УДК 004.056.55:004.312.2
DOI https://doi.org/10.32689/maup.it.2025.1.28

Володимир РУДНИЦЬКИЙ
доктор технічних наук, професор, головний науковий співробітник,
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, rvn_2008@ukr.net
***ORCID:** 0000-0003-3473-7433*

Віра БАБЕНКО
доктор технічних наук, професор, професор кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, v.babenko@chdtu.edu.ua
***ORCID:** 0000-0003-2039-2841*

Сергій РУДНИЦЬКИЙ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій проектування, Черкаський державний технологічний університет,
провідний науковий співробітник,
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, s.v.rudnitskiy@gmail.com
***ORCID:** 0000-0003-3071-7005*

Тимофій КОРОТКИЙ
здобувач ступеня доктор філософії, кафедра інформаційних технологій проектування, Черкаський державний технологічний університет, t.k.korotkyi.asp21@chdtu.edu.ua
***ORCID:** 0009-0003-5159-5892*

ГЕНЕРАЦІЯ ПОСЛІДОВНОСТІ НЕСИМЕТРИЧНИХ СЕТ-ОПЕРАЦІЙ З ТОЧНІСТЮ ДО ПЕРЕСТАНОВКИ ДРУГОГО ОПЕРАНДА

Анотація. *Стаття присвячена побудові несиметричних СЕТ-операцій придатних для криптографічного перетворення інформації, а саме СЕТ-шифрування. Застосування СЕТ-операцій при побудові потокових шифрів гарантує двонаправлевлену передачу інформації між абонентами. Особливість несиметричних СЕТ-операцій полягає в тому, що вони забезпечують в процесі шифрування однакової інформації з використанням однакових ключових послідовностей побудову різних шифрограм. Для вдосконалення потокових шифрів велике значення має можливість застосування замість однієї несиметричної двохоперандної СЕТ-операції декількох, які мають однакові властивості. Саме тому задачі синтезу груп СЕТ-операцій з точністю до перестановки надзвичайно актуальні. Адже їх вирішення дозволить будувати генератори псевдовипадкових послідовностей СЕТ-операцій з однаковими властивостями, щоб забезпечити побудову криптографічних алгоритмів потокового шифрування нового покоління.*

Метою роботи *є дослідження можливості застосування методу генерації груп несиметричних СЕТ-операцій з точністю до перестановки другого операнда для побудови малоресурсних несиметричних систем потокового шифрування.*

Методологія. *У роботі показано, що генерувати групи операцій строгого стійкого кодування доцільно на основі модифікації СЕТ-операції строгого стійкого кодування з точністю до перестановки другого операнда. Для синтезу моделей СЕТ-операцій, як прямих та і обернених, наведено один із способів реалізації їх методу побудови, що полягає в генерації послідовності несиметричних двохоперандних СЕТ-операцій з точністю до перестановки другого операнда. Здійснено перевірку коректності одержаних моделей для синтезу груп прямих і обернених несиметричних двохоперандних СЕТ-операцій на конкретних прикладах, що підтверджено результатами обчислювального експерименту для 2Сі-квантових несиметричних двохоперандних СЕТ-операцій. В ході проведеного дослідження використовувалися методи та принципи теорії інформації та кодування, булевої алгебри, дискретної математики, теорії синтезу та моделювання операцій та криптографії.*

Наукова новизна. *Наукова новизна роботи полягає в аналізі практичних аспектів застосування груп несиметричних СЕТ-операцій з точністю до перестановки другого операнда для побудови алгоритмів малоресурсної криптографії шляхом забезпечення генерації прямих і обернених несиметричних двохоперандних СЕТ-операцій за рахунок використання лише прямих одноопераднних СЕТ-операцій, що суттєво зменшує складність криптогафічного алгоритму і складність реалізації криптографічної системи.*

Висновок. *У результаті дослідження встановлено наступне: усі несиметричні СЕТ-операції, які належать до синтезованої групи з точністю до перестановки другого операнда, мають однакові криптографічні властивості, оскільки однаково випадково реалізують одні і ті самі набори таблиць підстановок; можливість генерації груп прямих і обернених несиметричних СЕТ-операцій з точністю до перестановки другого операнда на основі будь якої двохоперандної СЕТ-операції забезпечить як шифрування, так і розшифрування інформації для побудови систем потокового шифрування.*

Ключові слова: *малоресурсна криптографія, СЕТ-шифрування, моделювання СЕТ-операцій, дослідження СЕТ-операцій, несиметричні криптографічні перетворення, потокове шифрування.*

Volodymyr RUDNYTSKYI, Vira BABENKO, Serhii RUDNYTSKYI, Tymofii KOROTKYI. GENERATING A SEQUENCE OF ASYMMETRIC CET OPERATIONS WITH AN ACCURACY OF UP TO THE PERMUTATION OF THE SECOND OPERAND

Abstract. *The article is devoted to the construction of asymmetric CET operations suitable for cryptographic information transformation, namely CET encryption. The use of CET operations in the construction of streaming ciphers guarantees bidirectional transmission of information between subscribers. The specific feature of asymmetric CET operations is that they provide different ciphers in the process of encrypting the same information using the same key sequences. To improve stream ciphers, it is of great importance to be able to use several asymmetric two-operand CET operations with the same properties instead of one. That is why the problems of synthesizing groups of CET operations with permutation accuracy are extremely relevant. After all, their solution will allow us to build generators of pseudo-random sequences of CET operations with the same properties to ensure the construction of new generation of cryptographic algorithms of stream encryption.*

The purpose of the article is to study *the possibility of using the method of generating groups of asymmetric CET operations with an accuracy of up to the permutation of the second operand to build low-resource asymmetric stream encryption systems.*

Methodology. *The paper shows that it is expedient to generate groups of operations of strictly stable coding on the basis of modifying the CET operation of strictly stable coding with an accuracy of permutation of the second operand. To synthesize models of CET operations, both direct and reverse, one of the ways to implement their construction method is presented, which consists in generating a sequence of asymmetric two-operand CET operations with an accuracy of permutation of the second operand. The correctness of the obtained models for the synthesis of groups of direct and reverse asymmetric two-operand CET operations is verified on specific examples, which is confirmed by the results of a computational experiment for 2Ci-quantum asymmetric two-operand CET operations. In the course of the study, the methods and principles of information and coding theory, Boolean algebra, discrete mathematics, the theory of synthesis and modeling of operations, and cryptography were used.*

Scientific novelty. *The scientific novelty of the work is to analyze the practical aspects of using groups of asymmetric CET operations with an accuracy of up to the permutation of the second operand to build low-resource cryptography algorithms by ensuring the generation of direct and reverse asymmetric two-operand CET operations by using only direct one-operand CET operations, which significantly reduces the complexity of the cryptographic algorithm and the complexity of the cryptographic system implementation.*

Conclusion. *As a result of the study, the following was found: all asymmetric CET operations belonging to the synthesized group with an accuracy of up to the permutation of the second operand have the same cryptographic properties, since they implement the same sets of substitution tables in the same way by chance; the ability to generate groups of forward and reverse asymmetric CET operations with an accuracy of up to the permutation of the second operand on the basis of any two-operand CET operation will provide both encryption and decryption of information for building streaming encryption systems.*

Key words: *low-resource cryptography, CET encryption, modeling of CET operations, investigation of CET operations, asymmetric cryptographic transformations, stream encryption.*

Постановка проблеми. Стрімкий розвиток інформаційно-телекомунікаційних систем і комп'ютерних мереж зумовив різке зростання кіберзлочинів, пов'язаних з несанкціонованим доступом до інформації. Саме тому проблема криптографічного захисту конфіденційної інформації в комп'ютерних системах і мережах в умовах сьогодення є надзвичайно актуальною. Вирішення даної проблеми полягає в ефективному комплексному захисті інформації при її зберіганні [11, 12], при передачі [9, 16], і при обробці [14]. Одним із найефективніших засобів протидії несанкціонованому доступу до конфіденційної інформації є її шифрування. Традиційні стандартизовані криптографічні алгоритми забезпечують необхідний захист інформації, проте їх реалізація, як правило, ресурсноємна, а застосування є високо витратним. Відомо, що підвищення ефективності функціонування комп'ютерної мережі зумовлює зменшення ресурсів, які можуть бути виділені для реалізації криптографічного захисту інформації. Тому доцільно при реалізації захищених комп'ютерних мереж використовувати мало ресурсну криптографію [10, 15, 19, 20].

Необхідно відмітити, що забезпечення високої криптографічної стійкості вступає в протиріччя з необхідністю високошвидкісного захисту колосальних обсягів інформації в реальному часі, яка циркулює в кіберпросторі. Виходячи з цього, криптографічні системи розраховані на масове застосування повинні бути криптостійкими, малоресурсними та водночас і високошвидкісними, а також мати незначну вартість експлуатаційних витрат. Даним вимогам в достатній мірі можуть відповідати малоресурсні потокові шифри побудовані на основі несиметричних СЕТ-операцій. Застосування СЕТ-операцій при побудові потокових шифрів гарантує двонаправлевлену передачу інформації між абонентами. Особливість несиметричних СЕТ-операцій полягає в тому, що вони забезпечують в процесі шифрування однакової інформації з використанням однакових ключових послідовностей побудову різних шифрограм. Для вдосконалення потокових шифрів велике значення має можливість застосування замість однієї несиметричної двохоперандної СЕТ-операції декількох, які мають однакові властивості. Саме тому задачі синтезу груп СЕТ-операцій з точністю до перестановки надзвичайно актуальні. Адже їх вирішення дозволить будувати генератори псевдовипадкових послідовностей СЕТ-операцій з однаковими властивостями, щоб забезпечити побудову криптографічних алгоритмів потокового шифрування нового покоління.

Аналіз останніх досліджень і публікацій. Мінімальною складністю, простотою і високою швидкістю реалізації володіють потокові шифри на основі додавання за модулем два [13]. Проте дані потокові шифри мають недостатню криптостійкість, пов'язану з обмеженою довжиною псевдовипадкової

послідовності і використанням в процесі шифрування лише однієї операції криптографічного перетворення. Використання більшої кількості операцій, на основі яких виконується криптографічне перетворення інформації, ускладнює задачу криптоаналізу [8]. Це пов'язано з необхідністю визначення як псевдовипадкової послідовності, так і операції або набору операцій, на основі яких було реалізовано шифрування. Операції криптографічного додавання за будь яким модулем можна розглядати як симетричні двохоперандні СЕТ-операції [1,2]. Результати досліджень [3, 8] показали ефективність використання в потокових шифрах груп операцій з точністю до перестановки. Для побудови симетричних потокових шифрів використовуються групи модифікованих операцій криптографічного додавання з точністю до перестановки [5, 6], а також групи симетричних двохоперандних СЕТ-операцій, побудованих на основі кортежів одноопераднних СЕТ-операцій [7, 17, 18]. Проте на сьогоднішній день особливості реалізації методу синтезу груп несиметричних СЕТ-операцій з точністю до перестановки другого операнда для побудови систем потокового шифрування не досліджувалися.

Метою роботи є дослідження можливості застосування методу генерації груп СЕТ-операцій з точністю до перестановки другого операнда для побудови малоресурсних несиметричних систем потокового шифрування.

Виклад основного матеріалу. ***Результати моделювання груп несиметричних двохоперандних СЕТ-операцій з точністю до перестановки другого операнда.*** В ході дослідження операцій строгого стійкого кодування було встановлено, що генерувати групи операцій строгого стійкого кодування доцільно на основі модифікації СЕТ-операції строгого стійкого кодування з точністю до перестановки другого операнда [4].

Генерація груп прямих СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда може бути реалізована на основі моделі [8]:

$$C^*(x,y)=C\left(x,C_i(y)\right), \tag{1}$$

де $C(x,y)$ – двохоперандна СЕТ-операція строгого стійкого кодування; x –значення першого операнда; y –значення другого операнда, $C^*(x,y)$ – група двохоперандних СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда; $C_i(y)$ – одноопераднна СЕТ-операція для модифікації другого операнда, $i\in\{1;2;...;h\}$; h – кількість одноопераднних СЕТ-операцій для перетворення другого операнда, $h\le 2^m!$; m – кількість Сі-квантів інформації в другому операнді.

Генерація груп обернених двохоперандних СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда може бути задана виразом [8]:

$$C^{*/}(x,y)=C^{/}\left(x,C_i(y)\right), \tag{2}$$

де $C^{/}(x,y)$ – обернена двохоперандна СЕТ-операція строгого стійкого кодування $C^{*/}(x,y)$, – група обернених двохоперандних СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда.

Перевіримо коректність моделей (1) і (2) для синтезу груп прямих і обернених несиметричних двохоперандних СЕТ-операцій на прикладі.

Нехай модель несиметричної двохоперандної 2Сі-квантової СЕТ-операції [13] задана кортежем із чотирьох одноопераднних 2Сі-квантових СЕТ-операцій.

Якщо $C_1(x)=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=z$; $C_2(x)=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=z$; $C_3(x)=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=z$; $C_4(x)=\begin{bmatrix}x_2\\ x_1\end{bmatrix}=z$, де $C_i(x)$ – i-та одноопераднна СЕТ-операція; x_1 і x_2 перший і других Сі-кванти першого операнда (вхідна інформація); z – результат криптографічного перетворення (2 Сі-кванти), тоді:

$$C(x,y)=C\left(C_1(x),C_2(x),C_3(x),C_4(x)\right)=z; \tag{3}$$

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ y_1=0; y_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ y_1=1; y_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, якщо\ y_1=1; y_2=1\end{cases}=z, \tag{4}$$

де $C(x,y)$ – двохоперандна СЕТ-операція; y_1 і y_2 перший і других Сі-кванти другого операнда (інформація керування); z – результат криптографічного перетворення (2 Сі-кванти).

На основі моделі (1) отримаємо:

$$C(x,y)=\begin{bmatrix} x_1\cdot\overline{y}_1\oplus x_2\cdot y_1\oplus\overline{y}_2 \\ x_1\cdot y_1\oplus x_2\cdot\overline{y}_1\oplus\overline{y}_1\cdot y_2 \end{bmatrix}=z. \quad (5)$$

Слід відмітити, що для побудови систем потокового шифрування необхідно генерувати як псевдовипадкові послідовності СЕТ-операцій як для прямого, так і для оберненого криптографічного перетворення. Взаємно відповідність даних послідовностей забезпечить як шифрування, так і розшифрування інформації.

Оскільки $C_1^{/}(z)=\begin{bmatrix} z_1\oplus 1 \\ z_2 \end{bmatrix}=x$; $C_2^{/}(z)=\begin{bmatrix} z_1 \\ z_2\oplus 1 \end{bmatrix}=x$; $C_3^{/}(z)=\begin{bmatrix} z_2 \\ z_1\oplus 1 \end{bmatrix}=x$; $C_4^{/}(z)=\begin{bmatrix} z_2 \\ z_1 \end{bmatrix}=x$, тоді:

$$C^{/}(z,y)=C\left(C_1^{/}(z),C_2^{/}(z),C_3^{/}(z),C_4^{/}(z)\right)=x; \quad (6)$$

$$C^{/}(z,y)=\begin{cases} \begin{bmatrix} z_1\oplus 1 \\ z_2 \end{bmatrix}, якщо\ y_1=0; y_2=0 \\ \begin{bmatrix} z_1 \\ z_2\oplus 1 \end{bmatrix}, якщо\ y_1=0; y_2=1 \\ \begin{bmatrix} z_2 \\ z_1\oplus 1 \end{bmatrix}, якщо\ y_1=1; y_2=0 \\ \begin{bmatrix} z_2 \\ z_1 \end{bmatrix}, якщо\ y_1=1; y_2=1 \end{cases}=x. \quad (7)$$

На основі моделі (7) отримаємо

$$C^{/}(z,y)=\begin{bmatrix} z_1\cdot\overline{y}_1\oplus z_2\cdot y_1\oplus y_1\cdot y_2 \\ z_1\cdot y_1\oplus z_2\cdot\overline{y}_1\oplus(y_1\oplus y_2) \end{bmatrix}=z. \quad (8)$$

Модифікуємо другий операнд моделі прямої СЕТ-операції (4) одноопераднною операцією $C_3(x)$. У результаті модифікації отримаємо:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ y_1=1; y_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ y_1=0; y_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ y_1=1; y_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, якщо\ y_1=0; y_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ y_1=0; y_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, якщо\ y_1=0; y_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ y_1=1; y_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ y_1=1; y_2=1 \end{cases}=z;$$

$$C(x,y)=\begin{bmatrix} x_1\cdot\overline{y}_1\oplus x_2\cdot y_1\oplus y_1 \\ x_1\cdot y_1\oplus x_2\cdot\overline{y}_1\oplus\overline{y}_1\cdot\overline{y}_2 \end{bmatrix}=z; \quad (9)$$

$$C(x,y)=C\left(C_2(x),C_4(x),C_1(x),C_3(x)\right)=z. \quad (10)$$

Модифікуємо другий операнд моделі оберненої СЕТ-операції (7) одноопераднною операцією $C_3(x)$. У результаті реалізованої модифікації отримаємо:

$$C^{/}(z,y)=\begin{cases}\begin{bmatrix}z_1\oplus 1\\ z_2\end{bmatrix}, якщо\ y_1=1; y_2=0\\ \begin{bmatrix}z_1\\ z_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=0\\ \begin{bmatrix}z_2\\ z_1\oplus 1\end{bmatrix}, якщо\ y_1=1; y_2=1\\ \begin{bmatrix}z_2\\ z_1\end{bmatrix}, якщо\ y_1=0; y_2=1\end{cases}=\begin{cases}\begin{bmatrix}z_1\\ z_2\oplus 1\end{bmatrix}, якщо\ y_1=0; y_2=0\\ \begin{bmatrix}z_2\\ z_1\end{bmatrix}, якщо\ y_1=0; y_2=1\\ \begin{bmatrix}z_1\oplus 1\\ z_2\end{bmatrix}, якщо\ y_1=1; y_2=0\\ \begin{bmatrix}z_2\\ z_1\oplus 1\end{bmatrix}, якщо\ y_1=1; y_2=1\end{cases}=x.$$

$$C^{/}(z,y)=\begin{bmatrix}z_1\cdot\overline{y}_2\oplus z_2\cdot y_2\oplus y_1\cdot\overline{y}_2\\ z_1\cdot y_1\oplus z_2\cdot\overline{y}_1\oplus(y_1\oplus y_2\oplus 1)\end{bmatrix}=x. \quad (11)$$

$$C^{/}(z,y)=C\left(C_2^{/}(z),C_4^{/}(z),C_1^{/}(z),C_3^{/}(z)\right)=x. \quad (12)$$

За результатом моделювання можна зробити висновок про можливість генерації груп прямих і обернених несиметричних СЕТ-операцій з точністю до перестановки другого операнда на основі будь якої двохоперандної СЕТ-операції. Коректність даного висновку підтверджена результатами обчислювального експерименту для 2Сі-квантових несиметричних двохоперандних СЕТ-операцій.

Обговорення результатів моделювання груп несиметричних СЕТ-операцій з точністю до перестановки другого операнда. Оскільки моделі прямих несиметричних двохоперандних 2Сі-квантових СЕТ-операції (5) і (8) відрізняються, то можна стверджувати, що модифікація несиметричної СЕТ-операції з точністю до перестановки другого операнду призводить до зміни результату криптографічного перетворення.

Кортежі прямих несиметричних двохоперандних 2Сі-квантових СЕТ-операцій (3) і (10) включають в себе переставлені місцями одні і ті ж самі одноопераднді СЕТ-операції. Тому можна стверджувати, що модифікація несиметричної двохоперандної СЕТ-операції не призводить до зміни таблиць підстановок, на основі яких реалізується криптографічне перетворення.

Однакові послідовності прямих і обернених до них одноопераднді СЕТ-операцій в кортежах прямої (10) та оберненої (12) двохоперандних СЕТ-операцій продемонстрували коректність застосування моделей генерації псевдовипадкових послідовностей операцій (1) і (2).

Оскільки в процесі модифікації двохоперандної СЕТ-операції набір одноопераднді операцій не змінюється, а змінюється лише їх послідовність, можна стверджувати, що всі отримані операції будуть мати однакові криптографічні властивості, тому що реалізують однакові таблиці підстановок.

Реалізація генераторів груп прямих обернених несиметричних двохоперандних СЕТ-операцій з точністю до перестановки другого операнда вимагає застосування прямої і оберненої несиметричної СЕТ-операції та набору лише прямих одноопераднді СЕТ-операцій. Відсутність у моделях синтезу генерацій (1) і (2) обернених одноопераднді СЕТ-операції забезпечує суттєве спрощення алгоритмів СЕТ-шифрування.

Подальші дослідження будуть направлені на пошук методів синтезу груп несиметричних двохоперандних СЕТ-операцій, які забезпечать в процесі модифікації операції зміну таблиць підстановки (одноопераднді СЕТ-операцій).

Висновки. Зважаючи на вище наведений опис проведеного дослідження та проаналізувавши одержані результати, можна сформулювати наступні висновки:

1. За результатами дослідження встановлено, що метод генерації двохоперандних СЕТ-операцій з точністю до перестановки другого операнда може бути використаний для генерації груп несиметричних двохоперандних СЕТ-операцій.

2. Усі несиметричні СЕТ-операції, які належать до синтезованої групи з точністю до перестановки другого операнда, мають однакові криптографічні властивості, оскільки однаково випадково реалізують одні і ті самі набори таблиць підстановок.

3. Встановлено, що на основі будь-якої несиметричної двохоперандної СЕТ-операції з відомими криптографічними властивостями шляхом застосування даного методу може бути побудована група двохоперандних СЕТ-операцій з точністю до перестановки другого операнду. Всі модифіковані операції даної групи будуть мати однакові криптографічні властивості.

4. Для забезпечення генерації прямих і обернених несиметричних двохоперандних СЕТ-операцій використовуються лише прямі одноопернадні СЕТ-операції. Це суттєво зменшує складність криптогафічного алгоритму і складність реалізації криптографічної системи.

Список використаних джерел:

1. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації.* 2014. Вип. 2 (118). С. 116–118.
2. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. *Smart and Young: щомісячний наук. журн.* 2016. № 11–12. Ч. 1. С. 49–54.
3. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. *The scientific potential of the present: proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016)* / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. С. 108–111.
4. Лада Н. В., Бреус Р. В., Лада С. В. Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Science and Education a New Dimension Natural and Technical science.* 2020. V. 224. P. 31–37.
5. Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири. *Центральноукраїнський науковий вісник. Технічні науки.* 2019. Вип. 2 (33). С. 181–189. https://doi.org/10.32515/2664-262X.2019.2(33).181-189.
6. Лада Н. В., Рудницький С. В., Зажома В. М., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири. *Системи управління, навігації та зв'язку.* 2020. № 1 (59). С. 93–96. https://doi.org/10.26906/SUNZ.2020.1.093.
7. Рудницька Ю. В. Рудницький С. В. Моделювання симетричних операцій криптографічного кодування. *Проблеми інформатизації: Десята міжнар. наук.-техн. конф.:* тези доп., (24 – 25 листоп. 2022 р. Черкаси), 2022. Т. 2. С. 10.
8. Рудницький В. М., Лада Н. В., Кучук Г. А., Підласий Д. А. Архітектура СЕТ-операцій і технології потокового шифрування. Architecture of CET-operations and stream encryption technologies: монографія. Черкаси: видавець Пономаренко Р.В., 2024. 374 с. ISBN 978-966-2554-81-6 URL: https://dndivsovt.com/index.php/monograph/issue/view/22/22
9. Borky J. M., Bradley T. H. Protecting Information with Cybersecurity. *In: Effective Model-Based Systems Engineering.* Springer, Cham. 2019, pp. 345–404. https://doi.org/10.1007/978-3-319-95669-5_10
10. Dandin T.J.E., Krishnaveni D., Chandrasekhar K. Light Weight Cryptography and Its Application in Resource Constrained Environment Using Reversible Logic. In: Gunjan, V.K., Zurada, J.M. (eds) *Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Lecture Notes in Networks and Systems.* Springer, Singapore, 2022. Vol. 237, pp. 473–489. https://doi.org/10.1007/978-981-16-6407-6_43
11. Eldem T. Global Cyberspace Security and Critical Information Infrastructure Protection. In: Farazmand, A. (eds) *Global Encyclopedia of Public Administration, Public Policy, and Governance.* Springer, Cham. 2021, pp. 1–11. https://doi.org/10.1007/978-3-319-31816-5_3987-1
12. Keshattiwar P., Lokulwar P., Saraf P. Empowering Data Defender's Comprehensive Security Measures for Robust Information Protection in Robust-Cloud Environments. *2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET),* Nagpur, India, 2024, pp. 1–6. https://doi.org/10.1109/ICICET59348.2024.10616293
13. Massey J. L. An introduction to contemporary cryptology. *In Proceedings of the IEEE,* 1988. Vol. 76, no. 5, pp. 533–549. URL: https://scispace.com/pdf/an-introduction-to-contemporary-cryptology-60eevadgo7.pdf
14. Nadji B. Data Security, Integrity, and Protection. In: McClellan, S. (eds) *Data, Security, and Trust in Smart Cities. Signals and Communication Technology.* Springer, Cham. 2024, pp. 59–83. https://doi.org/10.1007/978-3-031-61117-9_4
15. Pandey S., Bhushan B. Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. *Wireless Netw,* 2024. Vol. 30, pp. 2987–3026. https://doi.org/10.1007/s11276-024-03714-4
16. Preyaa Atri. Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit. *International Journal of Computing and Engineering*. 2024. 5(4), pp. 44–55. https://doi.org/10.47941/ijce.1920
17. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. Constructing symmetric operations of cryptographic information encoding. *CEUR Workshop Proceedings,* 2022. Vol. 3187, pp. 182–194. URL: https://ceur-ws.org/Vol-3187/paper17.pdf
18. Rudnytskyi V., Lada N., Pochebut M., Melnyk O., Tarasenko Ya. Increasing the cryptographic strength of CET encryption by ensuring the transformation quality of the information block. *13th International Conference on Dependable Systems, Services and Technologies (DESSERT),* October 13-15, 2023, Athens, Greece, 2023, pp. 1–6. https://doi.org/10.1109/DESSERT61349.2023.10416546.
19. Yasmin N., Gupta R. Modified lightweight cryptography scheme and its applications in IoT environment. *Int. j. inf. tecnol.* 2023, 15, pp. 4403–4414. https://doi.org/10.1007/s41870-023-01486-2
20. Zakaria A., Azni A., Ridzuan F., Zakaria N., Maslina H. Daud Systematic literature review: Trend analysis on the design of lightweight block cipher. *IEEE Journal of King Saud University – Computer and Information Sciences,* 2023. Vol. 35, Is. 5, 101550. https://doi.org/10.1016/j.jksuci.2023.04.003