УДК 004.056.55
DOI https://doi.org/10.32782/2521-6643-2025-2-70.29

Рудницький В. М., доктор технічних наук, професор,
головний науковий співробітник
Державного науково-дослідного інституту випробувань
і сертифікації озброєння та військової техніки
ORCID: 0000-0003-3473-7433

Тарасенко Я. В., доктор технічних наук, доцент,
провідний науковий співробітник
Державного науково-дослідного інституту випробувань
і сертифікації озброєння та військової техніки
ORCID: 0000-0002-5902-8628

Лада Н. В., кандидат технічних наук,
провідний науковий співробітник
Державного науково-дослідного інституту випробувань
і сертифікації озброєння та військової техніки
ORCID: 0000-0002-7682-2970

Бабенко В. Г., доктор технічних наук, професор,
професор кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаського державного технологічного університету
ORCID: 0000-0003-2039-2841

Підласий Д. А., аспірант кафедри інформаційної безпеки
та комп'ютерної інженерії
Черкаського державного технологічного університету
ORCID: 0000-0002-9916-5256

АНАЛІЗ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ CET-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ КЕРОВАНИХ ІНФОРМАЦІЄЮ

У статті розглянуто актуальну на сьогоднішній день задачу синтезу CET-операцій на основі елементарних функцій операцій керованих інформацією. Роботу присвячено питанням зменшення складності генерації максимальної кількості CET-операцій на основі елементарних функцій операцій керованих інформацією для малоресурсних потокових шифрів. У роботі було проведено моделювання CET-операцій та отримано чотири підгрупи по 10 симетричних операцій. Будь яка з підгруп може бути використана для побудови 48 CET-операцій, які включають усі 10 операцій цієї підгрупи. Проведено аналіз обчислювального експерименту щодо моделювання CET-операцій на основі елементарних функцій операцій керованих інформацією. Встановлено відсутність перетину серед синтезованих множин CET-операцій, на основі модифікацій CET-операцій з різних підгруп. На основі вибору чотирьох CET-операцій (по одній з кожної групи) існує можливість синтезування повної групи CET-операцій на основі елементарних функцій керованих інформацією. Така група включає 192 операції. У роботі наведено групу елементарних функцій операцій керованих інформацією та підмножини симетричних CET-операцій на основі елементарних функцій операцій керованих інформацією. Описано вимоги, на основі яких необхідно проводити вибір базової групи для побудови методу синтезу CET-операцій на основі елементарних функцій операцій керованих інформацією. Наведено умови розгляду вимог до CET-операцій базової групи. За результатами обчислювального експерименту розроблено метод вибору базових груп симетричних CET-операцій, що дає можливість зменшити складність генерації максимальної кількості CET-операцій на основі елементарних функцій операцій керованих інформацією для малоресурсних потокових шифрів. Розроблений метод можливо застосовувати в малоресурсних телекомунікаційних системах як мобільного, так і стаціонарного типу. Перспективою подальших досліджень з напрямку є побудова малоресурсних систем криптографічного перетворення інформації із застосуванням CET-операцій на основі елементарних функцій операцій керованих інформацією.

Ключові слова: *CET-операції, операції керовані інформацією, Сі-квантові елементарні функції, автоматизований синтез операцій, обчислювальний експеримент.*

Rudnytskyi V. M., Tarasenko Ya. V., Lada N. V., Babenko V. H., Pidlasyi D. A. Analysis of simulation results of CET-operations based on elementary functions of information-driven operations

The article considers the currently relevant task of synthesizing CET operations based on elementary functions of information-driven operations. The work is devoted to reducing the complexity of generating the maximum number of CET operations based on elementary functions of information-driven operations for low-resource stream ciphers. The work involved modelling CET-operations and obtaining four subgroups of 10 symmetric operations. Any of the subgroups can be used to construct 48 CET-operations that include all 10 operations of that subgroup. An analysis of a computational experiment on modelling CET-operations based on elementary information-driven operations was conducted. The absence of intersection among the synthesized sets of CET-operations was established, based on modifications of CET-operations from different subgroups. Based on the selection of four CET-operations (one from each group), it is possible to synthesize a complete group of CET-operations based on elementary information-driven functions. Such a group includes 192 operations. The paper presents a group of elementary functions of information-driven operations and a subset of symmetric CET-operations based on elementary functions of information-driven operations. The requirements for selecting a base group for constructing a method for synthesizing CET-operations based on elementary functions of information-driven operations are described. The conditions for considering the requirements for CET-operations of the base group are presented. Based on the results of a computational experiment, a method for selecting basic groups of symmetric CET-operations has been developed, which makes it possible to reduce the complexity of generating the maximum number of CET-operations based on elementary information-driven operations for low-resource stream ciphers. The developed method can be applied in low-resource telecommunication systems of both mobile and stationary types. The prospect of further research in this area is the construction of low-resource systems for cryptographic information transformation using CET-operations based on elementary functions of information-driven operations.

Key words: *CET-operations, information-driven operations, Si-quantum elementary functions, automated synthesis of operations, computational experiment.*

Постановка проблеми. До найбільших викликів, з якими стикається суспільство в усіх сферах свого існування на сучасному етапі розвитку відносять питання захисту інформації. Проблема захисту даних, що передаються поширеними каналами не є новою. Зі стародавніх часів забезпечення цілісності та конфіденційності інформації було вкрай важливою задачею, яка з розвитком науки і техніки набуває нових проявів.

Сучасні загрози характеризуються високим потенціалом їх потенційної ефективності. У роботі [1] виділяється дві категорії в розрізі квантових загроз: перехопити зараз – розшифрувати пізніше (Harvest Now, Decrypt Later – HTDL); підробка цифрових підписів та сертифікатів.

У роботі [2] автори наголошують на вразливості багатьох криптографічних алгоритмів до атак реалізації. Відзначається недостатність алгоритмічної безпеки, що зумовлює важливість розвитку адаптивних можливостей криптографічних алгоритмів, що дозволить враховувати варіативність сучасних загроз та забезпечити стійкість до нових типів атак.

Розвиток обчислювальних систем, засобів передачі даних, нейромережевих технологій вимагає розробки нових підходів побудови елементарних операцій криптографічного кодування, які забезпечують варіативність та адаптивність криптографічних алгоритмів. Вкрай актуальною проблемою є дослідження операцій керованих інформацією в розрізі криптографічного захисту інформації. Такі операції характеризуються варіативністю своєї структури, що забезпечує динамічну залежність від змінної інформації, яка керує процесами та забезпечує криптографічну стійкість.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях СЕТ-шифрування виділяється як один з перспективних напрямків збільшення варіативності операцій потокового шифрування та розвитку криптографічного захисту інформації в цілому. Однією з головних переваг операцій СЕТ-шифрування є можливість їх застосування як при блоковому так і при потоковому шифруванні [3]. У роботах [4-5] представлені перші спроби синтезу двохоперандних СЕТ-операцій на основі додавання за модулем два та їх дискретно-алгебраїчного представлення. У подальшому проводились дослідження по синтезу операцій криптографічного перетворення інформації не лише на операціях 2-ої розрядності, а й на операціях 3-ої розрядності [6] та операціях 4-ої розрядності [7]. У роботі [7] встановлено також умови невиродженості нелінійних операцій розширеного матричного криптографічного перетворення n-ої розрядності, у складі яких є неповні функції розширеного матричного криптографічного перетворення інформації.

На основі попередніх досліджень операцій криптогоафічного перетворення розпочались дослідження СЕТ-операцій керованих інформацією. У роботі [8] проаналізовано основні елементарні операції, що входять до базової групи операцій перестановок, керованих інформацією та представлена дискретна модель базових груп операцій перестановок для криптоперетворення, керованих інформацією. Практична реалізація дискретних моделей СЕТ-операцій керованих інформацією наведена в роботі [9]. У роботі [10] запропоновано шлях підвищення швидкості та стійкості матричного криптографічного перетворення за рахунок використання операцій та алгоритмів криптоперетворення двох блоків змінних інформації. Окремої уваги потребують важливі роботи по синтезу обернених СЕТ-операцій [11-12]. Аналіз досліджень показав, що синтезу СЕТ-операцій на основі елементарних функцій операцій керованих інформацією та побудові їх базових груп приділена недостатня увага.

Мета статті – зменшення складності генерації максимальної кількості СЕТ-операцій на основі елементарних функцій операцій керованих інформацією для малоресурсних потокових шифрів за рахунок розробки методу вибору базових груп симетричних СЕТ-операцій на основі результатів обчислювального експерименту.

Виклад основного матеріалу. Для дослідження одноопераднних СЕТ-операцій на основі елементарних функцій операцій керованих інформацією необхідно мати множину даних операцій. Наявність даної множини і буде набором вхідних даних для проведення дослідження. Одноопераднді СЕТ-операції на основі елементарних функцій операцій керованих інформацією належать до групи 3Сі-квантових СЕТ-операцій. Повна група 3Сі-квантових СЕТ-операцій представляє собою всі підстановки з поля перестановок G_8 і включає в себе 40320 СЕТ-операцій. Всі 3Сі-квантові СЕТ-операції будуються на основі 70 3Сі-квантових елементарних функцій. Одноопераднді 3Сі-квантові СЕТ-операції на основі елементарних функцій операцій керованих інформацією будуються на основі 8 елементарних функцій операцій керованих інформацією [13-14]. Так як елементарних функцій всього 8 то кількість СЕТ-операцій які потрібно знайти для проведення дослідження буде значно меншою за 40320. Виходячи з незначної кількості елементарних функцій на основі яких будуються одноопераднді 3Сі-квантові СЕТ-операції на основі елементарних функцій операцій керованих інформацією доцільно для автоматизованого синтезу операцій використати повний перебір варіантів розміщення елементарних функцій в операціях. Даний підхід і було використано при проведенні обчислювального експерименту по моделюванню СЕТ-операцій на основі елементарних функцій операцій керованих інформацією. Група елементарних функцій операцій керованих інформацією представлена в таблиці 1 [6].

Таблиця 1

Група елементарних функцій операцій керованих інформацією

Елементарна функція	Результат реалізації	Елементарна функція	Результат реалізації
$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	00010111	$f_{232} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot \overline{x}_3$	11101000
$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3$	00101011	$f_{212} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3$	11010100
$f_{77} = x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3$	01001101	$f_{178} = \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3$	10110010
$f_{113} = \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	01110001	$f_{142} = x_1 \cdot \overline{x}_2 \vee x_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot \overline{x}_3$	10001110

У табл. 1 індекси елементарних функцій відповідають значенню десяткової цифри результату перетворення, за умови впорядкування повної множини вхідних даних по зростанню їх значень [6].

За результатами обчислювального експерименту було отримано 192 СЕТ-операції на основі елементарних функцій операцій керованих інформацією. Результати обчислювального експерименту наведені в додатку А.

Будь яку СЕТ-операцію можна модифікувати шляхом перестановки елементарних функцій, а також шляхом інверсії результатів виконання елементарної функції. СЕТ-операція на основі елементарних функцій операцій керованих інформацією є 3Сі-квантовою, то вона виконує криптографічне перетворення 3Сі-квантів вхідної інформації і формує 3Сі-кванти результату перетворення. Виходячи з цього її можна модифікувати за допомогою 6 операцій перестановки елементарних функцій і 8 операцій інверсії результатів. Виходячи з цього на основі будь якої СЕТ-операції можна отримати 48 її модифікацій.

Так як група СЕТ-операції на основі елементарних функцій операцій керованих інформацією включає в себе 192 операції то вона включає в себе модифікації 4 унікальних базових операцій (192:48=4). Дані 4 унікальні базові операції складають базову групу СЕТ-операції на основі елементарних функцій операцій керованих інформацією. З будь якої операції базової групи шляхом перестановок і інверсій будується множина модифікованих СЕТ-операцій. Кожна побудована операція з даної множини буде унікальною (не буде повторятися), а побудовані множини операцій не будуть перетинатися. Так як, множина модифікованих СЕТ-операцій будується шляхом перестановок і інверсій елементарних функцій базової операції та базова група операцій на основі елементарних функцій операцій керованих інформацією включає в себе будь які 4 операції, які належать до 4 різних множин модифікованих операцій.

В процесі дослідження одноопераднних СЕТ-операцій на основі елементарних функцій операцій керованих інформацією необхідно встановити правила побудови прямих і обернених СЕТ-операцій.

Для побудови правил синтезу прямих і обернених операцій доцільно дослідити правила побудови СЕТ-операцій базової групи, так як правила їх модифікації на основі перестановки і інверсії елементарних функцій відомі [35]. Сформовані підмножини симетричних СЕТ-операцій на основі елементарних функцій операцій керованих інформацією представлено у (табл. 2).

Таблиця 2

Підмножини симетричних СЕТ-операції на основі елементарних функцій операцій керованих інформацією

№	Множина 1	Множина 2	Множина 3	Множина 4
1	$C_{23,43,77}(x)$	$C_{23,43,142}(x)$	$C_{23,142,77}(x)$	$C_{43,77,113}(x)$
2	$C_{23,77,43}(x)$	$C_{43,23,113}(x)$	$C_{77,113,23}(x)$	$C_{77,113,43}(x)$
3	$C_{43,23,178}(x)$	$C_{43,142,232}(x)$	$C_{77,232,142}(x)$	$C_{113,43,77}(x)$
4	$C_{77,212,23}(x)$	$C_{113,23,43}(x)$	$C_{113,77,23}(x)$	$C_{113,77,43}(x)$
5	$C_{178,43,232}(x)$	$C_{142,232,212}(x)$	$C_{142,178,232}(x)$	$C_{142,178,212}(x)$
6	$C_{212,232,77}(x)$	$C_{212,113,23}(x)$	$C_{178,23,113}(x)$	$C_{142,212,178}(x)$
7	$C_{232,178,212}(x)$	$C_{212,232,142}(x)$	$C_{178,142,232}(x)$	$C_{178,142,212}(x)$
8	$C_{232,212,178}(x)$	$C_{232,212,113}(x)$	$C_{232,113,178}(x)$	$C_{212,178,142}(x)$

Нижні індекси в моделях СЕТ-операцій наведених у табл. 2 відображають індекси елементарних функцій з яких побудовано дані операції. Наприклад:

$$C_{77,212,23}(x) = \begin{bmatrix} f_{77}(x) \\ f_{212}(x) \\ f_{23}(x) \end{bmatrix} \tag{1}$$

Базова група СЕТ-операцій на основі елементарних функцій операцій керованих інформацією яка складається лише з симетричних операцій включає в себе по одній модифікованій операції з кожної множини. Наприклад:

- $C_{23,43,77}(x)$, $C_{23,43,142}(x)$, $C_{23,142,77}(x)$, $C_{43,77,113}(x)$;
- $C_{23,43,77}(x)$, $C_{43,23,113}(x)$, $C_{178,23,113}(x)$, $C_{142,178,212}(x)$;
- $C_{178,43,232}(x)$, $C_{142,232,212}(x)$, $C_{77,232,142}(x)$, $C_{178,142,212}(x)$.

Відповідно до табл. 2 кількість група СЕТ-операцій які складається з симетричних операцій буде визначатися як $8 \cdot 8 \cdot 8 \cdot 8 = 8^4 = 4096$.

Вибір базової групи для побудови методу синтезу СЕТ-операцій на основі елементарних функцій операцій керованих інформацією необхідно проводити на основі двох вимог:

1. Мінімальна простота синтезу 4 симетричних СЕТ-операцій базової групи. Дана вимога базується на необхідності зменшення обчислювальних ресурсів для моделювання систем захисту інформацій на основі СЕТ-шифрування.

2. Максимальна відмінність відповідних елементарних функцій в 4 симетричних СЕТ-операціях базової групи для реалізації вихідних Сі-квантів інформації. Дана вимога базується на бажанні максимального ускладнення крипто аналізу, для визначення правил формування послідовності крипто перетворень.

Наведені вимоги достатньо суперечливі і вимагають різних підходів до пошуку СЕТ-операцій базової групи. Необхідно відмітити, що незалежно яка базова група СЕТ-операцій буде взята за основу, це забезпечить побудову на основі перестановок і інверсій елементарних функцій отримати повну групу операцій. Вибір базової групи буде впливати лише на послідовність синтезу СЕТ-операцій.

Виходячи з цього доцільно розглядати вимоги до СЕТ-операцій базової групи незалежно одна від другої, а вже на основі отриманих результатів, за необхідністю спробувати знайти компроміс.

Висновки. У статті було отримано наступні результати:

1. За результатами аналізу СЕТ-операцій на основі елементарних функцій операцій керованих інформацією було виділено чотири підгрупи симетричних СЕТ-операцій з точністю до перестановки елементарних функцій і їх інверсій. Кожна підгрупа включає по 10 СЕТ-операцій. З будь-якої вибраної з підгрупи операції на основі перестановки елементарних функцій і їх інверсій можна побудувати 48 СЕТ-операцій які включають всі 10 операцій підгрупи.

2. Встановлено, що синтезовані множини СЕТ-операцій на основі модифікацій СЕТ-операцій з різних підгруп не перетинаються. На основі вибору чотирьох СЕТ-операцій (по одній з кожної підгрупи шляхом перестановки інверсій) можна синтезувати повну групу СЕТ-операцій на основі елементарних функцій операцій керованих інформацією, яка включає 192 операції.

3. За результатами обчислювального експерименту розроблено метод вибору базових груп симетричних СЕТ-операцій для зменшення складності генерації максимальної кількості СЕТ-операцій на основі елементарних функцій операцій керованих інформацією для малоресурсних потокових шифрів.

Сфера практичного застосування запропонованого методу полягає у його використанні в мобільних та стаціонарних малоресурсних телекомунікаційних системах.

Подальшого розгляду потребують питання побудови малоресурсних систем криптографічного перетворення інформації шляхом застосування СЕТ-операцій на основі елементарних функцій операцій керованих інформацією.

Список використаних джерел:

1. Benitez C. Mapping quantum threats: an engineering inventory of cryptographic dependencies. *arXiv*. 2025. URL: https://doi.org/10.48550/arXiv.2509.24623 (дата звернення: 15.10.2025).

2. Algorithmic security is insufficient: a comprehensive survey on implementation attacks haunting post-quantum security / A.C. Canto et al. *arXiv*. 2023. URL: https://doi.org/10.48550/arXiv.2305.13544 (дата звернення: 15.10.2025).

3. Архітектура СЕТ-операцій і технології потокового шифрування: монографія / В.М. Рудницький та ін. Черкаси: видавець Пономаренко Р.В., 2024. 374 с.

4. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*. 2012. Вип. 3 (101), Т. 1. С. 119–122.

5. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій / С.В. Голуб та ін. *Системи управління, навігації та зв'язку*. 2012. Вип. 2 (22). С. 163–168.

6. Бабенко В., Мельник О., Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Том 19, № 1. С. 56–59.

7. Стабецька Т. А. Умови невиродженості нелінійних операцій розширеного матричного криптографічного перетворення, що містять неповні функції РМКП. *Системи обробки інформації*. 2016. Вип. 1 (138). С. 131–133.

8. Миронюк Т. В., Ланських Є. В. Дискретна модель базових груп операцій перестановок, керованих інформацією, для криптоперетворення. *Smart and Young*. 2016. Вип. 11-12. С. 58–65.

9. Миронець І. В., Миронюк Т. В., Сисоєнко С. В. Апаратна реалізація базової групи операцій перестановок, керованих інформацією. *Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 23–25 листопада 2016 р.)*. Кропивницький : КНТУ, 2016. С. 141–142.

10. Сисоєнко С. В., Мельник О. Г. Використання операцій та алгоритмів криптоперетворення двох блоків змінних в криптографії. *Інноваційні тенденції сьогодення в сфері природничих, гуманітарних та точних наук : матеріали Міжнародної науково-практичної конференції (м. Івано-Франківськ, 17 жовтня 2017 р.)*. Одеса: Друкарик, 2017. Вип. 2. С. 47–49.

11. Сисоєнко С. В., Мельник О. Г., Пустовіт М. О. Синтез операцій оберненого групового матричного криптографічного перетворення інформації. *Вісник Черкаського державного технологічного університету. Технічні науки.* 2017. Вип. 22, № 4. С. 118–125.

12. Breus R. Synthesising the two-bit two-operand operations of strict stable cryptographic coding by the second operand's conversion. *Academic Journal. Control, Navigation and Communication Systems*. 2019. Vol. 5, № 57. P. 29–32. DOI: https://doi.org/10.26906/SUNZ.2019.5.029

13. Синтез дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією / В.М. Рудницький та ін. *Кібербезпека: освіта, наука, техніка*. 2024. Том 3, № 23. С. 6–16. DOI: https://doi.org/10.28925/2663-4023.2024.23.616

14. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій / В.М. Рудницький та ін. *Системи управління, навігації та зв'язку*. 2023. № 4. С. 96–101. DOI: https://doi.org/10.26906/SUNZ.2023.4.096

15. Криптографічне кодування: методи і засоби реалізації (частина 2): монографія / В.М. Рудницкий та ін. Х. : Видавництво «Щедра садиба плюс», 2014. 224 с.

References:

1. Benitez, C. (2025). Mapping quantum threats: an engineering inventory of cryptographic dependencies. *arXiv*. https://doi.org/10.48550/arXiv.2509.24623

2. Canto, A. C., et al. (2023). Algorithmic security is insufficient: a comprehensive survey on implementation attacks haunting post-quantum security. *arXiv*. https://doi.org/10.48550/arXiv.2305.13544

3. Rudnytskyi, V., et al. (2024). Arkhitektura SET-operatsii i tekhnolohii potokovoho shyfruvannia: monohrafiia [Architecture of CET-operations and stream encryption technologies: monograph]. Publisher Ponomarenko R.V. [in Ukrainian].

4. Golub, S. V., Babenko, V. G. & Rudnytskyi, S. V. (2012). Metod syntezu operatsii kryptohrafichnoho peretvorennia na osnovi dodavannia za modulem dva [A method for synthesizing cryptographic transformation operations based on addition modulo two]. *Systemy obrobky informatsii – Information Processing Systems*, 3 (101), 1, 119–122 [in Ukrainian].

5. Golub, S. V., et al. (2012). Vdoskonalennia metodu syntezu operatsii kryptohrafichnoho peretvorennia na osnovi dyskretno-alhebraiichnoho predstavlennia operatsii [Improvement of the Method for Synthesizing Cryptographic Transformation Operations Based on Discrete-Algebraic Representation of Operations]. *Systemy upravlinnia, navihatsii ta zviazku – Academic Journal. Control, Navigation and Communication Systems*, 22(2), 163–168 [in Ukrainian].

6. Babenko, V., Melnyk, O. & Melnyk, R. (2013). Klasyfikatsiia tryrozriadnykh elementarnykh funktsii dlia kryptohrafichnoho peretvorennia informatsii [Classification of three digit basic functions for cryptographic transformation of information]. *Bezpeka informatsii – Ukrainian Scientific Journal of Information Security*, 19(1), 56–59 [in Ukrainian].

7. Stabetska, T. A. (2016). Umovy nevyrodzhenosti neliniinykh operatsii rozshyrenoho matrychnoho kryptohrafichnoho peretvorennia, shcho mistiat nepovni funktsii RMKP [Conditions of non-degeneracy of nonlinear operations of the extended matrix cryptographic transformation containing incomplete functions of the EMCT]. *Systemy obrobky informatsii – Information Processing Systems*, 138(1), 131–133 [in Ukrainian].

8. Myroniuk, T. V. & Lanskikh, E. V. (2016). Dyskretna model bazovykh hrup operatsii perestanovok, kerovanykh informatsieiu, dlia kryptoperetvorennia [A discrete model of basic groups of information-driven permutation operations for cryptotransformation]. *Smart and Young*, 11-12, 58–65 [in Ukrainian].

9. Myronets, I. V., Myroniuk, T. V. & Sysoyenko, S. V. (2016). Aparatna realizatsiia bazovoi hrupy operatsii perestanovok, kerovanykh informatsieiu [Hardware implementation of a basic group of information-driven permutation operations]. *Aktualni zadachi ta dosiahnenia u haluzi kiberbezpeky – Current tasks and achievements in the field of cybersecurity* (p. 141–142). Kropyvnytskyi National Technological University [in Ukrainian].

10. Sysoyenko, S. V. & Melnyk, O. G. (2017). Vykorystannia operatsii ta alhorytmiv kryptoperetvorennia dvoh blokiv zminnykh v kryptohrafii [Using of the operations and algorithms of cryptographic transformation of two blocks of variables in cryptography]. *Innovatsiini tendentsii siohodennia v sferi pryrodnychnykh, humanitarnykh ta tochnykh nauk – Innovative Trends in the Field of Natural Sciences, Humanities and Exact Sciences* (p. 47–49). Drukaryk [in Ukrainian].

11. Sysoyenko, S. V., Melnyk, O. G. & Pustovit, M. O. (2017). Syntez operatsii obernenoho hrupovoho matrychnoho kryptohrafichnoho peretvorennia informatsii [Synthesis of operations of reverse group matrix cryptographic transformation of information]. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Tekhnichni nauky – Bulletin of Cherkasy State Technological University. Technical sciences*, 22(4), 118–125 [in Ukrainian].

12. Breus, R. (2019). Synthesising the two-bit two-operand operations of strict stable cryptographic coding by the second operand's conversion. *Academic Journal. Control, Navigation and Communication Systems*, 57(5), 29–32. https://doi.org/10.26906/SUNZ.2019.5.029

13. Rudnytskyi, V., et al. (2024). Syntez dyskretno-alhebraiichnykh modelei elementarnykh funktsii operatsii kerovanykh informatsieiu [Synthesis of discrete and algebraic models of elementary functions of data-controlled operations]. *Kiberbezpeka: osvita, nauka, tekhnika – Electronic scientific journal "Cyber Security: Education, Science, Technology"*, 23(3), 6–16. https://doi.org/10.28925/2663-4023.2024.23.616 [in Ukrainian].

14. Rudnytskyi, V., et al. (2023). Dyskretno-kazualne predstavlennia modelei elementarnykh funktsii i SET-operatsii [Discrete-casual presentation of models of elementary functions and set operations]. *Systemy upravlinnia, navihatsii ta zviazku – Academic Journal. Control, Navigation and Communication Systems*, 74(4), 96–101. https://doi.org/10.26906/SUNZ.2023.4.096 [in Ukrainian].

15. Rudnytskyi, V., et al. (2014). Kryptohrafichne koduvannia: metody i zasoby realizatsii (chastyna 2): monohrafiia [Cryptographic encoding: methods and implementation tools (Part 2): monograph]. Publisher "Shchedra Sadyba Plus" [in Ukrainian].

Дата надходження статті: 27.10.2025
Дата прийняття статті: 17.11.2025
Опубліковано: 30.12.2025