МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

БРЕУС Роксолана Василівна

УДК 004.421.5:004.056.55

ГЕНЕРАЦІЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ ДРУГОГО ОПЕРАНДА

05.13.05 – комп’ютерні системи і компоненти

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Черкаси – 2021

Дисертацією є рукопис.

Роботу виконано в Черкаському державному технологічному університеті Міністерства освіти і науки України.

Науковий керівник:	доктор технічних наук, професор **Рудницький Володимир Миколайович,** Черкаський державний технологічний університет, завідувач кафедри інформаційної безпеки та комп'ютерної інженерії.
Офіційні опоненти:	доктор технічних наук, професор **Можаєв Олександр Олександрович,** Харківський національний університет внутрішніх справ Міністерства внутрішніх справ України, професор кафедри інформаційних технологій та кібербезпеки.
	доктор технічних наук, професор **Грищук Руслан Валентинович**, Житомирський військовий інститут імені С. П. Корольова, начальник кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства;

Захист відбудеться «09» *лютого* 2021 р. о 12^{00} на засіданні спеціалізованої вченої ради Д 73.052.04 при Черкаському державному технологічному університеті за адресою: 18006, Черкаси, бульвар Шевченка, 460.

З дисертацією можна ознайомитися в бібліотеці Черкаського державного технологічного університету за адресою: 18006, Черкаси, бульвар Шевченка, 460.

Автореферат розіслано «04» *січня* 2021 р.

Учений секретар
спеціалізованої вченої ради Ю. Ю. Бондаренко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Науково-технічний прогрес відіграє важливу роль у сучасному суспільстві. Сучасна людина отримує в десятки разів більше інформації, ніж десятиліття тому. Це пояснюється тим, що інформація стає все доступнішою для будь-кого. У зв'язку з цим інформаційні ресурси стають уразливими, що, в свою чергу, призводить до збільшення комп'ютерних злочинів. Тому на даний час гостро постає питання захисту інформації.

Криптографічний захист інформації є одним із найефективніших на сьогодні. Тому виникає необхідність вдосконалення існуючих та створення нових методів та засобів криптографічного захисту інформації, у зв'язку зі зростанням кіберзлочинів. Для досягнення такого результату необхідне покращення вже розроблених або створення нових алгоритмів криптоперетворення. Отже, дослідження та побудова нових операцій криптоперетворення на сьогоднішній день є особливо актуальними.

У розвиток комп'ютерної криптографії значний внесок зробили такі вітчизняні та зарубіжні науковці, як І. Д. Горбенко, А. М. Олексійчук, Л. В. Ковальчук, К. Є. Шеннон, Брюс Шнайєр, Чарльз Г. Беннет, W. Diffie, Жиль Брассар, M. E. Hellman,U. M. Maurer, A. Shamir, N. Koblitz та ін.

Досить велика увага останнім часом приділяється криптографічному кодуванню, що являє собою один із напрямів комп'ютерної криптографії. Ще один напрям криптографії, який заслуговує на увагу – це побудова операцій із заданими властивостями. Досить цікавими дослідженнями можна назвати й ті, які направлені на побудову операцій криптоперетворення, що забезпечують максимальну невизначеність результатів шифрування. Проте залишилися ще не дослідженими процеси синтезу груп двохрозрядних двохоперандних операцій (ДДО) строгого стійкого криптографічного кодування (ССКК) як такі, що можуть становити інтерес для підвищення швидкості потокового шифрування в рамках розроблення методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії.

Таким чином, можна стверджувати, що тема дисертаційного дослідження «Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда» є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 30.01.19 №30 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2019–2023 рр.», а саме – пп. 1.2.8.1 Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії. Результати дисертаційної роботи включені в НДР

Черкаського державного технологічного університету: «Синтез операцій криптографічного перетворення з заданими характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), у яких автор брала участь як виконавець.

Мета і задачі дослідження. Основною метою дослідження є підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

– розроблення методу синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда;

– розроблення методу синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі перетворення другого операнда відомої операції;

– розроблення методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда та його реалізація.

Об’єкт дослідження – процеси захисту інформації в кіберпросторі.

Предмет дослідження – метод генерації псевдовипадкових послідовностей прямих та обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда та його реалізація.

Методи дослідження. У процесі розробки методу синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда використовувався математичний апарат криптографії, теорії інформації, теорії алгоритмів, дискретної математики. Для розробки методу синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі перетворення другого операнда відомої операції – методи дискретної математики, теорія алгоритмів, криптографія, логіки. Для розробки методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда та можливості його реалізації використано методи теорії ймовірності, алгоритмів, інформації, криптографії із застосуванням методів дискретної математики.

Наукова новизна одержаних результатів. У процесі вирішення поставлених задач автором одержано такі результати:

1) вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на

основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;

2) вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднної операції, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій;

3) вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення та робить можливим використання його при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні розроблених методів до дискретних моделей операцій та алгоритмів автоматичної генерації псевдовипадкових послідовностей операцій строгого стійкого кодування для систем потокового комп'ютерного шифрування.

Розширено варіативність криптографічних перетворень за рахунок збільшення кількості операцій з 12 до 24. Розроблений генератор псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування забезпечує синтез операцій на 15–20 % швидше порівняно з табличним методом синтезу при забезпеченні періоду послідовності $(24!)^2$. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування при максимальній невизначеності результатів перетворення.

Реалізація. Дисертаційна робота виконувалася відповідно до планів НДР Черкаського державного технологічного університету. Одержані в ній теоретичні й практичні результати використані та впроваджені у таких закладах, установах, організаціях:

– Черкаський державний технологічний університет на кафедрі інформаційної безпеки та комп'ютерної інженерії – у матеріалах лекційних курсів «Комплексні системи захисту інформації», «Програмний захист інформації в інформаційно-комунікаційних системах». Акт впровадження від 10.06.2019;

– ТОВ «Нова пошта» – для підвищення захисту особистих даних працйників та клієнтів пошти, а також захисту оплати послуг шляхом використання методу синтезу обернених ДДО ССКК на основі перетворення

другого операнда у вигляді реалізації моделі автомата побудови другого операнда оберненої операції. Акт впровадження від 15.12.2019;

– КНП «Черкаська міська консультативно-діагностична поліклініка» (філія №2) – для підвищення захисту персональних даних персоналу та пацієнтів за допомогою застосування методу синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції. Акт впровадження від 10.06.2020;

– ПАТ «Черкасиобленерго» – для підвищення захисту персональних даних, шляхом застосування методу генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда, у працівників підприємства та клієнтів. Акт впровадження від 20.12.2019.

Особистий внесок здобувача. Всі нові результати дисертаційної роботи отримано автором самостійно. Результати, опубліковані в [1, 7, 8], отримані одноосібно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, автору належать: синтез операцій строгого стійкого кодування на основі перетворення другого операнда заданої операції [2, 10], встановлення взаємозв'язків між прямими і оберненими двохрозрядними двохоперандними операціями строгого стійкого криптографічного кодування [3], синтез строгого стійкого криптографічного криптоперетворення [4, 6, 9], генерація операцій строгого стійкого кодування для прямого і оберненого криптографічного перетворення інформації [5].

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Четвертій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2016), Пятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2017), Сьомій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2019), The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, 17–18 September, 2020, Dortmund, Germany.

Публікації. Основні положення дисертації опубліковано у 10 друкованих працях, у тому числі: в 4 статтях у фахових виданнях України, 1 статті в закордонному виданні; колективній монографії, в матеріалах трьох міжнародних науково-технічних конференцій та в збірнику матеріалів міжнародного симпозіуму, проіндексованому в Scopus.

Структура і обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 190 сторінок. Основний зміст викладений на 154 сторінках, у тому числі – 12 таблиць, 12 рисунків. Список використаних джерел містить 127 найменувань. Робота містить 5 додатків.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтована актуальність теми, наведено зв'язок роботи з науковими програмами і планами, наводиться мета дослідження, задачі для її реалізації, а також методи дослідження які використовувалися, наведені наукова новизна і практичне значення дисертаційної роботи.

В **першому розділі** проводиться огляд і аналіз основних проблем комп'ютерної криптографії для захисту інформаційних ресурсів кіберпросторі України, з урахуванням специфіки нормативно-правової бази нашої держави. Розглянуто концепцію державної політики у сфері інформатизації та розвитку інформаційного суспільства, її значення та фактори впливу на забезпечення захисту інформаційного простору. Проведено аналітичний огляд найбільш поширених методів криптографічного захисту інформації та можливості їх використання для захисту інформації в глобальному кібернетичному просторі. Встановлено, що одним з перспективних шляхів розвитку комп'ютерної криптографії, є впровадження в перспективних комп'ютерних криптоалгоритмах операцій криптографічного кодування інформації. Приводиться огляд публікацій по синтезу операцій криптографічного кодування інформації. Визначені напрямки вдосконалення криптографічного кодування, сформульовані мета і на її основі – задачі дисертаційного дослідження.

Другий розділ присвячений синтезу обернених ДДО ССКК на основі перетворення другого операнда. Для забезпечення єдиного підходу для дослідження прямих та обернених операцій криптографічного перетворення інформації запропонована технологія дослідження взаємозв'язків між ними.

Для прикладу виберемо дві ДДО ССКК, наприклад $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$, такі, що O_2^k є оберненою до O_1^k. Для знаходження взаємозв'язку покажемо пряму та обернену операції криптоперетворення у розгорнутому представленні.

$$O_1^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \qquad O_2^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases}$$

Операції O_1^k та O_2^k відрізняються одна від одної порядком розміщення одноопераднної операції обробки першого операнда. Порядок розміщення одноопераднної операції обробки першого операнда визначається значенням другого операнда, тобто умовою виконання. Виходячи з цього, для побудови оберненої операції достатньо в прямій операції змінити умови її виконання. Мінімізувавши таблицю істинності перетворення O_1^k в O_2^k, отримуємо дискретну модель автомата побудови другого операнда оберненої операції: $k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$. Досліджено і встановлено взаємозв'язки між прямими і оберненими операціями в групі двохрозрядних двохоперандних операцій ССКК. На основі застосування запропонованої технології проведено синтез обернених двохрозрядних двохоперандних операцій ССКК на основі встановлених взаємозв'язків. Узагальнено результати дослідження взаємозв'язків між прямими та оберненими ДДО криптографічного кодування, а також результати синтезу операцій на основі встановлених взаємозв'язків (табл.1).

Сформульовано метод синтезу ДДО ССКК на основі перетворення другого операнда, який полягає в наступному:

1. Побудувати групу математичних моделей двохрозрядних двохоперандних операцій ССКК.

2. Встановити відповідність в групі математичних моделей двохрозрядних двохоперандних операцій ССКК між прямими і оберненими операціями криптоперетворення.

3. На основі аналізу математичних моделей операцій прямого і оберненого криптоперетворення побудувати модель автомата побудови другого операнда оберненої операції.

4. На основі застосування моделі автомата побудови другого операнду оберненої операції перетворити другий операнд заданої прямої операції криптоперетворення, що забезпечить синтез обернених двохрозрядних двохоперандних операцій ССКК.

Застосування синтезу ДДО ССКК на основі перетворення другого операнда в методі підвищення стійкості і надійності потокового шифрування забезпечить створення нових можливостей для розробників потокових шифрів.

Одержані в розділі результати опубліковано в [3, 4, 6, 8, 10].

Третій розділ присвячено розробці методу синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції. Наведені взаємозв'язки між прямими і оберненими операціями дозволяють синтезувати обернені операції, а кожна обернена операція, в свою чергу, є прямою операцією для іншої оберненої операції, то можна допустити, що шляхом перетворення другого операнда одноопераднною операцією можливо синтезувати іншу операцію.

Таблиця 1

Узагальнені результати синтезу операцій на основі встановлених взаємозв'язків

Пряма операція криптоперетворення	**Обернена операція криптоперетворення**	**Модель автомата побудови другого операнда оберненої операції**
$O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$k_1^* = k_2$, $k_2^* = k_1$
$O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	
$O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$k_1^* = \bar{k}_2$, $k_2^* = \bar{k}_1$
$O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	
$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	$k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$
$O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	
$O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	$k_1^* = k_1$, $k_2^* = \overline{k_1 \oplus k_2}$
$O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	
$O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	$k_1^* = \overline{k_1 \oplus k_2}$, $k_2^* = k_2$
$O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	
$O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$k_1^* = k_1 \oplus k_2$, $k_2^* = k_2$
$O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	

Розглянемо приклад. Якщо над другим операндом двохоперандної операції ССКК $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, то буде отримана операція $O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Таким чином отримуємо:

$$F(O_1^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases} = O_6^k = \begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} = O_6^k = \begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$$

Що й необхідно було довести.

Наведений приклад ілюструє запропоновану технологію синтезу групи ДДО ССКК, яка забезпечує побудову повної групи з 24 операцій на основі однієї відомої операції при використанні групи з 24 двохрозрядних одноопераднних операцій. Із застосуванням запропонованої технології проведено синтез декількох груп ДДО ССКК на основі перетворення другого операнда відомої операції.

Запропонований та перевірений підхід щодо синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції дав змогу розробити метод синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції, сутність якого полягає в наступному:

1. Визначити математичну модель двохрозрядної двохоперандної операції ССКК, на основі якої буде будуватися група операцій.

2. Провести синтез групи математичних моделей двохрозрядних одноопераднних операцій ССКК на основі застосування одного з відомих методів їх синтезу.

3. Вибрати першу математичну модель двохрозрядних одноопераднних операцій строгого стійкого криптографічного кодування.

4. Модифікувати визначену математичну модель двохрозрядної двохоперандної операції ССКК шляхом перетворення другого операнда даної операції на основі виконання над нею вибраної одноопераднної операції ССКК.

5. Якщо вибрана математична модель двохрозрядних одноопераднних операцій ССКК не остання в синтезованій групі, тоді вибрати наступну модель і повернутися до пункту 4.

6. Перевірити завершення побудови групи двохрозрядних двохоперандних операцій ССКК на основі кількісного співпадіння отриманих двохоперандних і одноопераднних операцій.

Для наведених результатів дослідження досягнуто збільшення варіативності алгоритмів в 24 рази, так як цей метод гарантовано дозволяє синтезувати з будь-якої операції 24 операції, які складають повну групу операцій в полі G_4 .

Одержані в розділі результати опубліковано в [1, 7, 9].

Четвертий розділ присвячено розробці методу генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда, для цього узагальнено результати синтезу груп ДДО ССКК на основі першої операції. Дані операції розміщено однотипно, відповідно до одноопераднних операцій, якими перетворювався другий операнд. Результати синтезу групи ДДО, в залежності від операції, на основі якої вони будуються, наведено в табл. 2 – 3.

Зведені результати синтезу 24 варіантів синтезу групи ДДО ССКК наведені в табл. 4.

В результаті даного дослідження було отримано генерацію груп з ДДО ССКК на основі використання одноопераднних операцій криптографічного кодування.

Сутність методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда можна представити наступним алгоритмом:

1. Визначення заданої двохрозрядної двохоперандної операції ССКК на основі перетворення другого операнда.
2. Випадкова генерація групи одноопераднних двохрозрядних операції ССКК.
3. Модифікація заданої двохрозрядної двохоперандної операції шляхом перетворення другого операнда відомої операції за допомогою одноопераднної операції.
4. Перевірка отриманого результату модифікованої операції.
5. Модифікація отриманої операції шляхом виконання повторної операції перетворення другого операнда відомої операції за допомогою одноопераднної операції.
6. Перевірка отриманого результату правильного виконання операції перетворення над другим операндом вибраної операції.
7. Пункти 3–6 повторюються до завершення використання повної групи модифікованих двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення.
8. Пункти 2–7 повторюються до повного завершення криптоперетворення інформації.

В процесі подальших досліджень отримані на основі перетворення другого операнда взаємозв’язки між прямими і оберненими операціями дозволили генерувати обернені операції при випадковій генерації прямих операцій криптоперетворення. Взаємозв’язки між прямими і оберненими операціями при їх випадковій генерації наведені на рис. 1.

Таблиця 2

Зведені результати синтезу ДДО ССК на основі O_1^k та O_2^k

Зведені результати синтезу ДДО ССК на основі O_1^k				Зведені результати синтезу ДДО ССК на основі O_2^k			
1	$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	13	$O_{18}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	1	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	13	$O_{21}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
2	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	14	$O_{13}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	2	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	14	$O_{20}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
3	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	15	$O_{17}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	3	$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	15	$O_{22}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
4	$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	16	$O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	4	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	16	$O_{24}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
5	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	17	$O_{14}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	5	$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	17	$O_{19}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
6	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	18	$O_{16}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	6	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	18	$O_{23}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
7	$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	19	$O_{22}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	7	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	19	$O_{17}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
8	$O_9^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	20	$O_{23}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	8	$O_{12}^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	20	$O_{16}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
9	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	21	$O_{21}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	9	$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	21	$O_{18}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
10	$O_{11}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	22	$O_{19}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	10	$O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	22	$O_{14}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
11	$O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	23	$O_{24}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	11	$O_{11}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	23	$O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
12	$O_{12}^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	24	$O_{20}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	12	$O_9^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	24	$O_{13}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$

Таблиця 3

Зведені результати синтезу ДДО ССК на основі O_3^k та O_4^k

Зведені результати синтезу ДДО ССК на основі O_3^k				Зведені результати синтезу ДДО ССК на основі O_4^k			
1	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	13	$O_{20}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}$	1	$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	13	$O_{11}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
2	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	14	$O_{21}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	2	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	14	$O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
3	$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	15	$O_{19}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	3	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	15	$O_{12}^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
4	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	16	$O_{23}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	4	$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	16	$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
5	$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	17	$O_{22}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	5	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	17	$O_9^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
6	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	18	$O_{24}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	6	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	18	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
7	$O_{16}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	19	$O_{12}^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	7	$O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	19	$O_{19}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
8	$O_{17}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	20	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	8	$O_{14}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	20	$O_{24}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
9	$O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	21	$O_{11}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	9	$O_{16}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	21	$O_{20}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
10	$O_{13}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	22	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	10	$O_{18}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	22	$O_{22}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
11	$O_{18}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	23	$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	11	$O_{13}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	23	$O_{23}^k=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
12	$O_{14}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	24	$O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	12	$O_{17}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	24	$O_{21}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$

Таблиця 4

Генерація повної групи послідовностей операцій криптоперетворення

O	Операції перетворення														
	1	2	3	4	5	6	7	8	9	…	20	21	22	23	24
O_1^k	O_1^k	O_6^k	O_2^k	O_4^k	O_5^k	O_3^k	O_8^k	O_9^k	O_7^k	…	O_{23}^k	O_{21}^k	O_{19}^k	O_{24}^k	O_{20}^k
O_2^k	O_2^k	O_3^k	O_1^k	O_5^k	O_4^k	O_6^k	O_7^k	O_{12}^k	O_8^k	…	O_{16}^k	O_{18}^k	O_{14}^k	O_{15}^k	O_{13}^k
O_3^k	O_3^k	O_2^k	O_4^k	O_6^k	O_1^k	O_5^k	O_{16}^k	O_{17}^k	O_{15}^k	…	O_7^k	O_{11}^k	O_9^k	O_8^k	O_{10}^k
O_4^k	O_4^k	O_5^k	O_3^k	O_1^k	O_6^k	O_2^k	O_{15}^k	O_{14}^k	O_{16}^k	…	O_{24}^k	O_{20}^k	O_{22}^k	O_{23}^k	O_{21}^k
O_5^k	O_5^k	O_4^k	O_6^k	O_2^k	O_3^k	O_1^k	O_{24}^k	O_{19}^k	O_{23}^k	…	O_{15}^k	O_{13}^k	O_{17}^k	O_{16}^k	O_{18}^k
O_6^k	O_6^k	O_1^k	O_5^k	O_3^k	O_2^k	O_4^k	O_{23}^k	O_{22}^k	O_{24}^k	…	O_8^k	O_{10}^k	O_{12}^k	O_7^k	O_{11}^k
O_7^k	O_7^k	O_{12}^k	O_8^k	O_{10}^k	O_{11}^k	O_9^k	O_2^k	O_3^k	O_1^k	…	O_{20}^k	O_{22}^k	O_{24}^k	O_{19}^k	O_{23}^k
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
O_{19}^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{11}^k	O_{10}^k	O_{12}^k	…	O_5^k	O_3^k	O_1^k	O_6^k	O_2^k
O_{20}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{12}^k	O_7^k	O_{11}^k	…	O_{17}^k	O_{15}^k	O_{13}^k	O_{18}^k	O_{14}^k
O_{21}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{17}^k	O_{16}^k	O_{18}^k	…	O_{12}^k	O_8^k	O_{10}^k	O_{11}^k	O_9^k
O_{22}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{18}^k	O_{13}^k	O_{17}^k	…	O_6^k	O_2^k	O_4^k	O_5^k	O_3^k
O_{23}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_6^k	O_1^k	O_5^k	…	O_{18}^k	O_{14}^k	O_{16}^k	O_{17}^k	O_{15}^k
O_{24}^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_5^k	O_4^k	O_6^k	…	O_{11}^k	O_9^k	O_7^k	O_{12}^k	O_8^k

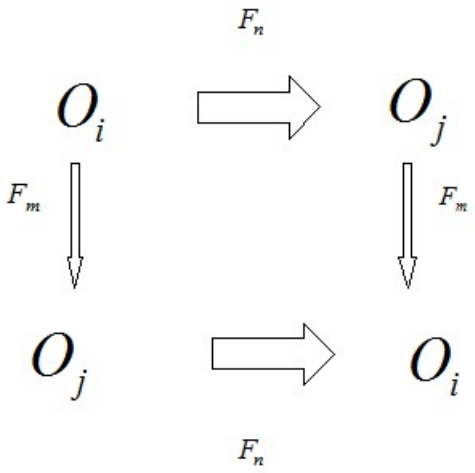

Рис. 1. Взаємозв’язки між прямими і оберненими операціями при псевдовипадковій генерації операцій

Запропоновану структурну схему удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення наведено на рис. 2.

Рис. 2. Структурна схема удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення

Запропонована структурна схема удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення реалізує автоматичну генерацію операцій ССКК. Ця структурна схема забезпечує реалізацію потокового шифрування, створюючи при цьому наступні переваги перед відомими технічними рішеннями, а саме:

- розширено варіативність криптографічних перетворень за рахунок збільшення кількості операцій, які застосовуються, з 12 до 24 операцій. Підвищення криптостійкості перетворення інформації досягнуто за рахунок збільшення варіативності шляхом розширення множини операцій;
- створено можливість застосувати в методі підвищення стійкості та надійності потокового шифрування операцій ССКК, які забезпечують максимальну невизначеність результатів перетворення;
- псевдовипадкові послідовності двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування генеруються на 15–20 % швидше порівняно з табличним методом синтезу операцій;

- забезпечено можливість автоматичної генерації псевдовипадкової послідовності операцій криптоперетворення, період якої визначається наступним чином: якщо T_g – період згенерованої псевдовипадкової послідовності операцій, O_n – кількість двохоперандних операцій криптоперетворення, F_m – кількість одноопераднних операцій крипто перетворення, тоді $T_g = O_n! \cdot F_m!$. При використанні двохрозрядних двохоперандних операцій криптоперетворення період згенерованої послідовності буде рівним $T_g = 24! \cdot 24!$.

Наведені переваги удосконаленого методу підвищення стійкості та надійності потокового шифрування забезпечують доцільність його застосування для захисту потоків конфіденційної інформації в кіберпросторі.

Одержані в розділі результати опубліковано в [2, 5].

У **додатках** наведено акти впровадження результатів дисертаційного дослідження та обов'язковий додаток.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда:

1) вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі множини двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, встановлених взаємозв'язків між прямими та оберненими операціями, шляхом перетворення другого операнда за рахунок реалізації побудованої моделі автомата синтезу другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;

2) вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі використання відомої двохрозрядної двохоперандної операції строгого стійкого криптографічного кодування та перетвореннями другого операнда шляхом послідовного виконання над даною операцією групи двохрозрядних одноопераднних операцій, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій.

3) вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного

кодування на основі використання груп двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування і двохрозрядних одноопераднних операцій строгого стійкого криптографічного кодування, шляхом перетворень других операндів прямих та обернених двохоперандних операцій, що дозволило досягти підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей прямих та обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування;

4) практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних алгоритмів генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Розширено варіативність криптографічних перетворень за рахунок збільшення кількості операцій з 12 до 24. Розроблений генератор псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування забезпечує синтез операцій на 15–20 % швидше порівняно з табличним методом синтезу при забезпеченні періоду послідовності $(24!)^2$. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування при максимальній невизначеності результатів перетворення.

Результати дисертації використані та впроваджені у таких організаціях, установах, на підприємствах: Черкаський державний технологічний університет, КНП «Черкаська міська консультативно-діагностична поліклініка» (філія №2), ТОВ «Нова Пошта», ПАТ «Черкасиобленерго».

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Бреус Р. В. Синтез двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2019. Вип. 5 (57). С 29–32.

2. Рудницький В. М., Бреус Р. В., Лада Н. В. Генерація послідовностей операцій криптографічного перетворення. *Вісник Інженерної академії України.* Київ, 2019. Вип. 3. С.75–80.

3. Rudnitsky V., Berdibayev R., Breus R., Lada N., Pustovit M. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. *Advanced Information Systems:* Quarterly scientific and technical

journal. Kharkiv: National Technical University «Kharkiv Polytechnic Institute», 2019. Vol. 3, No. 4, pp. 109–114.

4. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy. *Technology audit and production reserves.* № 2/2(52), 2020, pp. 28–31.

5. 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.* Budapest, 2020. V. 238, p. 27–30.

6. Криптографічне кодування: обробка та захист інформації: кол. монографія / під ред. В. М. Рудницького. Харків: ТОВ «ДІСА ПЛЮС», 2018. 139 с.

7. Бреус Р. В. Уніфікація опису операцій криптографічного перетворення. *Проблеми інформатизації: матеріали Четвертої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9.

8. Бреус Р.В. Математичні моделі побудови операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації: матеріали П'ятої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 13-15 листоп. 2017 р.). Черкаси: ЧДТУ, 2017. С. 13.

9. Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двоопераднних симетричних криптовалютних операцій. *Проблеми інформатизації: матеріали Сьомої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листопада 2019 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2019., Т.1, С. 85.

10. Jancarczyk D., Rudnytskyi V., Breus R., Pustovit M., Veselska O. and Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding With Different Operands' Bits. *The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 2020, Dortmund, Germany.

АНОТАЦІЯ

Бреус Р. В. Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Черкаський державний технологічний університет, Черкаси, 2021.

Дисертаційна робота присвячена підвищенню швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Для досягнення даного результату в другому розділі було розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції. В третьому розділі розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднодної операції. В четвертому розділі розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес синтезу групи операцій та робить можливим використання даних операцій у вдосконаленому методі підвищення стійкості і надійності потокового шифрування. Результати впроваджені в Черкаському державному технологічному університеті, Черкаській міській консультативно-діагностичній поліклініці (філія №2), ТОВ «Нова Пошта», ПАТ «Черкасиобленерго».

Ключові слова: комп'ютерна криптографія, операції криптографічного перетворення, потокові шифри, синтез операцій.

АННОТАЦИЯ

Бреус Р. В. Генерация псевдослучайных последовательностей операций строгого устойчивого криптографической кодирования на основе преобразования второго операнда. – Квалификационная научная работа на правах рукописи.

Диссертация на соискание научной степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Черкасский государственный технологический университет, Черкассы, 2021.

Диссертационная работа посвящена повышению скорости потокового шифрования за счет генерации псевдослучайных последовательностей группы двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования на основе преобразования второго операнда.

В первой главе выполнен обзор и анализ основных проблем компьютерной криптографии для защиты информационных ресурсов в киберпространстве. Проанализированы наиболее распространенные методы криптографической защиты информации и возможности их использования для

защиты информации в глобальном кибернетическом пространстве. Приводится обзор публикаций по синтезу операций криптографического кодирования информации. Определены направления совершенствования криптографического кодирования, сформулированы цель и задачи диссертационного исследования.

Во втором разделе впервые разработан метод синтеза обратных двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования на основе множества двухразрядных однооперандных операций строгого устойчивого криптографического кодирования, установленных взаимосвязей между прямыми и обратными операциями путем преобразования второго операнда за счет реализации построенной модели автомата синтеза второго операнда обратной операции, что обеспечило возможность практического применения данных операций.

В третьем разделе впервые разработан метод синтеза группы двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования на основе использования известной двухразрядной двухоперандной операции строгого устойчивого криптографического кодирования и преобразованиями второго операнда путем последовательного выполнения над данной операцией группы двухразрядных однооперандных операций, что обеспечило возможность увеличения вариативности криптопримитивов при практическом применении данных операций.

В четвертом разделе впервые разработан метод генерации псевдослучайных последовательностей двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования на основе использования групп двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования и двухразрядных однооперандных операций строгого устойчивого криптографического кодирования путем преобразований вторых операндов прямых и обратных двухоперандных операций, что позволило добиться повышения скорости потокового шифрования за счет генерации псевдослучайных последовательностей прямых и обратных двухразрядных двухоперандных операций строгого устойчивого криптографического кодирования. Предложенная структурная схема реализации усовершенствованного метода повышения устойчивости и надежности потокового шифрования путем генерации псевдослучайных последовательностей прямых и обратных операций криптопреобразования реализует автоматическую генерацию операций ССКК. Полученный результат обеспечил скорость реализации метода повышения устойчивости и надежности потокового шифрования.

Практическая ценность работы состоит в доведении соискателем полученных научных результатов до конкретных алгоритмов генерации псевдослучайных последовательностей двухразрядных двухоперандных операций строгого устойчивого криптографической кодирования на основе преобразования второго операнда. Расширена вариативность криптографических преобразований за счет увеличения количества операций с 12 до 24. Разработанный генератор псевдослучайных последовательностей двухразрядных двухоперандных операций строгого устойчивого криптографической кодирования обеспечивает синтез операций на 15–20 % быстрее по сравнению с табличным методом синтеза при обеспечении периода последовательности $(24!)^2$. Полученный результат обеспечил скорость реализации метода повышения устойчивости и надежности потокового шифрования при максимальной неопределенности результатов преобразования.

Результаты внедрены в Черкасском государственном технологическом университете, Черкасской городской консультативно-диагностической поликлинике (филиал №2), ТОО «Новая Почта», ПАО «Черкассыоблэнерго».

Ключевые слова: компьютерная криптография, операции криптографического преобразования, потоковые шифры, синтез операций.

Breus R. V. Generation of pseudo-random sequences of operations of strict stable cryptographic coding based on the transformation of the second operand. – Qualification scientific work as a manuscript.

Thesis for the degree of Candidate of Technical Sciences in the specialty 05.13.05 – Computer Systems and Components. – Cherkasy State Technological University, Cherkasy, 2021.

The dissertation is devoted to increasing the speed of streaming encryption by generating pseudo-random sequences of a group of two-bit two-operand operations of strict stable cryptographic coding based on the transformation of the second operand.

To achieve this result, a method for the synthesis of inverse two-bit two-operand operations of strict stable cryptographic coding based on the transformation of the second operand by implementing a model of automatic device for constructing the second operand of the inverse operation is developed in the second chapter. In the third chapter, a method for the synthesis of a group of two-bit two-operand operations of strict stable cryptographic coding based on the transformation of the second operand of a known operation by performing a two-bit single-operand operation on it is developed. The fourth chapter develops a method of generating pseudo-random sequences of two-bit two-operand operations of strict stable cryptographic coding based on the transformation of the second operand, which greatly simplifies the process of synthesis of a group of operations and makes possible to use these

operations in an improved method for the increase of the stability and reliability of streaming encryption. The results have been implemented at Cherkasy State Technological University, Cherkasy City Consultative and Diagnostic Polyclinic (branch No. 2), «Nova Poshta», «Cherkasyoblenerho».

Keywords: computer cryptography, cryptographic transformation operations, stream ciphers, synthesis of operations.