УДК 004.052.2

О. О. Харін, *аспірант кафедри*
інформаційної безпеки та комп'ютерної інженерії
e-mail: kharin_aa@mail.ua
Черкаський державний технологічний університет
б-р Шевченка, 460, Черкаси, 18006, Україна

ПОРІВНЯЛЬНА ОЦІНКА ФАКТОРІАЛЬНИХ КОДІВ

У роботі досліджено механізм утворення помилок декодування, їх зв'язок зі статистикою помилок та алгоритмами прийняття рішень у процесі декодування факторіальними кодами. Для виконання порівняльного оцінювання стійкості різних факторіальних кодів до впливу потоку помилок створено експериментально-розрахункові моделі для повного факторіального коду (ПФК), факторіального коду з відновленням даних (ФКВД), ФКВД з додатковими перевірними бітами (ФКВДд) та факторіального каскадного коду (ФКК). Для запропонованих кодів виконано оцінювання достовірності передачі даних, швидкості коду та величини енергетичного виграшу для однакових значень довжини інформаційного блока та ймовірності бітової помилки в каналі зв'язку за біноміального розподілу помилок на вході декодера. Виконано аналіз механізму утворення помилок декодування. На основі отриманих результатів розроблено рекомендації щодо застосування кожного з факторіальних кодів для вирішення задач забезпечення контролю цілісності інформації (КЦІ) та її криптографічного захисту.

Ключові слова:*факторіальний код, повний факторіальний код, факторіальний код з відновленням даних, достовірність передачі даних, енергетичний виграш, контроль цілісності інформації, криптографічний захист.*

Постановка проблеми. На сучасному етапі розвитку комп'ютерних систем і мереж актуальною є задача комплексного захисту інформації, що передбачає:

- захист інформації від несанкціонованого читання;
- забезпечення цілісності інформації, що включає захист від помилок, які виникають у каналі зв'язку під час її передавання, і захист від нав'язування хибних даних.

Розробка нових методів вирішення задач криптографічного захисту та КЦІ, а також їх поєднання дозволяють підвищити ефективність засобів обробки інформації за рахунок суміщення операцій захисту інформації від несанкціонованого зчитування, підміни та канального кодування і є актуальним напрямком досліджень.

Аналіз джерел і публікацій. Отримані в [1, 2, 3, 4, 5] результати показують ефективність використання факторіальних кодів для підвищення достовірності передавання інформації, а також для вирішення задач КЦІ та криптографічного захисту. Основною перевагою таких кодів є те, що вони поєднують у собі функції захисту від помилок у каналі зв'язку, захисту від нав'язування хибних даних, а також криптографічного захисту. В основі принципів факторіального кодування лежить побудова перестановок на основі факторіальної системи числення. Це здійснюється за рахунок відображення точок на числовій осі, що відповідають інформаційному вектору, в точки числової осі, що відповідають перестановці або відповідній контрольній сумі. Крім того, відзначимо, що більшість розглянутих факторіальних кодів мають здатність до самосинхронізації і не потребують введення в формат кадру синхроблока , що дозволяє зменшити внесену надлишковість. Це обумовлено тим, що символи перестановки $\{0;1;...;M-1\}$ зустрічаються в ній рівно по одному разу, а їх сума дорівнює $\sigma = 0,5M(M-1)$ [3]. Оскільки факторіальні коди не завжди забезпечують повний комплекс засобів із захисту інформації, залежно від характеру вирішуваних задач, було розроблено декілька видів факторіального кодування.

В [1] розглядається метод захисту інформації від помилок та нав'язування хибних даних (імітозахисту) за рахунок додавання до *k*-бітної інформаційної послідовності перевірної частини, що представлена перестановкою чисел $\{0,1,...,M-1\}$, де M – порядок переста-

новки. У результаті такої операції сформований блок даних містить $n = k + r$ біт, де $r = l_r \cdot M$, r – розмір перевірної частини, l_r – довжина кодової комбінації кожного елемента перестановки. Такий код отримав назву повного факторіального коду (ПФК). Його особливістю є те, що розмірність перевірної частини може бути довільною і залежить від необхідного рівня підвищення достовірності, а також необхідного рівня імітостійкості. Разом із тим, зі збільшенням розміру імітовставки зменшується швидкість коду. Крім того, слід зауважити, що інформаційна частина передається у відкритому вигляді і не захищена від несанкціонованого читання.

У [3] запропоновано повністю замінити інформаційну послідовність на перестановку, сформовану за цією послідовністю. Такий код отримав назву факторіального коду з відновленням даних за перестановкою (ФКВД). ФКВД являє собою нероздільний код, в якому носієм інформаційної послідовності з k біт є обчислена за всіма бітами інформаційної послідовності перестановка чисел порядку M, що обирається з умови $M! \geq 2^k$. При цьому частина перестановок відноситься до забороненої множини для забезпечення рівної потужності множини інформаційних векторів і множини перестановок. ФКВД забезпечує криптографічний захист та захист від помилок у каналі зв'язку. Значною перевагою такого коду є те, що він дозволяє виявляти всі помилки, що не призводять до трансформації одної перестановки в іншу з дозволеної множини перестановок. У роботах [4, 5] розглянуто методи, спрямовані на підвищення стійкості ФКВД до помилок, що призводять до трансформації перестановок за рахунок внесення додаткової надлишковості.

У [4] запропоновано метод підвищення достовірності передавання даних для ФКВД за рахунок зменшення розміру інформаційної послідовності і введення в неї додаткових перевірних біт. Такий метод отримав назву ФКВД з доповненням (ФКВДд). Додатково розглянуто код, в якому додаткові біти доповнювали вже сформовану перестановку і не змінювали початкову інформаційну послідовність. Такий метод кодування було названо факторіальним кодуванням з додатковими перевірними бітами (ФКДБ).

Інший метод підвищення достовірності передавання, розглянутий у [5], полягає у каскадуванні декількох кодів – рівноважного коду та ФКВД. Такий код отримав назву факторіального каскадного коду (ФКК). Недоліком такого коду є те, що рівноважний код, так само як і ФКВД, вразливий до помилок парної кратності. Також слід відзначити, що реалізація такого коду вимагає значних обчислювальних ресурсів.

Мета роботи. Метою цієї роботи є оцінювання набору якостей та основних властивостей факторіальних кодів, а також формулювання рекомендацій щодо оптимального вибору коду для конкретного застосування. Для цього необхідно виконати оцінювання існуючих факторіальних кодів у системах передачі даних з вирішальним зворотним зв'язком та порівняти отримані характеристики. При цьому треба оцінити:

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

Рішення задачі. Слід зазначити, що всі факторіальні коди, в першу чергу, вирішують задачу захисту інформації від помилок, що виникають у каналі зв'язку. Але порівняння факторіальних кодів лише за показником достовірності передавання даних не дає об'єктивної оцінки, оскільки не враховуються додаткові властивості, притаманні кожному з цих кодів. Тому, крім порівняння факторіальних кодів за швидкістю коду, енергетичним виграшем і ймовірністю помилкового декодування блока даних, також слід зазначити, за яких умов необхідно застосовувати кожен із досліджуваних кодів.

З метою порівняння факторіальних кодів розроблено розрахунково-експериментальні моделі для таких кодів: ПФК[1], ФКВД [3], ФКВДд [4], ФКДБ, ФКК [5].

У першу чергу, розглянемо особливості реалізації ПФК. Відзначимо, що, хоча ПФК передбачає довільний розмір перевірної частини, під час побудови розрахунково-експериментальної моделі порядок перестановки, що являє собою перевірну частину коду, обирався за умови $M! \geq 2^k$. Виконання цієї умови дозволяє уникнути колізій, коли декільком інформаційним векторам відповідає одна перестановка, і забезпечує вищу достовірність передавання даних за рахунок зниження швидкості коду.

У цій роботі будемо досліджувати ФКВДд [4] з одним додатковим перевірним бітом, що являє собою ознаку парності конт-

рольної суми, розрахованої за всіма бітами інформаційної послідовності:

$$a_{add} = a_0 \oplus a_1 \oplus ... \oplus a_{k-1},$$

де $\{a_0, a_1, ..., a_{k-1}\}$ – біти інформаційного вектора.

Як випливає з [4], такий спосіб дає змогу значно підвищити достовірність передавання даних за рахунок незначного зниження швидкості коду, причому зі збільшенням довжини інформаційного вектора зниженням швидкості можна знехтувати, що дозволяє ввести декілька перевірних біт. Очевидним недоліком такого коду є необхідність зменшення інформаційної частини для збільшення надлишковості.

У свою чергу, ФКДБ як варіант модифікації ФКВДд передбачає додавання перевірних біт до вже сформованої перестановки, що за умови вибору довжини інформаційного вектора, рівної $k = \lfloor \log_2 M! \rfloor$, дозволяє мінімізувати надлишковість і, як наслідок, отримати більшу швидкість коду. У цьому коді перевірні біти визначаються як ознаки парності суми всіх елементів синдрому та/або індексу перестановки [7]. Залежно від кількості та способу формування додаткових біт оцінюванню підлягають наступні варіанти побудови кодів ФКДБ.

1. Перестановка доповнюється одним перевірним бітом, який визначає парність числа інверсій перестановки, що розраховується як алгебраїчна сума всіх елементів синдрому за модулем 2:

$$check\_bit = \left| \sum_{i=0}^{M-1} b_i \right|_2,$$

де $check\_bit$ – перевірний біт, $\{b_{M-1}, b_{M-2}, ..., b_0\}$ – факторіальні коефіцієнти (елементи синдрому перестановки S_f).

2. Перестановка доповнюється трьома перевірними бітами, які визначають парність числа інверсій перестановки і дублюють один одного:

$$check\_bit_1 = check\_bit_2 =$$
$$= check\_bit_3 = \left| \sum_{i=0}^{M-1} b_i \right|_2.$$

3. Перестановка доповнюється трьома перевірними бітами, перший з яких визначає парність числа інверсій, другий – індекс інверсної перестановки, третій – індекс взаємної перестановки.

4. Перестановка доповнюється трьома перевірними бітами, перший з яких визначає парність числа інверсій всієї перестановки, другий – парність числа інверсій за парними елементами синдрому, третій – парність числа інверсій за непарними елементами синдрому:

$$check\_bit_1 = \left| \sum_{i=0}^{M-1} b_i \right|_2,$$

$$check\_bit_2 = \left| \sum_{i=0}^{\left\lceil \frac{M}{2} \right\rceil} b_{2i} \right|_2,$$

$$check\_bit_3 = \left| \sum_{i=0}^{\left\lceil \frac{M}{2} \right\rceil} b_{2i+1} \right|_2.$$

5. Перестановка доповнюється одним перевірним бітом, який визначає парність інформаційної частини (за аналогією з ФКВДд, за винятком того, що інформаційна частина вибирається з умови $k = \lfloor \log_2 M! \rfloor$, а біт перевірки дописується в кінці блока):

$$check\_bit = a_0 \oplus a_1 \oplus ... \oplus a_{k-1}.$$

6. Перестановка доповнюється трьома перевірними бітами, що обчислюються аналогічно п. 3, але рішення про коректність прийнятого блока приймається за мажоритарним принципом (за більшістю голосів). Якщо хоча б двоє з трьох перевірних бітів, прийнятих з каналу зв'язку, збігаються з розрахованими на приймальній стороні за прийнятою перестановкою, то такий блок даних вважається прийнятим без помилок.

У результаті дослідження властивостей ФКДБ встановлено, що контроль парності алгебраїчної суми елементів синдрому дозволяє виявляти всі двократні помилки, що призводять до транспозиції елементів перестановки. Також очевидно, що за рахунок накладання помилки на перевірні біти мають місце два специфічні види помилок декодування, властивих для всіх варіантів побудови ФКДБ:

1) помилка призвела до трансформації однієї перестановки в іншу, що належить дозволеній множині перестановок, а також відповідним чином змінила перевірні біти;

2) перестановка прийнята без помилок, але значення перевірних біт було спотворено помилкою. У цьому випадку має місце «хибна

помилка». Приймальна сторона вважає весь блок даних прийнятим з помилкою і формує сигнал на повторний запит блока.

Табл. 1 демонструє результати моделювання досліджуваних факторіальних кодів. Під час моделювання оцінювалися такі параметри, як: швидкість коду ν, імовірність помилкового декодування блока даних P_{ud} та енергетичний виграш ΔP. Моделювання виконувалося для біноміального закону розподілу помилок у каналі зв'язку, довжина інформаційного вектора k становила 15 біт, імовірність бітової помилки $p_0 = 1/15$. Порядок перестановки M обирається з умови $M! \geq 2^k$, довжина блока даних n залежить від способу кодування.

Таблиця 1

Результати моделювання факторіальних кодів

№	Код	k, біт	n, біт	M	P_{ud}	ν	ΔP, дБ
1	ПФК	15	39	8	0,000036	0,385	8,166
2	ФКВД	15	24	8	0,011550	0,625	5,371
3	ФКВДд	14	24	8	0,002808	0,583	6,179
4	ФКДБ, варіант 1	15	25	8	0,001126	0,600	6,649
5	ФКДБ, варіант 2	15	27	8	0,000335	0,556	7,213
6	ФКДБ, варіант 3	15	27	8	0,000549	0,556	7,005
7	ФКДБ, варіант 4	15	27	8	0,000522	0,556	7,027
8	ФКДБ, варіант 5	15	25	8	0,005753	0,600	5,812
9	ФКДБ, варіант 6	15	27	8	0,004598	0,556	5,979
10	ФКК	15	36	9	0,001125	0,417	6,816

Результати, відображені в таблиці, дають змогу оцінити якісні характеристики досліджених факторіальних кодів та сформулювати рекомендації щодо їх використання:

1. ПФК має найбільший енергетичний виграш, а також найменшу швидкість коду, що обумовлено його великою надлишковістю. При цьому ПФК забезпечує імітозахист і захист від помилок каналу зв'язку;
2. ФКВД має найбільшу швидкість коду серед усіх розглянутих кодів та найменший енергетичний виграш. Але головною його перевагою є те, що він виконує функцію шифрування і забезпечує захист інформації від несанкціонованого читання. Тому ФКВД доречно використовувати для передавання конфіденційної інформації;
3. ФКВДд та ФКДБ є варіантами підвищення ефективності ФКВД за рахунок введення додаткових перевірних бітів і, як наслідок, зменшення швидкості коду. Очевидно, що ці коди, як і ФКВД, виконують функцію шифрування і більш стійкі до помилок каналу зв'язку;
4. ФКК є спробою поєднання факторіальних кодів з іншими з метою підвищити стійкість факторіальних кодів до помилок парної кратності. У [5] запропоновано поєднання ФКВД та рівноважного кодів, що дало змогу отримати більший енергетичний виграш порівняно з ФКВД, але не дозволило виявити всі помилки парної кратності. Це обумовлено тим, що ФКВД сам по собі має властивість рівноважності, а підвищення достовірності передавання даних обумовлено попередньою обробкою інформаційного вектора. Варто зазначити, що ФКК зберігає властивість ФКВД із забезпечення захисту від несанкціонованого читання, а за умови збереження порядку перестановки M дає більший енергетичний виграш для сталої швидкості коду.

Висновки. Проведені дослідження дозволили проаналізувати та узагальнити інформацію про факторіальні коди. Виконано порівняння наступних факторіальних кодів: ПФК, ФКВД, ФКВДд, ФКК, ФКДБ – за критеріями:

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

Було розроблено розрахунково-експериментальні моделі, що дали змогу оці-

нити якісні характеристики факторіальних кодів. Окрім оцінювання кодів з точки зору достовірності передавання даних, розглянуто їх властивості по забезпеченню захисту від нав'язування хибних даних та криптозахисту. На основі отриманих результатів моделювання сформульовано рекомендації щодо застосування кожного з кодів.

Список літератури

1. Фауре Э. В., Швыдкий В. В., Щерба А. И. Контроль целостности информации на основе факториальной системы счисления. *Journal of Baku Engineering University. Mathematics and Computer Science.* 2017. № 1. Т. 2.
2. Фауре Э. В., Швыдкий В. В., Щерба А. И. 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. № 4. С. 57–61.
5. Харін О. О. Оцінка властивостей каскадного коду, що поєднує факторіальний та рівноважний код. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. № 2. С. 86–90.
6. Кнут Д. Э. Искусство программирования. Т. 1. Основные алгоритмы. Москва: Вильямс, 2002. 720 с.
7. Кнут Д. Э. Искусство программирования. Т. 2. Получисленные алгоритмы. Москва: Вильямс, 2007. 832 с.
8. Прокис Д. Г. Цифровая связь; пер. с англ. под ред. Д. Д. Кловского. Москва: Радио и связь, 2000. 800 с.
9. Пат. 117004 Україна, МПК H03M 13/09 (2006.01), H04L 1/16 (2006.01), G04C 1/06 (2006.01). Спосіб факторіального кодування з відновленням даних / Фауре Е. В., Харін О. О., Швидкий В. В., Щерба А. І.; заявник та патентовласник Черкаський державний технологічний університет. № u201613641; заявл. 30.12.2016; опубл. 12.06.2017, Бюл. № 11.
10. Пат. 106669 Україна, МПК G06F 21/64 (2013.01). Спосіб формування імітовставки / Фауре Е. В., Швидкий В. В., Щерба А. І.; заявник та патентовласник Черкаський державний технологічний університет. № a201505934; заявл. 16.06.2015; опубл. 10.05.2016, Бюл. № 9.

References

1. Faure, E. V., Shvydkyi, V. V., Shcherba, A. I. (2017) Information integrity control based on factorial number system. *Journal of Baku Engineering University. Mathematics and Computer Science,* No. 1, vol. 2 [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 the efficiency of factorial coding with data recovery. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 3, pp. 57–61 [in Russian].
5. Kharin, O. O. (2017) Estimation of properties of cascade code, which combines factorial and equilibrium codes. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky*, No. 2, pp. 86–90 [in Ukrainian].
6. Knut, D. E. (2002) The art of computer programming. Vol. 1. Fundamental algorithms. Moscow: Vil'yams, 720 p. [in Russian].
7. Knut, D. E. (2007) The art of computer programming. Vol. 2. Seminumerical algorithms. Moscow: Vil'yams, 832 p. [in Russian].
8. Proakis, J. G. (2001) Digital communications. Boston: McGraw-Hill.
9. Faure, E. V., Kharin, O. O., Shvydkyi, V. V., Shcherba, A. I. (2017) The mode of factorial coding with data recovery. Cherkasy State

Technological University, assignee. UA Patent 117004, printed June 12 [in Ukrainian].
10. Faure, E. V., Shvydkyi, V. V., Shcherba, A. I. (2016) The mode of staffing formation. Cherkasy State Technological University, assignee. UA Patent 106669, printed May 10 [in Ukrainian].

O. O. Kharin, *postgraduate student,*
postgraduate student of information security and computer engineering chair
e-mail: kharin_aa@mail.ua
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

COMPARATIVE EVALUATION OF FACTORIAL CODES

In the work, the mechanism of generation of decoding errors, their connection with error statistics and algorithms of decision making in the process of decoding by factorial codes are investigated in detail. To perform a comparative estimation of the stability of various factorial codes to the influence of the error flow, experimental-calculation models for full factorial code (FFC), factorial code with data recovery (FCDR), FCDR with additional verification bits (FCDRd) and factorial cascading code (FCC) were created. The reliability of the data transmission, the speed of the code and the value of the energy gain for proposed codes were evaluated with the same values of the length of the information block and the probability of a bit error in the communication channel in the binomial distribution of errors at the decoder input. An analysis of the mechanism of generation of decoding errors is performed. On the basis of the obtained results, recommendations were made for the use of each of the factorial codes when solving the problems of ensuring the control of the integrity of information and cryptographic protection.

Key words: *factorial code, full factorial code, factorial code with data recovery, reliability of data transmission, energy gain, integrity control of information, cryptographic protection.*

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