УДК 004.71

[0000-0002-1596-4123] **А. О. Лавданський**[1], *канд. техн. наук, доцент,*
e-mail: a.lavdanskyi@chdtu.edu.ua
[0000-0002-2046-481X] **Е. В. Фауре**[1], *д-р техн. наук, професор,*
[0000-0002-9326-9476] **С. Т. Тинимбаєв**[2], *канд. техн. наук, професор,*
[0000-0002-8632-1176] **А. Б. Скуцький**[1]
[1]Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2]Казахський національний технічний університет ім. К. І. Сатпаєва
вул. Сатпаєва, 22, м. Алмати, 050000, Казахстан

СИСТЕМА ЗАХИЩЕНОГО ІНФОРМАЦІЙНОГО ОБМІНУ ТЕКСТОВИМИ ДАНИМИ ЧЕРЕЗ РАДІОКАНАЛ ISM-ДІАПАЗОНУ

У роботі розроблено систему захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону. Система використовує нероздільне факторіальне кодування і дозволяє виконувати передавання та приймання текстових повідомлень, а також довільних двійкових даних. Повідомлення розбиваються на групи по два символи, з яких формується перестановка шляхом бієктивного перетворення двійкової послідовності у факторіальну систему числення. На приймальній стороні відбувається перевірка перестановки на належність до дозволеної множини перестановок та зворотне перетворення, після чого користувачу видається текстове повідомлення в тому вигляді, в якому воно було відправлено. Розроблено структурну схему приймально-передавального пристрою і програмне забезпечення командного рядка для реалізації процедур передавання та приймання повідомлень. Розроблена система може бути використана для встановлення захищеного зв'язку між терміналами за рахунок використання базової перестановки як ключової.

Ключові слова: *факторіальна система числення, перестановка, одноплатний комп'ютер, факторіальне кодування, захищений зв'язок.*

Вступ. Важливою задачею телекомунікаційних систем є забезпечення конфіденційності та контроль цілісності інформації, що передається. Для контролю цілісності інформації після впливу на неї помилок у каналі зв'язку використовуються коди виявлення та виправлення помилок (приклади реалізації наведено в [1]–[3]): контрольна сума, парність біт, коди Хеммінга, коди Боуза-Чоудхурі-Хоквінгема та інші. Для конфіденційності даних, що передаються, використовуються алгоритми шифрування (приклади реалізації наведено в [4]–[6]), наприклад AES, Twofish, RC6 тощо. Одним із методів, що одночасно дозволяє забезпечити функції виявлення помилок і криптозахист даних, є факторіальний код з відновленням даних за перестановкою (ФКВД) [7]. Такий код є нероздільним кодом і, окрім забезпечення захисту від несанкціонованого читання та захисту від помилок у каналі зв'язку, має властивість самосинхронізації за рахунок надлишкової структури кодового слова – перестановки. Створення системи передавання даних на основі ФКВД дозволить одночасно забезпечити криптозахист інформації, що передається, і виявити дані, які були вражені завадою в каналі зв'язку. Крім того, такий метод інтегрованого захисту даних від несанкціонованого читання та канальних помилок дозволить зменшити надлишковість даних і зменшити вимоги до обчислювальних ресурсів пристрою, що виконує обробку повідомлень.

Мета і задачі дослідження. Метою роботи є створення системи захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону на основі ФКВД та створення програмного забезпечення і макетних зразків, що реалізують цю систему. Для досягнення мети необхідно виконати такі завдання:

– розробити алгоритми кодування текстових повідомлень для реалізації на одноплатному комп'ютері (алгоритм містить процедури перетворення текстової інформації в десяткове ціле число, представлення цього числа у факторіальній системі числення з подальшим перетворенням в перестановку);

DOI: 10.24025/2306-4412.3.2022.267786

– виконати передавання перестановки радіоканалом ISM-діапазону;

– розробити алгоритм декодування текстових повідомлень для реалізації на одноплатному комп'ютері (алгоритм містить процедури перевірки перестановки на коректність і належність до дозволеної множини перестановок, а також послідовне перетворення перестановки в число в факторіальній, десятковій і двійковій системах числення і, насамкінець, представлення двійкового числа в символьному вигляді);

– розробити структурну схему, програмний код і макетні зразки системи передавання даних.

Завдання роботи за своєю суттю є розробкою протоколу передавання текстових повідомлень із використанням нероздільного факторіального кодування даних.

Виклад основного матеріалу. У роботі для передавання текстових повідомлень будемо використовувати ФКВД [7], де довжина перестановки – носія даних дорівнює $M = 8$. Потужність повної множини перестановок з $M = 8$ дорівнює $M! = 40320$. Цієї кількості перестановок буде достатньо для кодування повідомлення довжиною до $n = \lfloor \log_2 M! \rfloor = \lfloor \log_2 40320 \rfloor = 15$ біт.

Повідомлення, введені користувачем, розбиваються на групи по два символи (якщо кількість символів у повідомленні непарна, останнім символом додається символ пробілу). З отриманих пар символів формується числове значення наступним чином. Від ASCII коду кожного символу беруться молодші 7 біт (цієї кількості достатньо для передавання великих і малих латинських символів, чисел, деяких додаткових символів) і конкатенуються у 14-бітове двійкове число. Старшими 7 бітами є ASCII код першого символу, молодшими 7 бітами – ASCII код другого символу). Отримане 14-бітове двійкове число переводиться в десяткову систему числення. Це число однозначно ідентифікує дві літери та може бути перетворене в текст на приймальній стороні шляхом зворотного переведення у двійкову систему числення та розбиття отриманого значення на два 7-розрядних двійкових числа з подальшою інтерпретацією їх як ASCII кодів символів текстового повідомлення користувача.

Зауважимо, що для $M = 8$ загальна кількість перестановок ($8! = 40320$) буде меншою за загально можливу кількість двохсимвольних комбінацій (2^{14}). Це дозволяє сформувати ансамбль використовуваних перестановок і вести контроль за належністю прийнятої перестановки до цього ансамблю, а також відкидати її в разі належності до множини перестановок, яка не використовується джерелом.

Після перетворення двох текстових символів у десяткове число воно представляється у факторіальній системі числення: $x = \sum_{k=1}^{n} d_k \times k!$, де $0 \le d_k \le k$. З отриманого факторіального числа на основі деякої базової перестановки π_0 формується перестановка π. Процедуру такого перетворення детально описано в [8].

Наведемо приклад перетворення послідовності текстових символів у перестановку. Для цього візьмемо послідовність з двох латинських символів *ab*. ASCII коди цих символів – 97_{10} та 98_{10} відповідно. Переведемо ці значення в двійкову систему числення та виконаємо конкатенацію їх молодших 7 біт. Отримане значення 11000011100010_2 еквівалентне 12514_{10}. Запишемо число 12514_{10} у факторіальній системі числення:

$$12514_{10} = 2\times 7! + 3\times 6! + 2\times 5! + 1\times 4! +$$
$$+1\times 3! + 2\times 2! + 0\times 1! + 0\times 0! = 23211200_F$$

Для формування перестановки оберемо базову перестановку $\pi_0 = (0,1,2,3,4,5,6,7)$. Кожний розряд отриманого числа у факторіальній системі числення є індексом елемента базової перестановки. Почергово аналізуючи розряди факторіального числа, зчитуються відповідні елементи базової перестановки. При цьому зчитаний елемент вилучається з неї. Наприклад, для числа 23211200_F старший розряд, а отже й індекс у базовій перестановці, дорівнює 2. Другий елемент базової перестановки π_0 (число 2) зчитується, записується першим елементом результуючої перестановки π і вилучається з базової перестановки π_0. На поточному етапі базова перестановка π_0 буде мати наступний вигляд: $\pi_0' = (0,1,3,4,5,6,7)$. Оберемо наступний розряд факторіального числа 23211200_F (число 3). Зчитаємо елемент з індексом 3 з перестановки π_0' (це буде число 4), запишемо його другим елементом перестановки π й видали-

DOI: 10.24025/2306-4412.3.2022.267786

мо значення 4 з базової перестановки. Повторивши описаний алгоритм для всіх розрядів факторіального числа 23211200_F, отримаємо перестановку $\pi = (2,4,3,1,5,7,0,6)$. Таким чином, текстову послідовність із двох символів *ab* можна представити перестановкою $(2,4,3,1,5,7,0,6)$. Таку перестановку можна передати каналом зв'язку та однозначно перетворити в послідовність символів на приймальній стороні.

Варто зазначити, що під час передавання перестановки радіоканалом не обов'язково передавати елементи перестановки у вигляді ASCII символів, що займають 1 байт кожен. Оскільки в роботі прийнято використовувати значення $M = 8$, елементи перестановки будуть лежати в проміжку від 0 до 7. Для кодування 8 значень у двійковій системі числення достатньо $\log_2 8 = 3$ біти. Тому, виконавши конкатенацію трьох молодших біт кожного з елементів перестановки, можна упакувати двійкове представлення перестановки в $3 \times 8 = 24$ біти або 3 байти, передавання яких і виконується каналом зв'язку.

Зауважимо, що відправник і отримувач повинні використовувати одну й ту ж базову перестановку π_0. Тільки в цьому випадку повідомлення може бути коректно декодовано. Якщо відправник і отримувач будуть зберігати базову перестановку π_0, яка сформована випадковим чином, у секреті, канал передавання буде захищеним. У цьому випадку виникає задача узгодження початкової перестановки між абонентами. Цю задачу можливо вирішити, наприклад, за допомогою використання трьохетапного криптографічного протоколу на основі перестановок [9].

Під час отримання з каналу зв'язку перестановки приймач може визначити, чи перестановку прийнято коректно. Для цього перевіряються всі отримані $M = 8$ елементів (24 біти). Кожний елемент із множини цілих значень діапазону $[0, M-1]$ повинен бути присутнім і траплятися у перестановці лише один раз. Якщо в прийнятій послідовності є декілька однакових елементів або деякі елементи відсутні, таку послідовність не можна вважати перестановкою. Вона може бути відкинутою, а передавач змушений буде виконати повторне передавання перестановки. Крім того, оскільки відповідно до [7] параметри ФКВД обираються таким чином, щоб виконувалася рівність $M! \geq 2^k$, де k – кількість біт, що необхідно передати, завжди будуть присутні $M! - 2^k$ перестановок, які не використовуються джерелом. Перестановки з цієї множини теж необхідно обробляти як некоректні.

Приймач отримує перестановку, яку необхідно перетворити на послідовність текстових символів. Це перетворення відбувається наступним чином. Нехай отримано перестановку $\pi = (2,4,6,3,0,7,1,5)$. Спершу отриману перестановку необхідно перетворити в число у факторіальній системі числення. Це відбувається аналогічно перетворенню числа у факторіальній системі числення в перестановку за допомогою базової перестановки π_0, яке відбувається на етапі відправки повідомлення. Кожний елемент перестановки вказує на індекс елемента базової перестановки π_0, вилучаючи при цьому елемент з базової перестановки. Нехай базова перестановка $\pi_0 = (0,1,2,3,4,5,6,7)$. Тоді старший елемент перестановки π (число 2) визначає індекс (число 2) старшим розрядом у факторіальному числі, вилучаючи елемент зі значенням 2 з базової перестановки π_0. На поточному етапі початкова перестановка π_0 перетворюється в $\pi_0' = (0,1,3,4,5,6,7)$. Наступний елемент перестановки (число 4) визначає індекс (число 3) наступним розрядом у факторіальному числі, вилучаючи елемент зі значенням 4 з перестановки π_0'. Повторивши алгоритм для всіх елементів перестановки π, отримаємо число 23420200_F. Після його перетворення в десяткове число отримаємо:

$$23420200_F = 2\times 7! + 3\times 6! + 4\times 5! + 2\times 4! +$$
$$+0\times 3! + 2\times 2! + 0\times 1! + 0\times 0! = 12772_{10}$$

Десяткове число 12772_{10} дорівнює двійковому 11000111100100_2, яке розділимо на дві групи по 7 біт: 1100011_2, 1100100_2. Перетворивши отримані значення в символи, отримаємо символи *cd*.

Експериментальні дослідження. Як приймально-передавальний пристрій будемо використовувати SoC nRF52840 компанії Nordic Semiconductor [10]. Пристрій nRF52840 має вбудоване ядро ARM Cortex-M4, що працює на частотах до 64 МГц, радіомодуль на частоті 2,4 ГГц, що підтримує різноманітні

DOI: 10.24025/2306-4412.3.2022.267786

протоколи передавання (Bluetooth LE, Bluetooth mesh, Thread, Zigbee, 802.15.4, ANT, ESB), 1 MB Flash пам'яті, 256 KB оперативної пам'яті, вбудований апаратний USB 2.0 контролер з можливістю роботи в режимі CDC (USB serial).

На рисунку 1 наведемо структурну схему системи передавання інформації на основі ФКВД.

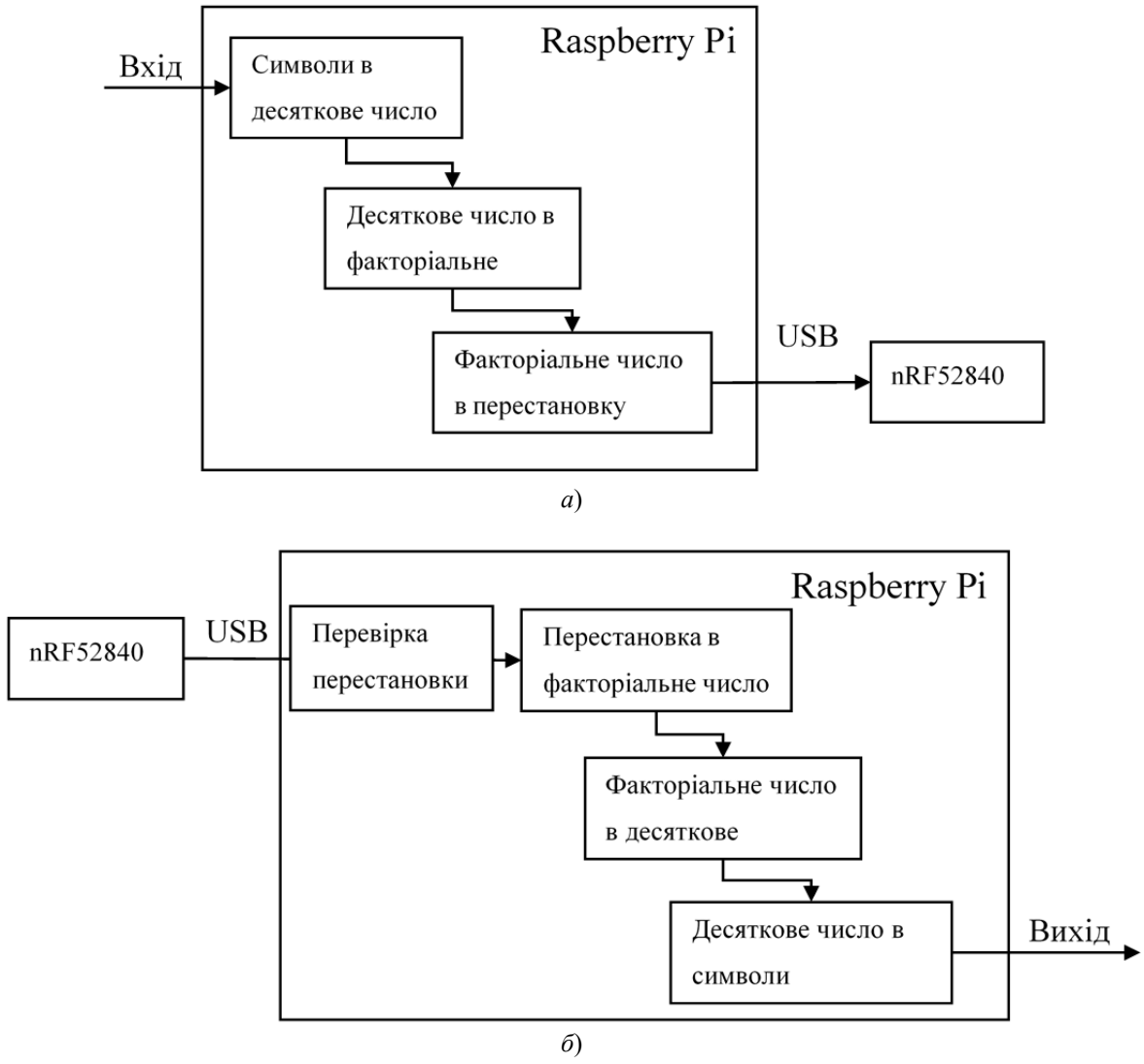


Рисунок 1. Структурна схема системи передавання (*а*) та приймання (*б*) інформації на основі ФКВД

Передавання інформації відбувається в пакетному режимі з фіксованою довжиною пакета, що дорівнює 3 байтам (для $M = 8$). Використання такого контролера дозволяє вести передавання інформації з будь-якого пристрою, що підтримує інтерфейс USB, та на якому запущено відповідне програмне забезпечення.

Варто зазначити, що протокол передавання даних не прив'язаний до апаратного забезпечення і може використовувати практично будь-які приймально-передавальні радіопристрої в різних діапазонах частот. З метою передавання інформації на частотах 433 МГц або 868 МГц (ISM-діапазони) може бути використаний контролер серії CC1352P компанії Texas Instruments [11]. ISM (industrial, scientific and medical)-діапазони доступні для безліцензійного використання практично в будь-якій країні. В Україні список доступних частот регламентується Постановою Кабінету Міністрів України № 1208 від 15.12.2005 р. «Про затвердження Національної таблиці розподілу смуг радіочастот України» [12].

DOI: 10.24025/2306-4412.3.2022.267786

Для формування ФКВД використано плату Raspberry Pi 4 Model B [13], на якій запущено програмне забезпечення на мові програмування Python [14]. Raspberry Pi 4 Model B – це одноплатний комп'ютер на основі ARM v8 архітектури, що працює з використанням операційної системи Linux. Для підключення nRF52840 використано вбудований інтерфейс USB, а для самого радіомодуля розроблено програмне забезпечення, що дозволяє виконувати двосторонній обмін перестановками радіоканалом через віртуальний COM-порт.

Фото макетних зразків приймально-передавальних пристроїв системи передавання інформації зображено на рисунку 2.

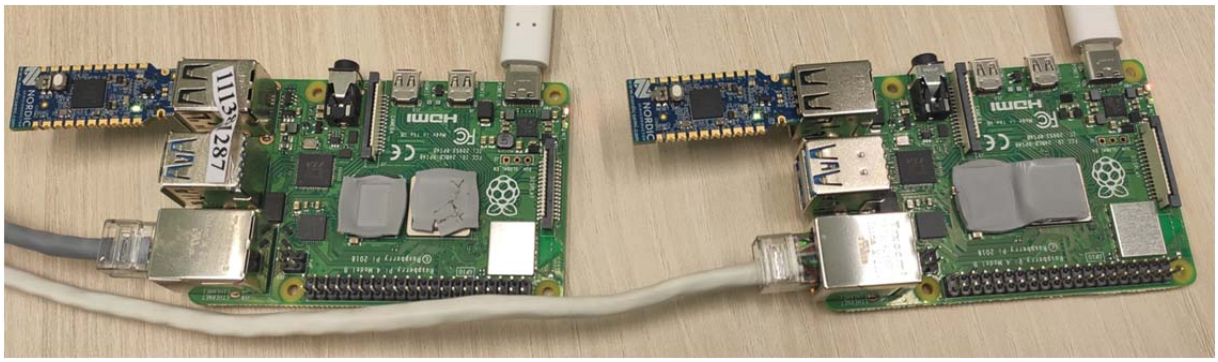
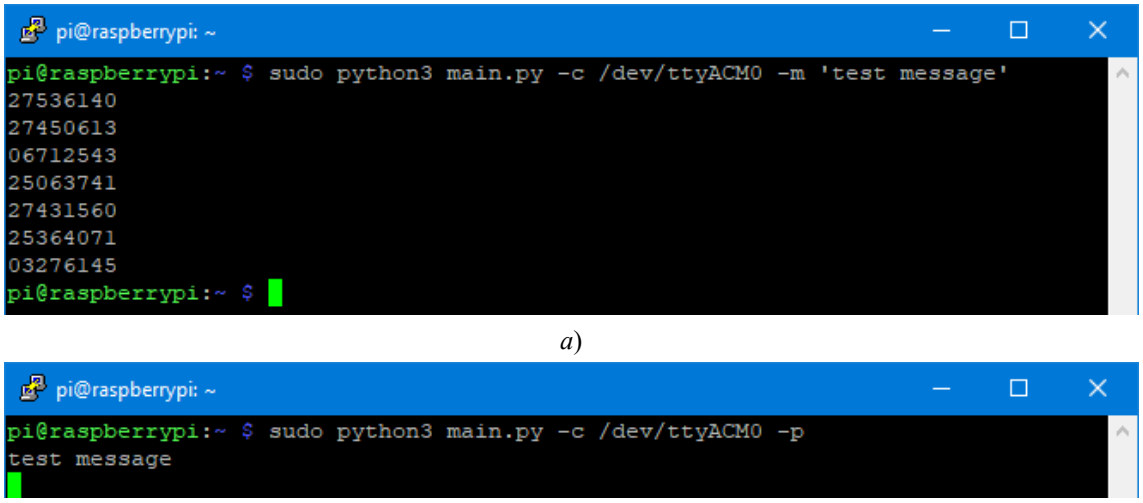


Рисунок 2. Розроблені макетні зразки системи захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону

Результати досліджень. Для передавання даних у системі використовується командний рядок віддаленого SSH доступу до Raspberry Pi (рисунок 3).

Приймальна сторона системи очікує нового повідомлення, виконує перевірку перестановки, перетворює її на текст та виводить користувачу.



а)

б)

Рисунок 3. Процес передавання (*а*) та приймання (*б*) повідомлення

Для початку отримання повідомлень на приймальній стороні необхідно запустити програму з ключем командного рядка *-p*. Для передавання повідомлення на передавальній стороні необхідно запустити програму з ключем командного рядка *-m* і ввести повідомлення, яке необхідно передати. В обох випадках додатково необхідно вказати інтерфейс віртуального COM порту за допомогою ключа командного рядка *-c*, через який буде вестись передавання. Під час передавання повідомлення в консоль передавача виводяться перестановки, що надсилаються в канал зв'язку. Приклад реалізації процесу передавання та приймання повідомлення з використанням

DOI: 10.24025/2306-4412.3.2022.267786

створених макетних зразків наведено на рисунку 3.

Обговорення результатів. Розроблену систему захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону можна використати для обміну як символьними, так і двійковими даними різної довжини. За рахунок збереження базової перестановки в секреті досягається конфіденційність зв'язку між абонентами. З метою узгодження ключової базової перестановки передбачається надалі використати трьохетапний криптографічний протокол [9].

Побудовану інформаційну систему та розроблені макетні зразки приймально-передавальних пристроїв можна використати як базові елементи для подальшої реалізації більш складних систем на основі ФКВД. Зокрема, проведені експерименти використовували високі показники відношення сигнал/шум у каналі зв'язку, що визначало нехтовно малі значення відносної частоти бітової помилки ($\sim 10^{-5}$). Разом з тим, у подальшій роботі необхідно виконати аналіз достовірності передавання інформації в умовах збільшення інтенсивності появи помилок – за умови збільшення відстані між передавачем і приймачем, зменшення потужності передавача, чутливості приймача чи створення штучних шумів у каналі.

Крім того, розроблена система не повною мірою використовує властивості та переваги ФКВД. Для виправлення цієї ситуації потрібно розробити власний канальний протокол, де б кодові слова ФКВД відігравали роль кадрів. У цьому випадку такі можливості ФКВД, як синхронізація та достовірне передавання даних за ймовірності бітової помилки, близької до 0,5, буде можливо реалізувати та оцінити практично.

Висновки. У роботі створено систему захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону на основі ФКВД, а також програмне забезпечення й макетні зразки, що реалізують цю систему.

Наукова новизна роботи полягає у формуванні моделей взаємодії компонентів системи захищеного інформаційного обміну на основі ФКВД, що дозволяє будувати структурні схеми, алгоритми і протоколи обробки та перетворення даних.

Практичну цінність роботи обумовлюють розроблені та реалізовані алгоритми захищеного інформаційного обміну текстовими даними, що включає перетворення текстової інформації в число у факторіальній системі числення з подальшим перетворенням у перестановку на передавальній стороні та зворотні операції декодування повідомлення на приймальній стороні. На основі розроблених алгоритмів створено структурну схему передавально-приймального пристрою, програмний код і макетні зразки системи захищеного інформаційного обміну текстовими даними.

Розроблену систему захищеного інформаційного обміну можна використати як основу для реалізації трьохетапного криптографічного протоколу на основі перестановок [9], операції над перестановками якого можна додатково прискорити за допомогою SIMD інструкцій сучасних процесорів [15].

Подяка. Роботу виконано в рамках науково-технічної (експериментальної) розробки молодих вчених «Розробка мобільної системи захищеного інформаційного обміну для військових і цивільних підрозділів державних структур» (№ ДР 0120U102607).

Список використаних джерел

[1] M. S. Abdulnabi, and H. Ahmed, "Design of efficient cyclic redundancy check-32 using FPGA", in *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, 2018, pp. 1–5.

[2] O. Khadir, "A simple coding-decoding algorithm for the Hamming code", *arXiv preprint arXiv:2201.02066*, 2022.

[3] S. Maheshwari, V. A. Bartlett, and I. Kale, "Energy efficient implementation of multiphase quasi-adiabatic Cyclic Redundancy Check in near field communication", *Integration*, vol. 62, pp. 341-352, 2018.

[4] D. Soni, V. Tiwari, B. Kaur, and M. Kumar, "Cloud computing security analysis based on RC6, AES and RSA algorithms in user-cloud environment", in *2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT)*, 2021, pp. 269–273.

[5] F. Sandoya, D. Dhamodharan, J. L. Hilario Rivas, L. Choque Flores, and S. Thaddeus, "Embedding elliptic curve cryptography and

DOI: 10.24025/2306-4412.3.2022.267786

twofish algorithm to improve data security in Internet of things", 2021.

[6] K.-L. Tsai, F.-Y. Leu, I. You, S.-W. Chang, S.-J. Hu, and H. Park, "Low-power AES data encryption architecture for a LoRaWAN", *IEEE Access*, vol. 7, pp. 146348-146357, 2019.

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

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

[9] A. Shcherba, E. Faure, and O. Lavdanska, "Three-pass cryptographic protocol based on permutations", in *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 2020, pp. 281–284.

[10] "nRF52840–Bluetooth 5.2 SoC - nordicsemi.com". [Online]. Available: https://www.nordicsemi.com/products/nrf52840.

[11] "CC1352P data sheet, product information and support". [Online]. Available: https://www.ti.com/product/CC1352P.

[12] *Про затвердження Національної таблиці розподілу смуг радіочастот України*. 15.12.2005.

[13] "Buy a Raspberry Pi 4 Model B – Raspberry Pi". [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/.

[14] "Welcome to Python.org". [Online]. Available: https://www.python.org/.

[15] А. О. Лавданський, Е. В. Фауре, та В. О. Щерба, "Підвищення швидкості операції множення перестановок за рахунок використання SIMD інструкцій", *Вісник Черкаського державного технологічного університету*, № 3, с. 36-43, 2021.

References

[1] M. S. Abdulnabi, and H. Ahmed, "Design of efficient cyclic redundancy check-32 using FPGA", in *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, 2018, pp. 1–5.

[2] O. Khadir, "A simple coding-decoding algorithm for the Hamming code", *arXiv preprint arXiv:2201.02066*, 2022.

[3] S. Maheshwari, V. A. Bartlett, and I. Kale, "Energy efficient implementation of multiphase quasi-adiabatic Cyclic Redundancy Check in near field communication", *Integration*, vol. 62, pp. 341-352, 2018.

[4] D. Soni, V. Tiwari, B. Kaur, and M. Kumar, "Cloud computing security analysis based on RC6, AES and RSA algorithms in user-cloud environment", in *2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT)*, 2021, pp. 269–273.

[5] F. Sandoya, D. Dhamodharan, J. L. Hilario Rivas, L. Choque Flores, and S. Thaddeus, "Embedding elliptic curve cryptography and twofish algorithm to improve data security in Internet of things", 2021.

[6] K.-L. Tsai, F.-Y. Leu, I. You, S.-W. Chang, S.-J. Hu, and H. Park, "Low-power AES data encryption architecture for a LoRaWAN", *IEEE Access*, vol. 7, pp. 146348-146357, 2019.

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

[8] E. V. Faure, V. V. Shvydkyi, and V. O. Shcherba, "Method of message authentication code formation based on permutations", *Zakhyst informatsii*, vol. 16, no. 4, p. 340, 2015 [in Russian].

[9] A. Shcherba, E. Faure, and O. Lavdanska, "Three-pass cryptographic protocol based on permutations", in *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 2020, pp. 281–284.

[10] "nRF52840–Bluetooth 5.2 SoC - nordicsemi.com". [Online]. Available: https://www.nordicsemi.com/products/nrf52840.

[11] "CC1352P data sheet, product information and support". [Online]. Available: https://www.ti.com/product/CC1352P.

[12] *On the approval of the National table of distribution of radio frequency bands of Ukraine*. Dec. 15, 2005 [in Ukrainian].

[13] "Buy a Raspberry Pi 4 Model B – Raspberry Pi". [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/.

DOI: 10.24025/2306-4412.3.2022.267786

[14] "Welcome to Python.org". [Online]. Available: https://www.python.org/.
[15] A. O. Lavdanskyi, E. V. Faure, and V. O. Shcherba, "Increase of the speed of the permutations multiplication operation due to the use of SIMD instructions", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 3, pp. 36-43, 2021 [in Ukrainian].

A. O. Lavdanskyi[1], *Ph. D., Associate Professor*,
e-mail: a.lavdanskyi@chdtu.edu.ua
E. V. Faure[1], *Dr. Sc., Professor,*
S. T. Tynymbaiev[2], *Ph. D., Professor*,
A. B. Skutskyi[1]
[1]Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
[2]Kazakh National Technical University named after K. I. Satpaev
Satpaev st., 22, Almaty, 050000, Kazakhstan

SYSTEM FOR SECURE INFORMATION EXCHANGE OF TEXT DATA THROUGH THE RADIO CHANNEL OF THE ISM BAND

A system of secure information exchange of text data through the radio channel of the ISM band is developed. The system uses non-separable factorial coding and allows the transmission and reception of text messages and arbitrary binary data. Messages are divided into groups of two symbols, from which a permutation is formed by bijectively transforming the binary sequence into a factorial number system. On the receiving side, the permutation is checked for belonging to the allowed set of permutations and reverse conversion is made, after which the text message is issued to the user in the form in which it has been sent.

The purpose of the work is to create a system of secure information exchange of text data through the radio channel of the ISM band based on factorial code with data recovery by permutation and to create software and prototypes that implement this system.

The scientific novelty of the work consists in the formation of models of the interaction of system components of secure information exchange based on factorial code with data recovery by permutation, which allows the building of structural schemes, algorithms, and protocols for data processing and transformation.

The practical value of the work is determined by the developed and implemented algorithms for secure information exchange of text data, which includes the transformation of text information into a number in the factorial coding system with further transformation into permutation on the transmitting side and reverse operations of decoding the message on the receiving side. On the basis of the developed algorithms, a structural diagram of the transceiver device, program code, and prototypes of the system of secure information exchange of text data have been created. The developed system can establish secure communication between terminals by using basic permutation as a key.

Keywords: *factorial number system, permutation, single-board computer, factorial coding, secure communication.*

Стаття надійшла 25.09.2022
Прийнято 14.10.2022

DOI: 10.24025/2306-4412.3.2022.267786