УДК 004.052.2

О. О. Харін, *аспірант*
kharin_aa@mail.ua
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ОЦІНКА ВЛАСТИВОСТЕЙ КАСКАДНОГО КОДУ, ЩО ПОЄДНУЄ ФАКТОРІАЛЬНИЙ ТА РІВНОВАЖНИЙ КОД

У роботі запропоновано і детально розглянуто принцип побудови каскадного кодування з використанням факторіального та рівноважного кодів. Запропонована комбінація кодів забезпечує підвищення достовірності передачі даних. Процес кодування передбачає послідовне використання рівноважного кодування та факторіального кодування з відновленням даних за перестановкою (ФКВД). Для запропонованого коду виконано оцінку достовірності передачі, швидкості та енергетичний виграш. Побудовано експериментально-розрахункову модель запропонованого каскадного коду з метою визначення залежності ймовірності помилкового декодування блоку даних від його розміру та ймовірності бітової помилки в каналі зв'язку для біноміального розподілу помилок на вході декодера. На основі отриманих експериментальних даних виконано порівняльний аналіз з ФКВД та надано рекомендації щодо його застосування.

***Ключові слова**: каскадний код, рівноважний код, факторіальний код, контроль цілісності інформації, криптографічний захист, достовірність передачі.*

Постановка проблеми. На сучасному етапі розвитку комп'ютерних систем і мереж актуальною задачею є підвищення достовірності передачі даних.

Засоби, направлені на вирішення цієї задачі, дозволяють покращити ефективність засобів обробки інформації за рахунок використання існуючої або внесення додаткової надлишковості, а пошук нових способів підвищення достовірності передачіє актуальним напрямком для дослідження.

Аналіз джерел та публікацій. Отримані в [1, 2, 3] результати показують ефективність використання факторіального кодування в каналах зв'язку зі зворотнім вирішальним зв'язком для задач контролю цілісності інформації (КЦІ). Особливої уваги заслуговує метод факторіального кодуванняз відновленням даних (ФКВД), що об'єднує функції виявлення помилок в каналі зв'язку та криптографічного захисту інформації. ФКВД передбачає заміну інформаційної послідовності з k біт на перестановку чисел порядку M, де $M! \geq 2^k$, причому значення, що перевищують 2^k вважаються забороненими і вказують на помилку під час передачі. Крім того, параметри перетворення інформаційної послідовності в перестановку можуть триматися в таємниці, що забезпечує захист даних від несанкціонованого доступу. Швидкість ФКВД залежить від розміру інформаційного блоку kі зростає з його збільшенням. Крім того, такий код забезпечує високу достовірність передачі даних за рахунок природної надлишковості ФКВД. У [3] також показано, що ФКВД вразливий допомилок парної кратності, які призводять до трансформації однієї перестановки дозволеної множинив іншу.

Таким чином, для підвищення достовірності передачі ФКВД необхідно підвищити стійкість до помилок парної кратності. Одним із таких способів є каскадне кодування, загальні принципи роботи якого описано в [5]. Каскадні коди дозволяють суттєво підвищити достовірність передачі даних за рахунок внесення додаткової надлишковості і, як наслідок, зниження пропускної здатності. Як показано в [5], в основі таких кодів лежить використання зовнішнього та внутрішнього кодування.

Мета роботи. Метою цієї роботи є розробка та аналіз методу каскадного кодування інформації, що поєднує факторіальний та рівноважний код і дозволяє підвищити достовірність передачі даних. Для цього в роботі необхідно виконати оцінку запропонованого каскадного коду в системах передачі даних з вирішальним зворотнім зв'язком та порівняти отримані характеристики з відповідними характеристиками ФКВД. При цьому необхідно оцінити:

- швидкість коду;
- імовірність помилкового декодування блоку даних;
- енергетичний виграш.

Рішення задачі. Попереднє перетворення інформаційної послідовності за допомогою коду, який дозволяє виявляти помилки парної кратності, є основою до підвищення достовірності передачіданих.

У якості внутрішнього коду, який дозволяє виконати часткове виявлення помилок парної кратності, обрано рівноважний код (EC – Equilibrium Code), властивості якого описано в [6]. Такий порядок слідування кодів дозволяє в повній мірі використати переваги ФКВД, а також зменшити ймовірність невиявленої каскадним кодом помилки. Далі такий каскадний код будемо називати факторіальним каскадним кодом (ФКК).

Рівноважний код передбачає заміну інформаційного блоку $A_k(x)$, що містить k біт, на послідовність $B_m(x)$ з m біт, що містить сталу кількість одиниць. Головною перевагою рівноважного коду є те, що він дозволяє виявляти всі помилки, окрім тих, що призводять одночасно до трансформації однакової кількості нулів та одиниць [6]. Інформаційна послідовність $B_m(x)$ перетворюється в перестановку $\pi_n(x)$, що містить n біт, за допомогою ФКВД, як описано в [3]. Описане послідовне перетворення має вигляд:

$$A_k(x) \to B_m(x) \to \pi_n(x). \qquad (1)$$

Для забезпечення можливості зворотного перетворення повинна виконуватися наступна вимога: кожному слову $A_k(x)$ повинно відповідати лише одне значення $B_m(x)$, а кожному значенню $B_m(x)$ – лише одне значення $\pi_n(x)$. Отже базова вимога до перетворення має вигляд:

$$M\{\pi_n(x)\} \ge M\{B_m(x)\} \ge M\{A_k(x)\}, \qquad (2)$$

де $M\{A_k(x)\} = 2^k$ – потужність множини інформаційних слів;

$M\{B_m(x)\} \ge \{C_m^{0.5m}, C_m^{0.5(m\pm1)}\}$ – потужність множини рівноважних слів для парних і непарних m відповідно. Надалі для спрощення запису замість виразу $\{C_m^{0.5m}, C_m^{0.5(m\pm1)}\}$ буде використовуватися запис тільки для парних m – $C_m^{0.5m}$. Вираз $C_m^{0.5m}$ показує, скільки існує векторів з розмірністю m і вагою Хеммінга $0.5m$. Такий вибір забезпечує найбільшу підмножину рівноважних слів;

$M\{\pi_n(x)\} = M!$ – потужність множини перестановок.

Оцінка основних параметрів коду. Під час розрахунку параметрів ФКК будемо спиратись на умову (2).

З виразу (1) слідує, що потужність множини рівноважних слів більша, ніж потужність інформаційних слів, тому очевидно, що розмірність інформаційного вектора $A_k(x)$ $k \le \log_2 C_m^{0.5m}$. Враховуючи, що $\log_2 C_m^{0.5m}$ може не бути цілим числом,

$$k \le \left[\log_2 C_m^{0.5m}\right]. \qquad (3)$$

Запис $[a]$ означає цілу частину від числа a.

Надлишковість рівноважного коду можна визначити за допомогою співвідношення:

$$\alpha_1 = \frac{2^m}{2^k} = 2^{m-k}. \qquad (4)$$

Очевидно, що $\alpha_1 \to \min$ для $k = \left[\log_2 C_m^{0.5m}\right]$.

Аналогічно, виходячи з умови $M\{\pi_n(x)\} \ge M\{B_m(x)\}$ і враховуючи, що $M\{\pi_n(x)\} = M!$, $\mathrm{M}\{B_m(x)\} = 2^m$ отримуємо відношення $M! \ge 2^m$. Звідси слідує, що

$$m \le \left[\log_2 M!\right]. \qquad (5)$$

Вираз (5) слугує для визначення порядку перестановки M, виходячи з якого визначається кількість біт перестановки

$$n = M \cdot \lceil \log_2 M \rceil. \qquad (6)$$

Вираз $\lceil a \rceil$ означає функцію округлення в більшу сторону числа a.

Надлишковість факторіального коду по відношенню до рівноважного визначається таким чином:

$$\alpha_2 = \frac{2^n}{2^m} = 2^{n-m}. \qquad (7)$$

Очевидно, що $\alpha_2 \to \min$ для $m = \left[\log_2 M!\right]$.

Надлишковість α_3 та швидкість ν ФКК визначаються наступним чином:

$$\alpha_3 = \alpha_1 \alpha_2 = 2^{n-k}, \qquad (8)$$

$$\nu = \frac{k}{n}. \qquad (9)$$

Використовуючи вирази (1)…(9), виконаємо оцінку параметрів ФКК для різних довжин k інформаційного слова $A_k(x)$. Результати оцінки наведено в табл. 1.

Таблиця 1

Оцінка основних параметрів ФКК

k	m	M	n	ν	α_1	α_2	α_3
12	15	8	24	0,54	2^3	2^9	2^{12}
43	45	16	64	0,67	2^2	2^{19}	2^{21}
114	118	32	160	0,71	2^4	2^{42}	2^{46}
210	215	50	300	0,7	2^5	2^{85}	2^{90}

З таблиці слідує, що ФКК має відносно високу швидкість коду та надлишковість, які зростають зі збільшенням розміру інформаційного блоку k і обумовлені властивостями ФКВД. Очевидно, що швидкість та надлишковість ФКК буде співпадати з відповідними параметрами ФКВД, окрім тих випадків, коли після перетворення $A_k(x) \to B_m(x)$ виникає необхідність збільшення порядку перестановки M: $2^k \le M! \le 2^m$. Також існуюча надлишковість може бути використана для підвищення достовірності передачі даних, як запропоновано в [4].

Оцінка достовірності передачі. Прийняту з каналу зв'язку послідовність будемо називати кодовим словом і позначимо як $\pi_n'(x) = \pi_n(x) + \varepsilon_n(x)$. Процес декодування відбувається у зворотному до (1) порядку: $\pi_n(x) \to B_m(x) \to A_k(x)$. Послідовність з n біт, що являє собою сформовану кодером перестановку $\pi_n(x)$ з накладеним на неї вектором помилки $\varepsilon_n(x)$, потрапляє на вхід декодера зовнішнього коду. У ФКК зовнішнім кодом є ФКВД, тому спочатку кодове слово перевіряється на належність до множини перестановок, що полягає у встановленні факту того, що кожне число з діапазону $\overline{0, M!-1}$ зустрічається в кодовому слові рівно один раз. Якщо ця умова не виконується, то формується запит на повторення блоку. Інакше визначається десяткове число, що відповідає отриманому кодовому слову і передається на вхід декодера рівноважного коду. Декодер визначає вагу кодового слова та його належність до дозволеної множини з 2^k кодових слів. Якщо прийнятий вектор належить до дозволеної множини і його вага становить 0.5m, то декодер рівноважного коду перетворює його в прийнятий вектор $A_k'(x) = A_k(x) + \varepsilon_k(x)$, де $\varepsilon_k(x)$ – вектор помилки, що накладається на передане слово $A_k(x)$. Якщо прийнятий вектор до забороненої множини кодових слів або його вага не рівна 0.5m, то формується запит на повторення блоку.

Оскільки каскадний код є поєднанням двох кодів, імовірність невиявленої помилки є добутком ймовірностей невиявлених помилок під час кодування інформації за допомогою ФКВД і рівноважного коду:

$$\begin{aligned} \mathrm{P}_{ud}(FCC, p_0) &= P_{ud}(FCDR, p_0) \times \\ &\times P_{ud}(\mathrm{EC}, p_0') \end{aligned}, \quad (10)$$

де p_0' – імовірність бітової помилки на вході декодера рівноважного коду (імовірність бітової помилки на виході ФКВД). Якщо вектор помилки $\varepsilon_n(x)$ призводить до трансформації перестановки в іншу перестановку з дозволеної множини, то має місце не виявлена ФКВД помилка. Імовірність та умови виникнення таких помилок визначено в [3].

Для рівноважного коду невиявленими будуть помилки, що не призводять до зміни кількості одиничних розрядів, тобто не змінюють вагу кодового слова. Така помилка можлива тоді і тільки тоді, коли рівно $t\left(t \le \lfloor m/2 \rfloor\right)$ одиничних біт перетворюються в нулі і рівно t нульових біт перетворюються в одиниці. За незалежних помилок на виході декодера ФКВД та їх біноміального розподілу ймовірність такої події визначається наступним чином:

$$\begin{aligned} &P_{ud}\left(\mathrm{EC}, p_0'\right) = \\ &= \sum_{t=1}^{[m/2]} \left(\begin{array}{l} \left(C_{[m/2]}^t \left(p_0'\right)^t \left(1-p_0'\right)^{[m/2]-t} \right) \times \\ \times \left(C_{m-[m/2]}^t \left(p_0'\right)^t \left(1-p_0'\right)^{m-[m/2]-t} \right) \end{array} \right) = \\ &= \sum_{t=1}^{[m/2]} \left(\begin{array}{l} C_{[m/2]}^t C_{m-[m/2]}^t \left(p_0'\right)^{2t} \left(1-p_0'\right)^{[m/2]-t} \times \\ \times \left(1-p_0'\right)^{m-[m/2]-t} \end{array} \right) \end{aligned} \quad (11)$$

У випадку, коли розмірність вектора рівноважного коду m парна, вираз (11) приймає наступний вигляд:

$$P_{ud}\left(\mathrm{EC}, p_0'\right) = \sum_{t=1}^{m/2} \left(C_{m/2}^t \left(p_0'\right)^t \left(1-p_0'\right)^{m/2-t} \right)^2 \quad (12)$$

Знаючи ймовірність невиявленої помилки, визначимо енергетичний виграш від застосування ФКК. Для цього розроблено розрахунково-експериментальну модель, що імітує роботу системи передачі даних, що складається з джерела та приймача інформації, кодера та декодера ФКК і каналу зв'язку. Вхідними параметрами моделі є розмір інформаційного блоку k, що породжується джерелом, імовірність бітової помилки в каналі зв'язку

p_0 і загальний обсяг вибірки V. Помилки в каналі зв'язку розподіляються за біноміальним законом. Модель дозволяє оцінити ймовірність виявлення кодом помилок та ймовірність помилкового декодування блоку даних рівноважним кодом та ФКВД окремо, а також ФКК в цілому. Результати моделювання представлені на рис. 1 і 2.

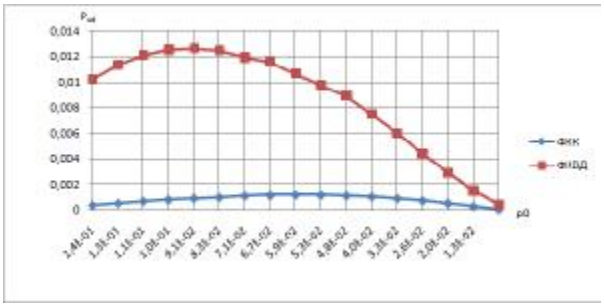

Рис. 1. Графік залежності ймовірності невиявленої кодом помилки від імовірності бітової помилки p_0 у каналі зв'язку для ФКК та ФКВД при k = 15

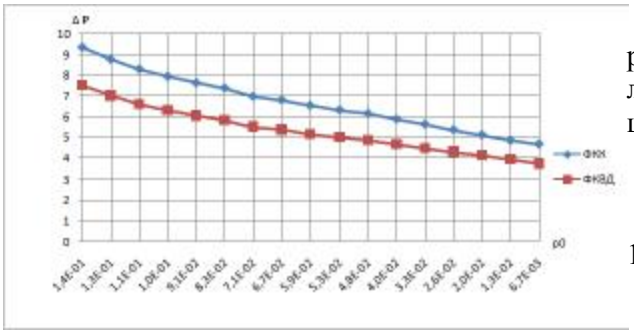

Рис. 2. Графік залежності енергетичного виграшу від імовірності бітової помилки p_0 у каналі зв'язку для ФКК та ФКВД при k = 15

Рис. 1 і 2 показують, що ймовірність невиявленої ФКК помилки менша, ніж у ФКВД, а енергетичний виграш від застосування ФКК більший у порівнянні з ФКВД ($\Delta P_{FCC} - \Delta P_{FCDR} \le 1.9 дБ$).

Виконаний аналіз властивостей ФКК дає змогу сформулювати рекомендації щодо його застосування:

1) запропонований каскадний код забезпечує енергетичний виграш на рівні 2 дБ у порівнянні з ФКВД та може бути використаний в системах передачі даних з використанням каналів дротового і радіозв'язку УКХ та мікрохвильового діапазонів;

2) побудова оптимального кодера рівноважного коду та ФКВД може суттєво підвищити ефективності ФКК в цілому.

Висновки. Виконана робота дозволила побудувати каскадний код, що поєднує рівноважний та факторіальний коди, та виконати аналіз його основних властивостей. Виконано порівняння ФКК та ФКВД.

Властивості ФКК:

- ФКК дозволяє підвищити достовірність передачі даних за рахунок кодування інформаційного вектора рівноважним кодом, що дозволяє частково виявляти помилки, що не можуть бути виявленні ФКВД;

- застосування ФКК дає приріст енергетичного виграшу у порівнянні з ФКВД на рівні 2 дБ;

- ФКК зберігає властивості ФКВД із забезпечення завадостійкого кодування та шифрування даних;

- ФКК має відносно велику швидкість коду та надлишковість, що зростають із збільшенням розміру інформаційного блоку. Існуюча надлишковість може бути використана для додаткового підвищення достовірності передачі даних.

Пошук оптимальних способів побудови рівноважного та факторіального кодів є актуальним напрямком для подальших досліджень, що дозволить підвищити ефективність ФКК.

Список літератури

1. Фауре Э. В., Швыдкий В. В., Щерба В. А. Метод формирования имитовставки на основе перестановок *Захист інформації*. 2014. № 4. Т. 16. С. 334–340.
2. Фауре Э. В., Швыдкий В. В., Щерба В. А Комбинированное факториальное кодирование и его свойства. *Радіоелектроніка, інформатика, управління.* 2016. № 3. С. 80–86.
3. Фауре Э. В. Факториальное кодирование с восстановлением данных *Вісник Черкаського державного технологічного університету*. *Серія: Технічні науки.* 2016. № 2. С. 33–39.
4. Фауре Э. В. Метод повышения эффективности факториального кодирования с восстановлением данных. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2016. № 3. С. 57–61.
5. Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: справочник. Москва: Горячая линия–Телеком, 2004. 126 с.: с ил.

6. Бородин Л. Ф. Введение в теорию помехоустойчивого кодирования. Москва: Советское радио, 1968. 408 с.
7. Гладких А. А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. Ульяновск: УЛГТУ, 2010. 379 с.
8. Прокис Д. Цифровая связь/пер. с англ. под ред. Д. Д. Кловского. Москва: Радио и связь, 2000. 800 с.
9. Кнут Д. Э. Искусство программирования. Том 1. Основные алгоритмы. Москва: Вильямс, 2002. 720 с.
10. Кнут Д. Э. Искусство программирования. Том 2. Получисленные алгоритмы. Москва: Вильямс, 2007. 832 с.

References

1. Faure, E. V., Shvydkyi, V. V., Shcherba, V. A. (2014) Method for formation of message authentication code based on permutations. *Zakhyst informatsiyi*, No. 4, vol. 16, pp. 334–340 [in Russian].
2. Faure, E. V., Shvydkyi, V. V., Shcherba, V. A. (2016) Combined factorial coding and its properties. *Radioelektronika, informatyka, upravlinnya*, No. 3, pp. 80–86 [in Russian].
3. Faure, E. V. (2016) Factorial coding with data recovery. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria*: *Tehnichni nauky,* No. 2, pp. 33–39 [in Russian].
4. Faure, E. V. (2016) The method of increasing of factorial coding with data recovery efficiency. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria*: *Tehnichni nauky,* No. 3, pp. 57–61 [in Russian].
5. Zolotarev, V. V., Ovechkin, G. V. (2004) Noiseless coding. Methods and algorithms. Moscow: Goryachaya liniya–Telekom, 126 p. [in Russian].
6. Borodin, L. F. (1968) Introduction in the theory of FEC. Moscow: Sovetskoye radio, 408 p. [in Russian].
7. Gladkih, A. A. (2010) Fundamentals of the theory of soft decoding of redundant codes in erasing channel. Ul'yanovsk: UlGTU, 379 p. [in Russian].
8. Proakis, John G. (2000) Digital communications. Boston: McGraw-Hill, 800 p.
9. Knut, D. E. (2002) The Art of computer programming. Vol. 1. Fundamental algorithms. Moscow: Vil'yams, 720 p. [in Russian].
10. Knut, D. E. (2007) The Art of computer programming. Vol. 2. Seminumerical algorithms. Moscow: Vil'yams, 832 p. [in Russian].

O. O. Kharin, *postgraduate student,*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
kharin_aa@mail.ua

ESTIMATION OF PROPERTIES OF CASCADE CODE, WHICH COMBINES FACTORIAL AND EQUILIBRIUM CODES

The principle of construction and properties of cascade code with the use of factorial and equilibrium codes is proposed and discussed in detail. The proposed combination of codes provides an increase in the reliability of data transmission. The coding process assumes the consistent use of equilibrium coding and factorial coding with data recovery (FCDR).The transmission reliability, code rate and energy gain are estimated. Experimental design model of the proposed cascade code is constructed to determine the dependence of the probability of a false decoding of a data block on its size and the probability of a bit error in the communication channel for binomial error distribution at the decoder input. Based on experimental data, a comparative analysis with FCDR is carried out and recommendations for its use are made.

Keywords: *cascade code, equilibrium code, factorial code, information integrity control, cryptographic protection, reliability of transmission.*

Рецензенти: Рудницький В. М., д.т.н., професор,
Голуб С. В., д.т.н., професор