АНОТАЦІЯ

Харін О.О. Методи та засоби інтегрованого захисту інформації в телекомунікаційних системах множинного доступу на основі факторіального кодування даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія». – Черкаський державний технологічний університет, Черкаси, 2020.

Дисертаційна робота спрямована на вирішення актуальної науково-технічної задачі, що полягає в підвищенні достовірності передавання інформації, забезпеченні її конфіденційності та цілісності на основі використання факторіального кодування даних. Ця задача передбачає необхідність удосконалення існуючих методів факторіального кодування, створення методу побудови телекомунікаційних систем на основі нероздільного факторіального кодування з динамічним розподілом ресурсів між користувачами системи в режимі реального часу.

У роботі проведено аналіз існуючих методів факторіального кодування, зокрема факторіального коду з відновленням даних за перестановкою, який показав, що вони вразливі до помилок парної кратності, таких, що призводять до трансформації однієї перестановки з дозволеної множини в іншу перестановку, що належить цій же множині. З метою підвищення стійкості факторіальних кодів до помилок парної кратності, сформульовано задачу роботи, яка полягає у розробці методів підвищення достовірності передавання даних у системах з нероздільним факторіальним кодуванням.

Ще одним напрямком досліджень, пов'язаним з факторіальним кодуванням, є процес формування сигнально-кодової конструкції для нероздільних методів факторіального кодування, зокрема факторіального кодування з відновленням даних за перестановкою, що дозволило б виявляти та виправляти помилки малої кратності. З метою забезпечення бажаного рівня достовірності передавання даних та максималізації швидкості коду, було сформульовано наступну задачу дисертаційної роботи, яка полягає у розробці

методу формування сигнально-кодової конструкції для систем *з* факторіальним кодування з відновленням даних за перестановкою.

Розглянуто існуючі методи кодування мовленнєвих сигналів. Проаналізовано методи кодування на основі згорткових кодів та методи на основі каскадних кодів. Аналіз згорткових кодів показав, що сформована кодова послідовність містить інформаційні символи у відкритому вигляді, що накладає обмеження на використання цих кодів під час передавання конфіденційної інформації, а також мають швидкість коду, яка не перевищує 1/2, тобто одному інформаційному символу ставиться у відповідність два символи кодової послідовності. У той же час, каскадні коди, за рахунок послідовного використання декількох кодів, дозволяють вирішити проблему захисту інформації від несанкціонованого читання, але вносять додаткову надлишковість, а також збільшують апаратні витрати. Виконаний аналіз дає змогу чітко сформулювати наступну задачу дисертаційного дослідження, яка полягає у розробці методів декодування факторіальних кодів з відновленням даних за перестановкою для систем передавання мовленнєвої інформації реального часу.

Виконано аналіз існуючих методів побудови телекомунікаційних систем з множинним доступом на базі мультиплексування пакетів та часового розподілу. Аналіз цих методів показав, що більшість з них передбачають наявність службових пакетів для реалізації механізму резервування / звільнення часових інтервалів під передачу даних, що зменшує загальну пропускну здатність каналу. Також у цих методах не реалізовано єдину процедуру забезпечення інтегрованого захисту інформації. Виходячи з цього, сформульовано ще одну задачу даної роботи, яка полягає в розробці методу побудови телекомунікаційних систем множинного доступу з використанням нероздільного факторіального кодування.

В рамках дисертаційного дослідження вперше розроблено методи підвищення достовірності передавання даних у системах з факторіальним кодування з відновленням даних за перестановкою, які за рахунок доповнення перестановки бітами ознак та комбінування завадостійких кодів дозволяють

підвищити здатність нероздільних факторіальних кодів до виявлення помилок. Розроблено алгоритм факторіального кодування з додатковими перевірними бітами. Реалізація алгоритму дає змогу зменшити ймовірність невиявленої кодом помилки, за незалежних бітових помилок, у порівнянні з факторіальним кодом з відновленням даних за перестановкою з доповненням на 2-4 порядки для $M = 8$ у залежності від ймовірності бітової помилки за рахунок незначної втрати в швидкості коду. Також розроблено алгоритм факторіального каскадного кодування. Реалізація алгоритму дає змогу на порядок зменшити ймовірність невиявленої кодом помилки, за незалежних бітових помилок, у порівнянні з ФКВД для $k = 15$ у залежності від ймовірності бітової помилки, при цьому за довжини блоку даних $k \geq 128$ швидкість коду не змінюється.

Вперше розроблено метод формування сигнально-кодової конструкції для систем з факторіальним кодування з відновленням даних за перестановкою, який за рахунок побудови решіток з високою щільністю розташування сигнальних векторів дозволяє максимізувати швидкість коду для заданого рівня достовірності передавання даних та відповідної мінімальної відстані між вузлами решітки. Побудовано решітки, вузлами якої є перестановки, що дозволяють виявляти помилки кратності $t \leq 5$ і виправляти помилки кратності $t \leq 2$ з максимальною швидкістю коду для $M = 5$, $k = 3$, $N_{sv} = 10$ та $M = 6$, $k = 5$, $N_{sv} = 60$.

Крім того, отримав подальший розвиток метод факторіального кодування з відновленням даних за перестановкою, який за рахунок відновлення даних з втратами на основі метрики Хеммінга або методу лінійної інтерполяції дозволяє забезпечити захист мовленнєвої інформації від помилок каналу зв'язку та несанкціонованого доступу в телекомунікаційних системах реального часу. Розроблено структурну схему пристрою декодування та алгоритм виправлення помилок з втратами у нероздільних факторіальних кодах в метриці Хеммінга, що забезпечує рівень шуму декодування, який не перевищує значень рівня комфортного шуму за ймовірності бітової помилки $p_0 \leq 10^{-2}$ у каналах з незалежними бітовими помилками. Розроблена схема дозволяє апаратно реалізувати пристрій декодування факторіальних кодів в

метриці Хеммінга. Розроблено структурну схему пристрою декодування та алгоритм виправлення помилок з втратами у нероздільних факторіальних кодах методом лінійної інтерполяції, що забезпечує рівень шуму декодування, який не перевищує значень рівня комфортного шуму за ймовірності бітової помилки $p_0 \leq 10^{-2}$ у каналах з пакетуванням бітових помилок. Розроблена схема дозволяє апаратно реалізувати пристрій декодування факторіальних кодів методом лінійної інтерполяції.

В заключній частині дисертаційного дослідження вперше розроблено метод побудови систем множинного доступу на основі нероздільного факторіального кодування, який за рахунок використання факторіального коду з заданим числом інверсій та виділення кожному з користувачів підмножини перестановок з певним набором властивостей забезпечує інтегрований захист інформації від несанкціонованого доступу та помилок каналу зв'язку, а також циклову синхронізацію без застосування окремого каналу синхронізації. Розроблено структурну схему та алгоритм роботи мультиплексора каналів зв’язку на основі факторіального коду з заданим числом інверсій, що не потребує організації синхронізуючого каналу та підтримує циклову синхронізацію за робочим сигналом. Розроблена схема дозволяє апаратно реалізувати мультиплексор каналів зв’язку. Розроблено структурну схему телекомунікаційної системи з множинним доступом з використанням мультиплексора каналів зв'язку на основі факторіального коду з заданим числом інверсій, розроблено алгоритм динамічного розподілу ресурсу пропускної здатності каналу залежно від значення навантаження, що створюється кожним з користувачів системи. Розроблена схема дозволяє апаратно реалізувати телекомунікаційну систему з множинним доступом на основі факторіального кодування.

Ключові слова: захист інформації, конфіденційність, цілісність, достовірність передавання даних, факторіальне кодування, сигнально-кодова конструкція, система множинного доступу.

SUMMARY

Kharin O. Methods and means of integrated protection of information in telecommunication systems with multiple access based on data factorial coding. – Qualified scientific work on the rights of the manuscript.

Thesis for a Doctor of Philosophy degree in specialty 123 "Computer engineering". – Cherkasy State Technological University, Cherkasy, 2020.

The dissertation is aimed at solving the actual scientific and technical problem of increasing the reliability of data transmission and ensuring their integrity using factorial codes that provide integrated protection of information (simultaneous protection against communication channel errors and protection against unauthorized modification and / or unauthorized access). This task includes the factorial codes improvements, create a method of construction of telecommunication systems that use these codes and have new features such as error correction with losses and dynamic allocation of resources between users of the system in real-time.

The paper analyzes the existing methods of factorial coding, including factorial code with data recovery by permutation, which showed that they are vulnerable to errors pair multiplicity which leading to a transformation of a permutation of the allowed set to another permutation, owned by the same set. To increase the robustness of factorial codes to even multiplicity errors, the task of the research is to develop the methods for improving the reliability of data transmission in systems with inseparable factorial coding.

Another area of research related to factorial coding is the process of forming a signal-code structure for inseparable methods of factorial coding, in particular, factorial code with data recovery by permutation. The following task of the dissertation is to develop the method of construction of signal-code structure for systems with factorial code with data recovery by permutation.

The existing methods of encoding speech signals are considered. Methods of coding based on convolutional codes and methods based on cascading codes are analyzed. Analysis convolutional codes showed that formed coding sequence contains unprotected information symbols, which restricts the use of these codes for confidential information exchange. Also, convolutional codes have speed code which

no more than 1/2. At the same time, cascading codes, through the consistent use of several codes, can solve the problem of protecting information from unauthorized reading, but they add additional redundancy and also increase hardware costs. The performed analysis allows to clearly formulate the next task of the research, which is to develop a methods of decoding of factorial code with data recovery by permutation for real-time telecommunication systems.

The analysis of existing methods of construction of telecommunication systems with multiple access based on multiplexing of packets and time distribution is made. An analysis of these methods showed that most of them involve the availability of service data to implement a reservation/ release mechanism of time slots for data transmission, which reduces the overall bandwidth of the channel. Also, these methods do not implement a single procedure for providing integrated information security. The results of the analysis made it possible to define clearly the tasks of the research to develop a method of construction of multiple access systems based on inseparable factorial coding.

As part of the research a new methods of improving the reliability of data transmission systems with factorial coding with data recovery by permutation were developed, which allows to increase the capacity of inseparable factorial codes to detect errors by adding of additional bits signs to the permutation and combining of the noise immunity codes. The algorithm of factorial coding with additional bits has been developed. Implementation of the algorithm allows reducing the undetected error probability, for independent bit errors, compared to the factorial code with data recovery by permutation with addition by $2 - 4$ orders of magnitude at $M = 8$ depending on the bit error probability due to a small loss in code speed. Also, the algorithm of factorial cascade coding has been developed. Implementation of the algorithm allows to reduce the undetected error probability, for independent bit errors, compared to the factorial code with data recovery by permutation by order of magnitude for $k = 15$ depending on the bit error probability with same code speed if the length of the data block is $k \geq 128$.

At first time a method of forming a code signal design for systems with factorial coding of data recovery permutation has been developed. It

allowed to maximize speed of code for a given level of reliability data and the corresponding minimum distance between the nodes by constructing arrays of high density arrangement of signal vectors. A lattice is constructed, the nodes of which are permutations that allow to detect errors of multiplicity $t \leq 5$, and correct errors of multiplicity $t \leq 2$ with a maximum speed of code for $M = 5,\ k = 3,$ $N_{sv} = 10$ and $M = 6, k = 5, N_{sv} = 60.$

In addition, the method of factorial coding with permutation data recovery has been further developed, which by data recovery with loss based on Hemming's metric or linear interpolation method allows protecting speech information from communication channel errors and unauthorized access in real-time telecommunications systems. The block diagram of the decoding device and the algorithm for error correction with losses in inseparable factorial codes in the Hamming metric are developed, which provides a decoding noise level that does not exceed the values of comfort noise level for bit error probability $p_0 \leq 10^{-2}$ in channels with independent bit errors. The developed scheme allows implementing a device for decoding factorial codes in the Hamming metric. The block diagram of the decoding device and the algorithm of error correction with losses in inseparable factorial codes by the method of linear interpolation are developed, which provides the level of decoding noise that does not exceed the values of comfort noise level in bit error probability $p_0 \leq 10^{-2}$ in channels with packets of errors. The developed scheme allows implementing a device for decoding factorial codes by linear interpolation.

In the final part of the dissertation research at first time a method of building multiple access systems based on inseparable factorial coding has been developed, which provides integrated protection of information from unauthorized access and as well as cyclic synchronization without the use of a separate synchronization channel. The structural scheme and algorithm of operation of the multiplexer of communication channels on the basis of the factorial code with the given number of inversions which does not required the organization of the synchronizing channel and supports cyclic synchronization on a working signal are developed. The developed scheme allows implementing multiplexer of communication channels on

hardware basis. The block diagram of telecommunications system with multiple access using multiplexer channels based on a factorial code with given number of inversions, the algorithm of dynamic resource allocation bandwidth based on the load generated by each of the users also have been developed The structural scheme allows to implement telecommunication in systems with multiple access based on factorial code on hardware basis.

Keywords: information security, confidentiality, integrity, reliability of data transmission, factorial coding, signal-code construction, multiple access systems.

Список основних публікацій здобувача

[1] О. О. Харін, «Оцінка властивостей каскадного коду, що поєднує факторіальний та рівноважний код», *Вісник Черкаського державного технологічного університету*, № 2, с. 86-90, 2017.

[2] О. О. Харін, «Порівняльна оцінка факторіальних кодів», *Вісник Черкаського державного технологічного університету. Серія: технічні науки*, № 4, с. 88-93, 2017.

[3] E. V. Faure, A. I. Shcherba and A. A. Kharin, «Factorial Code with a Given Number of Inversions», *Radio Electronics, Computer Science, Control*, vol. 2, p. 143-153, 2018.

[4] E. V. Faure, V. V. Shvydkyi, A. O. Lavdanskyi and O. O. Kharin, «Methods of factorial coding of speech signals», *Radio Electronics, Computer Science, Control*, vol. 4, p. 186-198, 2019.

[5] J. Al-Azzeh, B. Ayyoub, E. Faure, V. Shvydkyi, O. Kharin and A. Lavdanskyi, «Telecommunication Systems with Multiple Access Based on Data Factorial Coding», *International Journal on Communications Antenna and Propagation (IRECAP)*, vol. 10, issue 2, p. 102-113, 2020.

[6] Е. В. Фауре та О. О. Харін, «Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних», в *Актуальні задачі та досягнення у галузі кібербезпеки: Тези доповідей Всеукраїнської науково-практичної*

конференції, Кропивницький, 23-25 листопада 2016 р., Кропивницький, 2016, с. 178-179.

[7] Е. В. Фауре та 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: Тези доповідей Всеукраїнської науково-практичної Internet-конференції, Черкаси, 13-19 березня 2017 р.*, Черкаси: ЧДТУ, 2017, с. 74–76.

[8] О. О. Харін, «Підвищення достовірності передачі даних за допомогою факторіального кодування з виявленням транспозицій», в *Надзвичайні ситуації: безпека та захист: Тези доповідей VII Всеукраїнської науково-практичної конференції з міжнародною участю, Черкаси, 20-21 жовтня 2017 р.*, Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, 2017, с. 162-163.

[9] А. А. Харин и А. И. Щерба, «Организация замкнутой группировки абонентов в открытой сети коллективного пользования», в *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2018): Тези доповідей IV Міжнародної науково-практичної конференції, Черкаси, 17-18 травня 2018 р.*, Черкаси: ЧДТУ, 2018, с. 109-111.

[10] О. О. Харін, «Формування сигнально-кодової конструкції на основі теорії решіток», в *Наука України – погляд молодих вчених крізь призму сучасності: Тези доповідей II Всеукраїнської науково-практичної конференції з міжнародною участю, Черкаси, 26 вересня 2019 р.*, Черкаси: ЧДТУ, 2019, с.42-44.

[11] О. О. Харін, Е. В. Фауре та А. О. Лавданський, «Оцінка захищеності мовного сигналу в системах з факторіальним кодуванням», в *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2020): Тези доповідей V Міжнародної науково-практичної конференції, Черкаси, 21-23 травня 2020 р.*, Черкаси: ЧДТУ, 2020, с. 85-87.

[12] Е. В. Фауре, О. О. Харін, В. В. Швидкий та А. О. Лавданський, «Ефективність виявлення помилок факторіальними кодами», в

Інформаційні технології в освіті, науці і техніці (ІТОНТ-2020): Тези доповідей V Міжнародної науково-практичної конференції, Черкаси, 21-23 травня 2020 р., Черкаси: ЧДТУ, 2020, с. 94-95.

[13] Е. В. Фауре, О. О. Харін, В. В. Швидкий та А. І. Щерба, «Спосіб факторіального кодування з виявленням і виправленням помилок», Україна. Пат. 121361, 11.12.2017.

[14] Е. В. Фауре та О. О. Харін, «Пристрій кодування та декодування факторіальних кодів з виявленням і виправленням помилок», Україна. Пат. 123640, 12.03.2018.

[15] О. О.Харін та А. І. Щерба, «Спосіб факторіального кодування в метриці Хеммінга», Україна. Пат. 130458, 10.12.2018.

[16] Е. В. Фауре, О. О. Харін, В. В. Швидкий та А. І. Щерба, «Спосіб факторіального кодування з відновленням даних», Україна. Пат. 117004, 12.06.2017.

[17] А. О. Лавданський, Е. В. Фауре, О. О. Харін та В. В. Швидкий, «Спосіб декодування факторіального коду з відновленням вибірок мовного сигналу реального часу в метриці Хеммінга», Україна. Пат. 137722, 11.11.2019.

[18] А. О. Лавданський, Е. В. Фауре, О. О. Харін та В. В. Швидкий, «Спосіб декодування факторіального коду з відновленням вибірок мовного сигналу реального часу методом лінійної інтерполяції», Україна. Пат. 139760, 27.01.2020.