ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 004.052.2

[0000-0002-2046-481X] **Е. В. Фауре,** *д.т.н., професор*,
e-mail: e.faure@chdtu.edu.ua
[0000-0003-1791-6755] **О. О. Харін,**
[0000-0002-1596-4123] **А. О. Лавданський,** *к.т.н.*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ОЦІНКА ВЛАСТИВОСТЕЙ СИНТЕЗОВАНИХ НА ОСНОВІ ТЕОРІЇ РЕШІТОК СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ ДЛЯ НЕРОЗДІЛЬНИХ ФАКТОРІАЛЬНИХ КОДІВ

У роботі досліджено основні параметри систем передавання даних з нероздільним факторіальним кодуванням, що використовують сигнально-кодові конструкції, синтезовані на основі теорії решіток. Цей метод формування сигнально-кодових конструкцій дає можливість максимізувати швидкість коду для заданого рівня достовірності, що визначається мінімальною відстанню Хеммінга між перестановками. Виконано оцінювання таких параметрів, як відносна швидкість передавання і ймовірність невиявленої помилки. Побудовано експериментально-розрахункову модель, що дало змогу визначити, яким чином змінюються ймовірнісні характеристики коду залежно від імовірності бітової помилки в каналах зв'язку з незалежними бітовими помилками. На основі отриманих експериментальних даних виконано аналіз здатності досліджуваних сигнально-кодових конструкцій до виправлення помилок. Визначено переваги та недоліки методу формування сигнально-кодових конструкцій на основі теорії решіток.

Ключові слова: *факторіальний код, відносна швидкість передавання, ймовірність бітової помилки, завадостійке кодування, криптографічний захист.*

Вступ. Однією з головних функцій комп'ютерних систем і мереж є забезпечення безпеки інформації, що в них циркулює. Водночас не менш важливою функцією є захист інформації від впливу завад, що виникають у каналі зв'язку.

Використання факторіальних кодів є одним із підходів до поєднання завадостійкого кодування та криптографічного захисту, ефективність якого підтверджується результатами, отриманими в роботах [1]–[7]. Разом з тим, факторіальні коди з відновленням даних за перестановкою (ФКВД) [1], [3], [4] вразливі до помилок парної кратності, таких, що призводять до трансформації однієї перестановки з дозволеної множини в іншу перестановку, що належить цій же множині. Описаний у [8] метод дає змогу підвищити стійкість факторіального коду до таких помилок, виявляючи всі двократні помилки, але має низьку швидкість.

Мета дослідження полягає в оцінюванні основних характеристик методу формування сигнально-кодової конструкції (СКК) [9], [10] для ФКВД, що забезпечує досягнення необхідного значення достовірності передавання і дає можливість максимізувати швидкість коду за рахунок формування підмножини перестановок на основі теорії решіток. Оцінюванню підлягають відносна швидкість передавання та ймовірність невиявленої помилки в результаті застосування синтезованих СКК у системах з нероздільним факторіальним кодуванням.

Виклад основного матеріалу. Для оцінювання сутності методу формування СКК на основі теорії решіток спочатку визначимо деякі поняття та терміни.

Визначення 1. Питомою помилкою $f_{per}(t)$ називається математичне сподівання кількості невиявлених помилок кратності t для кожного з вузлів решітки.

Визначення 2. Сигнальним вектором називається перестановка π з дозволеної множини перестановок, представлена в двійковому вигляді.

Визначення 3. Сигнально-кодовою конструкцією називається множина сигнальних векторів, що використовується для кодування інформації.

Визначення 4. Решіткою називається СКК, в якій відстань Хеммінга $d_{i,j}$ між будь-якими двома сигнальними векторами (π_i, π_j) не менша деякого, наперед заданого значення $d_{\min}$. Водночас така СКК повинна бути не-

DOI: 10.24025/2306-4412.3.2020.214937

критичною (інваріантною) до розміщення вузлів усередині решітки.

Основними параметрами решітки є:

– мінімальна відстань $d_{\min}$;

– кількість вузлів решітки N_{sv}, відстань між якими не менша за $d_{\min}$;

– потужність множини символів перестановки (довжина перестановки) M.

Зазначимо, що збільшення мінімальної відстані $d_{\min}$ дає можливість підвищити достовірність передавання даних, але призводить до зменшення кількості вузлів решітки N_{sv} і, як наслідок, до зменшення швидкості коду. Відповідно до [10] метод формування СКК на основі теорії решіток передбачає наступні дії:

– обирається деяке початкове значення M, для якого будується підмножина не менше ніж з двох перестановок з попарними відстанями Хеммінга $d_{i,j} \geq 2t+1$. У результаті (після $M! \cdot M!$ перевірок) отримаємо не менше двох перестановок (π_i, π_j), де i і j – номери цих перестановок в упорядкованій множині всіх $M!$ перестановок з попарними відстанями $d_{i,j} \geq 2t+1$;

– потужність множини символів (довжина перестановки) M збільшується на одну одиницю, до значення $M+1$. Для цього по черзі над усіма вузлами сформованої решітки, що містять M символів, одночасно виконують одну з можливих підстановок і вставляють $(M+1)$-й символ між символами перестановки, після чого відбирають тільки такі перестановки, в яких між будь-якою парою перестановок (π_i, π_j) мінімальна відстань задовольняє умові $d_{i,j} \geq 2t+1$. За такої процедури потужність сформованої СКК збільшується в $(M+1)$ разів. Цю операцію повторюють доти, поки кількість перестановок у підмножині перестановок не досягне або не перевищить наперед заданого значення, що забезпечує необхідну швидкість коду. На цьому процедура формування підмножини перестановок, інваріантних до обертання осей СКК, завершена;

– після завершення процедури формування інваріантних перестановок (інваріантної підмножини перестановок) уточняється кількість біт k, що переносяться кожною перестановкою цієї підмножини;

– уточнивши склад інваріантної підмножини, формується СКК у вигляді таблиці відображення $\{A(x)\} \to \{\pi\}$ множини слів джерела $A(x)$ у множину перестановок π для кодера і таблиці відображення $\{\pi\} \to \{A(x)\}$ для декодера.

Для оцінювання ефективності запропонованого методу формування СКК використаємо методи факторіального кодування з відновленням даних за перестановкою (ФКВД) [1] та факторіального кодування з відновленням даних за перестановкою з виправленням помилок (ФКВДвп) для СКК в метриці Хеммінга (ФКВДвп-2) [11]–[14], де також представлено теоретичну оцінку ймовірності невиявленої помилки.

З метою визначення ймовірності невиявленої помилки розроблено експериментально-розрахункову модель, що імітує середовище передавання даних з незалежними бітовими помилками. Модель дає змогу для заданої якості каналу (ймовірності бітової помилки) оцінити наступні ймовірнісні характеристики:

– ймовірність виявлення помилки P_{det};

– ймовірність невиявлення помилки P_{ud};

– ймовірність прийому кодового слова без помилок Q.

Водночас сума всіх ймовірностей дорівнює одиниці: $P_{det} + P_{ud} + Q = 1$.

Відносна швидкість передавання визначається відповідно до формули

$$v_0 = v_1 v_2,$$

де $v_1 = k / n$ – швидкість коду;

v_2 – динамічна складова втрати швидкості внаслідок повторних запитів [15].

Для систем з ФКВД з виявленням помилок і їх виправленням шляхом перезапиту

$$v_2 = Q + P_{ud}.$$

Відзначимо, що для систем з ФКВДвп-2, де передбачено виправлення помилок, динамічна складова v_2 відсутня, тому відносна швидкість передавання в таких системах фактично дорівнює швидкості коду.

Результати досліджень. Першим етапом роботи розробленої експериментально-розрахункової моделі є формування СКК для заданої потужності множини символів перестановки M та мінімальної відстані між вузлами решітки $d_{\min}$. Після цього для отриманої множини перестановок визначається зна-

DOI: 10.24025/2306-4412.3.2020.214937

чення питомої помилки $f_{per}(t)$ для подальшого застосування в обчисленні ймовірнісних характеристик.

Наступним етапом роботи моделі є використання синтезованих решіток як таблиць замін у програмних моделях для систем з ФКВД та ФКВДвп-2 за різних значень імовірності бітової помилки p_0. Отримані на цьому етапі роботи моделі ймовірнісні характеристики дали змогу виконати оцінювання основних параметрів синтезованих решіток у системах з вирішальним зворотним зв'язком та з детермінованим виправленням помилок.

У таблицях 1 і 2 наведено значення питомої помилки на вузол решітки $f_{per}(t)$ для решіток на 10 та 60 вузлів. Зазначимо, що для сформованих за допомогою запропонованого методу СКК значення $f_{per}(t)$ не залежать від того, які саме перестановки входять в решітку, тобто вони інваріантні відносно складу сигнальних векторів СКК і залежать тільки від кількості вузлів у ній.

На рисунку 1 зображено графіки залежності ймовірностей невиявленої помилки ФКВД від імовірності бітової помилки p_0 за незалежних бітових помилок для $k=3$, $M=5$ та $k=5$, $M=6$ при $d_{\min}=5$.

На рисунку 2 зображено графік залежності ймовірності невиявленої помилки ФКВДвп-2 від ймовірності бітової помилки p_0 для розміру інформаційної частини $k=5$, $M=6$, $N_{sv}=60$, $d_{\min}=5$.

Таблиця 1 – **Значення $f_{per}(t)$ для решітки** $k=3$, $M=5$, $N_{sv}=10$, $d_{\min}=5$

Кратність помилки t	$f_{per}(t)$
1-5	0
6	4,5
7	0
8	1
9	0
10	1,5
11-15	0

Таблиця 2 – **Значення $f_{per}(t)$ для решітки** $k=5$, $M=6$, $N_{sv}=60$, $d_{\min}=5$

Кратність помилки t	$f_{per}(t)$
1-5	0
6	9,375
7	0
8	12,063
9	0
10	6,063
11	0
12	2,875
13	0
14	0,625
15-18	0

На рисунку 3 представлено результати порівняння ймовірностей невиявленої помилки ФКВД та ФКВДвп-2 для $k=5$, $M=6$, $N_{sv}=60$, $d_{\min}=5$.

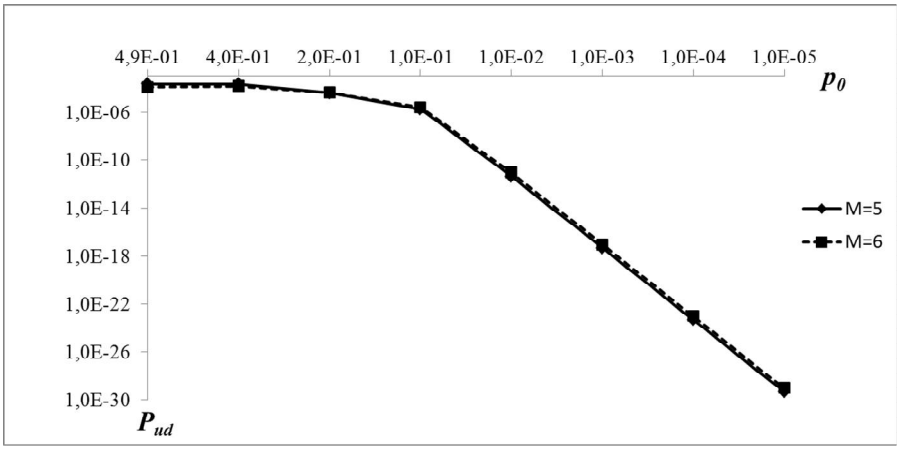

Рисунок 1 – Графіки залежностей імовірностей невиявленої помилки ФКВД від ймовірності бітової помилки для $k=3$, $M=5$, $N_{sv}=10$ та $k=5$, $M=6$, $N_{sv}=60$ та $d_{\min}=5$

DOI: 10.24025/2306-4412.3.2020.214937

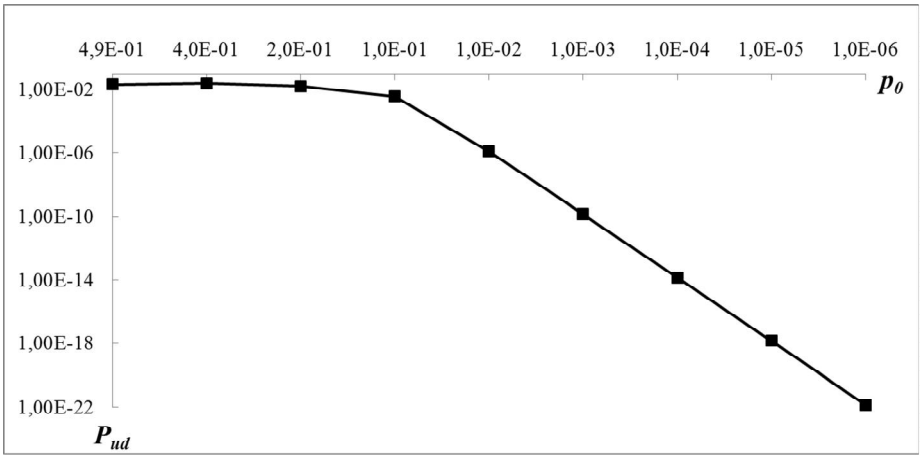

Рисунок 2 – Графік залежності ймовірностей невиявленої помилки ФКВДвп-2 від ймовірності бітової помилки p_0 для $k = 5$, $M = 6$, $N_{sv} = 60$, $d_{\min} = 5$

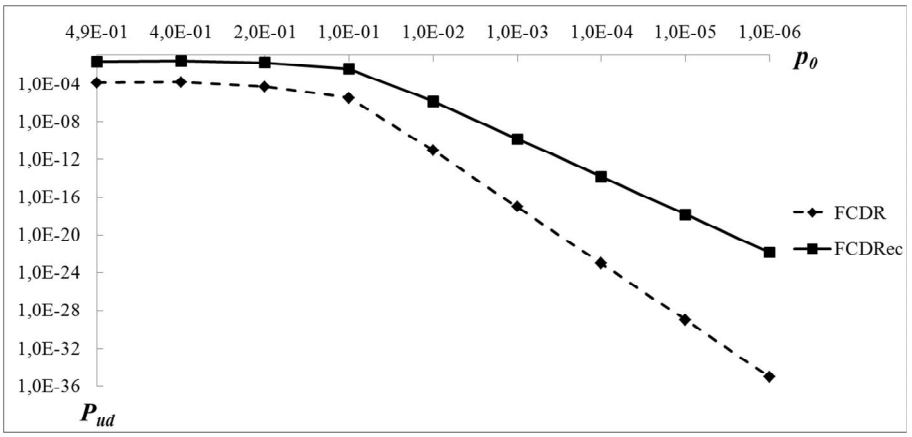

Рисунок 3 – Графіки залежностей імовірностей невиявленої помилки ФКВД та ФКВДвп-2 для $k = 5$, $M = 6$, $N_{sv} = 60$, $d_{\min} = 5$

На рисунку 4 зображено залежність швидкості коду ФКВДвп-2, СКК якого сформовано за допомогою запропонованого методу для різних довжин інформаційного вектора k.

Характер зображеної залежності подібний до характеру залежності швидкості ФКВД, зображеної на рисунку 1 в [1]. Такий вигляд обумовлений тим, що зі збільшенням довжини інформаційного вектора k виникає необхідність збільшення потужності множини символів перестановки M, щоб виконувалась умова $M! \geq 2^k$. У випадках, коли для деякого k справедливо $2^k \leq M! < 2^{k+1}$, збільшення значення M на одиницю призводить до різкого падіння швидкості коду внаслідок збільшення надлишковості через неоптимальну довжину інформаційного вектора.

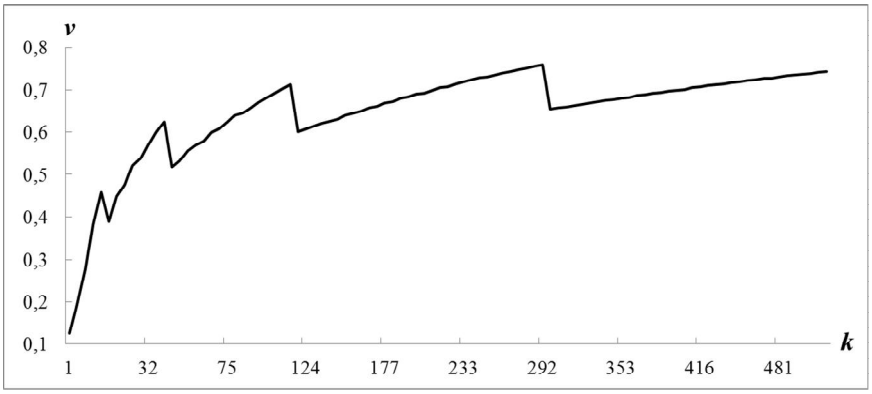

Рисунок 4 – Графік залежності швидкості коду ФКВДвп-2 від довжини блока даних на вході кодера для $d_{\min} = 5$

DOI: 10.24025/2306-4412.3.2020.214937

На рисунку 5 зображено залежність відносної швидкості передавання ФКВД і ФКВДвп-2 від імовірності бітової помилки p_0 для $k = 5$, $M = 6$.

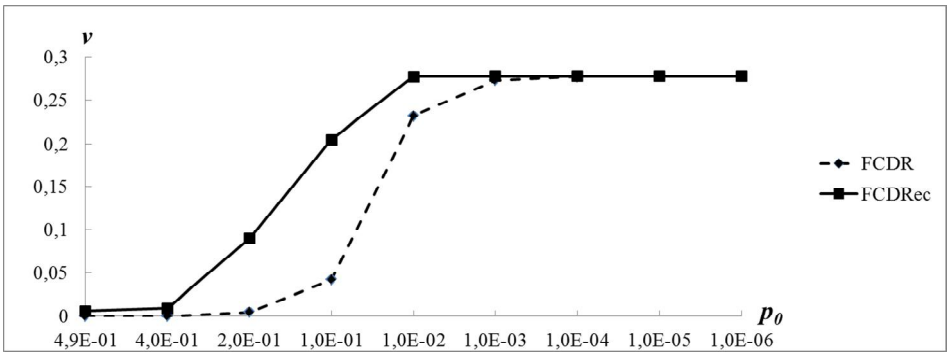

Рисунок 5 – Графіки залежностей відносної швидкості передавання ФКВД та ФКВДвп-2 для $k = 5$, $M = 6$

Обговорення результатів. Дані, наведені в таблицях 1 і 2, показують, що сформовані решітки забезпечують виявлення всіх помилок непарної кратності, а також усіх помилок з кратністю $t \le 5$.

Рисунок 1 показує, що сформована СКК забезпечує ймовірність невиявленої помилки, що не перевищує значення 10^{-4} для $p_0 = 0,49$, тобто в умовах, близьких до стану обриву каналу зв'язку, за якого на вхід приймача надходить лише шум. За такої ймовірності бітової помилки загальновідомі системи передавання даних не зможуть працювати через втрату циклової синхронізації, в той час, коли ФКВД має властивість до самосинхронізації. Це дає можливість використовувати цей метод формування СКК для кодування даних в умовах активної радіоелектронної боротьби або в умовах, коли достовірність передавання даних важливіша швидкості коду. Також з графіка видно, що синтезовані СКК забезпечують майже однакові значення ймовірності невиявленої помилки. Це обумовлено тим, що рівень достовірності визначається мінімальною відстанню між вузлами решітки $d_{\min}$ і майже не змінюється при зміні потужності множини символів M.

З рисунків 2 і 3 випливає, що ФКВДвп-2 має більшу ймовірність невиявленої помилки порівняно з ФКВД для заданої СКК, оскільки мінімальна відстань між вузлами решітки $d_{\min} = 5$, що забезпечує виправлення помилок кратності $t \le 2$. Усі помилки, кратність яких $t > 2$, призводять до помилки декодування, в той час, коли ФКВД виправляє такі помилки шляхом повторного запиту блока.

З рисунка 4 випливає, що запропонований метод формування СКК забезпечує відносно малу швидкість коду, яка зростає зі збільшенням кількості вузлів у решітці.

У свою чергу, рисунок 5 свідчить про те, що ФКВДвп-2 має значно вищу відносну швидкість передавання для каналів низької якості $(0,1 \le p_0 \le 0,49)$, але водночас забезпечує нижчу достовірність передавання даних через велику кількість помилок кратності $t > 2$, що призводять до помилкового декодування.

Разом з тим, зі зменшенням імовірності бітової помилки відносна швидкість передавання для обох методів вирівнюється внаслідок зменшення кількості помилок і, як результат, зменшення втрат часу на повторні запити спотворених блоків у системах з ФКВД.

Висновки. Виконаний у роботі аналіз методу формування СКК на основі теорії решіток для систем з нероздільним факторіальним кодуванням дав змогу визначити наступні параметри:

- питому помилку $f_{per}(t)$;
- імовірність невиявленої помилки P_{ud};
- відносну швидкість передавання v_0.

DOI: 10.24025/2306-4412.3.2020.214937

Показано, що метод формування СКК на основі теорії решіток дає змогу підвищити достовірність передавання даних за рахунок використання для перенесення інформації лише тих перестановок, що знаходяться на відстані Хеммінга, не меншій за $d_{\min}$, яке визначається на етапі проектування системи. Чим більше значення $d_{\min}$, тим вища достовірність передавання даних і тим менша швидкість коду, оскільки зменшується кількість перестановок-носіїв інформації.

Виконане порівняння зазначених характеристик для систем з ФКВД та ФКВДвп-2 показало, що ФКВДвп-2 має більшу відносну швидкість передавання в каналах низької якості, але водночас забезпечує гіршу достовірність передавання порівняно з ФКВД в результаті помилкового виправлення помилок.

Недоліком методу формування СКК є те, що він вимагає значних обчислювальних ресурсів для побудови решіток зі збільшенням потужності множини символів перестановки M. Крім того, зазначимо, що ФКВДвп передбачає детермінований процес виправлення помилок, що призводить до помилкового виправлення і, як наслідок, не виявленої кодом помилки у випадках, коли кратність помилки перевищує задане значення t.

Список використаних джерел

[1] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету*, № 2, с. 33-39, 2016.

[2] Е. В. Фауре, та О. О. Харін, "Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних", на *Всеукр. наук.-практ. конф. Актуальні задачі та досягнення у галузі кібербезпеки*: тези доп., Кропивницький, 2016, с. 178-179.

[3] Е. В. Фауре, О. О. Харін, В. В. Швидкий, та А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", *Укр. пат. 117004*, Черв. 12, 2017.

[4] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с восстановлением данных", *Вісник Черкаського державного технологічного університету*, № 4, с. 57-61, 2016.

[5] О. О. Харін, "Порівняльна оцінка факторіальних кодів", *Вісник Черкаського державного технологічного університету*, № 4, с. 88-93, 2017.

[6] Е. В. Фауре, О. О. Харін, В. В. Швидкий, та А. О. Лавданський, "Ефективність виявлення помилок факторіальними кодами", на *V Міжнар. наук.-практ. конф. Інформаційні технології в освіті, науці і техніці (ІТОНТ-2020)*: тези доп. Черкаси: ЧДТУ, 2020, с. 94-95.

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

[8] 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, pp. 143-153, 2018.

[9] О. О. Харін, та А. І. Щерба, "Спосіб факторіального кодування в метриці Хеммінга", *Укр. пат. 130458*, Груд. 10, 2018.

[10] О. О. Харін, "Формування сигнально-кодової конструкції на основі теорії решіток", на *ІІ Всеукр. наук.-практ. конф. з міжнар. участю. Наука України – погляд молодих вчених крізь призму сучасності:* тези доп., Черкаси: ЧДТУ, 2019, с. 42-44.

[11] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в *Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба*: монографія В. М. Безрука, В. В. Баранника, Харьков, Украина: Лидер, 2017, с. 291-323.

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

[13] Е. В. Фауре, та О. О. Харін, "Факторіальне кодування з відновленням даних і виправленням помилок", на *Всеукр. наук.-*

DOI: 10.24025/2306-4412.3.2020.214937

практ. Internet-конф. Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: тези доп., Черкаси: ЧДТУ, 2017, с. 74-76.

[14] Е. В. Фауре, О. О. Харін, В. В. Швидкий, та А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", *Укр. пат. 121361*, Груд. 11, 2017.

[15] Л. М. Финк, *Теория передачи дискретных сообщений*. Москва, Россия: Сов. радио, 1970.

References

[1] E. V. Faure, "Factorial coding with data recovery", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 2, pp. 33-39, 2016 [in Russian].

[2] E. V. Faure, and O. O. Kharin, "Investigation of the probability of decoding error when using factorial code with data recovery", in *Proc. All-Ukr. Conf. Current Challenges and Achievements in the Field of Cybersecurity,* Kropyvnytskyi, 2016, pp. 178-179 [in Ukrainian].

[3] E. V. Faure, O. O. Kharin, V. V. Shvydkyi, and A. I. Shcherba, "Method of factorial coding with data recovery", *Ukr. Patent 117004*, June 12, 2017 [in Ukrainian].

[4] E. V. Faure, "A method of increasing the efficiency of factorial coding with data recovery", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 4, pp. 57-61, 2016 [in Ukrainian].

[5] O. O. Kharin, "Comparative evaluation of factorial codes", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 4, pp. 88-93, 2017 [in Ukrainian].

[6] E. V. Faure, O. O. Kharin, V. V. Shvydkyi, and A. O. Lavdanskyi, "Efficiency of error detection by factorial codes", in *Proc. Vth Int. Conf. Information technologies in education, science and technology (ITONT-2020),* Cherkasy, 2020, pp. 94-95 [in Ukrainian].

[7] O. O. Kharin, "Estimation of properties of the cascade code, which combines the factorial and equilibrium codes", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 2, pp. 86-90, 2017 [in Ukrainian].

[8] A. A. Kharin, "Factorial code with a given number of inversions", *Radio Electronics, Computer Science, Control*, vol. 2, pp. 143-153, 2018.

[9] O. O. Kharin, and A. I. Shcherba, "The method of factorial coding in the Hamming metric", *Ukr. Patent 130458*, Dec. 10, 2018 [in Ukrainian].

[10] O. O. Kharin, "Formation of signal-code construction based on lattice theory", in *Proc. II Int. Conf. Science of Ukraine – the view of young scientists through the prism of modernity,* Cherkasy, 2019, pp. 42-44 [in Ukrainian].

[11] E. V. Faure, "Factorial coding with error correction. Theoretical substantiation and examples of implementation", in *Science-intensive technologies in infocommunications: information processing, cybersecurity, information warfare*: monograph by V. M. Bezruk, V. V. Barannik. Kharkiv, Ukraine: Lider, 2017, pp. 291-323 [in Russian].

[12] E. V. Faure, "Factorial coding with error correction", *Radio Electronics, Computer Science, Control*, no. 3, pp. 130-138, 2017 [in Russian].

[13] E. V. Faure, and O. O. Kharin, "Factorial coding with data recovery and error correction", in *Proc. All-Ukr. Internet-Conf. Automation and computer-integrated technologies in production and education: state, achievements, development prospects*, Cherkasy, 2017, pp. 74-76 [in Ukrainian].

[14] E. V. Faure, O. O. Kharin, V. V. Shvydkyi, and A. I. Shcherba, "Method of factorial coding with error detection and correction", *Ukr. Patent 121361*, Dec. 11, 2017 [in Ukrainian].

[15] L. M. Fink, *Discrete message transmission theory*. Moscow, Russia: Sov. radio, 1970 [in Russian].

DOI: 10.24025/2306-4412.3.2020.214937

E. V. Faure, *Dr.Sc., professor*,
e-mail: e.faure@chdtu.edu.ua
O. O. Kharin,
A. O. Lavdanskyi, *Ph.D.*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

EVALUATION OF PROPERTIES OF SIGNAL-CODE STRUCTURES SYNTHESIZED ON THE BASIS OF LATTICE THEORY FOR INSEPARABLE FACTORIAL CODES

One of the main functions of computer systems and networks is to ensure the security of information circulating in the system. At the same time, an equally important function is to protect information from the effects of interference in the communication channel.

The use of factorial codes is one approach to combining noise-tolerant encryption and cryptographic protection. But these codes are vulnerable to even errors, which lead to the transformation of one permutation from the allowed set to another permutation belonging to the same set. Therefore, the issue of improving the reliability of data transmission in systems with factorial coding is relevant.

The purpose of the study is to evaluate the method of forming a signal-code structure, which ensures the achievement of the required value of transmission reliability and allows to maximize the code speed by forming a subset of permutations based on lattice theory. The relative transmission rate and the probability of undetected error as a result of the use of synthesized signal-code constructs in systems with integral factorial coding are subject to evaluation.

To evaluate the efficiency of the synthesized signal-code constructions, the methods of factorial coding with data recovery by permutation and factorial coding with data recovery by permutation with error correction have been used. In order to determine the probability of undetected error, a software model has been developed that simulates a data transmission environment with independent bit errors.

The results of the software model have made it possible to establish the dependence of the probability of undetected error in systems with integral factorial coding on the probability of bit error in channels with independent bit errors. A comparative analysis of the relative transmission rate and the probability of undetected error in systems with factorial coding with data recovery by permutation and factorial coding with data recovery by permutation with error correction is also performed.

The results obtained in this paper have made it possible to determine the main advantages and disadvantages of the method of forming signal-code structures based on the lattice theory, as well as to determine the scope of this method.

Keywords: *factorial code, relative transmission rate, bit error probability, noise-tolerant encoding, cryptographic protection.*

Стаття надійшла 23.09.2020
Прийнято 06.10.2020

DOI: 10.24025/2306-4412.3.2020.214937