1992.

[251] *Security requirements for cryptographic modules*, US standard FIPS PUB 140-2, 25-

May-2001.

[252] Н. Г. Киевец и А. И. Корзун, "Система статистического тестирования генераторов случайных чисел электронных пластиковых карт", в *Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы международного научно-технического семинара.*, Минск, 2012, с. 65–70.

[253] А. Потий, С. Орлова и Т. Гриненко, "Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS", *Правове , нормативне та метрологічне забезпечення системи захисту інформації в Україні*, № 2, с. 206–214, 2001.

[254] Д. Н. Шевченко и С. В. Кривенков, "Методика тестирования и использования генераторов псевдослучайных последовательностей", *Проблемы физики, математики и техники*, №. 2(19), с. 89–95, 2014.

[255] W. Schindler, "Efficient Online Tests for True Random Number Generators", in *Cryptographic Hardware and Embedded Systems — CHES 2001*, vol. 2162, Ç. K. Koç, D. Naccache, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 103–117.

[256] W. Schindler, "Evaluation Criteria for Physical Random Number Generators", in *Cryptographic Engineering*, Ç. K. Koç, Ed. Boston, MA: Springer, 2008, pp. 25–54.

[257] W. Schindler, "Random Number Generators for Cryptographic Applications", in *Cryptographic Engineering*, Ç. K. Koç, Ed. Boston, MA: Springer, 2009, pp. 5–23.

[258] Н. В. Смирнов и И. В. Дунин-Барковский, *Курс теории вероятностей и математической статистики для технических приложений*. М.: Наука. Главная редакция физико-математической литературы, 1969.

[259] M. G. Kendall, *The Advanced Theory of Statistics*, vol. V. II. London: C. Griffin & Company limited, 1946.

[260] П. А. М. Дирак, *Принципы квантовой механики*, 2-е-е изд. М.: Наука, 1979.

[261] Большев Л.Н. и Смирнов Н.В., *Таблицы математической статистики*. Москва: Наука, 1983.

[262] G. E. P. Box and D. A. Pierce, "Distribution of Residual Autocorrelations in

Autoregressive-Integrated Moving Average Time Series Models", *Journal of the American Statistical Association*, vol. 65, no. 332, pp. 1509–1526, 1970.

[263] G. M. Ljung and G. E. P. Box, "On a Measure of Lack of Fit in Time Series Models", *Biometrika*, vol. 65, no. 2, p. 297, 1978.

[264] Е. В. Фауре і О. С. Гуденко, "Дослідження автокореляційних зв'язків послідовності перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 15.

[265] Е. В. Фауре, Д. І. Бібко і С. С. Нагорних, "Дослідження статистичних властивостей комбінацій рознесених вибірок послідовності перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 16.

[266] G. S. Vernam, "Secret Signalling System", USA patent 1310719, 22-Jul-1919.

[267] G. S. Vernam, "Ciphering Device", USA patent 1416765, 23-May-1922.

[268] G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, 1926.

[269] Е. В. Фауре, О. О. Харін і Д. О. Литвиненко, "Дослідження процедури формування контрольної суми повного факторіального коду на основі залишку за модулем", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ; Баку : ВА ЗС АР; Бельсько-Бяла: УтіГН ; Полтава: ПНТУ, 2017, с.16–17.

[270] У. Диффи и М. Хеллман, "Защищенность и имитостойкость: введение в криптографию", *ТИИЭР*, т. 67, № 3, с. 71–109, 1979.

[271] Р. Лидл и Г. Нидеррайтер, *Конечные поля*, т. 2, 2 т. М.: Мир, 1988.

[272] Д. Прокис, *Цифровая связь*. М.: Радио и связь, 2000.

[273] Л. М. Финк, *Теория передачи дискретных сообщений*, 2nd-e, перераб. и дополн. ed. М.: Советское радио, 1970.

[274] Н. Л. Теплов, *Помехоустойчивость систем передачи дискретной информации*. М.: Связь, 1964.

[275] Е. В. Фауре і А. Ю. Бойко, "Дослідження здатності виявлення помилок факторіальним кодом з декількома контрольними сумами", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 16.

[276] Е. В. Фауре і В. Л. Юрченко, "Дослідження здатності виявлення помилок факторіальним кодом з відновленням даних", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 16.

[277] P. A. MacMahon, "The Indices of Permutations and the Derivation Therefrom of Functions of a Single Variable Associated with the Permutations of any Assemblage of Objects", *American Journal of Mathematics*, vol. 35, no. 3, p. 281, 1913.

[278] L. Comtet, *Advanced combinatorics: the art of finite and infinite expansions*, Rev. and enl. ed. Dordrecht, Boston: D. Reidel Pub. Co, 1974.

[279] A. Mendes, "A Note on Alternating Permutations", *The American Mathematical Monthly*, vol. 114, no. 5, pp. 437–440, 2007.

[280] R. P. Stanley, *Enumerative combinatorics. Volume 1*, 2nd ed. Cambridge, NY: Cambridge University Press, 2012.

[281] R. H. Moritz and R. C. Williams, "A Coin-Tossing Problem and Some Related Combinatorics", *Mathematics Magazine*, vol. 61, no. 1, p. 24, 1988.

[282] "The on-line encyclopedia of integer sequences. A008302", 10.02.2018. [Online]. Available at: http://oeis.org/A008302.

[283] Е. В. Фауре і О. О. Харін, "Факторіальне кодування з відновленням даних і виправленням помилок", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 13-19 березня 2017 р.*, Черкаси, 2017, с. 74–76.

[284] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices, and groups*. New York: Springer, 1999.

[285] D. Shanks, *Solved and unsolved problems in number theory*, 3rd ed. New York, N.Y: Chelsea Pub. Co, 1985.

[286] S. Pemmaraju and P. S. Skiena, *Computational Discrete Mathematics: Combinatorics and Graph Theory with Mathematica*, 1st edition. Cambridge, U.K. ; New York: Cambridge University Press, 2003.

[287] "Modulo Multiplication Group", 20.09.2017. [Online]. Available at: http://mathworld.wolfram.com/ModuloMultiplicationGroup.html.

[288] В. И. Арнольд, "Топология алгебры: комбинаторика операции возведения в квадрат", *Функциональный анализ и его приложения*, т. 37, № 3, с. 20–35, 2003.

[289] В. И. Арнольд, "Топология и статистика формул арифметики", *Успехи математических наук*, т. 58, № 4 (352), с. 3–28, 2003.

[290] В. И. Арнольд, *Экспериментальное наблюдение математических фактов*. М.: Издательство МЦНМО, 2006.

[291] Ю. Г. Лега, Е. С. Лисицына, Э. В. Фауре и В. В. Швыдкий, "Основные характеристики систем цикловой синхронизации, использующих последовательности быстрого поиска", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 109–113, 2006.

[292] А. О. Гельфонд, *Решение уравнений в целых числах*. М.: Наука, 1978.

[293] А. . Курош, *Теория групп*, 3-е-е изд. М.: Издательство Физматлит, 2011.

[294] В. А. Щерба и Э. В. Фауре, "Свойства генератора конгруэнтных чисел и его применения", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 18-22 березня 2013 р.*, Черкаси, 2013, с. 85–87.

[295] Е. С. Лисицына, "Исследование циклов генераторов на регистрах сдвига с обратными связями", *Вісник Хмельницького національного університету. Технічні науки*, № 1, с. 121–125, 2014.

[296] Е. Лисицына, "Оценка статистических свойств (псевдо) случайных

последовательностей, образованных конкатенацией циклов регистров сдвига с обратными связями", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 2, с. 36–43, 2014.

[297] В. В. Веретельник, "Линейный генератор конгруэнтных чисел", *Системи обробки інформації*, № 2 (100), с. 155–159, 2012.

[298] P. L'Ecuyer and R. Simard, "TestU01. A Software Library in ANSI C for Empirical Testing of Random Number Generators", Universit´e de Montr´eal, 2013.

[299] Э. В. Фауре, "Подстановки и их использование в задачах формирования псевдослучайных последовательностей чисел", в *Праці IV Міжнародної науково-практичної конференції «Обробка сигналів і негауссівських процесів», присвяченої пам'яті професора Ю.П. Кунченка: Тези доповідей, Черкаси, 22-24 травня 2013 р.*, Черкаси, 2013, с. 171–173.

[300] В. В. Швыдкий, "Групповая обработка сигналов многоканальными конечными автоматами", *Техника средств связи*, no. 4 (25), pp. 58–64, 1978.

[301] Э. В. Фауре и Р. О. Бивзюк, "Методы и средства формирования остатков в многоканальных помехоустойчивых кодеках", в *Інформаційні технології та комп'ютерна інженерія. Тези доповідей Міжнародної науково-практичної конференції. м. Вінниця, 19-21 травня 2010 року*, Вінниця, 2010, с. 381–382.

[302] Э. В. Фауре, Д. В. Фауре и М. В. Сторчак, "Методы и средства формирования остатка в помехоустойчивых кодеках", в *Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р.*, Вінниця, 2011, с. 181.

[303] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе композиционного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 17-21 березня 2014 р.*, Черкаси, 2014, с. 53–54.

[304] "Random Class". [Online]. Available at: http://msdn.microsoft.com/library/system.random%28v=vs.110%29.aspx.

[305]"High Bit Rate Quantum Random Number Generator Service". [Online]. Available at: http://qrng.physik.hu-berlin.de/. [Accessed: 24-Feb-2016].

[306]"RANDOM.ORG - True Random Number Service". [Online]. Available at: https://www.random.org/. [Accessed: 24-Feb-2016].

[307]Э. В. Фауре, А. И. Щерб, и А. А. Лавданский, "Статистическая характеристика последовательности чисел комбинационного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 16-20 березня 2015 р.*, Черкаси, 2015, с. 51–52.

[308]J. Soto, "Statistical Testing of Random Number Generators", in *Proceedings of the 22nd National Information Systems Security Conference*, 1999, vol. 10, p. 12.

[309]Б. Ю. Лемешко и С. С. Помадин, "Корреляционный анализ наблюдений многомерных случайных величин при нарушении предположений о нормальности", *Сибирский журнал индустриальной математики*, т. V, № 3(11), с. 115–130, 2002.

[310]С. С. Помадин, "Исследование распределений статистик многомерного анализа данных при нарушении предположений о нормальности", дис. ... канд. техн. наук : 05.13.17, Новосибирский государственный технический университет, Новосибирск, 2004.

[311]T. W. Anderson and D. A. Darling, "Asymptotic Theory of Certain 'Goodness of Fit' Criteria Based on Stochastic Processes", *The Annals of Mathematical Statistics*, vol. 23, no. 2, pp. 193–212, Jun. 1952.

[312]А. И. Орлов, "О проверке однородности двух независимых выборок", *Заводская лаборатория*, т. 69, № 1, с. 55–60, 2003.

[313]А. И. Орлов, "Состоятельные критерии проверки абсолютной однородности независимых выборок", *Заводская лаборатория. Диагностика материалов*, т. 78, № 11, с. 66–70, 2012.

[314]Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Прихована передача інформації в звуковому частотному діапазоні", в *Науково-технічна*

конференція «Проблеми телекомунікацій»: Збірник тез, К., 2011, с. 108.

[315] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Ансамбль багатопозиційних шумоподібних ортогональних сигналів", в *Тези доповідей Міжнародної науково-практичної конференції 'Інформаційні технології в освіті, науці і техніці' (ІТОНТ-2012): Черкаси, 25-27 квітня 2012 р.*, Черкаси, 2012, т. 1, с. 65–66.

[316] И. Н. Выверица, А. А. Лавданский и Э. В. Фауре, "Двухконтурная защита информации от несанкционированного доступа в стегосистемах", в *Информационные технологии и системы 2012 (ИТС 2012) : материалы международной научной конференции, БГУИР, Минск, Беларусь, 24 октября 2012 г.*, Минск, 2012, с. 244–245.

[317] Э. В. Фауре, Е. С. Лисицына и Д. Ю. Нестеренко, "Метод повышения стойкости электронных кодовых замков", в *Сучасність, наука, час. Взаємодія та взаємовплив: матеріали дев'ятої Міжнародної науково-практичної інтернет-конференції, Київ, 19-21 листопада 2012 р.*, К., 2012, т. 2, с. 62–64.

[318] Е. В. Фауре і С. В. Сисоєнко, "Підвищення стійкості комп'ютерного криптографічного перетворення", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 13.

[319] Е. С. Вентцель и Л. А. Овчаров, *Прикладные задачи теории вероятностей*. М.: Радио и связь, 1983.

[320] В. М. Кузнецов, "Генераторы случайных и псевдослучайных последовательностей на цифровых элементах задержки (основы теории и методы построения)", дис. ... докт. техн. наук : 05.13.05, ГОУВПО «Казанский государственный технический университет», Казань, 2011.

[321] W. J. Dixon, "Further Contributions to the Problem of Serial Correlation", *Ann. Math. Statist.*, vol. 15, no. 2, pp. 119–144, 1944.

[322] Б. Ю. Лемешко, А. С. Комиссарова и А. Е. Щеглов, "Вопросы применения некоторых критериев проверки случайности и отсутствия тренда",

Метрология, № 12, с. 3–25, 2010.

[323] Л. Е. Варакин, *Системы связи с шумоподобными сигналами*. М.: Радио и связь, 1985.

[324] T. W. Anderson and A. M. Walker, "On the Asymptotic Distribution of the Autocorrelations of a Sample from a Linear Stochastic Process", *The Annals of Mathematical Statistics*, vol. 35, no. 3, pp. 1296–1303, 1964.

[325] P. A. P. Moran, "Some Theorems on Time Series: II The Significance of the Serial Correlation Coefficient", *Biometrika*, vol. 35, no. 3/4, pp. 255–260, 1948.

[326] J.-M. Dufour and R. Roy, "Some robust exact results on sample autocorrelations and tests of randomness", *Journal of Econometrics*, vol. 29, no. 3, pp. 257–273, 1985.

[327] А. И. Орлов, *Прикладная статистика. Учебник*. М.: Издательство «Экзамен», 2004.

[328] M. . Kendall, A. Stuart, and J. K. Ord, *The Advanced Theory of Statistics. Volume 3: Design and Analysis, and Time-Series. Fourth edition*, vol. 3, 3 vols. London: C. Griffin & Company limited, 1983.

[329] P. A. P. Moran, "Testing for Serial Correlation with Exponentially Distributed Variates", *Biometrika*, vol. 54, no. 3/4, pp. 395–401, 1967.

[330] Г. Крамер, *Математические методы статистики*, 2-е-е изд., стереот. изд. М.: Издательство «Мир», 1975.

[331] R. A. Fisher, "On the “Probable Error” of a Coefficient of Correlation Deduced From a Small Sample", *Metron*, no. 1, pp. 3–32, 1921.

[332] В. И. Коржик, "Одна оценка обнаруживающей способности бинарных групповых кодов", *Радиотехника и электроника*, № 11, 1965.

[333] В. И. Коржик и Л. М. Финк, *Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой*. М.: Связь, 1975.

[334] Н. Т. Березюк, А. Г. Андрущенко, С. С. Мощицкий и и др., *Кодирование информации (двоичные коды)*. Харьков: Издательское объединение «Вища школа», 1972.

[335] T. Fujiwara, T. Kasami, A. Kitai, and Shu Lin, "On the Undetected Error Probability for Shortened Hamming Codes", *IEEE Transactions on Communications*, vol. 33,

no. 6, pp. 570–574, 1985.

[336] G. Castagnoli, S. Brauer, and M. Herrmann, "Optimization of cyclic redundancy-check codes with 24 and 32 parity bits", *IEEE Transactions on Communications*, vol. 41, no. 6, pp. 883–892, Jun. 1993.

[337] G. Castagnoli, J. Ganz, and P. Graber, "Optimum cycle redundancy-check codes with 16-bit redundancy", *IEEE Transactions on Communications*, vol. 38, no. 1, pp. 111–114, Jan. 1990.

[338] T. Baicheva and F. Sallam, "CRC Codes for Error Control", *Mathematica Balkanica*, vol. 21, pp. 377–387, 2007.

[339] T. Baicheva, S. Dodunekov, and P. Kazakov, "On the cyclic redundancy-check codes with 8-bit redundancy", *Computer Communications*, vol. 21, no. 11, pp. 1030–1033, Aug. 1998.

[340] T. Baicheva, S. Dodunekov, and P. Kazakov, "Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy", *IEEE Proceedings - Communications*, vol. 147, no. 5, pp. 253–256, 2000.

[341] P. Kazakov, "Fast calculation of the number of minimum-weight words of CRC codes", *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1190–1195, 2001.

[342] P. Koopman, K. Driscoll, and B. Hall, "Selection of Cyclic Redundancy Code and Checksum Algorithms to Ensure Critical Data Integrity", U.S . Department of Transportation, Federal Aviation Administration, Final Report DOT/FAA/TC-14/49, 2015.

[343] J. C. Collins, "Testing, Selection, and Implementation of Random Number Generators", Aberdeen Proving Ground, MD, Final Report ARL-TR-4498, 2008.

[344] P. Koopman and T. Chakravarty, "Cyclic redundancy code (CRC) polynomial selection for embedded networks", in *Proc. of Internat. Conf. on Dependable Systems and Networks, DSN04*, Florence, 2004, pp. 145–154.

[345] J. Ray and P. Koopman, "Efficient High Hamming Distance CRCs for Embedded Networks", in *Proc. of Internat. Conf. on Dependable Systems and Networks, DSN 2006*, Philadelphia, PA, 2006, pp. 3–12.

[346] T. C. Maxino and P. J. Koopman, "The Effectiveness of Checksums for Embedded Control Networks", *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 1, pp. 59–72, 2009.

[347] P. Koopman, "32-bit cyclic redundancy codes for Internet applications", in *Proc. of Internat. Conf. on Dependable Systems and Networks, DSN 2002*, Washington, DC, 2002, pp. 459–468.

[348] P. Koopman, "Best CRC Polynomials", 01-Feb-2018. [Online]. Available at: http://users.ece.cmu.edu/~koopman/crc/index.html.

[349] P. Merkey and E. Posner, "Optimum cyclic redundancy codes for noisy channels (Corresp.)", *IEEE Transactions on Information Theory*, vol. 30, no. 6, pp. 865–867, 1984.

[350] K. Witzke and C. Leung, "A Comparison of Some Error Detecting CRC Code Standards", *IEEE Transactions on Communications*, vol. 33, no. 9, pp. 996–998, 1985.

[351] A. S. Tanenbaum and D. Wetherall, *Computer networks*, 5th ed. Boston: Pearson Prentice Hall, 2011.

[352] R. N. Williams, "A Painless Guide to CRC Error Detection Algorithms Index V3.00", 01-Feb-2018. [Online]. Available at: http://www.repairfaq.org/filipg/LINK/F_crc_v3.html.

[353] Т. В. Митянкина, В. В. Швыдкий и Э. В. Фауре, "Преобразование дискретных случайных процессов комбинационным автоматом", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № №3, с. 67–69, 2004.

[354] Э. В. Фауре, "Нелинейные преобразования дискретных случайных процессов", *Радіоелектронні і комп'ютерні системи*, № 6, с. 200–205, 2006.

[355] Э. В. Фауре, Д. В. Фауре и Д. А. Коляда, "Метод нелинейного формирования псевдослучайной последовательности чисел", в *Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р.*, Вінниця, 2011, с. 168.

ДОДАТКИ

Додаток А. Відомості щодо впровадження результатів роботи

Україна

МІНІСТЕРСТВО ПРОМИСЛОВОЇ ПОЛІТИКИ УКРАЇНИ
ДЕРЖАВНЕ ПІДПРИЄМСТВО
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ „АКОРД"

18029, м.Черкаси, вул.Одеська, 8, тел./факс. (0472) 33-35-13

ЗАТВЕРДЖУЮ
Директор Державного підприємства
«Науково-дослідний інститут «Акорд»
_____ Онойко В.М.
«26» _____ 2018 р.

АКТ
впровадження результатів дисертаційної роботи
на здобуття наукового ступеня доктора технічних наук
Фауре Еміля Віталійовича

Під час виконання Державним підприємством «Науково-дослідний інститут «Акорд» науково-дослідної та дослідно-конструкторської роботи для проведення моделювання та тестування системи дистанційного зв'язку, контролю та управління віддаленими об'єктами використано наступні наукові результати, одержані в дисертаційній роботі на здобуття наукового ступеня доктора технічних наук Фауре Еміля Віталійовича:

- метод формування послідовностей перестановок на основі лінійного конгруентного методу;
- метод формування послідовностей перестановок на основі використання для представлення синдрому формованої перестановки позиційної системи числення з факторіальною основою;
- метод двоконтурного потокового криптографічного перетворення даних.

Використання вказаних методів формування послідовностей перестановок за рахунок відсутності операції приведення випадкового числа до потрібного діапазону дозволило зменшити час формування перестановок у порівнянні з використанням алгоритму Р. Дуршенфельда до 1,7 разів. У свою чергу, це забезпечило можливість зменшення часу проведення моделювання і тестування системи дистанційного зв'язку, контролю та управління віддаленими об'єктами до 1,3 разів.

Використання двоконтурного потокового криптографічного перетворення даних для 16-розрядних слів дозволило збільшити потужність ключового простору в $3.6 \cdot 10^{18}$ разів, що, в свою чергу, зменшило ймовірність злому системи шифрування та підвищило її криптографічну стійкість.

Головний інженер
ДП «НДІ «Акорд» _____ Компанієць О. Г.

Провідний інженер _____ Олешко О. П.

ЗАТВЕРДЖУЮ
Директор Товариства з
обмеженною відповідальністю
"Діджитал Мастер"
_____Лобус Р.С.
«22» лютого 2018 р.

АКТ
впровадження результатів дисертаційної роботи
Фауре Еміля Віталійовича

У ТОВ «Діджитал Мастер» виконано науково-дослідні та дослідно-конструкторські роботи з розробки імітатора модуля керування метеорологічним локатором «Буран-А» авіаційного тренажера КТС-148 за договорами №09/1014, №10/1003, №10/1006 з ДП «Антонов». Основна функція розроблюваної підсистеми полягала в виконанні інформаційного обміну між стаціонарним сервером метеоданих та засобами їх відображення та керування в рухомій кабіні авіатренажера літака АН-148. Вирішення поставленої задачі зводилося до необхідності забезпечення комплексного захисту інформації, що включає захист від помилок внаслідок завад високої інтенсивності від роботи лінійних двигунів авіатренажера та виключення хибних даних.

Для вирішення поставленої задачі використано наукові результати, одержані в дисертаційній роботі на здобуття наукового ступеня доктора технічних наук Фауре Еміля Віталійовича, а саме: метод повного факторіального кодування інформації, що забезпечує контроль цілісності інформації та циклову синхронізацію приймача метеоданих без застосування спеціальної синхрокомбінації. Новизна розробленого методу підтверджена патентом України №107655 та публікаціями здобувача.

Технічні рішення, що реалізовані в підсистемі передавання даних: довжина інформаційної частини – 40 біт (5 байт), довжина перевірної частини – 64 біти (8 байт, порядок перестановки повного факторіального коду – 16), довжина блоку даних (кодового слова повного факторіального коду) – 104 біти (13 байт), для передавання інформації використовувалася фазова маніпуляція двійкових сигналів та когерентний приймач, імовірність бітової помилки в умовах реального польоту та інтенсивного зашумлення – $2 \cdot 10^{-2}$. Впровадження повного факторіального кодування інформації забезпечило отримання ймовірності невиявленої помилки на рівні $8{,}08 \cdot 10^{-17}$ та енергетичного виграшу в 12,37 дБ, що задовольнило поставленим вимогам.

Головний інженер
ТОВ «Діджитал Мастер» _____ Величко А.В.

Провідний інженер _____ Сокол В.М.

УКРАЇНА

Черкаська міська рада

ДЕПАРТАМЕНТ ОСВІТИ ТА ГУМАНІТАРНОЇ ПОЛІТИКИ

18000, м. Черкаси, вул. Гоголя, 251, тел./факс: (0472) 37-33-86,
Web: http://www.ogp.ck.ua. e-mail: uprosv@2upost.com Код ЄДРПОУ 36299692

13.04.2018 № 568-12-4/1

На № _____ від _____

Довідка
про впровадження результатів дисертаційної роботи здобувача вченого ступеня
доктора технічних наук Фауре Еміля Віталійовича

Запропонований у дисертаційному дослідженні Фауре Е.В. метод контролю цілісності інформації використано під час розробки системи обліку кадрів департаменту освіти та гуманітарної політики Черкаської міської ради.

У основі запропонованого методу контролю цілісності інформації лежить операція повного факторіального кодування, що передбачає використання факторіальної системи числення для формування перестановки, яка застосовується в якості перевірної частини блоку даних. Використання такого методу контролю цілісності інформації дозволяє забезпечити комплексний захист інформації під час її передавання та зберігання, який включає в себе:

– захист від нав'язування хибних даних;
– захист від помилок каналу зв'язку.

Запропонований Фауре Е.В. метод контролю цілісності інформації дозволяє зменшити до 2 разів кількість додатково введених перевірних біт за рахунок суміщення операцій імітозахисту та завадостійкого кодування.

Директор департаменту С.П.Воронов

«ЗАТВЕРДЖУЮ»
Перший проректор Черкаського державного технологічного університету
_____ Є.В. Ланських
«15» 05 2018 р.

АКТ

впровадження результатів дисертаційної роботи

Фауре Еміля Віталійовича в навчальний процес

Основні результати дисертаційного дослідження Фауре Еміля Віталійовича використовуються під час викладання дисциплін «Основи теорії інформації та кодування», «Теорія кодування», «Захист інформації в комп'ютерних системах», «Основи технічного захисту інформації», «Комплексні системи захисту інформації» студентам бакалаврату за напрямом підготовки 6.050102 «Комп'ютерна інженерія» (спеціальністю 123 «Комп'ютерна інженерія») та напрямом підготовки 6.170103 «Управління інформаційною безпекою» (спеціальністю 125 «Кібербезпека»). До курсу вказаних дисциплін включені такі результати, отримані Фауре Е.В.:

- метод формування псевдовипадкових послідовностей на основі лінійного конгруентного методу шляхом конкатенації в топологічній структурі лінійного конгруентного генератора не лише відособлених непересічних циклів, а і передциклів (дерев);
- метод двоконтурного криптографічного перетворення даних на основі використання операції гамування в першому контурі шифрування та використання принципів конкатенації зв'язних компонентів у топологічній структурі лінійного конгруентного генератора в другому контурі шифрування;
- метод формування випадкових послідовностей перестановок на основі використання для представлення синдрому формованої перестановки позиційної системи числення з факторіальною основою;

- методи роздільного та нероздільного факторіального кодування інформації.

Впровадження в навчальний процес результатів дисертаційної роботи Фауре Е.В. дозволило підвищити його ефективність за рахунок вивчення студентами нових методів формування псевдовипадкових послідовностей і комплексного захисту інформації, а також їх використання під час виконання практичних, лабораторних і розрахунково-графічних робіт.

Декан факультету інформаційних
технологій та систем,
к.т.н., доцент І.Б. Трегубенко

Завідувач кафедри інформаційної безпеки
та комп'ютерної інженерії,
к.т.н., доцент І.М. Федотова-Півень

Доцент кафедри інформаційної безпеки
та комп'ютерної інженерії,
к.т.н., доцент В.В. Швидкий

ЗАТВЕРДЖУЮ
В. о. начальника
Черкаського інституту пожежної безпеки
імені Героїв Чорнобиля
Національного університету
цивільного захисту України
кандидат технічних наук, професор

О. М. Тищенко

«10» 04 2018 р.

АКТ
впровадження результатів дисертаційної роботи
Фауре Еміля Віталійовича в навчальний процес
Черкаського інституту пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

Основні результати дисертаційного дослідження Фауре Еміля Віталійовича використовуються на кафедрі вищої математики та інформаційних технологій під час викладання навчальних дисциплін «Основи інформаційних технологій» за спеціальністю 261 «Пожежна безпека» (спеціалізація «Пожежна безпека») та спеціальністю 263 «Цивільна безпека» (спеціалізація «Цивільний захист»), «Прикладні інформаційні технології у сфері пожежної безпеки» за спеціальністю 261 «Пожежна безпека» (спеціалізаціями «Пожежна безпека» та «Експерт будівельний з пожежної та техногенної безпеки») та «Прикладні інформаційні технології у сфері цивільного захисту» за спеціальністю 263 «Цивільна безпека» (спеціалізація «Цивільний захист»).

До курсу вказаних дисциплін включені такі результати, отримані Фауре Е.В.:

- модель узагальненого графа станів лінійного конгруентного генератора, який є незв'язним об'єднанням циклів, оснащених добутками дерев, що дозволяє виконати класифікацію типів компонент зв'язності графа станів лінійного конгруентного генератора, виконати дослідження впливу параметрів на його топологію;
- метод формування псевдовипадкових послідовностей на основі лінійного конгруентного методу;
- метод двоконтурного криптографічного перетворення даних;
- метод оцінювання автокореляції часових рядів на основі інтегральної оцінки бічних пелюсток автокореляційної функції;

- методи роздільного та нероздільного факторіального кодування інформації, а також математичну модель оцінки ймовірності не виявленої декодером факторіального коду помилки.

Впровадження в навчальний процес результатів дисертаційної роботи Фауре Е.В. дозволило підвищити ефективність навчання за рахунок вивчення здобувачами вищої освіти нових методів формування псевдовипадкових послідовностей й оцінювання їх статистичних властивостей, а також методів комплексного захисту інформації.

Начальник кафедри
вищої математики та інформаційних технологій
канд. пед. наук, доцент
полковник с. ц. з. С. О. Касярум

Доцент кафедри
вищої математики та інформаційних технологій
канд. техн. наук, доцент В. І. Томенко

Старший викладач кафедри
вищої математики та інформаційних технологій
підполковник с. ц. з. К. В. Григоренко

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної роботи Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»
_____ В.М. Павленко
_____ 2018 р.

АКТ
впровадження результатів дисертаційної роботи
Фауре Еміля Віталійовича в навчальний процес

Основні результати дисертаційного дослідження Фауре Еміля Віталійовича використовуються під час викладання дисциплін «Формальний аналіз програмного забезпечення систем» та «Основи планування експерименту» студентам магістратури за напрямом підготовки спеціальності 121 «Інженерія програмного забезпечення». До лекційних матеріалів по зазначеним дисциплінам включено наступні результати дисертаційної роботи Фауре Е.В.:

- модель узагальненого графа станів лінійного конгруентного генератора, який є незв'язним об'єднанням циклів, оснащених добутками дерев;
- метод формування псевдовипадкових послідовностей на основі лінійного конгруентного методу;
- методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем;
- метод оцінювання автокореляції часових рядів на основі інтегральної оцінки бічних пелюсток автокореляційної функції;
- алгоритм аналізу розподілу серій (k-грам) символів у випадкових послідовностях чисел;
- критерій і методику перевірки послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел;
- методи роздільного та нероздільного факторіального кодування інформації для забезпечення її комплексної безпеки;
- математичну модель оцінки ймовірності не виявленої декодером факторіального коду помилки.

Впровадження в навчальний процес результатів дисертаційної роботи Фауре Е.В. дозволило підвищити ефективність навчання за рахунок вивчення студентами нових методів формування псевдовипадкових послідовностей та оцінювання їх статистичних властивостей, а також методів забезпечення комплексного захисту інформації.

Декан факультету програмної інженерії та бізнесу, к.т.н., доцент — Ю.Л. Прончаков

Завідувач кафедри інженерії програмного забезпечення, д.т.н., професор — І.Б. Туркін

Професор кафедри інженерії програмного забезпечення, д.т.н., професор — І.В. Шостак

Додаток Б. Дослідження статистичних властивостей контрольної суми повного факторіального коду в залежності від способу її формування

Б.1. Аналіз і вибір функції модифікації синдрому для забезпечення максимальної ентропії її результату

Визначимо абсолютні частоти появи кожної з можливих $M!$ перестановок на виході пристрою формування перевірної частини ПФК для всіх можливих варіантів ключової послідовності.

Алгоритм аналізу статистики перевірної частини наведено на рис. Б.1.

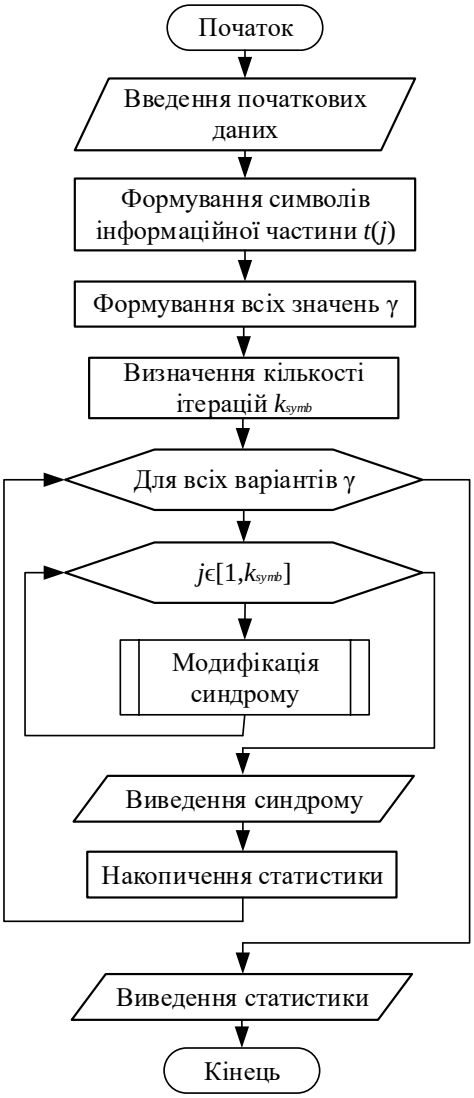


Рис. Б.1 – Блок-схема алгоритму аналізу закону розподілу перевірної частини ПФК

Розглянемо більш детально роботу алгоритму аналізу статистики перевірної

частини ПФК для кожної з визначених вище процедур модифікації синдрому та дослідимо статистику перестановок.

1. Модифікація синдрому за допомоги процедури $S_F(j)=\left(S_F(j-1)+\gamma(j)\right)\dot{+}t(j)$

Оскільки кількість укрупнених символів інформаційної частини дорівнює k_{symb}, послідовність γ також містить k_{symb} укрупнених символів. Відмінність полягає лише в тому, що структура слів різна: для інформаційної послідовності це l_k біт, для послідовності γ – M слів виду (1.13). Кількість можливих варіантів γ – $(M!)^{k_{symb}}$.

Кількість ітерацій модифікації синдрому відповідає кількості k_{symb} символів $t(j)$.

Введення початкових даних передбачає введення значення вектора початкового завантаження та кількості k_{symb} символів інформаційної частини.

Оскільки кожний символ інформаційної частини містить l_k біт, довжина інформаційної частини дорівнює $k=l_k\cdot k_{symb}$ біт. Інформаційна частина для кожної реалізації алгоритму аналізу статистики перевірної частини ПФК формується випадковим чином.

Перебираючи всі можливі варіанти ключової послідовності, алгоритм передбачає визначення абсолютних частот появи кожної перестановки.

Розглянемо отримані результати для $M=4$, різної кількості символів k_{symb} у повідомленні, різної довжини їх двійкового представлення l_k та різних ВПЗ $S(0)$. Результати дослідження наведено в таблиці Б.1.

Таблиця Б.1

Абсолютні частоти появи перестановок у залежності від інформаційної частини та ВПЗ для $M=4$

Номери перестановок	Абсолютні частоти			
	$t=0110$ $S(0)=0100$	$t=1111$ $S(0)=2110$	$t=11110101$ $S(0)=3210$	$t=11000001$ $S(0)=0010$
0..23	1	1	24	24

Як видно з таблиці Б.1, абсолютні частоти появи перестановок не залежить від

значень ПВЗ $S(0)$ та інформаційної частини, а залежить від кількості символів у інформаційній частини.

У таблиці Б.2 наведемо результати експерименту для $M=4$ та $k_{symb}=\{1,2,3\}$.

Таблиця Б.2

Абсолютні частоти появи перестановок порядку $M=4$ у залежності від k_{symb}

Номери перестановок	Абсолютні частоти		
	$k_{symb}=1$	$k_{symb}=2$	$k_{symb}=3$
0..23	1	24	576

У таблиці Б.3 наведемо аналогічні результати для $M=5$ та $k_{symb}=\{1,2,3\}$.

Таблиця Б.3

Абсолютні частоти появи перестановок порядку $M=5$ у залежності від k_{symb}

Номери перестановок	Абсолютні частоти		
	$k_{symb}=1$	$k_{symb}=2$	$k_{symb}=3$
0..119	1	120	14 400

Отримані результати показують, що абсолютні частоти появи перестановок залежать від кількості k_{symb} символів у інформаційній частині, а відносні частоти рівні між собою і не залежать від k_{symb}. Таким чином, перестановки мають рівномірний розподіл незалежно від кількості символів у повідомленні.

Таким чином, у випадку використання процедури модифікації синдрому $S_F(j)=\left(S_F(j-1)+\gamma(j)\right)\div t(j)$ імовірність появи кожної перестановки однакова, а значення інформаційної ентропії формувача перевірної частини (перестановки) максимальна і дорівнює $\log_a(M!)$.

2. Модифікація синдрому за допомоги процедури $b_i(j)=\left(b_i(j-1)+Z_i(j)\right)(\mathrm{mod}\, i)$

Ключ модифікації синдрому $Z_i(j)$ обчислюється наступним чином:

- двійкова послідовність даних t додається за модулем два з двійковою гамою γ, утворюючи гамовану послідовність даних $z=t\oplus\gamma$,

– група з h двійкових символів послідовності z накопичується в буферній пам’яті і після зчитування паралельним кодом утворює символ $Z_i(j)$.

У таблиці Б.4 представлено результати перевірки впливу значень гамованого інформаційного повідомлення z та ВПЗ $S(0)$ на статистику перевірної частини.

Таблиця Б.4

Абсолютні частоти появи перестановок для різних значень z та $S(0)$

№	Абсолютні частоти		
	$z=011001110000$ $S(0)=0210$	$z=011001110000$ $S(0)=0000$	$z=111111111111$ $S(0)=1210$
0	160	192	160
1	160	192	160
2	160	160	160
3	160	160	160
4	192	160	192
5	192	160	192
6	160	192	160
7	160	192	160
8	160	160	160
9	160	160	160
10	192	160	192
11	192	160	192
12	160	192	160
13	160	192	160
14	160	160	160
15	160	160	160
16	192	160	192
17	192	160	192
18	160	192	160
19	160	192	160
20	160	160	160
21	160	160	160
22	192	160	192
23	192	160	192

Статистичні властивості виходу пристрою формування перевірної частини ПФК не залежать від значення гамованої інформаційної частини та ВПЗ $S(0)$. Натомість, ці властивості залежать від кількості бітів l_k, які містяться в одному

укрупненому символі повідомлення, їх кількості та значення M. Результати моделювання для різної довжини повідомлення наведено в таблиці Б.5.

Таблиця Б.5

Абсолютні частоти появи перестановок для $l_k = 2$ та $k_{symb} = \{1,2,3,4\}$

№	Абсолютні частоти			
	$k_{symb} = 1$	$k_{symb} = 2$	$k_{symb} = 3$	$k_{symb} = 4$
0	4	192	11264	704512
1	4	192	11264	704512
2	2	160	10752	696320
3	2	160	10752	696320
4	2	160	10752	696320
5	2	160	10752	696320
6	4	192	11264	704512
7	4	192	11264	704512
8	2	160	10752	696320
9	2	160	10752	696320
10	2	160	10752	696320
11	2	160	10752	696320
12	4	192	11264	704512
13	4	192	11264	704512
14	2	160	10752	696320
15	2	160	10752	696320
16	2	160	10752	696320
17	2	160	10752	696320
18	4	192	11264	704512
19	4	192	11264	704512
20	2	160	10752	696320
21	2	160	10752	696320
22	2	160	10752	696320
23	2	160	10752	696320

Для $k_{symb} = 1$ максимальне відхилення відносної частоти від імовірності для рівномірного закону розподілу становить 0.02083, для $k_{symb} = 2$ – 0.0052083, $k_{symb} = 3$ – 0.001302. Таким чином, збільшення кількості слів на 1 призводить до зменшення максимального відхилення відносної частоти в 4 рази.

Результати моделювання для різних значень кількості бітів l_k наведено в таблиці Б.6.

Таблиця Б.6

Абсолютні частоти появи перестановок для $k_{symb}=1$ та $l_k=\{2,3,4,5\}$

№	Абсолютні частоти			
	$l_k=2$	$l_k=3$	$l_k=4$	$l_k=5$
0	4	24	192	1408
1	4	24	192	1408
2	2	24	160	1408
3	2	24	160	1408
4	2	16	160	1280
5	2	16	160	1280
6	4	24	192	1408
7	4	24	192	1408
8	2	24	160	1408
9	2	24	160	1408
10	2	16	160	1280
11	2	16	160	1280
12	4	24	192	1408
13	4	24	192	1408
14	2	24	160	1408
15	2	24	160	1408
16	2	16	160	1280
17	2	16	160	1280
18	4	24	192	1408
19	4	24	192	1408
20	2	24	160	1408
21	2	24	160	1408
22	2	16	160	1280
23	2	16	160	1280

Для $l_k=2$ максимальне відхилення відносної частоти від імовірності для рівномірного закону розподілу становить 0.02083, для $l_k=3$ – 0.01042, $l_k=4$ – 0.005208. Таким чином, збільшення кількості біт l_k на 1 призводить до зменшення максимального відхилення відносної частоти в 2 рази.

У таблицях Б.7 і Б.8 для різних l_k і k_{symb} наведено значення максимальної відносної похибки $\delta_{\max}=\dfrac{\max\left(\Delta n(x)\right)}{n_0(x)}$, при цьому використано позначення, застосовані в (4.27). Визначимо, для яких значень l_k і k_{symb} $\delta_{\max}<10^{-2}$.

Таблиця Б.7

Залежність максимальної відносної похибки $\delta_{\max}$ від l_k

l_k	2	3	4	5	6	7	8
$\delta_{\max}$	0,25	0,125	0,0625	0,03125	0,015625	0,007813	0,003906

Умова $\delta_{\max} < 10^{-2}$ виконується для $l_k \geq 7$.

Таблиця Б.8

Залежність максимальної відносної похибки $\delta_{\max}$ від k_{symb} для $l_k = 2$

k_{symb}	2	3	4	5
$\delta_{\max}$	0,125	0,03125	0,007813	0,001953

Умова $\delta_{\max} < 10^{-2}$ виконується для $k_{symb} \geq 4$.

Таким чином, для виконання умови $\delta_{\max} < 10^{-2}$ для $M = 4$ необхідно, щоб довжина інформаційної частини розбивалася на блоки довжиною не менше 7 бітів і містила не менше 5 таких блоків (символів).

Згідно виразу (4.28) виконаємо оцінку ξ точності відтворення рівномірного закону розподілу перестановок у залежності від значень l_k і k_{symb}. Результати зведемо до таблиць Б.9 і Б.10.

Таблиця Б.9

Залежність оцінки ξ від l_k

l_k	2	3	4	5	6	7	8
ξ	0,166667	0,083333	0,041667	0,020833	0,010417	0,005208	0,002604

Таблиця Б.10

Залежність оцінки ξ від k_{symb} для $l_k = 2$

k_{symb}	2	3	4	5
ξ	0,083333	0,020833	0,005208	0,001302

Будемо вимагати, щоб $\xi < 10^{-2}$. Тоді необхідно, щоб $l_k \geq 7$ і $k_{symb} \geq 4$.

Зважаючи на викладене, можна стверджувати, що під час використання перетворення $b_i(j) = \left(b_i(j-1) + Z_i(j)\right) (\mathrm{mod}\, i)$ збільшення значень k_{symb} та l_k призводить до зменшення помилки відтворення рівномірного закону розподілу

перестановок, а значення інформаційної ентропії формувача перевірної частини (перестановки) прямує до максимального – $\log_a(M!)$.

3. Модифікація синдрому за допомоги процедури $S_F(j-1) \to \pi(j-1) \to S_F'(j-1)$

Перетворення $S_F(j-1) \to \pi(j-1)$ та $\pi(j-1) \to S_F'(j-1)$ відбуваються на двох ключах – k_1 та k_2.

Виконаємо аналіз розподілу виходу формувача перевірної частини ПФК від ключів перетворення. Для цього визначимо перевірну частину ПФК для всіх можливих значень ключів k_1 та k_2. Потужність ключового простору $(M!)^2$.

Введення початкових даних передбачає введення значення ВПЗ та кількості символів k_{symb}. Кількість символів k_{symb} відповідає кількості ітерацій процедури формування перевірної частини ПФК.

Інформаційна частина для кожної реалізації алгоритму аналізу статистики перевірної частини ПФК формується випадковим чином.

Формування ключів виконується шляхом лексикографічного перебору всіх можливих перестановок порядку M.

У таблиці Б.11 наведено абсолютні частоти появи перестановок для $l_k = 4$ і $t(1) = 0$, $t(1) = 15$.

Таблиця Б.11

Абсолютні частоти появи перестановок для $l_k = 4$ і $t(1) = 0$, $t(1) = 15$

Номери перестановок	$t(1)$	
	0	15
0..23	24	24

Відносні частоти появи перестановок однакові, тому значення інформаційної ентропії формувача перевірної частини (перестановки) максимальна.

Б.2. Аналіз і вибір функції модифікації синдрому для забезпечення мінімальної ймовірності виникнення колізій

Визначимо абсолютні частоти появи кожної з можливих $M!$ перестановок на виході пристрою формування перевірної частини ПФК для всіх можливих варіантів інформаційної частини кодового слова.

Алгоритм аналізу статистики перевірної частини наведено на рис. Б.2.

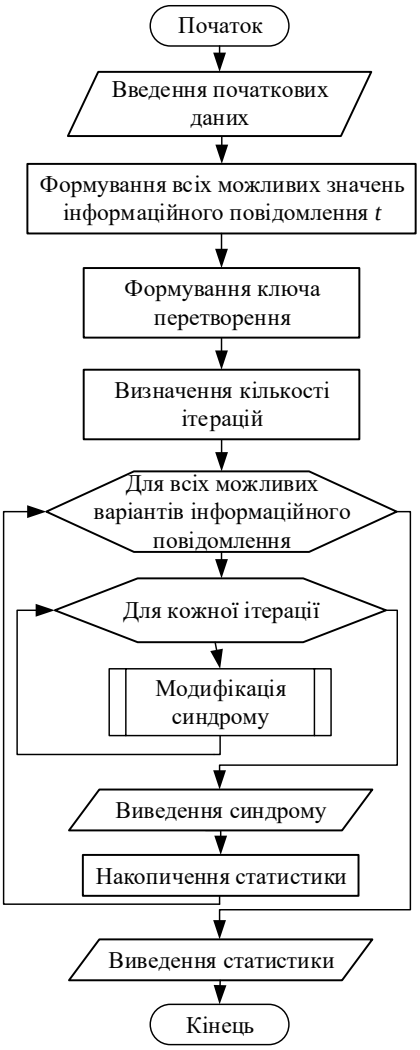


Рис. Б.2. Блок-схема алгоритму аналізу закону розподілу перевірної частини ПФК

Розглянемо більш детально роботу алгоритму для кожної з визначених вище процедур модифікації синдрому та дослідимо статистику перестановок.

1. Модифікація синдрому за допомоги процедури $S_F(j) = \left(S_F(j-1) + \gamma(j)\right) \dot{+} t(j)$

Кожен укрупнений символ $t(j)$ містить l_k бітів, тому чисельне значення символу $t(j)$ знаходиться в діапазоні $0 \le t(j) \le 2^{l_k} - 1$. Потужність значень інформаційної частини дорівнює $2^{l_k \cdot k_{symb}} = 2^k$.

У таблиці Б.12 наведено абсолютні частоти появи перестановок для $M = 4$, $l_k = 4$ та $k_{symb} = 2$ для різних значень $S(0)$ та γ.

Таблиця Б.12

Абсолютні частоти появи перестановок для різних значень $S(0)$ та γ

Номери перестановок	Абсолютні частоти			
	$S(0) = 0100$ $\gamma = (1,23)$	$S(0) = 3210$ $\gamma = (10,3)$	$S(0) = 0000$ $\gamma = (6,17)$	$S(0) = 1110$ $\gamma = (0,0)$
0	9	13	8	8
1	8	14	8	8
2	8	15	8	8
3	8	16	8	8
4	8	15	8	8
5	8	14	8	8
6	8	13	8	8
7	8	12	9	8
8	8	11	10	9
9	8	10	11	10
10	9	9	12	11
11	10	8	13	12
12	11	8	14	13
13	12	8	15	14
14	13	8	16	15
15	14	8	15	16
16	15	8	14	15
17	16	8	13	14
18	15	8	12	13
19	14	8	11	12
20	13	9	10	11
21	12	10	9	10
22	11	11	8	9
23	10	12	8	8

Характер отриманих розподілів значень перестановок інваріантний відносно інформаційного повідомлення та ВПЗ.

У таблиці Б.13 наведено абсолютні частоти появи перестановок для різних

значень довжини інформаційної частини.

Таблиця Б.13

Абсолютні частоти появи перестановок для різних довжин інформаційної частини

Номери перестановок	Абсолютні частоти			
	$k_{symb}=2$	$k_{symb}=3$	$k_{symb}=4$	$k_{symb}=5$
0	8	191	2721	42676
1	8	189	2764	42596
2	8	186	2806	42596
3	8	182	2844	42676
4	8	177	2875	42830
5	8	171	2896	43046
6	8	164	2904	43306
7	8	156	2896	43586
8	9	150	2875	43865
9	10	146	2844	44125
10	11	144	2806	44351
11	12	144	2764	44531
12	13	146	2721	44656
13	14	150	2680	44720
14	15	156	2644	44720
15	16	164	2616	44656
16	15	171	2596	44531
17	14	177	2584	44351
18	13	182	2580	44125
19	12	186	2584	43865
20	11	189	2596	43586
21	10	191	2616	43306
22	9	192	2644	43046
23	8	192	2680	42830

У таблиці Б.14 наведено залежності значення максимальної відносної похибки $\delta_{\max}$ від значення k. Визначимо, для яких значень k виконується умова $\delta_{\max}<10^{-2}$.

Таблиця Б.14

Залежність максимальної відносної похибки $\delta_{\max}$ від l_k

k	20	21	22	23	24
$\delta_{\max}$	0,025055	0,017339	0,013718	0,008003	0,007146

Для виконання умови $\delta_{\max}<10^{-2}$ для $M=4$ необхідно, щоб довжина інформаційної частини містила не менше 23 бітів.

Таким чином, під час використання перетворення $b_i(j)=\left(b_i(j-1)+Z_i(j)\right)(\mathrm{mod}\, i)$ збільшення довжини інформаційного повідомлення k призводить до вирівнювання частот появи перестановок і, отже, ймовірність виникнення колізій прямує до мінімуму.

2. Модифікація синдрому за допомоги процедури $b_i(j)=\left(b_i(j-1)+Z_i(j)\right)(\mathrm{mod}\, i)$

Абсолютні частоти появи перестановок у випадку перебору всіх значень інформаційного повідомлення співпадають з отриманими вище абсолютними частотами появи перестановок у випадку перебору всіх значень ключової послідовності. Тому під час використання модифікації синдрому виду $b_i(j)=\left(b_i(j-1)+Z_i(j)\right)(\mathrm{mod}\, i)$ значення інформаційної ентропії формувача перевірної частини (перестановки) прямує до максимального – $\log_a(M!)$, а ймовірність виникнення колізії прямує до мінімуму.

3. Модифікація синдрому за допомоги процедури $S_F(j-1)\to\pi(j-1)\to S_F'(j-1)$

Розглянемо наведені в таблиці Б.15 абсолютні частоти появи перевірної частини ПФК під час перебору всіх можливих векторів інформаційного повідомлення для $M=4$, $l_k=4$ та $k_{symb}=2$ для різних значень $S(0)$, k_1 та k_2.

Таблиця Б.15

Абсолютні частоти появи перестановок у залежності від значень $S(0)$, k_1 та k_2

Номери перестановок	Абсолютні частоти			
	$S(0)=2100$ $k_1=0312$ $k_2=2103$	$S(0)=3010$ $k_1=2013$ $k_2=0123$	$S(0)=3010$ $k_1=1203$ $k_2=3021$	$S(0)=2100$ $k_1=1203$ $k_2=3021$
0	8	9	11	8
1	8	9	10	8
2	8	10	9	8
3	8	11	8	8
4	9	11	8	8
5	10	11	8	8
6	11	11	8	8
7	12	10	8	9
8	13	10	8	10
9	14	10	8	11
10	14	10	8	12
11	14	10	8	13
12	13	10	9	14
13	12	11	10	15
14	12	12	11	16
15	12	13	12	15
16	11	13	13	14
17	10	13	14	13
18	10	12	15	12
19	10	11	16	11
20	10	11	15	10
21	10	10	14	9
22	9	9	13	8
23	8	9	12	8

Отримані статистичні властивості інваріантні по відношенню до значення ВПЗ, який лише вливає на зміщення розподілу.

У таблиці Б.16 наведено результати статистичного аналізу виходу формувача перевірної частини ПФК для $M=4$, $S(0)=0000$, $k_1=0123$, $k_2=2013$ і різної кількості символів інформаційного повідомлення.

Таблиця Б.16

Абсолютні частоти появи перестановок для різної кількості символів інформаційної частини

Номери перестановок	Абсолютні частоти				
	$k_{symb}=2$	$k_{symb}=3$	$k_{symb}=4$	$k_{symb}=5$	$k_{symb}=6$
0	11	175	2688	43965	697553
1	12	173	2687	44018	697129
2	13	168	2712	43922	697442
3	14	162	2739	43822	697730
4	14	157	2770	43648	698563
5	14	153	2801	43447	699617
6	14	152	2817	43342	700197
7	14	152	2827	43254	700765
8	13	153	2839	43137	701524
9	12	154	2853	43000	702411
10	11	159	2824	43131	701888
11	10	163	2805	43206	701654
12	10	168	2771	43397	700747
13	10	172	2740	43594	699728
14	9	178	2705	43760	699039
15	8	184	2670	43936	698266
16	8	184	2665	43970	698075
17	8	185	2652	44054	697612
18	8	185	2656	44019	697822
19	8	187	2648	44044	697768
20	8	187	2651	44027	697842
21	8	187	2651	44031	697807
22	9	182	2670	43970	697916
23	10	176	2695	43882	698121

У таблиці Б.17 наведено залежності значення максимальної відносної похибки $\delta_{\max}$ від значення k_{symb}. Визначимо умови, для яких значень k_{symb} виконується умова $\delta_{\max} < 10^{-2}$.

Таблиця Б.17

Залежність максимальної відносної похибки $\delta_{\max}$ від l_k

k_{symb}	4	5	6	7	8
$\delta_{\max}$	0,03125	0,013062	0,004379	0,00133	0,000362

Для виконання умови $\delta_{\max} < 10^{-2}$ для $M = 4$ необхідно, щоб довжина інформаційної частини містила не менше 6 укрупнених символів.

Таким чином, під час використання перетворення $S_F(j-1) \to \pi(j-1) \to S_F'(j-1)$ збільшення довжини інформаційного повідомлення призводить до вирівнювання частот появи перестановок і, отже, ймовірність виникнення колізій прямує до мінімуму.

У результаті проведеного аналізу визначено, що для всіх трьох розглянутих процедур модифікації синдрому перестановки під час збільшення довжини інформаційного повідомлення ймовірність виникнення колізій прямує до мінімуму.

Загалом, можна зробити наступні висновки:

– перетворення $S_F(j) = \left(S_F(j-1) + \gamma(j)\right) \dot{+}\, t(j)$ забезпечує максимальну інформаційну ентропію формувача перевірної частини ПФК та близьку до мінімальної ймовірність виникнення колізій;

– перетворення $b_i(j) = \left(b_i(j-1) + Z_i(j)\right) (\mathrm{mod}\, i)$ забезпечує близьку до максимальної інформаційну ентропію формувача перевірної частини ПФК та близьку до мінімальної ймовірність виникнення колізій;

– перетворення $S_F(j-1) \to \pi(j-1) \to S_F'(j-1)$ забезпечує максимальну інформаційну ентропію формувача перевірної частини ПФК та близьку до мінімальної ймовірність виникнення колізій.

Додаток В. Оцінка ймовірності невиявленої помилки для двійкового циклічного надлишкового коду (CRC) у системі з ВЗЗ

Врахуємо, що в системі з пакетним передаванням даних під час використання систематичного двійкового циклічного надлишкового коду блок даних $C_n(x)$ довжиною n біт складається з інформаційної частини $A_k(x)$ довжиною k біт і перевірної частини $R_r(x)$ довжиною r біт, $n = k + r$.

Вектор помилки, викликаний завадою, що діє в каналі зв'язку, можна представити в наступному вигляді:

$$\varepsilon_n(x) = Q_{n-r}(x) G_{r+1}(x) + \varepsilon_r(x),$$

де $G_{r+1}(x)$ – кодовий поліном степені r (кількість розрядів у двійковому поданні – $r+1$); $Q_{n-r}(x)$ і $\varepsilon_r(x)$ – відповідно ціла частина і залишок від ділення вектора помилки $\varepsilon_n(x)$ на кодовий поліном $G_{r+1}(x)$.

За незалежних бітових помилок помилка $\varepsilon_n(x)$ розподілена за біноміальним законом: імовірність $p_n(i)$ появи вектора ваги $i \in [0; n]$ дорівнює

$$p_n(i) = C_n^i p_0^i q_0^{n-i}. \qquad \text{(В.1)}$$

Декодер CRC-коду обчислює синдром помилки:

$$S(x) = \left| C_n(x) \oplus \varepsilon_n(x) \right|_{G_{r+1}(x)} = \left| \varepsilon_n(x) \right|_{G_{r+1}(x)}. \qquad \text{(В.2)}$$

За $S(x) \neq 0$ блок даних перезапитується, а за $S(x) = 0$ виводиться споживачеві.

Для визначення ймовірності невиявленої (залишкової) помилки декодера CRC-коду $P_{ud}(CRC, p_0)$ необхідно:

- розділити множину помилок $\varepsilon_n(x) \neq 0$ на дві складові:
  - помилки, які виявляються кодом, за $S(x) \neq 0$;
  - помилки, не виявляються кодом, за $S(x) = 0$ і $\varepsilon_n(x) \neq 0$;
- визначити число виявлених і невиявлених кодом помилок у залежності від їх ваги.

Позначимо через $f_{CRC}(i)$ число помилок ваги $i \in [0;n]$, які не виявляються CRC-кодом.

Нехай випадкова подія A^{**} = {помилка $\varepsilon_n(x)$ перетворює дозволену комбінацію CRC-коду в дозволену (в комбінацію з правильною контрольною сумою)}, $P(A^{**}) = P_{ud}(CRC, p_0)$; випадкова подія B_i^{**} = {поява помилки ваги i}, $P(B_i^{**}) = p_n(i)$. Тоді умовна ймовірність $P(A^{**} | B_i^{**}) = f_{CRC}(i)/C_n^i$ вказує ймовірність перетворення дозволеної комбінації коду в дозволену у випадку появи помилки ваги i. Унаслідок формули повної ймовірності і виразу (В.1),

$$P_{ud}(CRC, p_0) = \sum_{i=1}^{n} p_n(i) \cdot f_{CRC}(i)/C_n^i = \sum_{i=1}^{n} f_{CRC}(i)\, p_0^i q_0^{n-i}. \qquad (В.3)$$

З огляду на мінімальну кодову відстань d_0, імовірність появи помилки $\varepsilon_n(x)$, здатної перетворити дозволену комбінацію циклічного надлишкового коду в дозволену комбінацію (не включаючи саму в себе), дорівнює [332]–[334]

$$P_{ud}(CRC, p_0) = \sum_{i=d_0}^{n} f_{CRC}(i)\, p_0^i q_0^{n-i}. \qquad (В.4)$$

Твердження В.1. Загальна кількість векторів помилки $\varepsilon_n(x)$, здатних перетворити дозволену комбінацію циклічного надлишкового коду в дозволену комбінацію (не включаючи саму в себе), дорівнює

$$\sum_{i=d_0}^{n} f_{CRC}(i) = 2^k - 1. \qquad (В.5)$$

Доведення.

З (В.2) випливає, що помилка, що не виявляється кодом, виникає, якщо за $\varepsilon_n(x) \neq 0$ виконується умова $|\varepsilon_n(x)|_{G_{r+1}(x)} = 0$. Остання рівність справедлива, якщо $\varepsilon_n(x) = Q_{n-r}(x) G_{r+1}(x)$, де $Q_{n-r}(x)$ – будь-який ненульовий поліном, степінь якого не перевищує значення $n-r$. Таким чином, кількість не виявених CRC-кодом векторів помилки $\varepsilon_n(x)$ дорівнює кількості ненульових поліномів $Q_{n-r}(x)$:

$\mu\{Q_{n-r}(x)\neq 0\}=2^{n-r}-1$. Отже, $\sum_{i=0}^{n} f_{CRC}(i)=2^{n-r}-1$. З урахуванням мінімальної кодової відстані коду d_0 маємо: $\sum_{i=0}^{d_0-1} f_{CRC}(i)=0$, звідки випливає вираз (В.5). ■

Розглянемо окремий важливий випадок, за якого кодовий поліном CRC-коду є примітивним поліномом степені $\log_2(n+1)$ або добутком таких поліномів.

Теорема В.1. Якщо кодовий поліном циклічного надлишкового коду є примітивним поліномом степені $\log_2(n+1)$ або добутком таких поліномів, розподіл $f_{CRC}(i)$ кількості не виявлених кодом помилок у залежності від їх ваги симетричний відносно значення $n/2$, тобто

$$f_{CRC}(i)=f_{CRC}(n-i). \qquad (В.6)$$

Доведення.

Нехай $\varepsilon_n^{(i)}(x)$ – помилка ваги i, для якої $\left|C_n(x)\oplus\varepsilon_n^{(i)}(x)\right|_{G_{r+1}(x)}=0$. Тоді інверсна помилка $\varepsilon_n^{(n-i)}(x)=\varepsilon_n^{(i)}(x)\oplus E_n(x)$, де $E_n(x)$ – помилка ваги n. Синдром CRC у випадку впливу інверсної помилки $S(x)=\left|C_n(x)\oplus\varepsilon_n^{(n-i)}(x)\right|_{G_{r+1}(x)}=\left|C_n(x)\oplus\varepsilon_n^{(i)}(x)\oplus E_n(x)\right|_{G_{r+1}(x)}=\left|E_n(x)\right|_{G_{r+1}(x)}$.

Якщо кодовий поліном $G_{r+1}(x)$ є добутком примітивних поліномів $g(x)$ зі степенями ≥ 2, що ділять без залишку поліном x^n+1: $\left|x^n+1\right|_{g(x)}=0$, то $\left|x^n+1\right|_{G_{r+1}(x)}=0$. Врахуємо, що $x^n+1=(x+1)\cdot E_n(x)$. Оскільки $r+1>2$, з рівності $\left|x^n+1\right|_{G_{r+1}(x)}=\left|(x+1)\cdot E_n(x)\right|_{G_{r+1}(x)}=0$ випливає $\left|E_n(x)\right|_{G_{r+1}(x)}=0$.

Таким чином, якщо $\left|C_n(x)\oplus\varepsilon_n^{(i)}(x)\right|_{G_{r+1}(x)}=0$, то $\left|C_n(x)\oplus\varepsilon_n^{(i)}(x)\oplus E_n(x)\right|_{G_{r+1}(x)}=0$. Іншими словами, якщо помилка $\varepsilon_n^{(i)}(x)$ призводить до помилкового декодування, то і інверсна помилка $\varepsilon_n^{(n-i)}(x)=\varepsilon_n^{(i)}(x)\oplus E_n(x)$ також призводить до помилкового декодування. Тому кількість помилок ваги i і $n-i$, що

призводять до помилкового декодування, однакова: $f_{CRC}(i) = f_{CRC}(n-i)$. ■

Наслідок В.1. Якщо кодовий поліном циклічного надлишкового коду є примітивним поліномом степені $\log_2(n+1)$ або добутком таких поліномів, імовірність $P_{ud}(CRC, p_0)$ появи помилки $\varepsilon_n(x)$, здатної перетворити дозволену комбінацію в дозволену комбінацію (не включаючи саму в себе), дорівнює

$$P_{ud}(CRC, p_0) = \sum_{i=d_0}^{(n-1)/2} f_{CRC}(i)\left(p_0^i q_0^{n-i} + p_0^{n-i} q_0^i\right) + p_0^n. \qquad (В.7)$$

де

$$\sum_{i=d_0}^{(n-1)/2} f_{CRC}(i) = 2^{k-1} - 1. \qquad (В.8)$$

Враховуючи, що $p_0^{d_0} q_0^{n-d_0} > p_0^{n-d_0} q_0^{d_0}$ для $d_0 \le (n-1)/2$, а $p_0^n \xrightarrow[n\to\infty]{} 0$, маємо:

$$P_{ud}(CRC, p_0) \approx \sum_{i=d_0}^{(n-1)/2} f_{CRC}(i)\, p_0^i q_0^{n-i}. \qquad (В.9)$$

Наслідок В.2. Якщо кодовий поліном циклічного надлишкового коду є примітивним поліномом степені $\log_2(n+1)$ або добутком таких поліномів і $d_0 > (n-1)/2 - 1$, справедливі вирази

$$P_{ud}(CRC, p_0) = \left(2^{k-1} - 1\right)\left(p_0^{d_0} q_0^{n-d_0} + p_0^{n-d_0} q_0^{d_0}\right) + p_0^n, \qquad (В.10)$$

$$P_{ud}(CRC, p_0) \approx 2^{k-1} p_0^{d_0} q_0^{n-d_0}. \qquad (В.11)$$

Далі приймемо, що кодовий поліном циклічного надлишкового коду не обов'язково є примітивним.

У теперішній час є актуальною задача визначення значень $f_{CRC}(i)$ для обчислення ймовірності $P_{ud}(CRC, p_0)$ за (В.4). Вона тісно пов'язана з проблемою знаходження найбільш ефективних поліномів для заданої довжини n кодового слова, для яких імовірність невиявленої помилки $P_{ud}(CRC, p_0)$ мінімальна. Цій проблемі присвячено роботи [335]–[350].

Слід зауважити, що аналітично значення $f_{CRC}(i)$ можуть бути обчислені для кодів Хеммінга з $d_0 = \{3;4\}$ і кодів Ріда-Мюллера [273, с. 680]. Для інших циклічних

кодів знаходження $f_{CRC}(i)$ є складною емпіричною задачею, трудомісткість якої істотно підвищується зі збільшенням ваги помилки i. Разом з тим, як показано в [342, с. 6], під час обчислення $P_{ud}(CRC, p_0)$ найбільш значущими є значення $f_{CRC}(d_0)$ і $f_{CRC}(d_0+1)$. Тому на практиці обчислюють значення $f_{CRC}(i)$ для ваг $i \in [2; d_1]$, де d_1 на кілька одиниць перевищує d_0. Найбільш повно $f_{CRC}(i)$ представлено в [348].

Визначимо похибку обчислення ймовірності невиявленої помилки, якщо у формулі (В.4) верхню межу підсумовування зменшити до значення $d_1 < n$ (тобто якщо замість $n+1-d_0$ доданків використовувати тільки перші d_1+1-d_0).

Для цього розділимо суму в виразі (В.4) на дві складові.

Визначення В.1. Імовірність $P_{ud}(CRC, p_0)$ появи помилки $\varepsilon_n(x)$, здатної перетворити дозволену комбінацію циклічного надлишкового коду в іншу дозволену комбінацію, дорівнює сумі:

$$P_{ud}(CRC, p_0) = \sum_{i=d_0}^{d_1} f_{CRC}(i)\, p_0^i q_0^{n-i} + \Delta_{CRC}(d_1), \qquad \text{(В.12)}$$

де

$$\Delta_{CRC}(d_1) = \sum_{i=d_1+1}^{n} f_{CRC}(i)\, p_0^i q_0^{n-i}. \qquad \text{(В.13)}$$

Теорема В.2. В умовах застосування апроксимаційної формули Пуассона для біноміального розподілу ймовірність $\Delta_{CRC}(d_1)$ появи помилки $\varepsilon_n(x)$ з вагою $i \ge d_1+1$, $d_0 \le d_1 \le n-1$, здатної перетворити дозволену комбінацію циклічного надлишкового коду в іншу дозволену комбінацію, може бути оцінена зверху:

$$\Delta_{CRC}(d_1) \le \frac{1}{C_{n+t-d_1-1}^{t}} \cdot \frac{\lambda^{d_1+1}}{(d_1+1)!} e^{-\lambda} \cdot \frac{d_1+2}{d_1+2-\lambda(t+1)}, \qquad \text{(В.14)}$$

де $\lambda = n \cdot p_0$, $t = \left\lfloor \frac{d_0-1}{2} \right\rfloor$ і $d_1 > \lambda(t+1) - 2$.

Доведення.

Якщо відомі n, k і мінімальна кодова відстань d_0, для $i \in [d_0; n]$ справедлива

оцінка [332]:

$$f_{CRC}(i) \le \frac{C_n^{i-t}}{C_i^t}. \qquad \text{(B.15)}$$

Підставляючи (B.15) в (B.13), маємо:

$$\Delta_{CRC}(d_1) \le \sum_{i=d_1+1}^{n} \frac{C_n^{i-t}}{C_i^t} p_0^i q_0^{n-i} = \sum_{i=d_1+1}^{n} \frac{C_n^{i-t}}{C_i^t C_n^i} p_n(i) = \sum_{i=d_1+1}^{n} \frac{n!\cdot t!\cdot (i-t)!\cdot i!\cdot (n-i)!}{(i-t)!\cdot (n-i+t)!\cdot i!\cdot n!} p_n(i) =$$

$$= \sum_{i=d_1+1}^{n} \frac{t!\cdot (n-i)!}{(n-i+t)!} p_n(i) = \sum_{i=d_1+1}^{n} \frac{1}{C_{n-i+t}^t} p_n(i).$$

Згідно апроксимаційної формули Пуассона,

$$p_n(i) \simeq \frac{\lambda^i}{i!} e^{-\lambda}. \qquad \text{(B.16)}$$

Підставляючи $p_n(i)$ з (B.16) у нерівність $\Delta_{CRC}(d_1) \le \sum_{i=d_1+1}^{n} \frac{1}{C_{n-i+t}^t} p_n(i)$, отримаємо:

$$\Delta_{CRC}(d_1) \le \sum_{i=d_1+1}^{n} \frac{1}{C_{n-i+t}^t} \cdot \frac{\lambda^i}{i!} e^{-\lambda} =$$

$$= e^{-\lambda} \left(\frac{1}{C_{n+t-d_1-1}^t} \cdot \frac{\lambda^{d_1+1}}{(d_1+1)!} + \frac{1}{C_{n+t-d_1-2}^t} \cdot \frac{\lambda^{d_1+2}}{(d_1+2)!} + \frac{1}{C_{n+t-d_1-3}^t} \cdot \frac{\lambda^{d_1+3}}{(d_1+3)!} + \ldots + \frac{\lambda^n}{n!} \right).$$

Нехай $\zeta_i = \frac{1}{C_{n+t-i}^t} \cdot \frac{\lambda^i}{i!}$, де $d_1 + 1 \le i \le n$. Тоді для $d_1 + 2 \le i \le n$

$Z_i = \frac{\zeta_i}{\zeta_{i-1}} = \frac{C_{n+t-i+1}^t}{C_{n+t-i}^t} \cdot \frac{\lambda^i \cdot (i-1)!}{i!\cdot \lambda^{i-1}} = \frac{n+t-i+1}{n-i+1} \cdot \frac{\lambda}{i} = \left(1 + \frac{t}{n+1-i}\right) \cdot \frac{\lambda}{i}$, звідки

$$\Delta_{CRC}(d_1) \le \frac{1}{C_{n+t-d_1-1}^t} \cdot \frac{\lambda^{d_1+1}}{(d_1+1)!} e^{-\lambda} \left(1 + Z_{d_1+2} + Z_{d_1+2} \cdot Z_{d_1+3} + \ldots + \prod_{j=d_1+2}^{n} Z_j \right).$$

Для оцінки суми геометричної прогресії визначимо максимальне значення функції Z_i. Для цього обчислимо її першу похідну за i: $\frac{dZ_i}{di} = \lambda \left(-\frac{1}{i^2} - \frac{t(n+1-2i)}{i^2 (n+1-i)^2} \right)$. Прирівнюючи її до нуля, знаходимо, що для $d_1 + 2 \le i \le n$ локальний екстремум функції Z_i знаходиться в точці

$i=\left(n+1+t\right)-\sqrt{t\left(n+1+t\right)}$. Обчислимо другу похідну: $\frac{d^2Z_i}{di^2}=2\lambda\left(\frac{1}{i^3}+t\frac{i\left(n+1-i\right)+\left(n+1-2i\right)^2}{i^3\left(n+1-i\right)^3}\right)$. Для $\forall i\in\left[d_1+2;n\right]$ справедливо $\frac{d^2Z_i}{di^2}>0$, тому в точці $i=\left(n+1+t\right)-\sqrt{t\left(n+1+t\right)}$ функція Z_i має локальний мінімум. Звідси оцінка значень Z_i для $d_1+2\le i\le n$ має вигляд: $Z_i\le\max\left(Z_{d_1+2};Z_n\right)$.

Для простоти обчислень скористаємося наступним. Оскільки для $d_1+2\le i\le n$ справедливими є нерівності $1+\frac{t}{n+1-i}\le 1+t$ і $\frac{\lambda}{i}\le\frac{\lambda}{d_1+2}$, має місце оцінка: $Z_i\le\left(1+t\right)\cdot\frac{\lambda}{d_1+2}$. Тоді

$$\Delta_{CRC}\left(d_1\right)\le\frac{1}{C^t_{n+t-d_1-1}}\cdot\frac{\lambda^{d_1+1}}{\left(d_1+1\right)!}e^{-\lambda}\left(\begin{array}{l}1+\left(t+1\right)\cdot\frac{\lambda}{d_1+2}+\left(\left(t+1\right)\cdot\frac{\lambda}{d_1+2}\right)^2+\ldots+\\+\left(\left(t+1\right)\cdot\frac{\lambda}{d_1+2}\right)^{n-d_1-1}\end{array}\right).$$

Для $d_1>\lambda\left(t+1\right)-2$ виконується $\left(t+1\right)\cdot\frac{\lambda}{d_1+2}<1$, тому сума геометричної прогресії

$$1+\left(t+1\right)\cdot\frac{\lambda}{d_1+2}+\left(\left(t+1\right)\cdot\frac{\lambda}{d_1+2}\right)^2+\ldots+\left(\left(t+1\right)\cdot\frac{\lambda}{d_1+2}\right)^{n-d_1-1}=$$

$$=\frac{1-\left(\left(t+1\right)\cdot\frac{\lambda}{d_1+2}\right)^{n-d_1-1}}{1-\left(t+1\right)\cdot\frac{\lambda}{d_1+2}}\le\frac{d_1+2}{d_1+2-\lambda\left(t+1\right)},$$

звідки випливає оцінка (В.14). ■

Наслідок В.3. Якщо кодовий поліном циклічного надлишкового коду ділиться без залишку на $x+1$, оцінка зверху для ймовірності $\Delta_{CRC}\left(d_1\right)$, $\left|d_1\right|_2=0$, має вигляд:

$$\Delta_{CRC}\left(d_1\right) \le \frac{1}{C^t_{n+t-d_1-2}} \cdot \frac{\lambda^{d_1+2}}{\left(d_1+2\right)!} e^{-\lambda} \cdot \frac{2\left(d_1+3\right)^2}{2\left(d_1+3\right)^2 - \lambda^2\left(t+2\right)^2}, \tag{B.17}$$

де $d_1 > \dfrac{\lambda\left(t+2\right)}{\sqrt{2}} - 3.$

Доведення.

Якщо $x+1$ є дільником кодового полінома $G\left(x\right)$ $\left(\left|G\left(x\right)\right|_{x+1} = 0\right)$, то CRC-код дозволяє виявляти всі помилки $\varepsilon_n\left(x\right)$ непарної ваги Хеммінга [342, с. 27], [351, с. 239], [352, розд. 8]. Тоді

$$f_{CRC}\left(i\right)\begin{cases} = 0 \text{ для } i = 2j+1, \\ \le \dfrac{C^{i-t}_n}{C^t_i} \text{ для } i = 2j; \end{cases} \tag{B.18}$$

де $\dfrac{d_0}{2} \le j \in \mathbb{Z} \le \left\lfloor \dfrac{n}{2} \right\rfloor.$

Підставляючи (B.18) в (B.13), для $\left|d_1\right|_2 = 0$ маємо:

$$\Delta_{CRC}\left(d_1\right) \le \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \frac{C^{2j-t}_n}{C^t_{2j}} p_0^{2j} q_0^{n-2j} = \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \frac{C^{2j-t}_n}{C^t_{2j} C^{2j}_n} p_n\left(2j\right) =$$

$$= \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \frac{n! \cdot t! \cdot \left(2j-t\right)! \cdot \left(2j\right)! \cdot \left(n-2j\right)!}{\left(2j-t\right)! \cdot \left(n-2j+t\right)! \cdot \left(2j\right)! \cdot n!} p_n\left(2j\right) =$$

$$= \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \frac{t! \cdot \left(n-2j\right)!}{\left(n-2j+t\right)!} p_n\left(2j\right) = \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \frac{1}{C^t_{n-2j+t}} p_n\left(2j\right).$$

Підставляючи $p_n\left(i\right)$ з (B.16) у нерівність $\Delta_{CRC}\left(d_1\right) \le \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \dfrac{1}{C^t_{n-2j+t}} p_n\left(2j\right)$, отримаємо:

$$\Delta_{CRC}(d_1) \le \sum_{j=d_1/2+1}^{\lfloor n/2 \rfloor} \frac{1}{C_{n-2j+t}^{t}} \cdot \frac{\lambda^{2j}}{(2j)!} e^{-\lambda} =$$

$$= e^{-\lambda} \left(\frac{1}{C_{n+t-d_1-2}^{t}} \cdot \frac{\lambda^{d_1+2}}{(d_1+2)!} + \frac{1}{C_{n+t-d_1-4}^{t}} \cdot \frac{\lambda^{d_1+4}}{(d_1+4)!} + \frac{1}{C_{n+t-d_1-6}^{t}} \cdot \frac{\lambda^{d_1+6}}{(d_1+6)!} + \ldots + \right.$$

$$\left. + \frac{1}{C_{n+t-2\lfloor n/2 \rfloor}^{t}} \cdot \frac{\lambda^{2\lfloor n/2 \rfloor}}{(2\lfloor n/2 \rfloor)!} \right).$$

Приймемо $\zeta_{2j} = \frac{1}{C_{n+t-2j}^{t}} \cdot \frac{\lambda^{2j}}{(2j)!}$, де $\frac{d_1}{2} \le j \in \mathbb{Z} \le \left\lfloor \frac{n}{2} \right\rfloor$. тоді для $\frac{d_1}{2}+1 \le j \in \mathbb{Z} \le \left\lfloor \frac{n}{2} \right\rfloor$

$$Z_{2j} = \frac{\zeta_{2j}}{\zeta_{2(j-1)}} = \frac{C_{n+t-2j+2}^{t}}{C_{n+t-2j}^{t}} \cdot \frac{\lambda^{2j} \cdot (2(j-1))!}{(2j)! \cdot \lambda^{2(j-1)}} =$$

$$= \frac{(n+t-2j+1)(n+t-2j+2)}{(n-2j+1)(n-2j+2)} \cdot \frac{\lambda^2}{(2j-1) \cdot 2j} =$$

$$= \left(1 + \frac{t}{n+1-2j}\right)\left(1 + \frac{t}{n+2-2j}\right) \cdot \frac{\lambda^2}{(2j-1) \cdot 2j},$$

звідки

$$\Delta_{CRC}(d_1) \le \frac{1}{C_{n+t-d_1-2}^{t}} \cdot \frac{\lambda^{d_1+2}}{(d_1+2)!} e^{-\lambda} \left(1 + Z_{d_1+4} + Z_{d_1+4} \cdot Z_{d_1+6} + \ldots + \prod_{j=d_1/2+2}^{\lfloor n/2 \rfloor} Z_{2j} \right).$$

Оскільки для $\frac{d_1}{2}+2 \le j \le \left\lfloor \frac{n}{2} \right\rfloor$ справедливими є нерівності $1 + \frac{t}{n+1-2j} \le 1+t$, $1 + \frac{t}{n+2-2j} \le 1+t$ і $\frac{\lambda^2}{(2j-1) \cdot 2j} \le \frac{\lambda^2}{(d_1+3)(d_1+4)}$, має місце оцінка: $Z_{2j} \le \frac{\lambda^2 (t+1)(t+2)}{2(d_1+3)(d_1+4)} \le \frac{\lambda^2 (t+2)^2}{2(d_1+3)^2}$. Тоді

$$\Delta_{CRC}(d_1) \le \frac{1}{C_{n+t-d_1-2}^{t}} \cdot \frac{\lambda^{d_1+2}}{(d_1+2)!} e^{-\lambda} \left(1 + \frac{\lambda^2 (t+2)^2}{2(d_1+3)^2} + \left(\frac{\lambda^2 (t+2)^2}{2(d_1+3)^2} \right)^2 + \ldots + \right.$$

$$\left. + \left(\frac{\lambda^2 (t+2)^2}{2(d_1+3)^2} \right)^{\lfloor n/2 \rfloor - d_1/2 - 1} \right).$$

Для $d_1 > \frac{\lambda(t+2)}{\sqrt{2}} - 3$ виконується $\frac{\lambda^2(t+2)^2}{2(d_1+3)^2} < 1$, тому сума геометричної прогресії

$$1 + \frac{\lambda^2(t+2)^2}{2(d_1+3)^2} + \left(\frac{\lambda^2(t+2)^2}{2(d_1+3)^2}\right)^2 + \ldots + \left(\frac{\lambda^2(t+2)^2}{2(d_1+3)^2}\right)^{\lfloor n/2 \rfloor - d_1/2 - 1} =$$

$$= \frac{1 - \left(\frac{\lambda^2(t+2)^2}{2(d_1+3)^2}\right)^{n-d_1-1}}{1 - \frac{\lambda^2(t+2)^2}{2(d_1+3)^2}} \le \frac{2(d_1+3)^2}{2(d_1+3)^2 - \lambda^2(t+2)^2},$$

звідки випливає оцінка (В.17). ■

Зауваження В.1. Значення $P_{ud}(CRC, p_0)$ обчислюється відповідно до виразу (В.12), де $\Delta_{CRC}(d_1)$ оцінюється за (В.14) або (В.17) і не перевищує максимальної абсолютної похибки обчислень ε.

Оскільки величина $P_{ud}(CRC, p_0)$ може приймати свої значення в широких межах, доцільно для оцінювання точності обчислень використовувати відносну похибку обчислень $\delta_{CRC}(d_1) = \frac{\Delta_{CRC}(d_1)}{\sum_{i=d_0}^{d_1} f_{CRC}(i)\, p_0^i q_0^{n-i}} \le \delta'_{CRC}(d_1) = \frac{\Delta_{CRC}(d_1)}{f_{CRC}(d_0)\, p_0^{d_0} q_0^{n-d_0}}$, яка не повинна перевищувати необхідного значення δ_{CRC}.

Зауваження В.2. У цій роботі для оцінки ймовірності невиявленої циклічним завадостійким кодом помилки $P_{ud}(CRC, p_0)$ будемо застосовувати вирази (В.12), (В.14) і (В.17), використовуючи значення $f_{CRC}(i)$ з [348].

Додаток Д. Приклади реалізації факторіального кодування з відновленням даних і виправленням помилок та їх оцінка

Д.1. Приклади реалізації факторіального кодування з відновленням даних і виправленням помилок

Виконаємо побудову СКК і визначимо показники швидкості та достовірності передавання у випадку їх використання для ФКВД і ФКВДвп. Порівняльний аналіз досліджуваних параметрів кодів наведемо в наступному пункті цього розділу.

Д.1.1. Факторіальне кодування з відновленням даних і виправленням помилок з сигнально-кодовою конструкцією першого типу

Приймемо $k=3$, а $M=4$. Відповідно до (3.24) $D_{\min}\le 3$. Тоді сигнальними точками є точки 1, 4, 7, 10, 13, 16, 19, 22, а СКК для базової перестановки $\pi(0)=\{0;1;2;3\}$ представлена в таблиці Д.1. З таблиці видно, що така СКК забезпечує $d_{\min}=2$.

Таблиця Д.1

СКК-1 для ФКВДвп при $k=3,\ M=4$

Сигнальні точки	СКК-1
1	00 01 11 10
4	00 11 01 10
7	01 00 11 10
10	01 11 00 10
13	10 00 11 01
16	10 11 00 01
19	11 00 10 01
22	11 10 00 01

Розташування сигнальних точок показано на рис. Д.1.

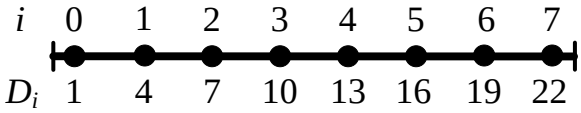


Рис. Д.1. Розташування сигнальних точок для СКК-1

Визначимо ймовірність невиявленої помилки ФКВДвп з СКК-1, представленої в таблиці Д.1.

Помилка не виявляється кодом, якщо кодове слово, що відповідає i-й сигнальної точці, буде перетворено завадою в комбінацію, що відповідає будь-якій точці числової осі, яка не належить діапазону $[D_i - 1; D_i + 1]$.

Для СКК-1 побудуємо матрицю відстаней Хеммінга між множиною сигнальних точок та множиною всіх точок числової осі (таблиця Д.2).

Таблиця Д.2

Матриця відстаней між сигнальними точками і точками числової осі

Точки числової осі		D_i							
		1	4	7	10	13	16	19	22
0	00 01 10 11	2	4	4	4	4	4	4	6
1	00 01 11 10	0	2	2	4	4	6	6	8
2	00 10 01 11	4	2	4	4	4	4	6	4
3	00 10 11 01	4	4	4	6	2	4	4	4
4	00 11 01 10	2	0	4	2	6	4	8	6
5	00 11 10 01	4	4	6	4	4	2	4	4
6	01 00 10 11	4	6	2	4	4	6	2	4
7	01 00 11 10	2	4	0	4	4	8	4	6
8	01 10 00 11	6	4	4	2	6	4	4	2
9	01 10 11 00	4	4	2	4	4	6	4	4
10	01 11 00 10	4	2	4	0	8	4	6	4
11	01 11 10 00	4	4	4	2	6	4	4	4
12	10 00 01 11	4	4	4	6	2	4	4	4
13	10 00 11 01	4	6	4	8	0	4	2	4
14	10 01 00 11	4	4	6	4	4	2	4	4
15	10 01 11 00	2	4	4	6	2	4	4	6
16	10 11 00 01	6	4	8	4	4	0	4	2
17	10 11 01 00	4	2	6	4	4	2	6	4
18	11 00 01 10	4	4	2	4	4	6	4	4
19	11 00 10 01	6	8	4	6	2	4	0	2
20	11 01 00 10	4	4	4	2	6	4	4	4
21	11 01 10 00	4	6	4	4	4	4	2	4
22	11 10 00 01	8	6	6	4	4	2	2	0
23	11 10 01 00	6	4	4	4	4	4	4	2

Сірим кольором для сигнальної точки i в таблиці виділені відстані для точок діапазону $[D_i - 1; D_i + 1]$.

Представлені результати повністю узгоджуються з наведеною в розділі 5 теоретичною оцінкою кількості помилок ваги t, що перетворюють перестановку в перестановку: $f_{per}(0) = 1$, $f_{per}(2) = 4$, $f_{per}(4) = 14$, $f_{per}(6) = 4$, $f_{per}(8) = 1$.

Імовірність не виявленої ФКВДвп помилки визначається за (3.26). Приймемо,

що всі слова застосовуються джерелом з однаковою ймовірністю, яка дорівнює $P_w(i) = P_w = \frac{1}{2^k}$. Для розглянутого прикладу $P_w = \frac{1}{8}$, $l_r = 2$, а $r = 8$. Врахуємо також, що вага помилок, які призводять до помилкового декодування, парна. Тоді $P_{ud}\left(FCDRec, p_0\right) = \frac{1}{8}\sum_{i=0}^{7}\sum_{t=1}^{4} f_{per}^{ud}\left(i, 2t\right) p_0^{2t} q_0^{8-2t}$.

Значення $f_{per}^{ud}\left(i, 2t\right)$ для даних з таблиці Д.2 наведено в таблиці Д.3.

Таблиця Д.3

Значення $f_{per}^{ud}\left(i, 2t\right)$ для ФКВДвп з СКК-1

t	сигнальна точка							
	0	1	2	3	4	5	6	7
1	3	4	3	3	3	3	4	3
2	13	12	13	13	13	13	12	13
3	4	4	4	4	4	4	4	4
4	1	1	1	1	1	1	1	1

Результати обчислення $P_{ud}\left(FCDRec, p_0\right)$ відповідно до (3.26) для різних p_0 представлено в таблиці Д.4.

Таблиця Д.4

Імовірність невиявленої помилки для ФКВДвп з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{ud}\left(FCDRec, p_0\right)$	$1.81\cdot10^{-2}$	$3.06\cdot10^{-4}$	$3.23\cdot10^{-6}$	$3.25\cdot10^{-8}$	$3.25\cdot10^{-10}$	$3.25\cdot10^{-12}$

Динамічна складова втрати швидкості внаслідок перезапитів визначається за (3.28):

$$\begin{aligned} &\nu_2\left(FCDRec, p_0\right) = 1 - P_{det}\left(FCDRec, p_0\right) = \\ &= Q + P_{EC}\left(FCDRec, p_0\right) + P_{ud}\left(FCDRec, p_0\right), \end{aligned} \qquad (Д.1)$$

де $Q = \left(1 - p_0\right)^r$ – імовірність прийому кодового слова без помилок;

$P_{det}\left(FCDRec, p_0\right)$ – імовірність перезапиту;

$P_{EC}\left(FCDRec, p_0\right)$ – імовірність виправлення помилок, що визначається за (3.29).

З урахуванням парності помилок, що перетворюють перестановку в перестановку, для СКК-1 $P_{EC}\left(FCDRec, p_0\right) = \sum_{i=0}^{2^k-1}\left(P_w\left(i\right) \cdot \sum_{t=1}^{[r/2]} f_{per}^{EC}\left(i, 2t\right) p_0^{2t} q_0^{r-2t} \right)$.

Значення $f_{per}^{EC}\left(i, 2t\right)$ для даних з таблиці Д.2 наведено в таблиці Д.5.

Таблиця Д.5

Значення $f_{per}^{EC}\left(i, 2t\right)$ для ФКВДвп з СКК-1

t	Сигнальна точка							
	0	1	2	3	4	5	6	7
1	1	0	1	1	1	1	0	1
2	1	2	1	1	1	1	2	1

Результати обчислення $P_{EC}\left(FCDRec, p_0\right)$ для різних p_0 наведено в таблиці Д.6.

Таблиця Д.6

Імовірність виправлення помилки для ФКВДвп з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{EC}\left(FCDRec, p_0\right)$	$4.07 \cdot 10^{-3}$	$7.06 \cdot 10^{-5}$	$7.46 \cdot 10^{-7}$	$7.50 \cdot 10^{-9}$	$7.50 \cdot 10^{-11}$	$7.50 \cdot 10^{-13}$

Значення енергетичного виграшу за оптимального некогерентного прийому двійкових символів для ФКВДвп з СКК-1 представлено в таблиці Д.7.

Таблиця Д.7

Енергетичний виграш ФКВДвп з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\Delta P\left(FCDRec, p_0\right)$, дБ	3.525	3.328	3.219	3.164	3.132	3.111

Значення залишкової ймовірності помилкового прийому в результаті застосування ФКВДвп з СКК-1, обчислені за (З.33), представлено в таблиці Д.8.

Таблиця Д.8

Залишкова ймовірність помилкового прийому ФКВДвп з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{res}\left(FCDRec, p_0\right)$	$4.00 \cdot 10^{-2}$	$3.32 \cdot 10^{-4}$	$3.26 \cdot 10^{-6}$	$3.25 \cdot 10^{-8}$	$3.25 \cdot 10^{-10}$	$3.25 \cdot 10^{-12}$

Значення динамічної складової втрати швидкості для ФКВДвп з СКК-1

представлено в таблиці Д.9.

Таблиця Д.9

Динамічна складова втрати швидкості ФКВДвп з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\nu_2\left(FCDRec, p_0\right)$	0.453	0.923	0.992	0.9992	0.99992	0.999992

Д.1.2. Факторіальне кодування з відновленням даних з сигнально-кодовою конструкцією першого типу

Визначимо ймовірність невиявленої помилки і значення динамічної складової втрати швидкості для ФКВД в режимі виявлення помилок, який використовує СКК-1.

Кількість $f_{per}^{ud}\left(i, 2t\right)$ помилок ваги $2t$, що призводять до помилкового декодування, для кожної сигнальної точки i цього коду наведено в таблиці Д.10.

Таблиця Д.10

Значення $f_{per}^{ud}\left(i, 2t\right)$ для ФКВД з СКК-1

t	сигнальна точка							
	0	1	2	3	4	5	6	7
1	2	2	1	1	1	1	2	2
2	2	2	4	4	4	4	2	2
3	2	2	1	1	1	1	2	2
4	1	1	1	1	1	1	1	1

Результати обчислення за (3.26) $P_{ud}\left(FCDR, p_0\right)$ для ФКВД з СКК-1 та різних p_0 представлено в таблиці Д.11.

Таблиця Д.11

Імовірність невиявленої помилки для ФКВД з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{ud}\left(FCDR, p_0\right)$	$9.47\cdot10^{-3}$	$1.65\cdot10^{-4}$	$1.74\cdot10^{-6}$	$1.75\cdot10^{-8}$	$1.75\cdot10^{-10}$	$1.75\cdot10^{-12}$

Значення енергетичного виграшу в результаті застосування ФКВД з СКК-1 за оптимального некогерентного прийому двійкових символів наведено в таблиці Д.12.

Таблиця Д.12

Енергетичний виграш ФКВД з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\Delta P\left(FCDR, p_0\right)$, дБ	4.211	3.636	3.420	3.314	3.251	3.210

Значення залишкової ймовірності помилкового прийому в результаті застосування ФКВД з СКК-1 представлені в таблиці Д.13.

Таблиця Д.13

Залишкова ймовірність помилкового прийому ФКВД з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{res}\left(FCDR, p_0\right)$	$2.15\cdot10^{-2}$	$1.79\cdot10^{-4}$	$1.75\cdot10^{-6}$	$1.75\cdot10^{-8}$	$1.75\cdot10^{-10}$	$1.75\cdot10^{-12}$

Значення динамічної складової втрати швидкості внаслідок перезапитів $\nu_2\left(FCDR, p_0\right) = 1 - P_{req}\left(FCDR, p_0\right) = Q + P_{ud}\left(FCDR, p_0\right)$ наведено в таблиці Д.14.

Таблиця Д.14

Динамічна складова втрати швидкості для ФКВД з СКК-1

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\nu_2\left(FCDR, p_0\right)$	0.44	0.923	0.992	0.9992	0.99992	0.999992

Д.1.3. Факторіальне кодування з відновленням даних і виправленням помилок з сигнально-кодовою конструкцією другого типу

У таблиці Д.15 представлено СКК-2 з 8 сигнальних векторів з $d_{\min} = 4$, що забезпечує виправлення однократної бітової помилки в кодовому слові.

Таблиця Д.15

СКК-2 для ФКВДвп при $k = 3,\ M = 4$

СКК	сигнальні точки
00 01 10 11	0
01 00 11 10	7
10 11 00 01	16
11 10 01 00	23
11 01 10 00	21
01 11 00 10	10
10 00 11 01	13
00 10 01 11	2

Ця СКК побудована наступним чином:

1) у якості першого кодового слова обрано представлену в двійковому вигляді тривіальну перестановку $\{0;1;2;3\}$;
2) друге кодове слово утворено шляхом перестановки 1 і 2, а також 3 і 4 символів першого кодового слова;
3) третє кодове слово утворено шляхом перестановки 1 і 3, а також 2 і 4 символів першого кодового слова;
4) четверте кодове слово утворено шляхом перестановки 1 і 4, а також 2 і 3 символів першого кодового слова;
5) кодові слова 5-8 утворені шляхом запису справа наліво кодових слів 1-4.

Розглянемо ймовірнісні характеристики ФКВДвп для СКК-2 з таблиці Д.15.

Експериментально встановлено, що цей код дозволяє виправити тільки будь-які помилки кратності $t=1$, а помилка не виявляється тоді і тільки тоді, коли кодове слово, що відповідає i-ому сигнальному вектору, перетворюється завадою в комбінацію, для якої відстань Хеммінга до будь-якого іншого сигнального вектора не перевищує одиницю.

Для цієї СКК-2 побудуємо матрицю відстаней Хеммінга між i-им $\left(i\in[0,7]\right)$сигнальним вектором і множиною векторів, що утворюють в метриці Хеммінга сфери одиничного радіуса з центрами в сигнальних точках. Результати зведемо в таблицю Д.16.

Сірим кольором для сигнальної точки i в таблиці виділені відстані до точок власної одиничною сфери.

Імовірність не виявленої кодом помилки обчислюється за (3.26). Приймемо також, що всі слова застосовуються джерелом з однаковою ймовірністю $P_w=1/8$. Значення $f_{per}^{ud}(i,t)$ для даних з таблиці Д.16 наведено в таблиці Д.17 ($f_{per}^{ud}(i,t)=0$ для $t\le 2$).

Як можна бачити, розподіл кількості $f_{per}^{ud}(i,t)$ помилок ваги t, що призводять до помилкового декодування ФКВДвп з СКК-2, не залежить від сигнальної точки.

Таблиця Д.16

Матриця відстаней між сигнальними векторами і векторами, що приводять до помилкового декодування

Одиничні сфери		D_i							
		0	2	7	10	13	16	21	23
Центр	00 01 10 11	0	4	4	8	4	4	4	4
	10 01 10 11	1	5	3	7	3	5	3	5
	01 01 10 11	1	3	5	7	3	3	5	5
	00 11 10 11	1	5	3	7	5	3	5	3
	00 00 10 11	1	3	5	7	5	5	3	3
	00 01 00 11	1	5	3	7	5	3	5	3
	00 01 11 11	1	3	5	7	5	5	3	3
	00 01 10 01	1	5	3	7	3	5	3	5
	00 01 10 10	1	3	5	7	3	3	5	5
Центр	01 00 11 10	4	0	8	4	4	4	4	4
	11 00 11 10	5	1	7	3	3	5	3	5
	00 00 11 10	3	1	7	5	5	5	3	3
	01 10 11 10	5	1	7	3	5	3	5	3
	01 01 11 10	3	1	7	5	3	3	5	5
	01 00 01 10	5	1	7	3	5	3	5	3
	01 00 10 10	3	1	7	5	3	3	5	5
	01 00 11 00	5	1	7	3	3	5	3	5
	01 00 11 11	3	1	7	5	5	5	3	3
Центр	10 11 00 01	4	8	0	4	4	4	4	4
	00 11 00 01	3	7	1	5	5	3	5	3
	11 11 00 01	5	7	1	3	3	3	5	5
	10 01 00 01	3	7	1	5	3	5	3	5
	10 10 00 01	5	7	1	3	5	5	3	3
	10 11 10 01	3	7	1	5	3	5	3	5
	10 11 01 01	5	7	1	3	5	5	3	3
	10 11 00 11	3	7	1	5	5	3	5	3
	10 11 00 00	5	7	1	3	3	3	5	5
Центр	11 10 01 00	8	4	4	0	4	4	4	4
	01 10 01 00	7	3	5	1	5	3	5	3
	10 10 01 00	7	5	3	1	5	5	3	3
	11 00 01 00	7	3	5	1	3	5	3	5
	11 11 01 00	7	5	3	1	3	3	5	5
	11 10 11 00	7	3	5	1	3	5	3	5
	11 10 00 00	7	5	3	1	3	3	5	5
	11 10 01 10	7	3	5	1	5	3	5	3
	11 10 01 01	7	5	3	1	5	5	3	3

Продовження таблиці Д.16

Центр	11 01 10 00	4	4	4	4	0	4	4	8
	01 01 10 00	3	3	5	5	1	3	5	7
	10 01 10 00	3	5	3	5	1	5	3	7
	11 11 10 00	5	5	3	3	1	3	5	7
	11 00 10 00	5	3	5	3	1	5	3	7
	11 01 00 00	5	5	3	3	1	3	5	7
	11 01 11 00	5	3	5	3	1	5	3	7
	11 01 10 10	3	3	5	5	1	3	5	7
	11 01 10 01	3	5	3	5	1	5	3	7
Центр	01 11 00 10	4	4	4	4	4	0	8	4
	11 11 00 10	5	5	3	3	3	1	7	5
	00 11 00 10	3	5	3	5	5	1	7	3
	01 01 00 10	3	3	5	5	3	1	7	5
	01 10 00 10	5	3	5	3	5	1	7	3
	01 11 10 10	3	3	5	5	3	1	7	5
	01 11 01 10	5	3	5	3	5	1	7	3
	01 11 00 00	5	5	3	3	3	1	7	5
	01 11 00 11	3	5	3	5	5	1	7	3
Центр	10 00 11 01	4	4	4	4	4	8	0	4
	00 00 11 01	3	3	5	5	5	7	1	3
	11 00 11 01	5	3	5	3	3	7	1	5
	10 10 11 01	5	5	3	3	5	7	1	3
	10 01 11 01	3	5	3	5	3	7	1	5
	10 00 01 01	5	5	3	3	5	7	1	3
	10 00 10 01	3	5	3	5	3	7	1	5
	10 00 11 11	3	3	5	5	5	7	1	3
	10 00 11 00	5	3	5	3	3	7	1	5
Центр	00 10 01 11	4	4	4	4	8	4	4	0
	10 10 01 11	5	5	3	3	7	5	3	1
	01 10 01 11	5	3	5	3	7	3	5	1
	00 00 01 11	3	3	5	5	7	5	3	1
	00 11 01 11	3	5	3	5	7	3	5	1
	00 10 11 11	3	3	5	5	7	5	3	1
	00 10 00 11	3	5	3	5	7	3	5	1
	00 10 01 01	5	5	3	3	7	5	3	1
	00 10 01 10	5	3	5	3	7	3	5	1

Таблиця Д.17

Значення $f_{per}^{ud}(i,t)$ для ФКВДвп з СКК-2

t	Сигнальна точка							
	0	1	2	3	4	5	6	7
3	24	24	24	24	24	24	24	24
4	6	6	6	6	6	6	6	6
5	24	24	24	24	24	24	24	24
6	0	0	0	0	0	0	0	0
7	8	8	8	8	8	8	8	8
8	1	1	1	1	1	1	1	1

Значення $P_{ud}\left(FCDRec, p_0\right)$ для різних p_0 наведено в таблиці Д.18.

Таблиця Д.18

Імовірність невиявленої помилки для ФКВДвп з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{ud}\left(FCDRec, p_0\right)$	$1.47\cdot10^{-2}$	$2.29\cdot10^{-5}$	$2.39\cdot10^{-8}$	$2.4\cdot10^{-11}$	$2.4\cdot10^{-14}$	$2.4\cdot10^{-17}$

Імовірність виправлення помилок $P_{EC}\left(FCDRec, p_0\right)$ визначається за (3.29). З урахуванням того, що цей ФКВДвп з СКК-2 виправляє тільки помилки одиничної ваги, $f_{per}^{EC}\left(i,t\right)=\begin{cases}8, \ если \ t=1,\\ 0, \ если \ t\neq 1.\end{cases}$ Результати обчислення $P_{EC}\left(FCDRec, p_0\right)$ для різних p_0 представлено в таблиці Д.19.

Таблиця Д.19

Імовірність виправлення помилки для ФКВДвп з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{EC}\left(FCDRec, p_0\right)$	0.383	$7.46\cdot10^{-2}$	$7.94\cdot10^{-3}$	$7.99\cdot10^{-4}$	$8\cdot10^{-5}$	$8\cdot10^{-6}$

Енергетичний виграш у результаті застосування ФКВДвп з СКК-2 за оптимального некогерентного прийому двійкових символів наведено в таблиці Д.20.

Таблиця Д.20

Енергетичний виграш ФКВДвп з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\Delta P\left(FCDRec, p_0\right)$, дБ	4.401	4.524	4.608	4.652	4.677	4.694

Значення залишкової ймовірності помилкового прийому в результаті застосування ФКВДвп з СКК-2 представлено в таблиці Д.21.

Таблиця Д.21

Залишкова ймовірність помилкового прийому ФКВДвп з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{res}\left(FCDRec, p_0\right)$	$1.78\cdot10^{-2}$	$2.29\cdot10^{-5}$	$2.39\cdot10^{-8}$	$2.40\cdot10^{-11}$	$2.40\cdot10^{-14}$	$2.40\cdot10^{-17}$

Визначені за (Д.1) значення динамічної складової втрати швидкості внаслідок

перезапитів для ФКВДвп з СКК-2 представлено в таблиці Д.22.

Таблиця Д.22

Динамічна складова втрати швидкості ФКВДвп з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$v_2\left(FCDRec, p_0\right)$	0.828	0.997	0.99997	$1-2.8\cdot10^{-7}$	$1-2.8\cdot10^{-9}$	$1-2.8\cdot10^{-11}$

Д.1.4. Факторіальне кодування з відновленням даних за перестановкою з сигнально-кодовою конструкцією другого типу

Для ФКВД в режимі виявлення помилок, який використовує СКК-2 з таблиці Д.15, кількість $f_{per}^{ud}\left(i,2t\right)$ помилок ваги $2t$, що призводять до помилкового декодування, для кожної сигнальної точки i наведено в таблиці Д.23.

Таблиця Д.23

Значення $f_{per}^{ud}\left(i,2t\right)$ для ФКВД з СКК-2

t	сигнальна точка							
	0	1	2	3	4	5	6	7
1	0	0	0	0	0	0	0	0
2	6	6	6	6	6	6	6	6
3	0	0	0	0	0	0	0	0
4	1	1	1	1	1	1	1	1

Як можна бачити, розподіл кількості $f_{per}^{ud}\left(i,2t\right)$ помилок ваги $2t$, що призводять до помилкового декодування ФКВД в режимі виявлення помилок з СКК-2, не залежить від сигнальної точки.

Результати обчислення $P_{ud}\left(FCDR, p_0\right)$ для ФКВД з СКК-2 для різних p_0 представлено в таблиці Д.24.

Таблиця Д.24

Імовірність невиявленої помилки для ФКВД з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{ud}\left(FCDR, p_0\right)$	$3.94\cdot10^{-4}$	$5.76\cdot10^{-8}$	$5.98\cdot10^{-12}$	$6\cdot10^{-16}$	$6\cdot10^{-20}$	$6\cdot10^{-24}$

Значення енергетичного виграшу в результаті застосування ФКВД з СКК-2 за оптимального некогерентного прийому двійкових символів представлено в таблиці Д.25.

Таблиця Д.25

Енергетичний виграш ФКВД з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\Delta P\left(FCDR, p_0\right)$, дБ	6.628	6.379	6.256	6.194	6.158	6.134

Значення залишкової ймовірності помилкового прийому в результаті застосування ФКВД з СКК-2 представлено в таблиці Д.26.

Таблиця Д.26

Залишкова ймовірність помилкового прийому ФКВД з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{res}\left(FCDR, p_0\right)$	$9.14\cdot10^{-4}$	$6.25\cdot10^{-8}$	$6.02\cdot10^{-12}$	$6.00\cdot10^{-16}$	$6.00\cdot10^{-20}$	$6.00\cdot10^{-24}$

Значення динамічної складової втрати швидкості внаслідок перезапитів $\nu_2\left(FCDR, p_0\right) = 1 - P_{req}\left(FCDR, p_0\right) = Q + P_{ud}\left(FCDR, p_0\right)$ наведено в таблиці Д.27.

Таблиця Д.27

Динамічна складова втрати швидкості для ФКВД з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\nu_2\left(FCDR, p_0\right)$	0.43	0.923	0.992	0.9992	0.99992	0.999992

Д.1.5. Факторіальне кодування з відновленням даних і виправленням помилок з розширеною сигнально-кодовою конструкцією другого типу

Приймемо, як і в попередньому прикладі ФКВДвп з СКК-2, $M = 4$ і $d_{\min} = 4$. Визначимо, чи існує СКК, що забезпечує $d_{\min} = 4$ для $M = 4$ і сигнальних векторів, кількість яких перевищує 8.

У таблиці Д.28 представлено СКК-2 з 12 сигнальних векторів з $d_{\min} = 4$.

Цю СКК побудовано наступним чином:

1) у якості першого сигнального вектора обрано представлену в двійковому вигляді тривіальну перестановку $\{0;1;2;3\}$;
2) сформовані $f_{per}\left(2\right) = 4$ вектори, віддалених від першого сигнального на відстань $d = 2$: 01 00 10 11, 10 01 00 11, 00 11 10 01, 00 01 11 10,

3) для кожного з отриманих векторів сформовано ще по 3 вектори, віддалені від них на відстань $d=2$. Два з них збігаються між собою, залишається множина з 10 векторів, що утворюють сигнальні вектори;
4) останнім сигнальним вектором є вектор, віддалений від першого сигнального вектора на відстань $d=8$.

Таблиця Д.28

СКК-2 для ФКВДвп при $M=4$

СКК	сигнальні точки
00 01 10 11	0
11 00 10 01	19
01 10 00 11	8
01 00 11 10	7
11 01 00 10	20
10 11 00 01	16
10 00 01 11	12
01 11 10 00	11
00 10 11 01	3
10 01 11 00	15
00 11 01 10	4
11 10 01 00	23

Зауважимо, що сигнальні точки для СКК з таблиці Д.28 розташовані на числовій осі парами: 0, 3-4, 7-8, 11-12, 15-16, 19-20, 23. Таким чином, сусідні вектори з відстанню Евкліда $D_{i,i+1}=1$ можуть мати відстань Хеммінга $d_{i,i+1}=4$.

Зазначимо також, що вектори, які не увійшли в СКК з таблиці Д.28, утворюють також СКК з $d_{\min}=4$.

Розглянемо ймовірнісні характеристики ФКВДвп для СКК-2 з таблиці Д.28.

Оскільки $d_{\min}=4$, цей код дозволяє виправити тільки будь-які помилки кратності $t=1$, а помилка не виявляється тоді і тільки тоді, коли кодове слово, що відповідає i-ому сигнальному вектору, буде перетворено завадою в комбінацію, для якої відстань Хеммінга до будь-якого іншого сигнального вектора не перевищує одиницю. Розподіл кількості $f_{per}^{ud}(i,t)$ помилок ваги t, що призводять до помилкового декодування, інваріантний відносно сигнального вектора i для наведеної в таблиці Д.29 СКК. Значення $f_{per}^{ud}(i,t)$ для нього наведено в таблиці Д.32

($f_{per}^{ud}(i,t)=0$ з $t\le 2$).

Таблиця Д.29

Значення $f_{per}^{ud}(i,t)$ для ФКВДвп з розширеною СКК-2

t	3	4	5	6	7	8
$f_{per}^{ud}(i,t)$	40	10	40	0	8	1

Значення $P_{ud}(FCDRec, p_0)$ для різних p_0 представлені в таблиці Д.30.

Таблиця Д.30

Імовірність невиявленої помилки для ФКВДвп з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{ud}(FCDRec, p_0)$	$2.46\cdot10^{-2}$	$3.81\cdot10^{-5}$	$3.98\cdot10^{-8}$	$4.00\cdot10^{-11}$	$4.00\cdot10^{-14}$	$4.00\cdot10^{-17}$

Оскільки код виправляє тільки помилки одиничної ваги, $f_{per}^{EC}(i,t)=\begin{cases}8, & если\ t=1,\\ 0, & если\ t\ne 1.\end{cases}$ Значення ймовірності виправлення помилок $P_{EC}(FCDRec, p_0)$ за (3.29) для різних p_0 збігаються зі значеннями з таблиці Д.19.

Значення енергетичного виграшу в результаті застосування ФКВДвп з розширеною СКК-2 з таблиці Д.25 за оптимального некогерентного прийому двійкових символів представлено в таблиці Д.31.

Таблиця Д.31

Енергетичний виграш ФКВДвп з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\Delta P(FCDRec, p_0)$, дБ	4.075	4.392	4.527	4.593	4.632	4.657

Значення залишкової ймовірності помилкового прийому в результаті застосування ФКВДвп з розширеною СКК-2 представлено в таблиці Д.32.

Таблиця Д.32

Залишкова ймовірність помилкового прийому ФКВДвп з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{res}(FCDRec, p_0)$	$2.93\cdot10^{-2}$	$3.82\cdot10^{-5}$	$3.98\cdot10^{-8}$	$4.00\cdot10^{-11}$	$4.00\cdot10^{-14}$	$4.00\cdot10^{-17}$

Визначені за (Д.1) значення динамічної складової втрати швидкості внаслідок перезапитів для ФКВДвп з розширеною СКК-2 представлено в таблиці Д.33.

Таблиця Д.33

Динамічна складова втрати швидкості ФКВДвп з СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$v_2\left(FCDRec, p_0\right)$	0.838	0.997	0.99997	$1-2.8\cdot10^{-7}$	$1-2.8\cdot10^{-9}$	$1-2.8\cdot10^{-11}$

Д.1.6. Факторіальне кодування з відновленням даних за перестановкою з розширеною сигнально-кодовою конструкцією другого типу

Для ФКВД в режимі виявлення помилок, який використовує розширену СКК-2 з таблиці Д.28, кількість $f_{per}^{ud}\left(i,2t\right)$ помилок ваги $2t$, що призводять до помилкового декодування, для кожної сигнальної точки i наведено в таблиці Д.34. Розподіл кількості $f_{per}^{ud}\left(i,2t\right)$ помилок ФКВД у режимі виявлення помилок з наведеної в таблиці Д.28 СКК-2, інваріантний відносно сигнального вектора i.

Таблиця Д.34

Значення $f_{per}^{ud}\left(i,2t\right)$ для ФКВД з розширеною СКК-2

t	1	2	3	4
$f_{per}^{ud}\left(i,2t\right)$	0	10	0	1

Результати обчислення $P_{ud}\left(FCDR, p_0\right)$ для ФКВД з розширеною СКК-2 для різних p_0 представлено в таблиці Д.35.

Таблиця Д.35

Імовірність невиявленої помилки для ФКВД з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{ud}\left(FCDR, p_0\right)$	$6.56\cdot10^{-4}$	$9.61\cdot10^{-8}$	$9.96\cdot10^{-12}$	$1.00\cdot10^{-15}$	$1.00\cdot10^{-19}$	$1.00\cdot10^{-23}$

Значення енергетичного виграшу в результаті застосування ФКВД з розширеною СКК-2 за оптимального некогерентного прийому двійкових символів представлено в таблиці Д.36.

Таблиця Д.36

Енергетичний виграш ФКВД з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\Delta P\left(FCDR, p_0\right)$, дБ	6.318	6.246	6.170	6.131	6.108	6.092

Значення залишкової ймовірності помилкового прийому в результаті застосування ФКВД з розширеною СКК-2 представлено в таблиці Д.37.

Таблиця Д.37

Залишкова ймовірність помилкового прийому ФКВД з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$P_{res}\left(FCDR, p_0\right)$	$1.52\cdot10^{-3}$	$1.04\cdot10^{-7}$	$1.00\cdot10^{-11}$	$1.00\cdot10^{-15}$	$1.00\cdot10^{-19}$	$1.00\cdot10^{-23}$

Значення динамічної складової втрати швидкості внаслідок перезапитів $\nu_2\left(FCDR, p_0\right) = 1 - P_{req}\left(FCDR, p_0\right) = Q + P_{ud}\left(FCDR, p_0\right)$ наведено в таблиці Д.38.

Таблиця Д.38

Динамічна складова втрати швидкості для ФКВД з розширеною СКК-2

p_0	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}
$\nu_2\left(FCDR, p_0\right)$	0.431	0.923	0.992	0.9992	0.99992	0.999992

Д.2. Порівняльна оцінка реалізацій факторіальних кодів з відновленням даних і виправленням помилок

Д.2.1. Порівняння факторіальних кодів з відновленням даних і виправленням помилок з сигнально-кодовими конструкціями першого і другого типів

Зведемо отримані вище результати і представимо їх графічно. На рис. Д.2 показано графіки залежностей імовірностей невиявленої помилки від імовірності бітової помилки p_0 для розглянутих кодів: ФКВДвп з СКК-1 (FCDRec-1) і СКК-2 (FCDRec-2), а також ФКВД з СКК-1 (FCDR-1) і СКК-2 (FCDR-2).

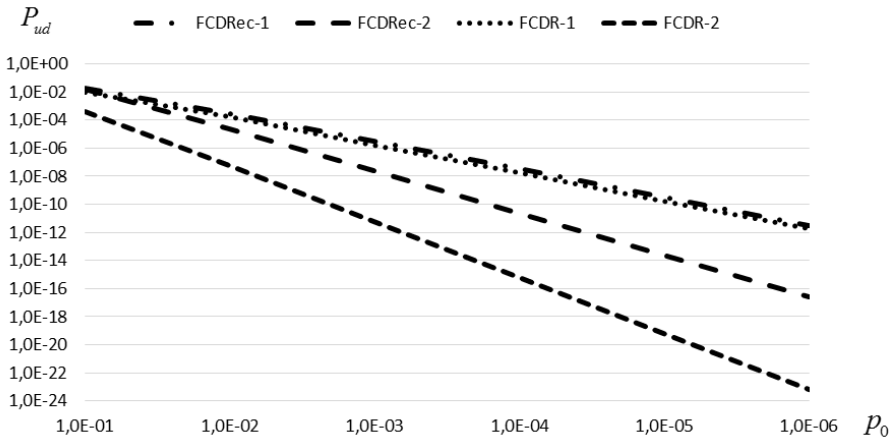


Рис. Д.2. Графіки залежностей імовірностей невиявленої помилки від імовірності бітової помилки

На рис. Д.3 для цих же кодів показано графіки залежностей енергетичних виграшів за оптимального некогерентного прийому двійкових символів від імовірності бітової помилки p_0.

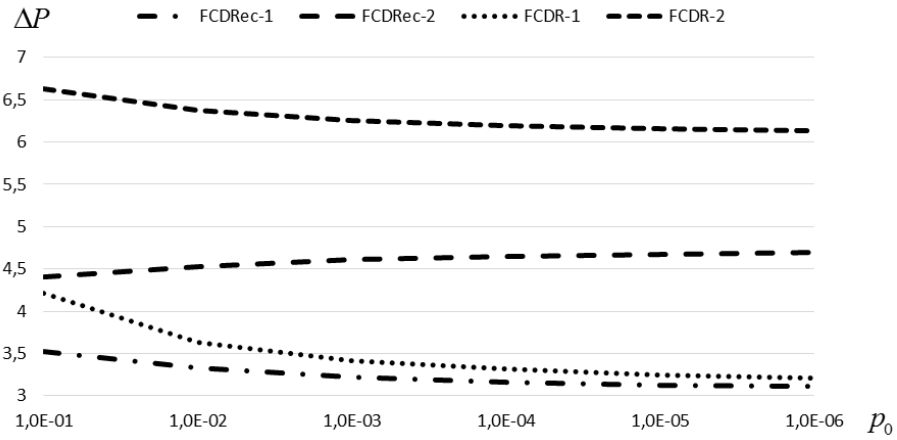


Рис. Д.3. Графіки залежностей енергетичних виграшів від імовірності бітової помилки

Графіки залишкових імовірностей помилкового прийому в результаті застосування розглянутих кодів ФКВДвп і ФКВД з СКК-1 і СКК-2 у залежності від імовірності бітової помилки p_0 представлено на рис. Д.4.

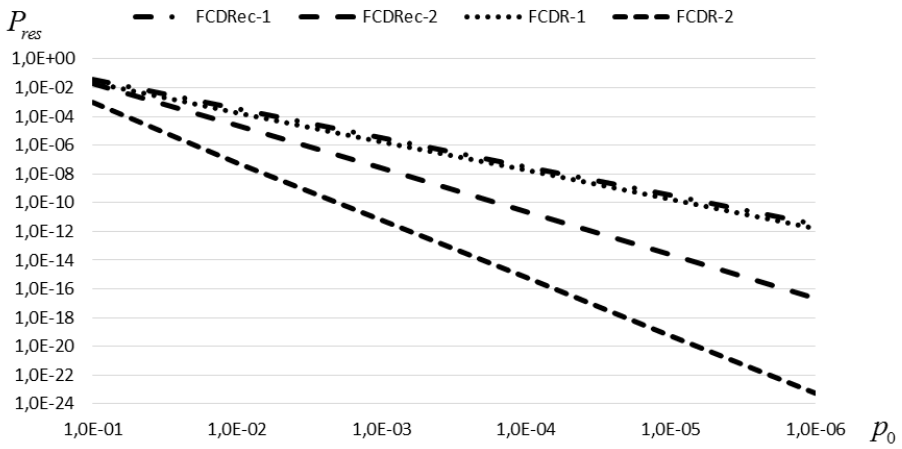


Рис. Д.4. Графіки залежностей залишкових ймовірностей помилкового прийому від імовірності бітової помилки

На рис. Д.5 для цих кодів показано графіки залежностей величини $1-\nu_2$, яка показує, наскільки близько динамічна складова втрати швидкості наближається до свого максимального значення, від ймовірності бітової помилки p_0.

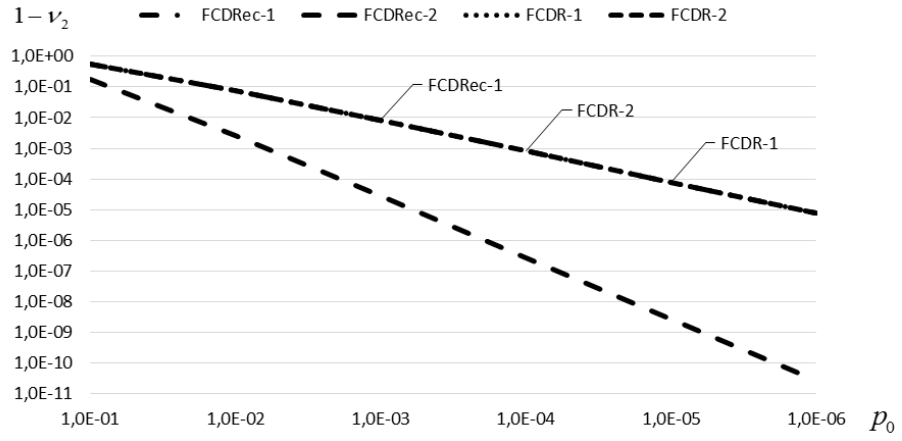


Рис. Д.5. Графіки залежностей величини $1-\nu_2$ від імовірності бітової помилки

З представлених графіків випливає, що найбільшу ймовірність невиявленої помилки і найменший енергетичний виграш з розглянутих кодів має ФКВДвп з СКК-1. Практично в два рази ця ймовірність менша для ФКВД з СКК-1. Водночас динамічна складова втрати швидкості для ФКВДвп і ФКВД з СКК-1 несуттєво розрізняються (наприклад, за ймовірності бітової помилки $p_0 = 0.1$ відмінність

становить $1.27\cdot10^{-2}$ (менше 3%) і зменшується зі зменшенням p_0). Тому в цьому випадку під час порівняння ФКВДвп з СКК-1 і ФКВД з СКК-1 перевагу слід віддати ФКВД в режимі виявлення помилок. Разом з тим з цього поки не випливає висновок в загальному випадку про меншу ефективність ФКВДвп у порівнянні з ФКВД для СКК першого типу.

Найменшу ймовірність невиявленої помилки і найбільший енергетичний виграш з розглянутих кодів має ФКВД з СКК-2 в режимі виявлення помилок. Відношення ймовірностей невиявленої помилки для ФКВД з СКК-2 і СКК-1 пропорційно величині $0.1(p_0)^{-2}$ і для $p_0=0.1$ становить $2.4\cdot10^{1}$, а для $p_0=0.001$ – $2.9\cdot10^{5}$ (різниця в енергетичному виграші для $p_0=0.1$ становить $\Delta P=2.42$ дБ, а для $p_0=0.001$ – $\Delta P=2.84$ дБ), вказуючи на більшу ефективність СКК-2 для ФКВД.

Використання ж СКК-2 для ФКВДвп збільшує в порівнянні з ФКВД ймовірність невиявленої помилки пропорційно величині $(p_0)^{-1}$. Так, для $p_0=0.1$ відношення ймовірностей невиявленої помилки для ФКВДвп з СКК-2 і ФКВД з СКК-2 становить $3.7\cdot10^{1}$, а для $p_0=0.001$ – $4\cdot10^{3}$; різниця в енергетичному виграші для $p_0=0.1$ становить $\Delta P=2.23$ дБ, а для $p_0=0.001$ – $\Delta P=1.65$дБ. Разом з тим динамічна складова втрати швидкості для ФКВД з СКК-2 практично не відрізняється від динамічної складової втрати швидкості для ФКВДвп і ФКВД з СКК-1 (наприклад, за ймовірності бітової помилки $p_0=0.1$ різниця між ФКВД з СКК-1 становить $9.07\cdot10^{-3}$ (2,06%) і зменшується зі зменшенням p_0), у той час, як динамічна складова втрати швидкості для ФКВДвп з СКК-2 може значно перевершувати динамічну складову втрати швидкості для ФКВД з СКК-2 (наприклад, за ймовірності бітової помилки $p_0=0.1$ різниця цих показників для ФКВДвп і ФКВД з СКК-2 становить $0.828-0.431\approx0.4$ (понад 92%) і збільшується зі збільшенням p_0). Відношення значень для ФКВДвп і ФКВД при цьому має порядок p_0: для $p_0=10^{-1}$ маємо $\dfrac{1-\nu_2(DCDRec-2)}{1-\nu_2(DCDR-2)}\approx3\cdot10^{-1}$, для $p_0=10^{-3}$ –

$\frac{1-\nu_2(DCDRec-2)}{1-\nu_2(DCDR-2)} \approx 3.5\cdot 10^{-3}$, для $p_0 = 10^{-5}$ – $\frac{1-\nu_2(DCDRec-2)}{1-\nu_2(DCDR-2)} \approx 3.5\cdot 10^{-5}$.

Таким чином, для ФКВДвп і ФКВД з СКК-2 стає більше помітний ефект обміну достовірності передавання на пропускну здатність, пояснений вище.

Застосування СКК-2 замість СКК-1 для ФКВДвп дозволяє збільшити динамічну складову втрати швидкості до 82,9% для $p_0 = 0.1$ (на $8\cdot 10^{-4}$ % для $p_0 = 10^{-6}$), водночас імовірність невиявленої помилки зменшується в 1,23 рази (в $1.35\cdot 10^5$ разів для $p_0 = 10^{-6}$).

Таким чином, наведений аналіз однозначно вказує, що для розглянутих кодів ФКВД (вп) з СКК-1 і СКК-2 більшою ефективністю володіють ФКВД (вп) з СКК-2. Разом з тим з цього ще не випливає висновок в загальному випадку про меншу ефективність СКК першого типу в порівнянні з СКК другого типу.

У будь-якому випадку, принцип побудови СКК грає одну з найбільш важливих ролей під час проектування ФКВД і ФКВДвп.

Д.2.2. Порівняння факторіальних кодів з відновленням даних і виправленням помилок з сигнально-кодовою конструкцією другого типу і розширеною сигнально-кодовою конструкцією другого типу

На рис. Д.6 показано графіки залежностей імовірностей невиявленої помилки від імовірності бітової помилки p_0 для наступних кодів: ФКВДвп з СКК-2 (FCDRec-2) і розширеною СКК-2 (FCDRec-2ext), а також ФКВД з СКК-2 (FCDR-2) і розширеною СКК-2 (FCDR-2ext).

На рис. Д.7 для цих же кодів показано графіки залежностей енергетичних виграшів за оптимального некогерентного прийому двійкових символів від імовірності бітової помилки p_0.

Графіки залишкових імовірностей помилкового прийому в результаті застосування кодів ФКВДвп і ФКВД з СКК-2 і розширеною СКК-2 в залежності від імовірності бітової помилки p_0 представлено на рис. Д.8.

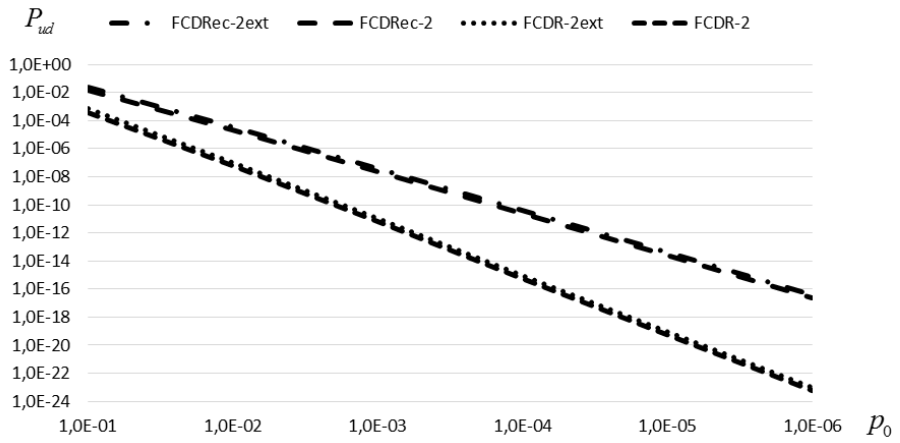


Рис. Д.6. Графіки залежностей імовірностей невиявленої помилки від імовірності бітової помилки

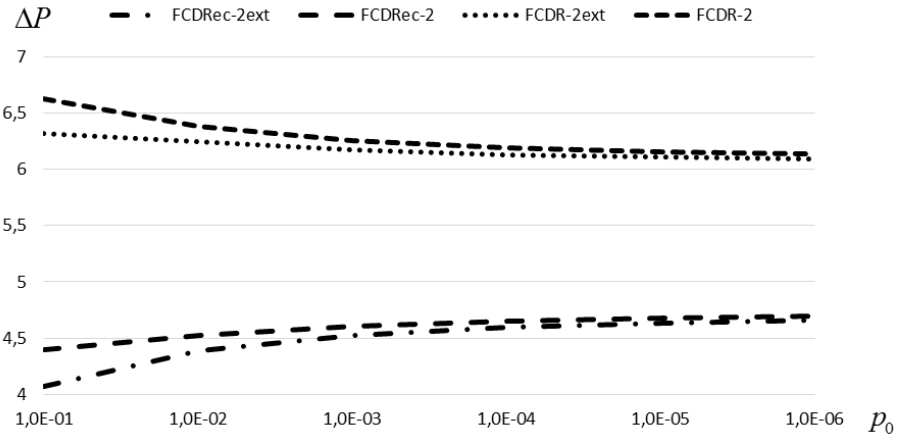


Рис. Д.7. Графіки залежностей енергетичних виграшів від імовірності бітової помилки

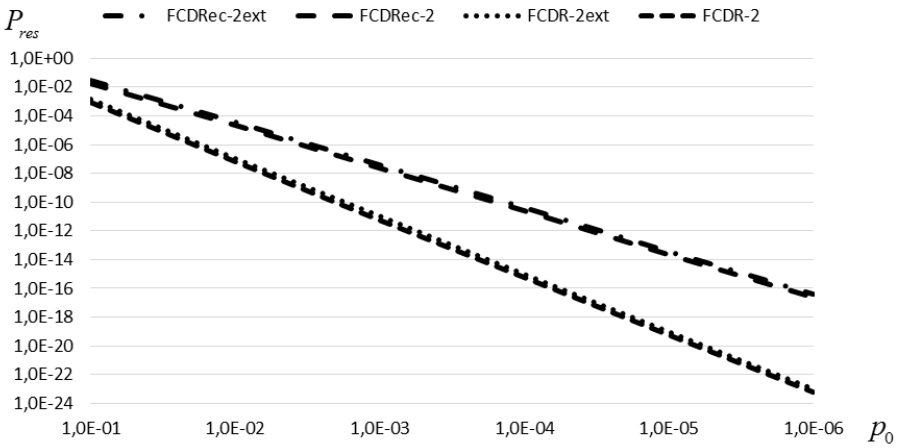


Рис. Д.8. Графіки залежностей залишкових імовірностей помилкового прийому від імовірності бітової помилки

На рис. Д.9 для цих кодів показано графіки залежностей величини $1-\nu_2$ від імовірності бітової помилки p_0.

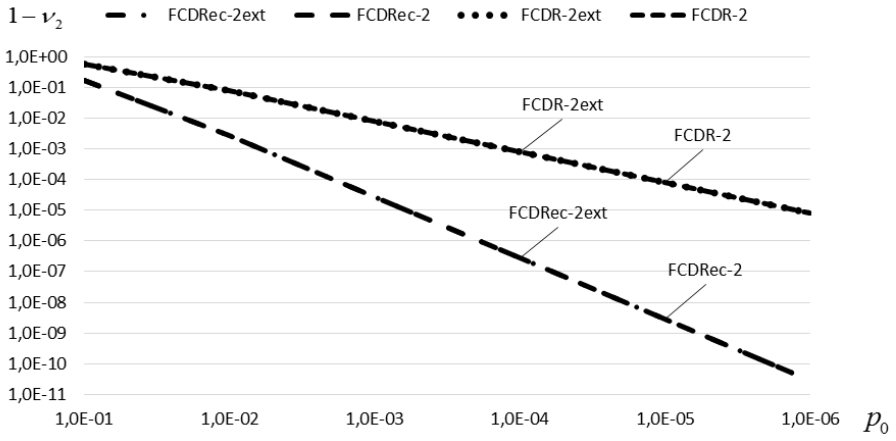


Рис. Д.9. Графіки залежностей величини $1-\nu_2$ від імовірності бітової помилки

З представлених графіків випливає, що стійкість ФКВД(вп) з розширеною СКК-2 з 12 сигнальними векторами поступається завадостійкості ФКВД(вп) з СКК-2 з 8 сигнальними векторами. Так, для ФКВДвп:

– імовірність помилкового декодування, а також залишкова ймовірність помилкового прийому збільшується в 1,67 рази;
– енергетичний виграш зменшується від 0,326 дБ для $p_0 = 0.1$ до 0,038 дБ для $p_0 = 10^{-6}$;

для ФКВД:

– імовірність помилкового декодування, а також залишкова ймовірність помилкового прийому збільшується в 1,67 рази;
– енергетичний виграш зменшується від 0,310 дБ для $p_0 = 0.1$ до 0,041 дБ для $p_0 = 10^{-6}$.

Водночас динамічна складова втрати швидкості для ФКВДвп з розширеною СКК-2 практично не відрізняється від динамічної складової втрати швидкості для ФКВДвп з СКК-2 (наприклад, за ймовірності бітової помилки $p_0 = 0.1$ відносна величина різниці цих величин становить 1,17% (абсолютна – $9.83 \cdot 10^{-3}$) і

зменшується зі зменшенням p_0, досягаючи для $p_0 = 10^{-3}$ значення $1.59 \cdot 10^{-6}$% (абсолютне значення – $1.59 \cdot 10^{-8}$)). Аналогічно динамічна складова втрати швидкості для ФКВД з розширеною СКК-2 практично не відрізняється від динамічної складової втрати швидкості для ФКВД з СКК-2 (наприклад, за ймовірності бітової помилки $p_0 = 0.1$ відносна величина різниці цих величин становить $6.09 \cdot 10^{-2}$% (абсолютна – $2.62 \cdot 10^{-4}$) і зменшується зі зменшенням p_0, досягаючи для $p_0 = 10^{-3}$ значення $4.02 \cdot 10^{-10}$% (абсолютне значення – $3.98 \cdot 10^{-12}$)).

Таким чином, для ФКВД і ФКВДвп розширена СКК-2 з 12 сигнальних векторів програє в завадостійкості в порівнянні з СКК-2 з 8 сигнальних векторів, зберігаючи динамічну складову втрати швидкості.

Розглянемо додатково для кожного з кодів залежність відносної швидкості передавання $\nu_0 = \nu_1 \cdot \nu_2$ від імовірності бітової помилки p_0. Графіки цих залежностей наведено на рис. Д.10. Для СКК-2 з 8 сигнальних векторів швидкість коду $\nu_1 = 3/8$, а для розширеної СКК-2 з 12 сигнальних векторів швидкість коду $\nu_1 = \dfrac{\log_2 12}{8}$.

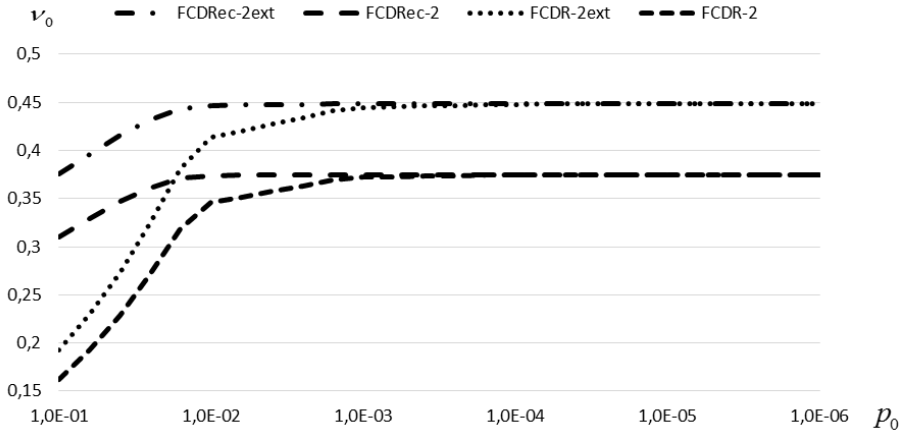


Рис. Д.10. Графіки залежностей відносної швидкості передавання від імовірності бітової помилки

Аналіз графіків рис. Д.10 підтверджує, що збільшення числа сигнальних векторів збільшує відносну швидкість передавання.

Рис. Д.10 також показує, що:

- відносна швидкість передавання для ФКВДвп не поступається, а в деяких випадках істотно перевершує відносну швидкість передавання для ФКВД з такою ж СКК-2 (наприклад, за ймовірності бітової помилки $p_0 = 0.1$ різниця цих показників для ФКВДвп і ФКВД з СКК-2 становить $0.310 - 0.162 \approx 0.149$, що відповідає більше 92% (для ФКВДвп і ФКВД з розширеною СКК-2 ця різниця дорівнює $0.375 - 0.193 \approx 0.182$, що відповідає більше 94%) і зменшується зі збільшенням p_0);
- у більшості випадків відносна швидкість передавання для представлених кодів з розширеною СКК-2 з 12 сигнальними векторами перевищує відносну швидкість передавання кодів з СКК-2 з 8 сигнальними векторами. Разом з тим існує діапазон значень p_0, для яких відносна швидкість передавання ФКВДвп з СКК-2 з 8 сигнальними векторами перевищує відносну швидкість передавання ФКВД з СКК-2 з 12 сигнальними векторами: $\nu_0\left(FCDRec-2, p_0\right) - \nu_0\left(FCDR-2ext, p_0\right) > 0$ для $p_0 \geq 2.38 \cdot 10^{-2}$;
- збільшення числа сигнальних векторів з 8 до 12 для ФКВД і ФКВДвп збільшує відносну швидкість передавання коду на величину від 19,5% для $p_0 = 10^{-6}$ до 20,9% (для ФКВДвп) і 19,6% (для ФКВД) для $p_0 = 0.1$, за цих обставин імовірність невиявленої помилки збільшується в 1,67 рази.

Таким чином, у процесі проведеного дослідження показано можливість факторіального кодування інформації, яке поєднує функції виправлення і виявлення помилок, що виникають у каналі зв'язку під час передавання повідомлення. Таке поєднання дозволяє підвищити динамічну складову втрати швидкості і, як наслідок, відносну швидкість передавання, в порівнянні факторіальним кодуванням, що виявляє помилки, за рахунок зниження завадостійкості коду.

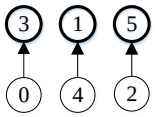
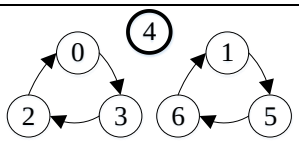
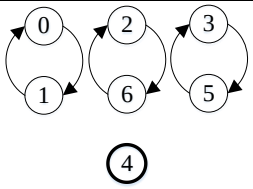
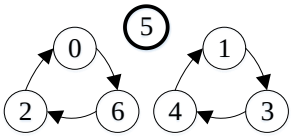
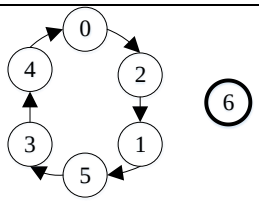
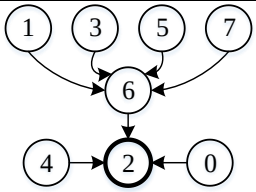
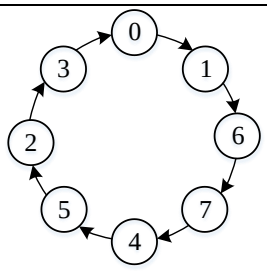
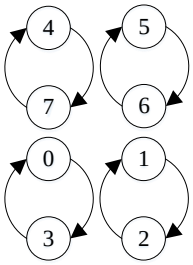
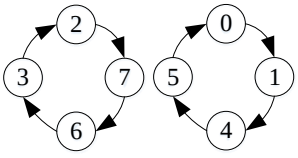
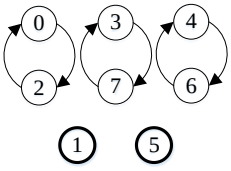
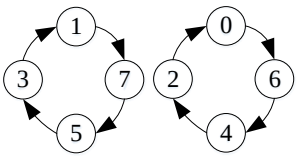
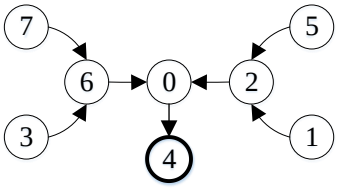
Встановлено також, що показники завадостійкості факторіального кодування з відновленням даних, а також з відновленням даних і виправленням помилок не є інваріантними відносно вибору сигнально-кодової конструкції, якщо в якості сигнальних векторів використовується деяка власна підмножина множини векторів всіх можливих перестановок порядку M.

Додаток Е

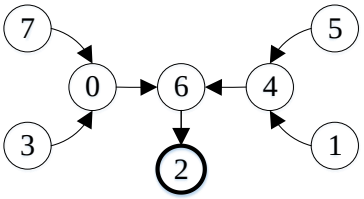
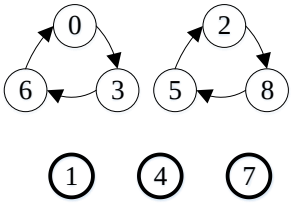
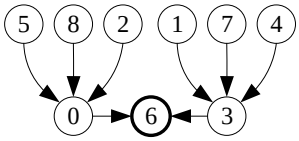
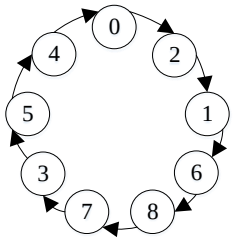
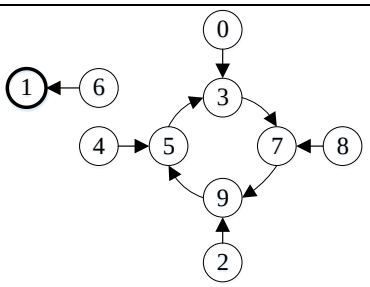
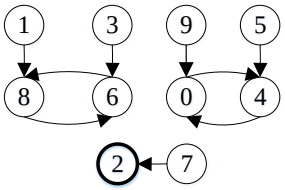
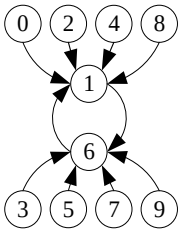
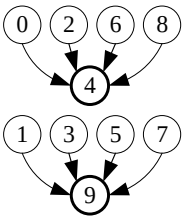
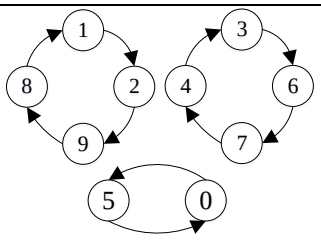
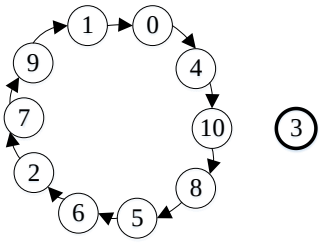
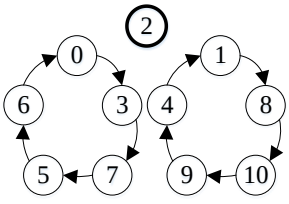
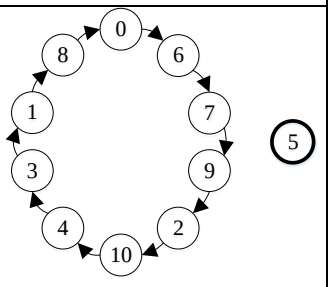
Топологія графів станів лінійного конгруентного генератора

Таблиця Е.1

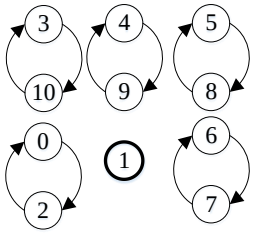
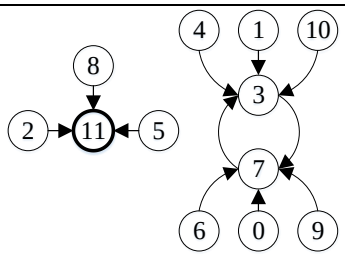
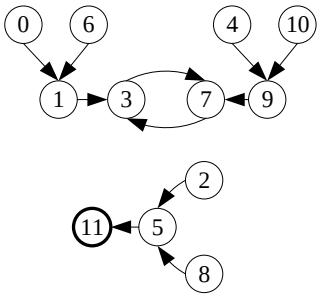
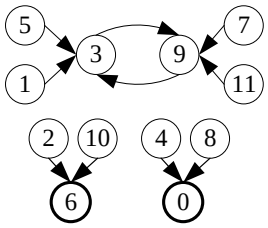
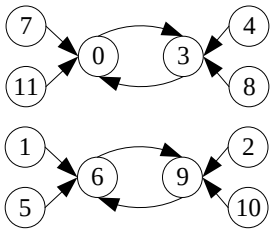
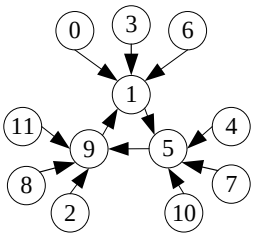
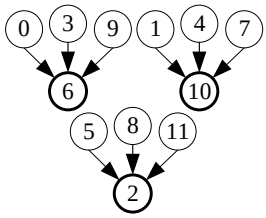
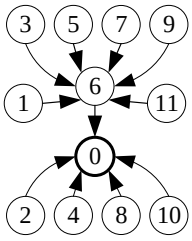
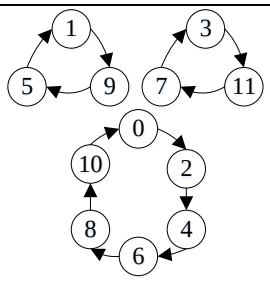
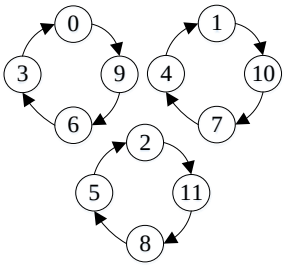
Орієнтовані графи станів ЛКГ для деяких його параметрів

Параметри ЛКГ			**Граф станів**	**Параметри ЛКГ**			**Граф станів**
M	*K*	*C*		*M*	*K*	*C*	
6	4	3		7	2	3	
7	6	1		7	4	6	
7	3	2		8	4	2	
8	5	1		8	7	3	
8	3	1		8	7	2	
8	1	6		8	6	4	

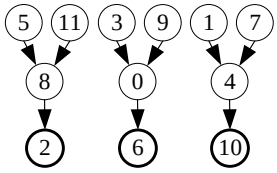
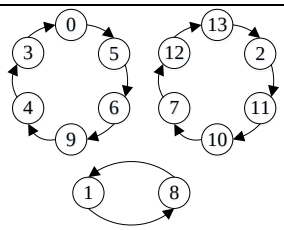
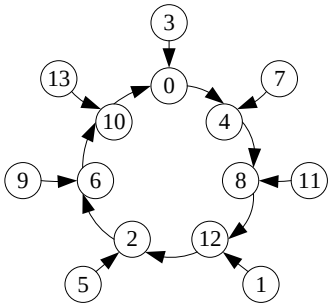
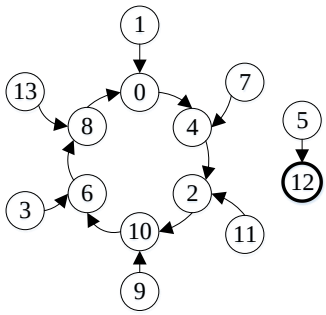
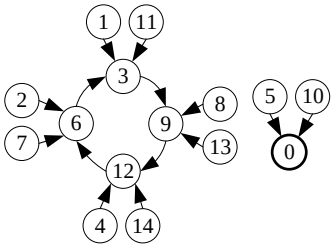
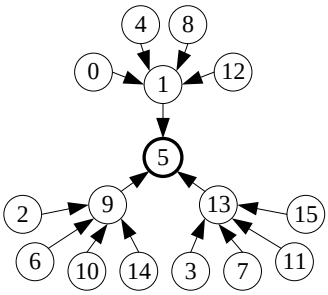
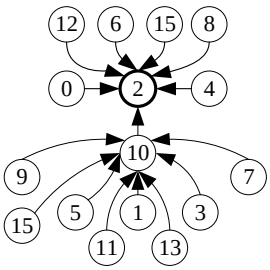
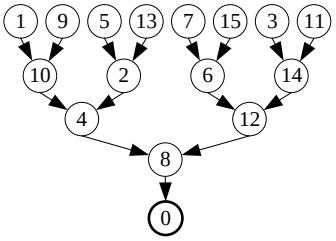
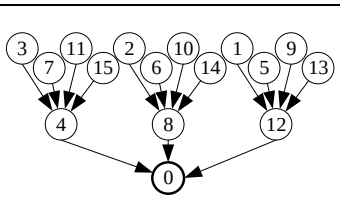
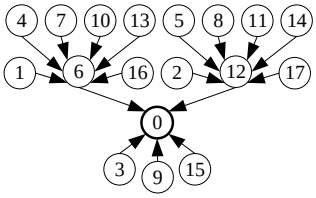
Продовження таблиці Е.1

Параметри ЛКГ			Граф станів	Параметри ЛКГ			Граф станів
M	*K*	*C*		*M*	*K*	*C*	
8	6	6		9	7	3	
9	6	6		9	4	2	
10	8	3		10	4	4	
10	5	1		10	5	4	
10	7	5		11	7	4	
11	5	3		11	2	6	

Продовження таблиці Е.1

Параметри ЛКГ			**Граф станів**	**Параметри ЛКГ**			**Граф станів**
M	*K*	*C*		*M*	*K*	*C*	
11	10	2		12	8	7	
12	2	1		12	3	0	
12	3	3		12	4	1	
12	4	6		12	6	0	
12	7	2		12	9	1	

Продовження таблиці Е.1

Параметри ЛКГ			**Граф станів**	**Параметри ЛКГ**			**Граф станів**
M	*K*	*C*		*M*	*K*	*C*	
12	10	6		14	3	5	
14	8	4		14	10	4	
15	3	0		16	4	1	
16	8	2		16	10	0	
16	12	0		18	6	0	

Таблиця Е.2

Топологія графів лінійного конгруентного генератора для $M \le 20$

Параметри ЛКГ			**Структура графа**
M	K	C	
M	1	0	MO_1
M	1	1	O_M
3	1	2	O_3
	2	C	$O_2 + O_1$
4	1	2	$2O_2$
		3	O_4
	2	C	T_{2^2}
	3	0, 2	$O_2 + 2O_1$
		1,3	$2O_2$
5	1	$C \ge 2$	O_5
	2, 3	C	$O_4 + O_1$
	4	C	$2O_2 + O_1$
6	1	2, 4	$2O_3$
		3	$3O_2$
		5	O_6
	2	C	$A_2 + A_1$ $\left(\text{или } T_{2^1} * O_2 + T_{2^1}\right)$
	3	0, 2, 4	$2E_3$ $\left(\text{или } 2T_{3^1}\right)$
		1, 3, 5	$E_3 * O_2$ $\left(\text{или } T_{3^1} * O_2\right)$
	4	0, 3	$3A_1$ $\left(\text{или } 3T_{2^1}\right)$
		1, 2, 4, 5	A_3 $\left(\text{или } T_{2^1} * O_3\right)$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
	5	0, 2, 4	$2O_2 + 2O_1$
		1, 3, 5	$3O_2$
7	1	$C \geq 2$	O_7
	2, 4	*C*	$2O_3 + O_1$
	3, 5	*C*	$O_6 + O_1$
	6	*C*	$3O_2 + O_1$
8	1	2, 6	$2O_4$
		3, 5, 7	O_8
		4	$4O_2$
	2, 6	*C*	T_{2^3}
	3	0, 2, 4, 6	$3O_2 + 2O_1$
		1, 3, 5, 7	$2O_4$
	4	*C*	$E_4 * A_1$ (или $T_{4^1} * T_{2^1}$)
	5	0, 4	$2O_2 + 4O_1$
		1, 3, 5, 7	O_8
		2, 6	$2O_4$
	7	0, 2, 4, 6	$3O_2 + 2O_1$
		1, 3, 5, 7	$4O_2$
9	1	2, 4, 5, 7, 8	O_9
		3, 6	$3O_3$
	2, 5	*C*	$O_6 + O_2 + O_1$
	3, 6	*C*	T_{3^2}
	4, 7	0, 3, 6	$2O_3 + 3O_1$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
		1, 2, 4, 5, 7, 8	O_9
	8	*C*	$4O_2 + O_1$
10	1	2, 4, 6, 8	$2O_5$
		3, 7, 9	O_{10}
		5	$5O_2$
	2, 8	*C*	$A_4 + A_1$ (или $T_{2^1} * O_4 + T_{2^1}$)
	3, 7	0, 2, 4, 6, 8	$2O_4 + 2O_1$
		1, 3, 5, 7, 9	$2O_4 + O_2$
	4	*C*	$2A_2 + A_1$ (или $2(T_{2^1} * O_2) + T_{2^1}$)
	5	0, 2, 4, 6, 8	$2E_5$ (или $2T_{5^1}$)
		1, 3, 5, 7, 9	$E_5 * O_2$ (или $T_{5^1} * O_2$)
	6	0, 5	$5O_2$
		1, 2, 3, 4, 6, 7, 8, 9	A_5 (или $T_{2^1} * O_5$)
	9	0, 2, 4, 6, 8	$4O_2 + 2O_1$
		1, 3, 5, 7, 9	$5O_2$
11	1	$C \geq 2$	O_{11}
	2, 6, 7, 8	*C*	$O_{10} + O_1$
	3, 4, 5, 9	*C*	$2O_5 + O_1$
	10	*C*	$5O_2 + O_1$
12	1	2, 10	$2O_6$
		3, 9	$3O_4$
		4, 8	$4O_3$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
		5, 7, 11	O_{12}
		6	$6O_2$
	2	*C*	$T_{2^2} * O_2 + T_{2^2}$
	3	0, 2, 4, 6, 8, 10	$E_3 * O_2 + 2E_3$ $\left(\text{или } T_{3^1} * O_2 + 2T_{3^1}\right)$
		1, 3, 5, 7, 9, 11	$2E_3 * O_2$ $\left(\text{или } 2\left(T_{3^1} * O_2\right)\right)$
	4	0, 3, 6, 9	$3E_4$ $\left(\text{или } 3T_{4^1}\right)$
		1, 2, 4, 5, 7, 8, 10, 11	D_3 $\left(\text{или } T_{4^1} * O_3\right)$
	5	0, 4, 8	$4O_2 + 4O_1$
		1, 3, 5, 7, 9, 11	$3O_4$
		2, 6, 10	$6O_2$
	6	*C*	$E_6 * A_1$ $\left(\text{или } T_{6^1} * T_{2^1}\right)$
	7	0, 6	$3O_2 + 6O_1$
		1, 2, 5, 7, 11	$2O_6$
		3, 9	$6O_2$
		4, 8, 10	$O_6 + 2O_3$
	8	*C*	$D_2 + D_1$ $\left(\text{или } T_{4^1} * O_2 + T_{4^1}\right)$
	9	0, 4, 8	$4E_3$ $\left(\text{или } 4T_{3^1}\right)$
		1, 3, 5, 7, 9, 11	$E_3 * O_4$ $\left(\text{или } T_{3^1} * O_4\right)$
		2, 6, 10	$2E_3 * O_2$ $\left(\text{или } 2\left(T_{3^1} * O_2\right)\right)$
	10	0, 3, 6	$3T_{2^2}$
		1, 2, 4, 5, 7, 10, 11	$T_{2^2} * O_3$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
	11	0, 2, 4, 6, 8, 10	$5O_2 + 2O_1$
		1, 3, 5, 7, 9, 11	$6O_2$
13	1	$C \geq 2$	O_{13}
	2, 6, 7, 11	*C*	$O_{12} + O_1$
	3, 9	*C*	$4O_3 + O_1$
	4, 10	*C*	$2O_6 + O_1$
	5, 8	*C*	$3O_4 + O_1$
	12	*C*	$6O_2 + O_1$
14	1	2, 4, 6, 8, 10, 12	$2O_7$
		3, 5, 9, 11, 13	O_{14}
		7	$7O_2$
	2, 4	*C*	$2A_3 + A_1 \ \left(\text{или } 2\left(T_{2^1} * O_3\right) + T_{2^1}\right)$
	3, 5	0, 2, 4, 6, 8, 10, 13	$2O_6 + 2O_1$
		1, 3, 5, 7, 9, 11, 13	$2O_6 + O_2$
	6	*C*	$3A_2 + A_1 \ \left(\text{или } 3\left(T_{2^1} * O_2\right) + T_{2^1}\right)$
	7	0, 2, 4, 6, 8, 10, 13	$2E_7 \ \left(\text{или } 2T_{7^1}\right)$
		1, 3, 5, 7, 9, 11, 13	$E_7 * O_2 \ \left(\text{или } T_{7^1} * O_2\right)$
	8	0, 7	$7A_1 \ \left(\text{или } 7T_{2^1}\right)$
		1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13	$A_7 \ \left(\text{или } T_{2^1} * O_7\right)$
	9, 11	0, 2, 4, 6, 8, 10, 12	$4O_3 + 2O_1$
		1, 3, 5,7, 9, 11, 13	$2O_6 + O_2$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
	10, 12	*C*	$A_6 + A_1$ (или $T_{2^1} * O_6 + T_{2^1}$)
	13	0, 2, 4, 6, 8, 10, 13	$6O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13	$7O_2$
15	1	2, 4, 7, 8, 11, 13, 14	O_{15}
		3, 6, 9, 12	$3O_5$
		5, 10	$5O_3$
	2, 8	*C*	$3O_4 + O_2 + O_1$
	3, 12	*C*	$E_3 * O_4 + E_3$ (или $T_{3^1} * O_4 + T_{3^1}$)
	4	0, 3, 6, 9, 12	$6O_2 + 3O_1$
		1, 2, 4, 5, 7, 8, 10, 11, 13, 14	$2O_6 + O_3$
	5	*C*	$E_5 * O_2 + E_5$ (или $T_{5^1} * O_2 + T_{5^1}$)
	6	0, 5, 10	$5E_3$ (или $5T_{3^1}$)
		1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14	$E_3 * O_5$ (или $T_{3^1} * O_5$)
	7, 13	0, 3, 6, 9, 12	$3O_4 + 3O_1$
		1, 2, 4, 5, 7, 8, 10, 11, 13, 14	$O_{12} + O_3$
	9	*C*	$2E_3 * O_2 + E_3$ (или $2(T_{3^1} * O_2) + T_{3^1}$)
	10	0, 3, 6, 9, 12	$3E_5$ (или $3T_{5^1}$)
		1, 2, 4, 5, 7, 8, 10, 11, 13, 14	$E_5 * O_3$ (или $T_{5^1} * O_3$)
	11	0, 5, 10	$5O_2 + 5O_1$
		1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14	$O_{10} + O_5$
	14	*C*	$7O_2 + O_1$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
16	1	2, 6, 10, 14	$2O_8$
		3, 5, 7, 9, 11, 13, 15	O_{16}
		4, 12	$4O_4$
		8	$8O_2$
	2, 6, 10, 14	*C*	T_{2^4}
	3, 11	0, 2, 4, 6, 8, 10, 12, 14	$2O_4 + 3O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13, 15	$2O_8$
	4, 12	*C*	T_{4^2}
	5, 13	0, 4, 8, 12	$2O_4 + 2O_2 + 4O_1$
		1, 3, 5, 7, 9, 11, 13, 15	O_{16}
		2, 6, 10, 14	$2O_8$
	7	0, 2, 4, 6, 8, 10, 12, 14	$7O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13, 15	$4O_4$
	8	*C*	$E_8 * A_1$ $\left(\text{или } T_{8^1} * T_{2^1}\right)$
	9	0, 8	$4O_2 + 8O_1$
		1, 3, 5, 7, 9, 11, 13, 15	O_{16}
		2, 6, 10, 14	O_{16}
		4, 12	$4O_4$
	15	0, 2, 4, 6, 8, 10, 12, 14	$7O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13, 15	$8O_2$
17	1	$C \geq 2$	O_{17}
	2, 8, 9, 15	*C*	$2O_8 + O_1$
	3, 5, 6, 7,	*C*	$O_{16} + O_1$

Продовження таблиці Е.2

Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
	10, 11, 12, 14		
	4, 13	*C*	$4O_4 + O_1$
	16	*C*	$8O_2 + O_1$
18	1	2, 4, 8, 10, 14, 16	$2O_9$
		3, 15	$3O_6$
		5, 7, 11, 13, 17	O_{18}
		6, 12	$6O_3$
		9	$9O_2$
	2, 14	*C*	$A_6 + A_2 + A_1$ $\left(\text{или } T_{2^1} * O_6 + T_{2^1} * O_2 + T_{2^1}\right)$
	3, 15	0, 2, 4, 6, 8, 10, 12, 14, 16	$2T_{3^2}$
		1, 3, 5, 7, 9, 11, 13, 15, 17	$T_{3^2} * O_2$
	4, 16	0, 3, 6, 9, 12, 15	$2A_3 + 3A_1$ $\left(\text{или } 2\left(T_{2^1} * O_3\right) + 3T_{2^1}\right)$
		1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17	A_9 $\left(\text{или } T_{2^1} * O_9\right)$
	5, 11	0, 2, 4, 6, 8, 10, 12, 14, 16	$2O_6 + 2O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13, 15, 17	$2O_6 + 3O_2$
	6, 12	*C*	$E_6 * E_3$ $\left(\text{или } T_{6^1} * T_{3^1}\right)$
	7, 13	0, 6, 12	$4O_3 + 6O_1$
		1, 5, 7, 11, 13, 17	O_{18}
		2, 4, 8, 10, 14, 16	$2O_9$
		3, 9, 15	$2O_6 + 3O_2$

Продовження таблиці Е.2

Параметри ЛКГ			Структура графа
M	*K*	*C*	
	8	*C*	$4A_2 + A_1 \left(\text{или } 4\left(T_{2^1} * O_2\right) + T_{2^1}\right)$
	9	0, 2, 4, 6, 8, 10, 12, 14, 16	$2E_9 \left(\text{или } 2T_{9^1}\right)$
		1, 3, 5, 7, 9, 11, 13, 15, 17	$E_9 * O_2 \left(\text{или } T_{9^1} * O_2\right)$
	10	0, 9	$9A_1 \left(\text{или } 9T_{2^1}\right)$
		1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17	$A_9 \left(\text{или } T_{2^1} * O_9\right)$
		3, 6, 12, 15	$3A_3 \left(\text{или } 3\left(T_{2^1} * O_3\right)\right)$
	17	0, 2, 4, 6, 8, 10, 12, 14, 16	$8O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13, 15, 17	$9O_2$
19	1	$C \geq 2$	O_{19}
	2, 3, 10, 13, 14, 15	*C*	$O_{18} + O_1$
	4, 5, 6, 9, 16, 17	*C*	$2O_9 + O_1$
	7, 11	*C*	$6O_3 + O_1$
	8, 12	*C*	$3O_6 + O_1$
	18	*C*	$9O_2 + O_1$
20	1	2, 4, 6, 10, 14, 18	$2O_{10}$
		3, 7, 9, 11, 13, 17, 19	O_{20}
		5, 15	$5O_4$
		8, 12, 16	$4O_5$
	2, 18	C	$T_{2^2} * O_4 + T_{2^2}$
	3, 7	0, 2, 4, 6, 8, 10, 12, 14, 16, 18	$4O_4 + O_2 + 2O_1$

Продовження таблиці Е.2

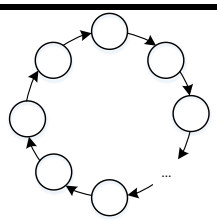
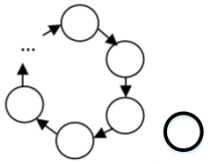
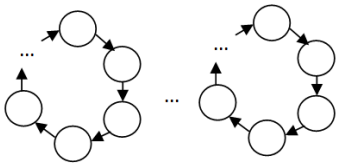
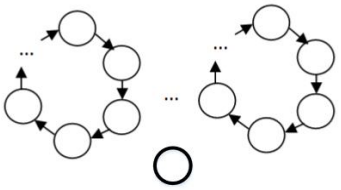
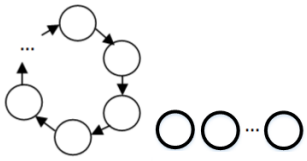
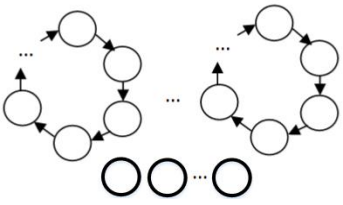
Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
		1, 3, 5, 7, 9, 11, 13, 15, 17, 19	$4O_4 + 2O_2$
	4	C	$2E_4 * O_2 + E_4 \ \left(\text{или } 2\left(T_{4^1} * O_2\right) + T_{4^1}\right)$
	5	0, 4, 8, 12, 16	$4E_5 \ \left(\text{или } 4T_{5^1}\right)$
		1, 3, 5, 7, 9, 11, 13, 15, 17, 19	$E_5 * O_4 \ \left(\text{или } T_{5^1} * O_4\right)$
		2, 6, 10, 14, 18	$2E_5 * O_2 \ \left(\text{или } 2\left(T_{5^1} * O_2\right)\right)$
	6	0, 5, 10, 15	$5T_{2^2}$
		1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19,	$T_{2^2} * O_5$
	8, 12	C	$E_4 * O_4 + E_4 \ \left(\text{или } T_{4^1} * O_4 + T_{4^1}\right)$
	9	0, 4, 8, 12, 16	$8O_2 + 4O_1$
		1, 3, 5, 7, 9, 11, 13, 15, 17, 19	$5O_4$
		2, 6, 10, 14, 18	$10O_2$
	10	C	$E_{10} * A_1 \ \left(\text{или } T_{10^1} * T_{2^1}\right)$
	11	0, 10	$5O_2 + 10O_1$
		1, 3, 7, 9, 11, 13, 17, 19	$2O_{10}$
		2, 4, 6, 8, 12, 14, 16, 18	$O_{10} + 2O_5$
		5, 15	$10O_2$
	13, 17	0, 4, 8, 12, 16	$4O_4 + 4O_1$
		1, 3, 5, 7, 9, 11, 13, 15, 17, 19	$5O_4$
		2, 6, 10, 14, 18	$4O_4 + 2O_2$
	14	C	$2\left(T_{2^2} * O_2\right) + T_{2^2}$

Продовження таблиці Е.2

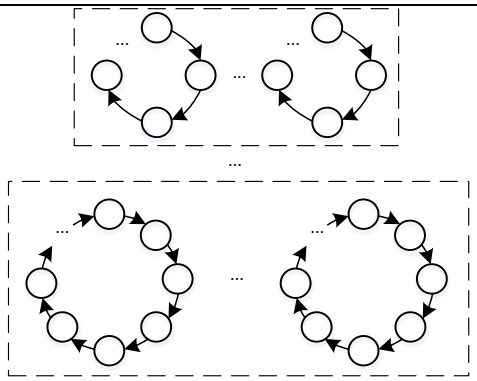
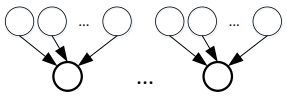
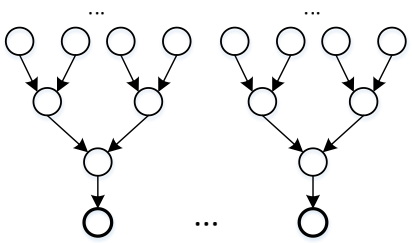
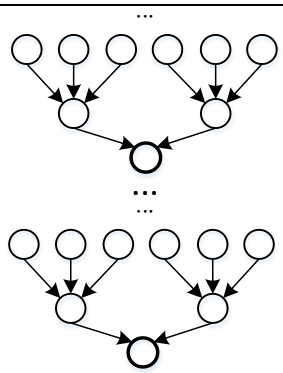
Параметри ЛКГ			**Структура графа**
M	*K*	*C*	
	15	0, 2, 4, 6, 8, 10, 12, 14, 16, 18	$E_5 * O_2 + 2E_5$ $\left(\text{или } T_{5^1} * O_2 + 2T_{5^1}\right)$
		1, 3, 5, 7, 9, 11, 13, 15, 17, 19	$2\left(E_5 * O_2\right)$ $\left(\text{или } 2\left(T_{5^1} * O_2\right)\right)$
	16	0, 5, 10, 15	$5E_4$ $\left(\text{или } 5T_{4^1}\right)$
		1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19	$E_4 * O_5$ $\left(\text{или } T_{4^1} * O_5\right)$
	19	0, 2, 4, 6, 8, 10, 12, 14, 16, 18	$9O_2 + 2O_1$
		1, 3, 5, 7, 9, 11, 13, 15, 17, 19	$10O_2$

Таблиця Е.3

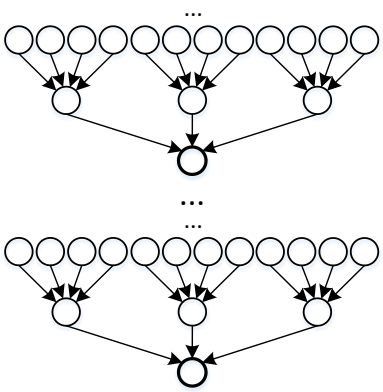
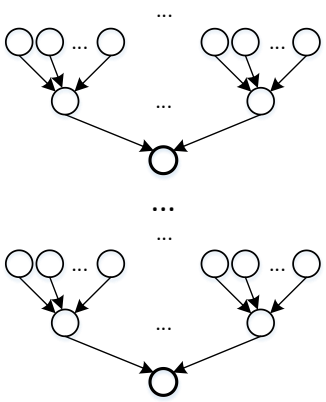
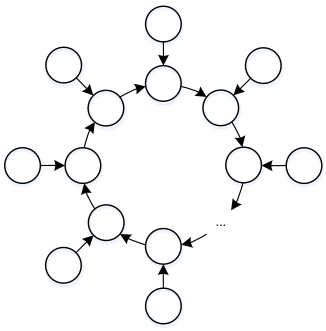
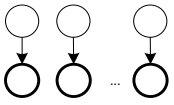
Типові орієнтовані графи станів ЛКГ

№	Опис	Графічне представлення	Компоненти графа
1. Цикли			
1.1	Один цикл довжини M		O_M
1.2	M нуль-циклів		MO_1
1.3	Один цикл довжини $M-1$ і один нуль-цикл		$O_{M-1}+O_1$
1.4	Група циклів довжини t $\left(d=\frac{M}{t}\right)$		dO_t
1.5	Група циклів довжини t і один нуль-цикл ($t>1$, $\sum_i dt = M-1$)		dO_t+O_1
1.6	Один цикл довжини t і група Z нуль-циклів $(t+Z=M)$		O_t+ZO_1
1.7	Група циклів довжини t і Z нуль-циклів ($t>1$, $Z>1$, $\sum_i dt = M-Z$)		dO_t+ZO_1

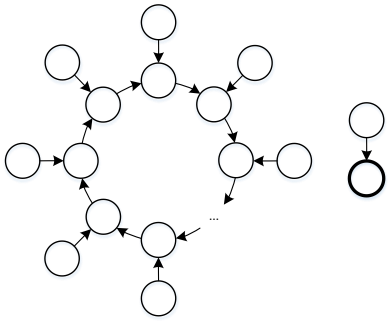
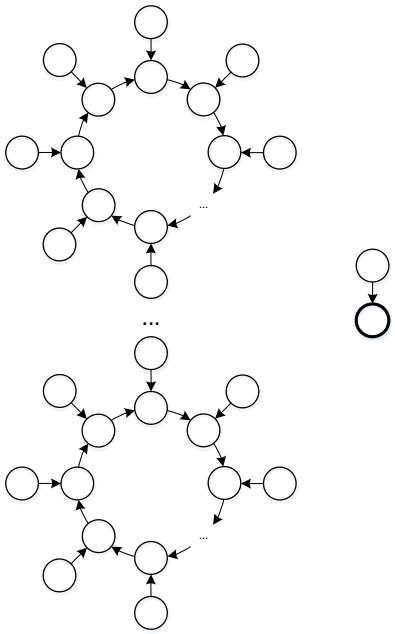
Продовження таблиці Е.3

№	Опис	Графічне представлення	Компоненти графа
Узагальнений граф циклів			
1.8	Групи циклів довжини t_i ($i \geq 1,\ t_i \geq 1,\ \sum_i d_i t_i = M$)		$\sum_i d_i O_{t_i}$
2. Дерева			
2.1	Група кореневих дерев з n вершинами, з кожної з яких ребро веде прямо в корінь $(dn = M)$		dE_n $\left(dT_{n^1}\right)$
2.2	Група бінарних дерев з n поверхами $\left(d2^n = M\right)$		dT_{2^n}
2.3	Група 3^n-вершинних дерев з n поверхами $\left(d3^n = M\right)$		dT_{3^n}

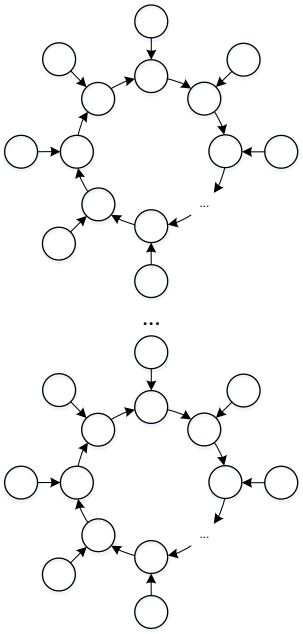
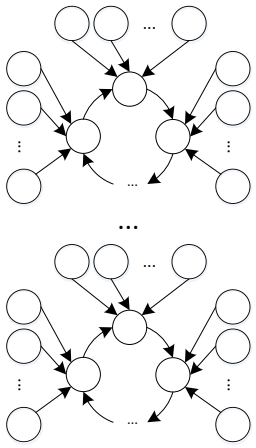
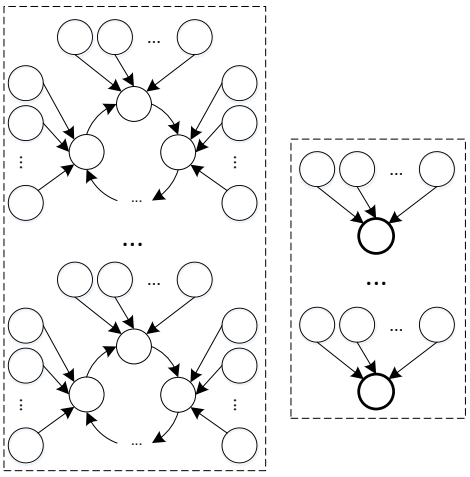
Продовження таблиці Е.3

№	Опис	Графічне представлення	Компоненти графа
2.4	Група 4^n-вершинних дерев з n поверхами $\left(d4^n = M\right)$		dT_{4^n}
Узагальнений граф дерев			
2.5	Група a^n-вершинних дерев з n поверхами $(a \geq 2,\ da^n = M)$		dT_{a^n}
3. Комбінації циклів і дерев			
3.1	Цикл довжини t, оснащений t одноребернними деревами, що входять по одному в кожну з t вершин циклу $\left(t = \frac{M}{2}\right)$		A_t $\left(T_{2^1} * O_t\right)$
3.2	Група циклів довжини 1, оснащених одним одноребернім деревом $\left(d = \frac{M}{2}\right)$		dA_1 $\left(dT_{2^1}\right)$

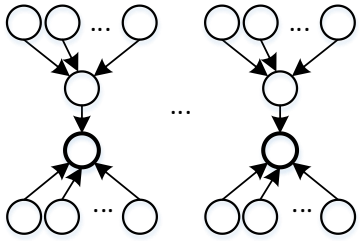
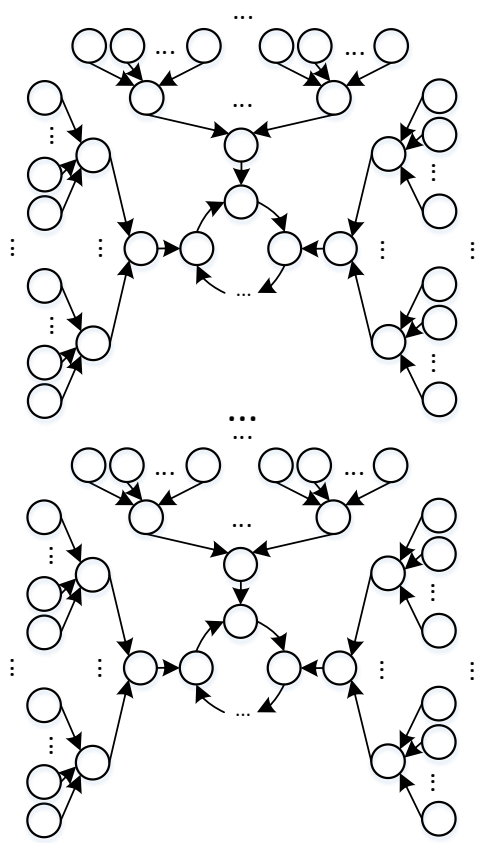
Продовження таблиці Е.3

№	Опис	Графічне представлення	Компоненти графа
3.3	Цикл довжини t, оснащений t одноребернимидеревами, що входять по одному в кожну з t вершин циклу, і один нуль-цикл, оснащений одним одноребернимдеревом $\left(t=\frac{M-2}{2}\right)$		$A_t + A_1$ $\left(T_{2^1} * O_t + T_{2^1}\right)$
3.4	Група циклів довжини t, оснащених t одноребернимидеревами, що входять по одному в кожну з t вершин циклу, і один нуль-цикл, оснащений одним одноребернимдеревом $\left(dt=\frac{M-2}{2}\right)$		$dA_t + A_1$ $\left(d\left(T_{2^1} * O_t\right) + T_{2^1}\right)$

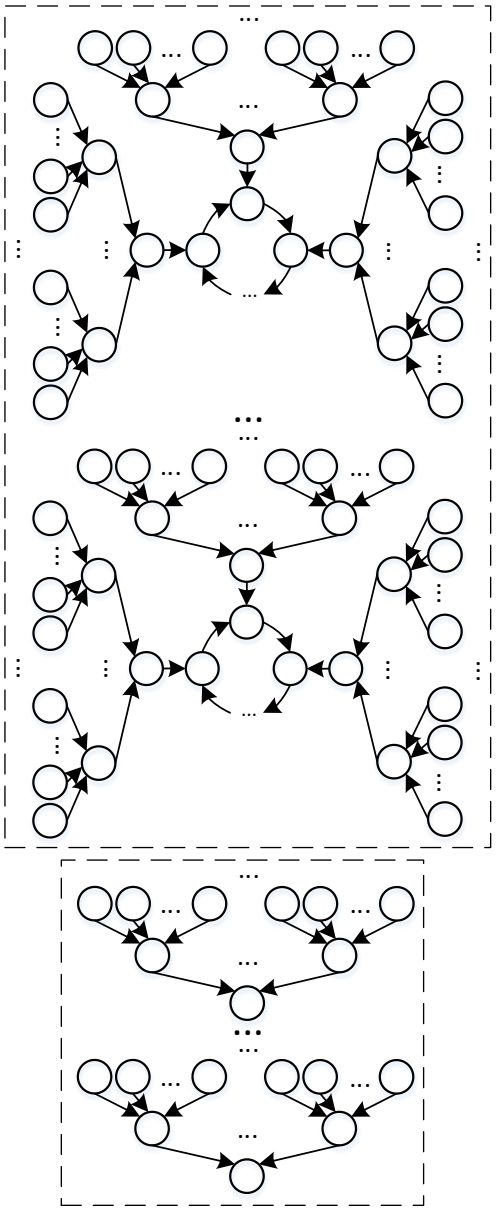
Продовження таблиці Е.3

№	Опис	Графічне представлення	Компоненти графа
3.5	Групи циклів довжини t_i, оснащених t_i одноребернимі деревами ($i \geq 1,\ t_i \geq 1,\ \sum_i d_i t_i = \frac{M}{2}$)		$\sum_i d_i A_{t_i}$
3.6	Група циклів довжини t, оснащених у кожній своїй вершині $(n-1)$ вхідними ребрами (які утворюють разом з цією належною циклу вершиною кореневе дерево E_n) $(dnt = M)$		$d(E_n * O_t)$ $\left(d\left(T_{n^1} * O_t\right)\right)$
3.7	Група циклів довжини t, оснащених у кожній своїй вершині $(n-1)$ вхідними ребрами, і група кореневих дерев з n вершинами, з кожної з яких ребро веде прямо в корінь $(n(dt+k)=M)$		$d(E_n * O_t) + kE_n$ $\left(d\left(T_{n^1} * O_t\right) + kT_{n^1}\right)$

Продовження таблиці Е.3

№	Опис	Графічне представлення	Компоненти графа
3.8	Група нуль-циклів з вхідними в них одноребернимі деревами, оснащеними в кожній своїй вершині кореневими деревами з n вершинами, з кожної з яких ребро веде прямо в корінь $\left(dn = \frac{M}{2} \right)$		$d\left(E_n * A_1\right)$ $\left(d\left(T_{n^1} * T_{2^1}\right)\right)$
3.9	Група циклів довжини t, оснащених t a^n-вершинними деревами з n поверхами $\left(n \geq 2, da^n t = M\right)$		$d\left(T_{a^n} * O_t\right)$

Продовження таблиці Е.3

№	Опис	Графічне представлення	Компоненти графа
3.10	Група циклів довжини t, оснащених t a^n-вершинними деревами з n поверхами, і група a^n-вершинних дерев з n поверхами $\left(n \geq 2, a^n\left(dt+k\right)=M\right)$		$d\left(T_{a^n} * O_t\right)+kT_{a^n}$

Додаток Ж. Закон розподілу дискретної випадкової величини на виході двійкового комбінаційного генератора

У роботах автора [353], [354] виконано статистичний аналіз перетворень первинних дискретних випадкових процесів (величин) X і Y відповідно до виразів (Ж.1):

$$\begin{aligned} &Z_1 = X \cap Y, \quad Z_3 = \bar{X} \cap \bar{Y}, \quad Z_5 = X \oplus Y, \quad Z_7 = X \cap Y, \quad Z_9 = \bar{X} \cap \bar{Y}, \\ &Z_2 = \bar{X} \cap Y, \quad Z_4 = X \cap \bar{Y}, \quad Z_6 = X \equiv Y, \quad Z_8 = \bar{X} \cap Y, \quad Z_{10} = X \cap \bar{Y}. \end{aligned} \tag{Ж.1}$$

Прийнято, що ймовірності появи одиниці для X і Y дорівнюють

$$P_X(1) = \frac{m_1}{n_1},\ P_Y(1) = \frac{m_2}{n_2}, \tag{Ж.2}$$

де $m_1,\ n_1,\ m_2,\ n_2$ – деякі цілі невід'ємні числа, причому $\begin{cases} m_1 \le n_1 \\ m_2 \le n_2 \end{cases}$.

У результаті наведеного в роботах [353], [354] аналізу визначено в аналітичному вигляді частоту повторень векторів Z_i розмірності n як функцію ваги:

$$\begin{aligned} &Z_1 : W_1(j) = (m_1 m_2)^j (n_1 n_2 - m_1 m_2)^{n-j}; \\ &Z_2 : W_2(j) = m_1^j (n_2 - m_2)^j (n_1 n_2 - m_1 (n_2 - m_2))^{n-j}; \\ &Z_3 : W_3(j) = m_2^j (n_1 - m_1)^j (n_1 n_2 - m_2 (n_1 - m_1))^{n-j}; \\ &Z_4 : W_4(j) = (n_1 - m_1)^j (n_2 - m_2)^j (n_1 m_2 + n_2 m_1 - m_1 m_2)^{n-j}; \\ &Z_5 : W_5(j) = (m_1 (n_2 - m_2) + m_2 (n_1 - m_1))^j ((n_1 - m_1)(n_2 - m_2) + m_1 m_2)^{n-j}; \\ &Z_6 : W_6(j) = (m_1 (n_2 - m_2) + m_2 (n_1 - m_1))^{n-j} ((n_1 - m_1)(n_2 - m_2) + m_1 m_2)^j; \\ &Z_7 : W_7(j) = W_4(n - j); \\ &Z_8 : W_8(j) = W_3(n - j); \\ &Z_9 : W_9(j) = W_2(n - j); \\ &Z_{10} : W_{10}(j) = W_1(n - j). \end{aligned} \tag{Ж.3}$$

Така закономірність дозволила сформулювати загальне правило обчислення закону розподілу ймовірності композицій Z_i, перерахованих у (Ж.1), за будь-якої розрядності випадкових векторів. Імовірність появи кожного вектору ваги j в композиції Z_i дорівнює

$$P_{i,j}^{1} = \frac{W_i(j)}{V},$$

де $V = (n_1 n_2)^n$, а $W(j)$ визначається за (Ж.3).

Відповідно, ймовірність появи будь-якого вектору ваги j в композиції Z_i дорівнює

$$P_{i,j} = \frac{W(j) \cdot C_n^j}{V}. \qquad (Ж.4)$$

Імовірність появи одиниці в композиції Z_i дорівнює сумі добутків ймовірності появи вектору ваги $j \in \{0,1,\ldots,n\}$ і ймовірності появи одиниці в цьому векторі, тобто:

$$P_{Z_i}(1) = \sum_{j=1}^{n} P_{i,j} \cdot \frac{j}{n} = \sum_{j=1}^{n} \frac{W(j) \cdot C_n^j \cdot j}{V \cdot n}. \qquad (Ж.5)$$

Визначимо ймовірності появи одиниці в результаті перетворення двох первинних випадкових процесів, ймовірності появи одиниці в яких визначаються за (Ж.2). У якості комбінаційної функції будемо розглядати тільки ті булеві функції, на результат яких впливають обидві змінні. Ці функції наведені в таблиці Ж.1. При цьому перевизначимо функції з (Ж.1). Нагадаємо, що кількість всіх булевих функцій n змінних дорівнює 2^{2^n}.

Таблиця Ж.1

Булеві функції двох змінних для комбінаційної функції генератора

		Значення змінних	X	0	0	1	1
			Y	0	1	0	1
	Назва функції	Позначення функції		Значення функції			
Z_1	Кон’юнкція	$Z_1 = X \cap Y$		0	0	0	1
Z_2	Диз’юнкція	$Z_2 = X \cup Y$		0	1	1	1
Z_3	Сума за модулем два, строга диз’юнкція	$Z_3 = X \oplus Y$		0	1	1	0
Z_4	Еквіваленція, тотожність	$Z_4 = X \equiv Y$		1	0	0	1

Продовження таблиці Ж.1

Z_5	Імплікація	$Z_5 = X \to Y$	1	1	0	1
Z_6	Імплікація	$Z_6 = Y \to X$	1	0	1	1
Z_7	Штрих Шеффера	$Z_7 = \overline{X \cap Y}$	1	1	1	0
Z_8	Стрілка Пірса	$Z_8 = \overline{X \cup Y}$	1	0	0	0
Z_9	Заперечення імплікації	$Z_9 = \overline{X \to Y}$	0	0	1	0
Z_{10}	Заперечення імплікації	$Z_{10} = \overline{Y \to X}$	0	1	0	0

Імовірності появи нулів і одиниць первинних випадкових величин X і Y визначатимемо згідно (Ж.2). На прикладі функції $Z_1 = X \cap Y$ розглянемо методику визначення ймовірностей появи нулів і одиниць у результаті перетворення Z_1. Можливі події для нього перераховано в таблиці Ж.2.

Таблиця Ж.2

Можливі події для перетворення $Z_1 = X \cap Y$ і їх ймовірності

Значення змінних	X	0	0	1	1
	Y	0	1	0	1
Функція		$Z_1 = X \cap Y$			
Значення функції		0	0	0	1
Імовірності		$\frac{(n_1 - m_1)(n_2 - m_2)}{n_1 n_2}$	$\frac{(n_1 - m_1) m_2}{n_1 n_2}$	$\frac{m_1 (n_2 - m_2)}{n_1 n_2}$	$\frac{m_1 m_2}{n_1 n_2}$

Таким чином, імовірність появи одиниці в комбінації $Z_1 = X \cap Y$ складе $P_{Z_1}(1) = \frac{m_1 m_2}{n_1 n_2}$, а нуля – $P_{Z_1}(0) = 1 - \frac{m_1 m_2}{n_1 n_2}$. Для того, щоб імовірність появи нуля й одиниці в результаті комбінації були однаковими, тобто $P_{Z_1}(1) = P_{Z_1}(0)$, потрібно,

щоб $\frac{m_1}{n_1}\cdot\frac{m_2}{n_2}=\frac{1}{2}$.

Виконаємо подібні обчислення для перетворень Z_i, $i=2,3,\ldots,10$. Імовірності появи нуля й одиниці та умови їх рівності для кожного з перетворень зведені в таблицю Ж.3.

Таблиця Ж.3

Можливі події для перетворень Z_i та їх ймовірності

Функція	$P_{Z_i}(1)$	$P_{Z_i}(0)$	$P_{Z_i}(1)=P_{Z_i}(0)$
Z_1	$\frac{m_1m_2}{n_1n_2}$	$\frac{n_1n_2-m_1m_2}{n_1n_2}$	$n_1n_2=2m_1m_2$ $P_X(1)P_Y(1)=0.5$
Z_2	$\frac{n_1m_2+m_1n_2-m_1m_2}{n_1n_2}$	$\frac{(n_1-m_1)(n_2-m_2)}{n_1n_2}$	$2m_1n_2+2n_1m_2=n_1n_2+2m_1m_2$ $P_X(1)+P_Y(1)-P_X(1)P_Y(1)=0.5$
Z_3	$\frac{m_1n_2+m_2n_1-2m_1m_2}{n_1n_2}$	$\frac{(n_1-m_1)(n_2-m_2)+m_1m_2}{n_1n_2}$	$n_1n_2+4m_1m_2=2m_1n_2+2m_2n_1$ $P_X(1)+P_Y(1)-2P_X(1)P_Y(1)=0.5$
Z_4	$\frac{(n_1-m_1)(n_2-m_2)+m_1m_2}{n_1n_2}$	$\frac{m_1n_2+m_2n_1-2m_1m_2}{n_1n_2}$	$n_1n_2+4m_1m_2=2m_1n_2+2m_2n_1$ $P_X(1)+P_Y(1)-2P_X(1)P_Y(1)=0.5$
Z_5	$\frac{n_1n_2-m_1(n_2-m_2)}{n_1n_2}$	$\frac{m_1(n_2-m_2)}{n_1n_2}$	$n_1n_2+2m_1m_2=2m_1n_2$ $P_X(1)(1-P_Y(1))=0.5$
Z_6	$\frac{n_1n_2-(n_1-m_1)m_2}{n_1n_2}$	$\frac{(n_1-m_1)m_2}{n_1n_2}$	$n_1n_2+2m_1m_2=2m_2n_1$ $P_Y(1)(1-P_X(1))=0.5$
Z_7	$\frac{n_1n_2-m_1m_2}{n_1n_2}$	$\frac{m_1m_2}{n_1n_2}$	$n_1n_2=2m_1m_2$ $P_X(1)P_Y(1)=0.5$
Z_8	$\frac{(n_1-m_1)(n_2-m_2)}{n_1n_2}$	$\frac{n_1m_2+m_1n_2-m_1m_2}{n_1n_2}$	$2m_1n_2+2n_1m_2=n_1n_2+2m_1m_2$ $P_X(1)+P_Y(1)-P_X(1)P_Y(1)=0.5$
Z_9	$\frac{m_1(n_2-m_2)}{n_1n_2}$	$\frac{n_1n_2-m_1(n_2-m_2)}{n_1n_2}$	$n_1n_2+2m_1m_2=2m_1n_2$ $P_X(1)(1-P_Y(1))=0.5$
Z_{10}	$\frac{(n_1-m_1)m_2}{n_1n_2}$	$\frac{n_1n_2-(n_1-m_1)m_2}{n_1n_2}$	$n_1n_2+2m_1m_2=2m_2n_1$ $P_Y(1)(1-P_X(1))=0.5$

Як можна бачити з таблиці Ж.3, для отримання двійкової послідовності з рівномірним розподілом нулів і одиниць, утвореної за допомогою перетворень первинних випадкових процесів, можна скористатися будь-якою з функцій Z_i,

$i = 1,2,\ldots,10$, за умови, що ймовірності $P_X(1)$ і $P_Y(1)$ задовольняють вимогам, наведеним у таблиці Ж.3.

Разом з тим, особливий інтерес представляє результат комбінації двох рівномірно розподілених первинних двійкових випадкових величин. У цьому випадку $P_X(1) = P_Y(1) = \frac{1}{2}$, $m_1 = m_2 = 1$, $n_1 = n_2 = 2$. Підставивши ці значення у вирази таблиці Ж.3, можна бачити, що рівномірно розподілену випадкову величину можна отримати тільки для перетворень $Z_3 = X \oplus Y$ і $Z_4 = X \equiv Y$. Зауважимо, що $Z_4 = X \equiv Y = \overline{X \oplus Y} = \overline{Z_3}$.

Розглянемо приклад формування ПВП з рівномірним розподілом в ній нулів і одиниць. У якості первинних ПВП будемо використовувати різні комбінації послідовностей, сформованими генератором М-послідовності і ЛКГ.

1. Первинні послідовності – дві М-послідовності.

Кількість одиниць у М-послідовності періоду T на одиницю більше, ніж кількість нулів. Таким чином, імовірність появи нуля й одиниці в послідовності максимальної довжини дорівнюють $P(1) = \frac{T+1}{2T}$, $P(0) = \frac{T-1}{2T}$.

Загальновідомим фактом є також те, що комбінація у вигляді суми за модулем два двох М-послідовностей з періодами $T_1 = 2^{n_1} - 1$ і $T_2 = 2^{n_2} - 1$ є послідовністю періоду $T_3 = НОК(T_1, T_2)$. Якщо хоча б один з періодів T_1 або T_2 є простим числом Мерсенна, то $T_3 = T_1 \cdot T_2$. Імовірності появи нуля й одиниці в отриманій послідовності $P(1) = \frac{T_3+1}{2T_3}$, $P(0) = \frac{T_3-1}{2T_3}$.

Розглянемо можливість формування послідовності з рівномірним розподілом нулів і одиниць на основі первинних рандомізованих М-послідовностей. У цьому випадку $P_X(0) = P_Y(0) = P_X(1) = P_Y(1) = \frac{1}{2}$, а місце вставки нуль-циклу в послідовність є випадковим. Розглянемо приклад перетворення рандомізованих М-послідовностей одного періоду.

У якості послідовностей X і Y оберемо рандомізовані М-послідовності з

генераторними поліномами $G_X(x) = x^5 + x^3 + 1$ і $G_Y(x) = x^5 + x^2 + 1$. Операція перетворення – функція тотожності $Z_4 = X \equiv Y$. Результати перетворення зведені в таблицю Ж.4.

Таблиця Ж.4

Комбінації рандомізованих М-послідовностей

X_1	0	0	0	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1	0
Y_1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0
$Z_4^{(1,1)}$	1	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	1	0	1	1
X_1	0	0	0	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1	0
Y_2	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	0
$Z_4^{(1,2)}$	0	1	0	0	1	1	1	0	0	1	1	1	0	1	0	1	1	1	0	1	1	1	0	1	1	1	1	0	0	0	1	1
X_1	0	0	0	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1	0
Y_3	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	0	1	1	1	1	1	0	0	1	1	0	1
$Z_4^{(1,3)}$	1	1	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	1	1	1	0	1	1	1	0	0

Послідовності Y_2 і Y_3, наведені в таблиці Ж.4, відрізняються від послідовності Y_1 вектором початкового завантаження (початковим станом генератора М-послідовності) і положенням нуль-циклу в послідовності, відповідно.

З таблиці Ж.4 можна бачити, що:

1) результатом комбінації $Z_4^{(1,1)} = X_1 \equiv Y_1$ є послідовність з рівномірним розподілом нулів і одиниць;
2) результатами комбінацій $Z_4^{(1,2)} = X_1 \equiv Y_2$ і $Z_4^{(1,3)} = X_1 \equiv Y_3$ є послідовності з нерівномірним розподілом нулів і одиниць.

Аналіз статистичних властивостей комбінацій рандомізованої і нерандомізованої М-послідовностей, а також комбінацій двох рандомізованих М-послідовностей різного періоду показує залежність закону розподілу нулів і одиниць у отриманих комбінаціях від вектору початкового завантаження і положення нуль-циклу в початкових послідовностях.

2. Первинні послідовності – М-послідовність і послідовність на виході ЛКГ.

Методика створення гіперциклу на основі циклів ЛКГ дозволяє формувати

ПВП довжини L без необхідності використання генератора з параметрами такого ж порядку, що і L. Сформуємо послідовність чисел ЛКГ для $S_0 = 1, K = 11, C = 1, M = 31$. Доповнимо її нуль-циклом і значенням 31. У якості двійкової послідовності, яку породжує генератор, приймемо послідовність значень молодших розрядів у двійковому представленні сформованих чисел. У якості другого операнду комбінації оберемо рандомізовану М-послідовність довжиною 32. Результати занесемо в таблицю Ж.5.

Таблиця Ж.5

Комбінації рандомізованих М-послідовності і послідовності ЛКГ

X_2	1	0	1	1	0	0	0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	0	1	1
Y_4	0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0
$Z_4^{(2,4)}$	0	1	0	0	0	1	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0	1	1	1	0	1	0	1	0	1	1	0
X_2	1	0	1	1	0	0	0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	0	1	1
Y_5	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0	0	0
$Z_4^{(2,5)}$	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	1	0	1	1	0	1	1	1	0	1	1	0	0
X_2	1	0	1	1	0	0	0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	0	1	1
Y_6	0	1	0	0	1	0	1	1	0	0	1	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0	0
$Z_4^{(2,6)}$	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	1	1	1	1	0	1	0	0	0	0	1	0	1	0	0

Послідовності Y_5 і Y_6 відрізняються від послідовності Y_4 вектором початкового завантаження і положенням нуль-циклу в послідовності, відповідно.

Таблиця Ж.5 показує, що:

1) результатом комбінації $Z_4^{(2,4)} = X_2 \equiv Y_4$ є послідовність з рівномірним розподілом нулів і одиниць;
2) результатами композицій $Z_4^{(2,5)} = X_2 \equiv Y_5$ і $Z_4^{(2,6)} = X_2 \equiv Y_6$ є послідовності з нерівномірним розподілом нулів і одиниць.

Аналіз статистичних властивостей комбінацій рандомізованої і нерандомізованої М-послідовностей і послідовностей, породжених ЛКГ, у тому числі при формуванні первинними генераторами потоків слів, показує залежність закону розподілу нулів і одиниць в отриманих комбінаціях від векторів початкового завантаження і положення нуль-циклу в початкових послідовностях.

3. Первинні послідовності – дві послідовності ЛКГ.

За допомогою ЛКГ сформуємо послідовності чисел для $K=10,\ C=7,\ M=31$ і $K=10,\ C=3,\ M=31$. Доповнимо їх нуль-циклами і значеннями 31. Як і у випадку з попереднім прикладом, у якості двійкової послідовності, яку породжує генератор, приймемо послідовність значень молодших розрядів у двійковому представленні сформованих чисел. Результати перетворення занесемо в таблицю Ж.6.

Таблиця Ж.6

Комбінації рандомізованих послідовностей ЛКГ

X_3	1	0	0	0	1	0	1	0	1	1	0	1	1	0	1	0	1	0	1	1	0	0	0	0	1	1	0	0	0	1	1	1
Y_7	1	1	0	1	0	1	0	0	1	1	1	1	0	0	1	0	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	0
$Z_4^{(3,7)}$	1	0	1	0	0	0	0	1	1	1	0	1	0	1	1	1	0	1	0	1	0	1	0	0	1	0	0	1	1	0	1	0
X_3	1	0	0	0	1	0	1	0	1	1	0	1	1	0	1	0	1	0	1	1	0	0	0	0	1	1	0	0	0	1	1	1
Y_8	1	1	0	1	0	1	0	0	1	1	1	1	0	0	1	1	1	0	1	1	1	0	1	0	0	0	0	0	0	0	1	0
$Z_4^{(3,8)}$	1	0	1	0	0	0	0	1	1	1	0	1	0	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	1	0	1	0
X_3	1	0	0	0	1	0	1	0	1	1	0	1	1	0	1	0	1	0	1	1	0	0	0	0	1	1	0	0	0	1	1	1
Y_9	1	1	0	1	0	1	0	0	1	1	1	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	0	0	0	1
$Z_4^{(3,9)}$	1	0	1	0	0	0	0	1	1	1	0	1	0	1	1	1	0	1	0	1	1	0	1	0	1	1	1	0	1	0	0	1

Послідовності Y_8 і Y_9 відрізняються від послідовності Y_7 вектором початкового завантаження і положенням нуль-циклу в послідовності, відповідно.

З таблиці Ж.6 видно, що

1) послідовність, отримана внаслідок виконання операції $Z_4^{(3,7)} = X_3 \equiv Y_7$, є послідовністю з рівномірним розподілом нулів і одиниць;
2) послідовності $Z_4^{(3,8)} = X_3 \equiv Y_8$ і $Z_4^{(3,9)} = X_3 \equiv Y_9$ є послідовності з нерівномірним розподілом нулів і одиниць.

Залежність статистичних властивостей отриманих комбінацій від параметрів вихідних процесів зберігається, якщо перетворення послідовності ЛКГ в двійкову послідовність виконувати за словами, тобто двійковим представленням кожного з чисел на виході ЛКГ.

Виконане дослідження дозволило сформувати наступні висновки:

– статистичні властивості перетворень (підсумовування за модулем два, операція тотожності) двох рандомізованих, а також рандомізованої і нерандомізованої М-послідовностей довільних періодів залежать від вектору початкового завантаження генераторів вихідних послідовностей і положення в них нуль-циклу;
– статистичні властивості перетворень (підсумовування за модулем два, операція тотожності) рандомізованих і нерандомізованих – у будь-якому їх поєднанні – М-послідовності і послідовності на виході ЛКГ, а також двох послідовностей ЛКГ довільних періодів залежать від вектору початкового завантаження генераторів вихідних послідовностей, положення в них нуль-циклів, а також від порядку обходу циклів ЛКГ.

Таким чином, застосування генераторів М-послідовності і ЛКГ у якості первинних джерел ПВП для формування двійкової послідовності з рівномірним розподілом появи в ній нулів і одиниць є допустимим, проте вимагає попередньої перевірки статистичних властивостей комбінацій перед їх використанням.

Визначимо закон розподілу дискретної випадкової величини на виході двійкового комбінаційного генератора з комбінаційною функцією підсумовування за модулем два

Нехай комбінаційний генератор містить два первинних генератора випадкових двійкових чисел. При цьому ймовірності появи нулів і одиниць на виході першого генератора дорівнюють

$$\begin{cases} P_1(0) = \dfrac{1}{2} - \Delta_1, \\ P_1(1) = \dfrac{1}{2} + \Delta_1; \end{cases}$$

а другого генератора –

$$\begin{cases} P_2(0) = \dfrac{1}{2} - \Delta_2, \\ P_2(1) = \dfrac{1}{2} + \Delta_2; \end{cases}$$

де Δ_1, Δ_2 – величини відхилення ймовірностей появи нулів і одиниць від

значення $\frac{1}{2}$.

У результаті підсумовування за модулем два значень на виходах двох первинних генераторів імовірності появи нулів і одиниць дорівнюють, відповідно,

$$\begin{cases} P(0)=\left(\frac{1}{2}-\Delta_1\right)\left(\frac{1}{2}-\Delta_2\right)+\left(\frac{1}{2}+\Delta_1\right)\left(\frac{1}{2}+\Delta_2\right), \\ P(1)=\left(\frac{1}{2}-\Delta_1\right)\left(\frac{1}{2}+\Delta_2\right)+\left(\frac{1}{2}+\Delta_1\right)\left(\frac{1}{2}-\Delta_2\right). \end{cases}$$

Розкривши дужки, отримаємо:

$$\begin{cases} P(0)=\frac{1}{2}+2\Delta_1\Delta_2, \\ P(1)=\frac{1}{2}-2\Delta_1\Delta_2. \end{cases}$$

Для того, щоб імовірності появи нулів і одиниць у результуючому потоці вирівнювалися, необхідно виконання умов

$$\begin{cases} |2\Delta_1\Delta_2|<|\Delta_1|, \\ |2\Delta_1\Delta_2|<|\Delta_2|. \end{cases} \Rightarrow \begin{cases} |\Delta_2|<\frac{1}{2}, \\ |\Delta_1|<\frac{1}{2}. \end{cases}$$

Таким чином, для вирівнювання статистики необхідно, щоб величини відхилення ймовірностей появи нулів і одиниць від значення $\frac{1}{2}$ у первинних потоках були менше $\frac{1}{2}$.

Розглянемо приклад.

Нехай $P_1(0)=\frac{1}{4}$, $P_1(1)=\frac{3}{4}$, $P_2(0)=\frac{2}{3}$, $P_2(1)=\frac{1}{3}$, звідки $\Delta_1=-\frac{1}{4}$, $\Delta_2=\frac{1}{6}$. Тоді ймовірності появи нулів і одиниць на виході комбінаційного генератора складуть $P(0)=\frac{1}{2}-\frac{1}{12}=\frac{5}{12}$, $P(1)=\frac{1}{2}+\frac{1}{12}=\frac{7}{12}$. Представлені на рис. Ж.1 гістограми розподілів ймовірностей двійкових випадкових величин до і після перетворення дозволяють візуально оцінити ступінь близькості розподілів до рівномірного закону.

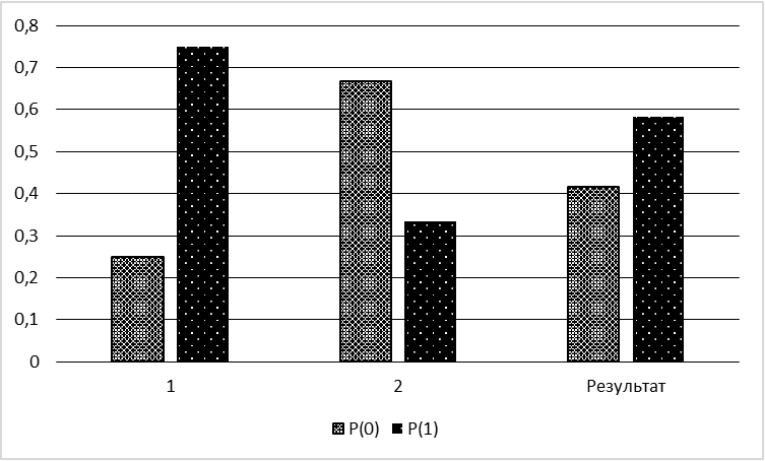


Рис. Ж.1. Гістограми розподілів імовірностей двійкових випадкових величин до і після перетворення

Імовірності появи нулів і одиниць у послідовності біт на виході комбінаційного генератора з n первинними генераторами для $\begin{cases} P_i(0) = \frac{1}{2} - \Delta_i, \\ P_i(1) = \frac{1}{2} + \Delta_i; \end{cases}$ де i – номер первинного генератора, дорівнюють, відповідно:

$$\begin{cases} P(0) = \frac{1}{2} + (-1)^n 2^{n-1} \prod_{i=1}^{n} \Delta_i, \\ P(1) = \frac{1}{2} + (-1)^{n-1} 2^{n-1} \prod_{i=1}^{n} \Delta_i. \end{cases} \quad (Ж.6)$$

Очевидно, що збільшення кількості первинних генераторів і дотриманні умови $|\Delta_i| < \frac{1}{2}$ призводить до зменшення величини відхилення ймовірностей появи нулів і одиниць від значення $\frac{1}{2}$ у результуючому потоці, що призведе до вирівнювання його статистики.

Розглянемо приклад.

Нехай комбінаційний генератор містить три первинних генератора, що є генераторами М-послідовностей з генераторними поліномами зі степенями 3, 5 і 7. Тоді $\Delta_1 = \frac{1}{2} - \frac{2^{3-1}-1}{2^3-1} = \frac{1}{14}$, $\Delta_2 = \frac{1}{2} - \frac{2^{5-1}-1}{2^5-1} = \frac{1}{62}$, $\Delta_3 = \frac{1}{2} - \frac{2^{7-1}-1}{2^7-1} = \frac{1}{254}$. Згідно (Ж.6),

імовірності появи нулів і одиниць у результуючій послідовності на виході комбінаційного генератора дорівнюють

$$P(0)=\frac{1}{2}-4\left(\frac{1}{14}\cdot\frac{1}{62}\cdot\frac{1}{254}\right)=\frac{1}{2}-\frac{1}{2\cdot 7\cdot 31\cdot 127}=\frac{1}{2}-\frac{1}{55118}\ \text{ і }\ P(1)=\frac{1}{2}+\frac{1}{55118}.$$

Проведене дослідження дозволило отримати наступні результати:

– визначено закон розподілу д.в.в. на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем два слів, отриманих від n первинних генераторів випадкових чисел, розподіли яких мають відхилення від рівномірного закону;

– показано, що за відхилень імовірностей появи нулів і одиниць від значення $\frac{1}{2}$ для первинних генераторів на рівні $|\Delta_i|<\frac{1}{2}$ відхилення ймовірностей появи нулів і одиниць від значення $\frac{1}{2}$ на виході комбінаційного генератора з комбінаційною функцією підсумовування за модулем два будуть зменшуватися і складати значення $2^{n-1}\prod_{i=1}^{n}|\Delta_i|$.

Основні наведені результати відображені в роботах автора [6], [7], [355].

Додаток К. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації

[1] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в *Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография*, под ред. В. М. Безрук, и В. В. Баранник, Харьков: Лидер, 2017, с. 291-323.

[2] Е. В. Фауре, "Методологія захисту інформації на основі факторіального кодування даних", в *Криптографічне кодування: обробка та захист інформації: колективна монографія*, під ред. В. М. Рудницький, Харків: Щедра садиба плюс, 2018, с. 85-95.

[3] Э. В. Фауре, В. В. Швыдкий и В. А. Щерба, "Комбинированное факториальное кодирование и его свойства", *Радіоелектроніка, інформатика, управління*, № 3, с. 80-86, 2016.

[4] E. V. Faure, A. I. Shcherba, and V. M. Rudnytskyi, "The Method and Criterion for Quality Assessment of Random Number Sequences", *Cybernetics and Systems Analysis,* vol. 52, no. 2, pp. 277-284, 2016.

[5] Е. В. Фауре, "Факториальное кодирование с исправлением ошибок", *Радіоелектроніка, інформатика, управління*, № 3, с. 130-138, 2017.

[6] E. V. Faure, A. I. Shcherba, and A. A. Kharin, "Factorial code with a given number of inversions", *Radio Electronics, Computer Science, Control*, no. 2, pp. 143-153, 2018.

[7] Э. В. Фауре, Д. В. Фауре и И. Н. Коротеев, "Выбор параметров генератора конгруэнтных чисел", *Сучасна спеціальна техніка*, № 1(20), с. 30-35, 2010.

[8] Є. В. Ланських, Е. В. Фауре і А. В. Очеретяна, "Метод організації ключового обміну з використанням прихованого каналу в телефонних мережах загального користування", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 18-21, 2010.

[9] Е. С. Лисицына, В. В. Швыдкий, А. И. Щерба и Э. В. Фауре, "Разделение векторной смеси сигнала и помехи по методу максимального правдоподобия", *Системи обробки інформації*, № 8(89), с. 62-67, 2010.

[10] Р. О. Бивзюк, Д. В. Фауре и Э. В. Фауре, "Устройство формирования остатков в многоканальных помехоустойчивых кодеках", *Вісник Хмельницького національного університету*, № 4, с. 75-78, 2010.

[11] N. Alishov, E. Faure, D. Faure, and V. Shadkhin, "Method of linear formation of pseudorandom processes", *Journal of Qafqaz University. Mathematics and computer science*, no. 30, pp. 17-24, 2010.

[12] Э. В. Фауре, Д. В. Фауре, М. В. Сторчак и В. А. Кучеренко, "Исследование и оптимизация методов формирования контрольной суммы помехоустойчивых кодов", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 63-67, 2011.

[13] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Прихована передача інформації у полосі звукових частот", *Сучасний захист інформації*, № 2, с. 22-30, 2011.

[14] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Ансамбль ортогональних шумоподібних сигналів для скритних систем з обмеженим спектром", *Наукові записки УНДІЗ*, № 1(21), с. 33-38, 2012.

[15] А. С. Береза, А. А. Лавданский, В. В. Швыдкий и Э. В. Фауре, "Генерация конгруэнтных последовательностей чисел с заданными свойствами", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 2, с. 3-8, 2012.

[16] В. В. Швыдкий, Э. В. Фауре, В. В. Веретельник и В. А. Щерба, "Генерация стохастической последовательности генератором конгруэнтных чисел", *Системи обробки інформації*, № 3, с. 74-80, 2012.

[17] В. Ю. Шадхін, Е. В. Фауре і О. В. Костомаров, "Криптографічні засоби захисту інформації в автоматизованих системах дистанційного навчання", *Вісник Хмельницького національного університету*, № 1, с. 126-130, 2012.

[18] Э. В. Фауре, А. С. Береза и Е. А. Ярославская, "Оценка точности

воспроизведения закона распределения дискретной случайной величины при ее преобразовании", *Вестник Хмельницкого национального университета*, № 5, с. 176–182, 2012.

[19] Э. В. Фауре, Е. В. Ланских, Д. А. Коляда и Ю. И. Черевко, "Преобразование процессов на выходе генераторов М-последовательности и конгруэнц-генераторов", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 17-21, 2012.

[20] Ю. Г. Лега, Э. В. Фауре и А. А. Лавданский, "Технология генерации случайных последовательностей с большой разрядностью чисел", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 3, с. 3-8, 2012.

[21] Э. В. Фауре, Е. С. Лисицына и Д. Ю. Нестеренко, "Метод повышения стойкости электронных кодовых замков", *Вісник Інженерної академії України*, № 2, с. 137-141, 2013.

[22] А.А. Лавданский, В.В. Швыдкий и Э.В. Фауре, "Метод формирования последовательностей случайных чисел и его использование в системах потокового шифрования", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 1, с. 5-10, 2013.

[23] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе комбинационного генератора", *Безпека інформації*, т. 20, № 2, с. 153-158, 2014.

[24] Э. В. Фауре, В. В. Швыдкий и А. И. Щерба, "Метод формирования воспроизводимой непредсказуемой последовательности перестановок", *Безпека інформації*, т. 20, № 3, с. 253-258, 2014.

[25] Е. В. Фауре, М. І. Вишня і В. А. Чорнобай, "Оцінка закону розподілу випадкових чисел комбінаційного генератора у k-вимірному просторі", *Вісник Херсонського національного технічного університету*, № 4(51), с. 169-173, 2014.

[26] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Анализ корреляционных свойств последовательностей (псевдо) случайных чисел", *Наука і техніка Повітряних Сил Збройних Сил України*, № 1(18), с. 142-150, 2015.

[27] Э. В. Фауре, В. В. Швыдкий и В. А. Щерба, "Метод формирования имитовставки на основе перестановок", *Захист інформації*, т. 16, № 4, с. 340, 2015.

[28] А. А. Лавданский и Э. В. Фауре, "Оценка статистических свойств последовательностей на выходе комбинационного генератора с помощью графических тестов", *Системні дослідження та інформаційні технології*, № 2, с. 39-50, 2015.

[29] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором", *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, № 18, с. 165-171, 2015.

[30] Е. В. Фауре, С. В. Сисоєнко і Т. В. Миронюк, "Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення", *Системи управління, навігації та зв'язку*, № 4(36), с. 85-87, 2015.

[31] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 57-61, 2016.

[32] В. М. Рудницький, Е. В. Фауре і С. В. Сисоєнко, "Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем", *Вісник Інженерної академії України*, № 3, с. 219-221, 2016.

[33] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, т. 1, № 2, с. 33-39, 2016.

[34] Э. В. Фауре, "Факториальное кодирование с несколькими контрольными суммами", *Вісник Житомирського державного технологічного університету. Серія: Технічні науки*, № 3 (78), с. 104-113, 2016.

[35] Э. В. Фауре, В. В. Швыдкий и А. И. Щерба, "Контроль целостности информации на основе факториальной системы счисления", *Journal of Baku Engineering University. Mathematics and computer science*, т. 1, № 1, с. 3-13, 2017.

Наукові праці, які засвідчують апробацію матеріалів дисертації

[1] Э. В. Фауре и В. А. Старовер, "Подсистема защиты информации в скрытом канале системы охранного видеонаблюдения", в *Системний аналіз та інформаційні технології: Матеріали XI Міжнародної науково-технічної конференції (26-30 травня 2009 р., Київ)*, Київ, 2009, с. 582.

[2] Э. В. Фауре и А. И. Музыченко, "Домовое переговорное устройство по сетям электропитания", в *II міжвузівська науково-практична конференція „Актуальні проблеми технічних та природничих наук у забезпеченні цивільного захисту“ (30-31 березня 2009 року. м. Черкаси). Збірник матеріалів: Частина 1*, Черкаси, 2009, с. 180-181.

[3] Э. В. Фауре и Р. О. Бивзюк, "Методы и средства формирования остатков в многоканальных помехоустойчивых кодеках", в *Інформаційні технології та комп'ютерна інженерія. Тези доповідей Міжнародної науково-практичної конференції. м. Вінниця, 19-21 травня 2010 року*, Вінниця, 2010, с. 381-382.

[4] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Прихована передача інформації в звуковому частотному діапазоні", в *Науково-технічна конференція «Проблеми телекомунікацій»: Збірник тез*, К., 2011, с. 108.

[5] Э. В. Фауре, Д. В. Фауре и М. В. Сторчак, "Методы и средства формирования остатка в помехоустойчивых кодеках", в *Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р.*, Вінниця, 2011, с. 181.

[6] Э. В. Фауре, Д. В. Фауре и Д. А. Коляда, "Метод нелинейного формирования псевдослучайной последовательности чисел", в *Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р.*, Вінниця, 2011, с. 168.

[7] Э. В. Фауре, Е. С. Лисицына и Д. Ю. Нестеренко, "Метод повышения стойкости электронных кодовых замков", в *Сучасність, наука, час. Взаємодія та взаємовплив: матеріали дев'ятої Міжнародної науково-практичної інтернет-*

конференції, Київ, 19-21 листопада 2012 р., К., 2012, т. 2, с. 62-64.

[8] И. Н. Выверица, А. А. Лавданский и Э. В. Фауре, "Двухконтурная защита информации от несанкционированного доступа в стегосистемах", в *Информационные технологии и системы 2012 (ИТС 2012) : материалы международной научной конференции, БГУИР, Минск, Беларусь, 24 октября 2012 г.*, Минск, 2012, с. 244-245.

[9] Р. М. Дідковський, Е. В. Фауре і В. В. Олексієнко, "Ансамбль багатопозиційних шумоподібних ортогональних сигналів", в *Тези доповідей Міжнародної науково-практичної конференції 'Інформаційні технології в освіті, науці і техніці' (ІТОНТ-2012): Черкаси, 25-27 квітня 2012 р.*, Черкаси, 2012, т. 1, с. 65-66.

[10] Э. В. Фауре и А. А. Лавданский, "Способ определения структуры графа состояний линейного конгруэнтного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 18-22 березня 2013 р.*, Черкаси, 2013, с. 110-112.

[11] В. А. Щерба и Э. В. Фауре, "Свойства генератора конгруэнтных чисел и его применения", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 18-22 березня 2013 р.*, Черкаси, 2013, с. 85-87.

[12] Э. В. Фауре, "Подстановки и их использование в задачах формирования псевдослучайных последовательностей чисел", в *Праці IV Міжнародної науково-практичної конференції «Обробка сигналів і негауссівських процесів», присвяченої пам'яті професора Ю.П. Кунченка: Тези доповідей, Черкаси, 22-24 травня 2013 р.*, Черкаси, 2013, с. 171-173.

[13] E. Faure, V. Chornobai, and M. Vyshnia, "Some statistical properties of pseudorandom number sequences formed by combination generator", in *Современные достижения в науке и образовании : сб. тр. IX междунар. науч.*

конф., 22-29 сентября 2014 г., Нетания (Израиль)., Хмельницкий, 2014, pp. 56-58.

[14] Э. В. Фауре и В. В. Швыдкий, "Формирование имитовставки на основе перестановок", в *Проблеми інформатизації: Матеріали другої міжнародної науково-технічної конференції, Черкаси, 25-26 листопада 2014 р.*, Черкаси, 2014, с. 12.

[15] А. А. Лавданский и Э. В. Фауре, "Комбинационный метод формирования последовательности псевдослучайных чисел", в *Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014 р.*, К., 2014, с. 403-404.

[16] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе композиционного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 17-21 березня 2014 р.*, Черкаси, 2014, с. 53-54.

[17] Э. В. Фауре, "Статистические характеристики оценок нормированных коэффициентов автокорреляции последовательностей (псевдо) случайных чисел", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 16-20 березня 2015 р.*, Черкаси, 2015, с. 46-47.

[18] Э. В. Фауре, А. И. Щерба и А. А. Лавданский, "Статистическая характеристика последовательности чисел комбинационного генератора", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 16-20 березня 2015 р.*, Черкаси, 2015, с. 51-52.

[19] Е. В. Фауре, Д. І. Бібко і С. С. Нагорних, "Дослідження статистичних властивостей комбінацій рознесених вибірок послідовності перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної*

конференції, Черкаси, 12-13 листопада 2015 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 16.

[20] Е. В. Фауре і А. М. Ткаченко, "Дослідження здатності виявлення помилок завадостійким кодом на основі перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 17.

[21] Е. В. Фауре і О. С. Гуденко, "Дослідження автокореляційних зв'язків послідовності перестановок", в *Проблеми інформатизації: Матеріали третьої міжнародної науково-технічної конференції, Черкаси, 12-13 листопада 2015 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2015, с. 15.

[22] Е. В. Фауре і С. В. Сисоєнко, "Підвищення стійкості комп'ютерного криптографічного перетворення", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 13.

[23] Э. В. Фауре, "Методика оценки вероятности преобразования перестановки чисел в перестановку при ее передаче по каналу связи", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 14-20 березня 2016 р.*, Черкаси, 2016, с. 78-80.

[24] Е. В. Фауре і С. В. Сисоєнко, "Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу", в *The scientific potential of the present [text]: Proceedings of the International Scientific Conference, St. Andrews, Scotland, UK, December 1, 2016*, Vinnytsia, 2016, с. 119-122.

[25] Э. В. Фауре и Р. К. Еременко, "Исследование способности обнаружения ошибок полным факториальным кодом", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4*

листопада 2016 р., Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 12.

[26] Э. В. Фауре и А. В. Магуров, "Исследование способности обнаружения ошибок комбинированным факториальным кодом", в *Проблеми інформатизації: Тези доповідей четвертої Міжнародної науково-технічної конференції, Черкаси, 3-4 листопада 2016 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2016, с. 13.

[27] Е. В. Фауре і О. О. Харін, "Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних", в *Актуальні задачі та досягнення у галузі кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції, Кропивницький, 23-25 листопада 2016 р.*, Кропивницький, 2016, с. 178-179.

[28] Е. В. Фауре і О. О. Харін, "Факторіальне кодування з відновленням даних і виправленням помилок", в *Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 13-19 березня 2017 р.*, Черкаси, 2017, с. 74-76.

[29] Е. В. Фауре і В. С. Рузальонок, "Дослідження структури графа станів лінійного конгруентного генератора", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 15-16.

[30] Е. В. Фауре, О. О. Харін і М. О. Качалова, "Дослідження процедури формування контрольної суми повного факторіального коду на основі ітераційного перетворення", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 17.

[31] Е. В. Фауре, О. О. Харін і Д. О. Литвиненко, "Дослідження процедури формування контрольної суми повного факторіального коду на основі залишку

за модулем", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 16-17.

[32] Е. В. Фауре і А. Ю. Бойко, "Дослідження здатності виявлення помилок факторіальним кодом з декількома контрольними сумами", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 16.

[33] Е. В. Фауре і В. Л. Юрченко, "Дослідження здатності виявлення помилок факторіальним кодом з відновленням даних", в *Проблеми інформатизації: Тези доповідей П'ятої Міжнародної науково-технічної конференції, Черкаси, 13-15 листопада 2017 р.*, Черкаси : ЧДТУ ; Баку : ВА ЗС АР; Бельсько-Бяла : УтіГН ; Полтава : ПНТУ, 2017, с. 16.

Наукові праці, які додатково відображають наукові результати дисертації

[1] Е. В. Фауре, Д. В. Фауре і Р. О. Бівзюк, "Пристрій формування залишків у багатоканальних завадостійких кодеках", патент України №55711, 27.12.2010.

[2] В. В. Швидкий, А. І. Щерба, Е. В. Фауре і В. В. Веретельник, "Спосіб формування некорельованої послідовності рівномірно розподілених чисел", патент України №74628, 12.11.2012.

[3] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, А. І. Щерба і А. О. Лавданський, "Спосіб двоконтурного поточного шифрування", патент України №82044, 25.07.2013.

[4] А. О. Лавданський, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування послідовності рівномірно розподілених випадкових чисел", патент України №86718, 10.01.2014.

[5] Ю. Г. Лега, В. В. Швидкий, Е. В. Фауре, О. С. Лісіцина і А. О. Лавданський, "Спосіб формування послідовності випадкових чисел", патент України №86705, 10.01.2014.

[6] Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування випадкової послідовності перестановок", патент України №106668, 10.05.2016.

[7] Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб формування імітовставки", патент України №106669, 10.05.2016.

[8] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб комбінованого кодування інформації", патент України №107657, 24.06.2016.

[9] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий і А. І. Щерба, "Спосіб контролю цілісності інформації", патент України №107655, 24.06.2016.

[10] Е. В. Фауре, О. О. Харін, В. В. Швидкий і А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", патент України №117004, 12.06.2017.

[11] Е. В. Фауре, О. О. Харін, В. В. Швидкий і А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", патент України №121361, 11.12.2017.

[12] Е. В. Фауре і О. О. Харін, "Пристрій кодування та декодування факторіальних кодів з виявленням і виправленням помилок", патент України №123640, 12.03.2018.

Апробацію результатів дисертації проведено на:

– XI Міжнародній науково-технічній конференції «Системний аналіз та інформаційні технології» (Київ, 26-30 травня 2009) – заочна участь;

– XVI Міжнародній науково-технічній конференції «Системний аналіз та інформаційні технології» (Київ, 26-30 травня 2014) – очна участь;

– II Міжвузівській науково-практичній конференції «Актуальні проблеми технічних і природних наук у забезпеченні цивільного захисту» (Черкаси, 30-31 березня 2009) – очна участь;

– Міжнародній науково-практичній конференції «Інформаційні технології та комп’ютерна інженерія» (Вінниця, 19-21 травня 2010) – заочна участь;

– Науково-технічній конференції «Проблеми телекомунікацій» (Київ, 2011) – заочна участь;

– V Міжнародній науково-технічній конференції «Сучасні проблеми

радіоелектроніки, телекомунікацій та приладобудування» (Вінниця, 19-21 травня 2011) – очна участь;

– Міжнародній науково-практичній конференції «Інформаційні технології в освіті, науці і техніці» (Черкаси, 25-27 квітня 2012) – очна участь;

– Міжнародній науковій конференції «Информационные технологии и системы» (Мінськ, Білорусь, 24 жовтня 2012) – заочна участь;

– Міжнародній науково-практичній інтернет-конференції «Сучасність, наука, година. Взаємодія та взаємовплив» (Київ, 19-21 листопада 2012) – заочна участь;

– Всеукраїнській науково-практичній Internet-конференції «Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку» (Черкаси, 18-22 березня 2013, 17-21 березня 2014, 16-20 березня 2015, 14-20 березня 2016, 13-19 березня 2017) – дистанційна участь;

– Міжнародній науково-практичній конференції «Обробка сигналів і негауссівських процесів» (Черкаси, 22-24 травня 2013) – очна участь;

– IX Міжнародній науковій конференції «Сучасні досягнення в науці і освіті» (Нетанія, Ізраїль, 22-29 вересня 2014) – очна участь;

– Doctoral Summer School (Berlin, Germany, 4-7 серпня 2015) – очна участь;

– II, III, IV, V Міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси, 25-26 листопада 2014, 12-13 листопада 2015, 3-4 листопада 2016, 13-15 листопада 2017) – очна участь;

– International Scientific Conference «The scientific potential of the present» (St. Andrews, Scotland, UK, 1 грудня 2016) – заочна участь;

– Всеукраїнській науково-практичній конференції «Актуальні задачі та досягнення у галузі кібербезпеки» (Кропивницький, 23-25 листопада 2016) – заочна участь.