

УДК 519.7.004

[https://doi.org/10.52058/2786-6025-2023-13\(27\)-829-841](https://doi.org/10.52058/2786-6025-2023-13(27)-829-841)

Селіванов Віктор Левович кандидат технічних наук, доцент кафедри обчислювальної техніки факультету ФІОТ, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Перемоги, 37, м. Київ, 03056 тел.: (044)236-79-89, <https://orcid.org/0000-0001-8519-6038>

Халіл Хана Ала Ель-Дін студентка кафедри обчислювальної техніки факультету ФІОТ, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Перемоги, 37, м. Київ, 03056 тел.: (044)236-79-89, <https://orcid.org/0000-0001-5275-8305>

Саницький Артур Павлович студент кафедри обчислювальної техніки факультету ФІОТ, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Перемоги, 37, м. Київ, 03056 тел.: (044)236-79-89, <https://orcid.org/0009-0004-0132-715X>

Сергійчук Назар Сергійович студент кафедри обчислювальної техніки факультету ФІОТ, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Перемоги, 37, м. Київ, 03056 тел.: (044)236-79-89, <https://orcid.org/0009-0006-4753-970X>

РОТАЦІЙНО-КОМПЕНСАЦІЙНИЙ МЕТОД ПОБУДОВИ МАГІЧНИХ КВАДРАТІВ ДЛЯ КРИПТОГРАФІЧНИХ ЗАСТОСУВАНЬ

Анотація. В статті теоретично обґрунтовано, розроблено та досліджено підхід до збільшення ефективності технології побудови магічних квадратів непарних порядків, за рахунок зменшення обчислювальної складності її комп'ютерної реалізації.

Для прискорення комп'ютерної реалізації побудови магічних квадратів непарних порядків запропоновано використати заздалегідь заповнену вихідну матрицю, над елементами якої здійснюються спеціальні операції зсуву. В статті детально розроблено метод побудови магічних квадратів непарних порядків. Виклад ілюстровано прикладом побудови магічного квадрату 5×5 . Приведено математично строгі доведення конструктивності запропонованого методу, тобто того, що розроблена система комбінацій циклічних зсувів

утворює магічний квадрат. Теоретично обґрунтовано, що запропонований метод дозволяє прискорити створення магічного квадрату за рахунок використання більш простих логічних операцій циклічного зсуву на противагу арифметичним операціям, які застосовуються в відомих методах. Показано, що одна операція циклічного зсуву дозволяє замінити при цьому декілька більш складних в обчислювальному плані арифметичних операцій. Саме це дозволяє зменшити обчислювальну складність реалізації побудови магічного квадрату. Крім того, запропонований метод, на відміну від відомих, не використовує ресурсоємких технологій перебору. Цей чинник також є вагомим для зменшення обчислювальної складності комп'ютерної реалізації побудови магічних квадратів, особливо при збільшенні їх розмірності.

Теоретично та експериментально досліджено ефективність запропонованого методу в плані прискорення комп'ютерної реалізації побудови магічних квадратів непарних порядків. Теоретично доведено, що використання запропонованого підходу до створення магічних квадратів забезпечує зменшення обчислювальної складності в чотири рази в порівнянні з відовими методами. Експериментальні дослідження з використанням розроблених програм в цілому підтвердити отриману теоретичним шляхом оцінку ефективності запропонованого підходу.

Розроблений метод комп'ютерного синтезу магічних квадратів великої розмірності орієнтований на використання в системах та засобах криптографічного захисту інформації.

Ключові слова. Магічні квадрати, магічна сума, методи конструювання магічних квадратів, циклічні зсуви, криптографічний захист даних.

Selivanov Viktor Levovych Candidate of Technical Sciences, Associate Professor Department of Computer Science of the FICE, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Peremohy Ave., Kyiv, 03056, tel.: (044) 236-79-89, <https://orcid.org/0000-0001-8519-6038>

Khalil Hana Ala El-Din Student of the Department of Computer Science of the FICE, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Peremohy Ave., Kyiv, 03056, tel.: (044)236-79-89, <https://orcid.org/0000-0001-5275-8305>

Sanytskyi Artur Pavlovych Student of the Department of Computer Science of the FICE, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Peremohy Ave., Kyiv, 03056, tel.: (044)236-79-89, <https://orcid.org/0009-0004-0132-715X>

Serhiichuk Nazar Sergijovich, student of the Department of Computer Science of the FICE, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Peremohy Ave., Kyiv, 03056, tel.: (044)236-79-89, <https://orcid.org/0009-0006-4753-970X>

ROTATION-COMPENSATION METHOD FOR CONSTRUCTING MAGIC SQUARES FOR CRYPTOGRAPHIC APPLICATIONS

Abstract. The article theoretically justifies, develops, and investigates an approach to enhance the efficiency of constructing magic squares of odd orders by reducing the computational complexity of its computer implementation.

To expedite the computer implementation of constructing magic squares of odd orders, it is proposed to use a pre-filled initial matrix, upon which specific shifting operations are performed on its elements. The article elaborates on the method for constructing magic squares of odd orders in detail. The method is illustrated by an example of construction a 5×5 magic square. Mathematically rigorous proofs of the constructiveness of the proposed method are provided, demonstrating that the developed system of combinations of cyclic shifts forms a magic square. It is theoretically substantiated that the proposed method accelerates the creation of a magic square by utilizing simpler logical cyclic shift operations, as opposed to arithmetic operations employed in well-known methods. It is demonstrated that one cyclic shift operation can replace several arithmetic operations. This reduction in computational complexity contributes to the efficient implementation of magic square construction. Furthermore, the proposed method, unlike known methods, does not rely on resource-intensive exhaustive techniques. This factor also plays a significant role in reducing the computational complexity of computer-based magic square construction, especially as the dimensions increase.

The efficiency of the proposed method in accelerating the computer implementation of constructing magic squares of odd orders has been theoretically and experimentally investigated. Theoretical proof establishes that using the proposed approach for creating magic squares reduces computational complexity by a factor of four compared to known methods. Experimental studies, employing the developed programs, confirm the efficiency evaluation obtained through theoretical analysis.

The developed method of computer synthesis of large-scale magic squares is aimed at being used in systems and tools for cryptographic information protection.

Keywords: magic square, magic sum, methods for constructing magic squares, cyclic shifts, cryptographic data protection.

Постановка проблеми Магічні квадрати мають довгу історію і були відомі щонайменше з 190 року до н.е. в Китаї [1]. У різні періоди вони набували магічного або міфічного значення і використовувалися як символи в творах мистецтва [2]. В сучасних умовах магічні квадрати отримали практичне використання, в таких галузях як кодування даних в системах їх передачі та розподіленого зберігання в хмарах [3,4,5]. Одним із найбільш важливих застосувань магічних квадратів в сучасних умовах є системи криптографічного захисту інформації.

Магічний квадрат – це матриця розмірністю $n \times n$, яка містить n^2 унікальних цілих чисел від 1 до n^2 , причому суми всіх елементів стовпців, рядків та діагоналей рівні між собою [6]. Розмірність матриці n називається порядком магічного квадрату. Сума всіх чисел в магічному квадраті може бути обчислена як арифметична прогресія значень від 1 до n^2 . Звідси випливає, що загальна сума всіх чисел у магічному квадраті дорівнює $(n^2+1)/2 \cdot n^2$. Таким чином, сума елементів в кожному окремому стовпці (рядку або діагоналі) магічного квадрата (позначена як σ), що в літературі отримала назву «магічна сума», дорівнює $((n^2+1)/2 \cdot n^2)/n = (n^2+1)/2 \cdot n$, оскільки квадрат має n рядків/стовпців, суми елементів яких є рівними між собою.

Побудова магічного квадрату великої розмірності являє собою складну комбінаторну задачу, вирішення якої потребує значних за обсягом обчислювальних ресурсів.

Відповідно, важливою та актуальною задачею є створення ефективних методів побудови магічних квадратів орієнтованих, в першу чергу, на комп'ютерну реалізацію, для засобів криптографічного захисту інформації.

Аналіз останніх досліджень і публікацій. До теперішнього часу створено велику кількість методів синтезу магічних квадратів [7]. Магічні квадрати класифікуються відповідно до парності їх порядку: непарні, подвійної парності (n ділиться на 4), одинарної парності (n парне, але не ділиться на 4). Така класифікація використовується через те, що описані типи квадратів потребують різних методів для їх побудови [6].

Одним із основних критеріїв ефективності синтезу магічних квадратів є обчислювальна складність. Серед найпоширеніших методів побудови магічних квадратів можна виділити метод Ейлера [8] та метод границь [9]. Основна ідея методу Ейлера полягає в побудові двох попередніх квадратів, які після виконання операції додавання утворюють магічний квадрат [8]. Перевагою описаного методу є можливість синтезу $(n-1)! \cdot (n-1)!/4$ магічних квадратів. Основний недолік цього методу полягає в високій обчислювальній складності, яка дорівнює $O(3n^2)$. Технологія методу границь полягає в побудові магічних квадратів, починаючи з невеликого ядра, яке потім обрамляється зовнішніми шарами [9]. Метод границь дозволяє побудувати велику кількість магічних квадратів, але зі збільшенням порядку значно зростає складність алгоритму заповнення матриці, через наявність великої кількості арифметичних операцій та ресурсоємких технологій перебору. В результаті аналізу відомих методів цілком очевидно, що особливості використання магічних квадратів в сучасних умовах потребують збільшення ефективності їх створення.

Мета статті – збільшення ефективності технології побудови магічних квадратів непарних порядків, за рахунок зменшення обчислювальної складності її комп'ютерної реалізації.

Виклад основного матеріалу. Для досягнення поставленої мети пропонується метод побудови магічних квадратів непарних порядків, який передбачає послідовний зсув елементів заздалегідь заповненої матриці.

Запропонований метод передбачає використання матриці A заповненої елементами від 1 до n^2 , які послідовно зростають по стовпцях:

$$\begin{pmatrix} 1 & n+1 & \cdots & n \cdot (n-1) + 1 \\ 2 & n+2 & \cdots & n \cdot (n-1) + 2 \\ \vdots & \vdots & & \vdots \\ n & n+n & \cdots & n^2 \end{pmatrix}$$

Кожен елемент матриці A визначається за наступною формулою:

$$a_{ji} = i \cdot n + j + 1, \forall i, j \in \{0, \dots, n-1\}, \quad (1)$$

де i – індекс стовпців, j – індекс рядків, а n – розмірність матриці.

В розробленому методі використовуються вертикальний та горизонтальний зсуви. Вертикальний зсув передбачає циклічний зсув кожного стовпця матриці A на q позицій. Для зростаючого вертикального зсуву стовпці з номерами менше $(n-1)/2$ зсуваються вгору, а стовпці з номерами більше $(n-1)/2$ – вниз. Для спадаючого вертикального зсуву рух стовпців змінюється у зворотному напрямку. Горизонтальний зсув передбачає циклічний зсув кожного рядка матриці A на q позицій. Для зростаючого горизонтального зсуву рядки з номерами менше $(n-1)/2$ зсуваються вправо, а рядки з номерами більше $(n-1)/2$ – ліворуч. Для спадаючого горизонтального зсуву рух рядків змінюється у зворотному напрямку.

Метод передбачає вибір однієї з чотирьох можливих варіацій зсувів:

Спочатку зростаючий вертикальний зсув, потім – зростаючий горизонтальний зсув.

Спочатку спадаючий вертикальний зсув, потім – спадаючий горизонтальний зсув.

Спочатку зростаючий горизонтальний зсув, потім – зростаючий вертикальний зсув.

Спочатку спадаючий горизонтальний зсув, потім – спадаючий вертикальний зсув.

Побудова магічного квадрату непарного порядку за запропонованим методом зводиться до виконання наступної послідовності дій:

1. Значення M встановлюється в 0.
2. Значення k встановлюється в 0.
3. Значення q встановлюється в $(n-1)/2$.
4. Здійснюється циклічний зсув k -го стовпця/рядка матриці A на q позицій, згідно з обраним варіантом.

5. Лічильник k -го стовпця/рядка матриці A збільшується на одиницю: $k = k+1$.
6. Лічильник q позицій зсуву зменшується на одиницю: $q = q-1$.
7. Якщо для лічильника k виконується умова: $k < (n-1)/2$, то здійснюється повернення до п. 4. Інакше здійснюється перехід до наступного кроку.
8. Лічильник q позицій зсуву встановлюється в 1.
9. Здійснюється циклічний зсув $(n-k)$ -го стовпця/рядка матриці A на q позицій, згідно з обраним варіантом.
10. Лічильник k -го стовпця/рядка матриці A зменшується на одиницю: $k = k-1$.
11. Лічильник q позицій зсуву збільшується на одиницю: $q = q+1$.
12. Якщо для лічильника k виконується умова: $k > 1$, то здійснюється повернення до п. 9. Інакше здійснюється перехід до наступного кроку.
13. Лічильник M збільшується на один: $M = M+1$.
14. Якщо для лічильника M виконується умова: $M \leq 1$, то здійснюється повернення до п. 2 із переходом на другий етап обраного варіанту зсуву, інакше – кінець.

Розроблений метод побудови магічних квадратів непарних порядків ілюструється наступним прикладом. Нехай потрібно побудувати магічний квадрат п'ятого порядку, тобто $n=5$. Згідно зі створеним методом застосовується вихідна матриця A розмірністю 5×5 , заповнена елементами від 1 до $n^2 = 25$, які послідовно зростають по стовпцях (рис. 1).

1	6	11	16	21
2	7	12	17	22
3	8	13	18	23
4	9	14	19	24
5	10	15	20	25

Рис. 1. Вихідна матриця A розмірністю 5×5

У відповідності з описаною процедурою перед здійсненням системи циклічних зсувів обирається одна із чотирьох можливих варіацій зсувів, в рамках поточного прикладу обрано комбінацію «спочатку зростаючий вертикальний зсув, потім – зростаючий горизонтальний зсув».

Згідно п.1 – п.3 процедури лічильники M та k встановлюються в нуль, а лічильник $q = (5-1)/2 = 2$. Відповідно до обраних параметрів під час виконання п.4 процедури створення магічного квадрату реалізується циклічний вертикальний зсув на дві позиції вгору стовпця з індексом 0. В рамках п.5

лічильник k збільшується на одиницю: $k=k+1$. Під час виконання п.6 лічильник зменшується на одиницю: $q = q-1$. Оскільки лічильник $k=1 < (5-1)/2$, то здійснюється перехід до п.4 процедури. Після повернення до п.4 процедури відбувається циклічний вертикальний зсув на одну позицію вгору стовпця з індексом 1, оскільки $q = 1$. В рамках виконання п.5 лічильник k збільшується на одиницю: $k=k+1$. Під час виконання п.6 лічильник зменшується на одиницю: $q = q-1$. Оскільки лічильник $k=2 = (5-1)/2$, то здійснюється перехід до п.8 процедури. При цьому стовпець з індексом 2 лишається незмінним. Згідно п.8 лічильник q позицій зсуву встановлюється в 1. Під час виконання п.9 процедури стовпець із індексом 3 зсувається циклічно на одну позицію вниз. Згідно п.10 та п.11 процедури лічильник k зменшується на одиницю: $k=k-1$, а q – збільшується на одиницю $q = q+1$. Після цього оскільки значення лічильника $k=2$ більше одного, здійснюється повернення до п.9 процедури. В цьому пункті процедури останній стовпець із індексом 4 зсувається циклічно на дві позиції вниз. Оскільки лічильник $k=1$, то здійснюється перехід до п.13, в рамках якого лічильник M збільшується на одиницю: $M = M+1$. Результат описаної послідовності дій представлено на рисунку 2, з якого видно, що суми елементів в кожному рядку дорівнюють магічній сумі.

3	7	11	20	24
4	8	12	16	25
5	9	13	17	21
1	10	14	18	22
2	6	15	19	23

Рис. 2. Матриця A з однаковими сумами рядків

В результаті перевірки в рамках п.14 процедури створення магічного квадрату здійснюється повернення до п.2. Згідно п.2 та п.3 процедури лічильник k встановлюється в нуль, а лічильник $q = (5-1)/2 = 2$. Відповідно до обраних параметрів під час виконання п.4 процедури створення магічного квадрату реалізується циклічний горизонтальний зсув на дві позиції ліворуч рядка з індексом 0. В рамках п.5 лічильник k збільшується на одиницю: $k=k+1$. Під час виконання п.6 лічильник зменшується на одиницю: $q = q-1$. Оскільки лічильник $k=1 < (5-1)/2$, то здійснюється перехід до п.4 процедури. Після повернення до п.4 процедури відбувається циклічний горизонтальний зсув на 1 позицію ліворуч рядка з індексом 1, оскільки $q = 1$. В рамках виконання п.5 лічильник k збільшується на одиницю: $k=k+1$. Під час виконання п.6 лічильник зменшується на одиницю: $q = q-1$. Оскільки лічильник $k=2 = (n-1)/2$, то

здійснюється перехід до п.8 процедури. Рядок з індексом 2, при цьому, лишається незмінним. Згідно п.8 лічильник q позицій зсуву встановлюється в 1. Під час виконання п.9 процедури рядок із індексом 3 зсувається циклічно на одну позицію праворуч. Згідно п.10 та п.11 процедури лічильник k зменшується на одиницю: $k=k-1$, а q – збільшується на одиницю $q = q + 1$. Після чого здійснюється перевірка лічильника $k=2 > 1$ і здійснюється повернення до п.9 процедури. В цьому пункті процедури останній рядок із індексом 4 зсувається циклічно на дві позиції праворуч. Оскільки лічильник $k=1$, то здійснюється перехід до п.13 процедури розробленого методу, в рамках якого лічильник M збільшується на одиницю: $M = M+1$. Результат описаної послідовності дій представлений на рисунку 3. З нього видно, що після циклічного горизонтального зсуву всіх рядків згідно з розробленим методом суми елементів кожного рядка дорівнюють магічній сумі.

Наведений приклад показує, що запропонований метод створення магічних квадратів непарного порядку забезпечує правильний результат.

Конструктивність розробленого методу може бути доведена, шляхом встановлення того факту, що результатом застосування запропонованої системи зсувів до вихідної матриці є магічний квадрат. Нижче наведено строго математичне доведення зазначеного факту.

11	20	24	3	7
8	12	16	25	4
5	9	13	17	21
22	1	10	14	18
19	23	2	6	15

Рис. 3. Матриця A з однаковими сумами рядків і стовпців

Згідно з запропонованим методом елементи початкової матриці A розташовані таким чином, що вони утворюють арифметичну прогресію. З цього випливає, що циклічний зсув елементів рядка або стовпця на q позицій, еквівалентний перестановці $(q+b)$ -го елемента на місце b -го, де b -індекс поточного рядка/стовпця. При цьому, якщо елемент $(q+b)$ виходить за межі матриці, то він переставляється в початок або кінець поточного рядка або стовпця. Тобто, за умови, що $(q+b) < 0$, здійснюється перестановка цього елемента на позицію $n+(q+b)$, а при $(q+b) > n-1$ – на позицію $(q+b)-n$.

Оскільки $q \in [1;(n-1)/2]$, то елементи матриці A після вертикального зсуву вгору визначаються за наступною формулою:

$$i \in [0; n-1]: \begin{cases} j \in \left[0; \frac{n-1}{2}\right], & q \in \left[1; \frac{n-1}{2}\right]: & a_{ji} = i \cdot n + j + q + 1 \\ j \in \left[\frac{n+1}{2}; n-1\right], & q \in [1; n-j-1]: & a_{ji} = i \cdot n + j + q + 1 \\ j \in \left[\frac{n+1}{2}; n-1\right], & q \in \left[n-j; \frac{n-1}{2}\right]: & a_{ji} = i \cdot n + j + q - n + 1 \end{cases} \quad (2)$$

Аналогічно елементи матриці A після вертикального зсуву вниз визначаються за наступною формулою:

$$i \in [0; n-1]: \begin{cases} j \in \left[0; \frac{n-1}{2}\right], & q \in \left[1+j; \frac{n-1}{2}\right]: & a_{ji} = i \cdot n + j + n - q + 1 \\ j \in \left[0; \frac{n-1}{2}\right], & q \in [1; j]: & a_{ji} = i \cdot n + j - q + 1 \\ j \in \left[\frac{n+1}{2}; n-1\right], & q \in \left[1; \frac{n-1}{2}\right]: & a_{ji} = i \cdot n + j - q + 1 \end{cases} \quad (3)$$

Відповідно до формул (2) та (3), суми елементів кожного j -го рядка у верхній ($j \in [0; (n-1)/2-1]$) або нижній ($j \in [(n+1)/2; n-1]$) частині матриці після застосування вертикального спадаючого або зростаючого зсувів визначаються наступним чином:

$$\sum_{i=0}^{n-1} (i \cdot n + j + 1) + \sum_{q=1}^{\frac{n-1}{2}} q - \sum_{q=1}^j q + \sum_{q=j+1}^{\frac{n-1}{2}} (n - q) = \frac{n^2 + 1}{2} \cdot n.$$

Відповідно до формул (2) та (3), суми елементів кожного j -го рядка у нижній ($j \in [(n+1)/2; n-1]$) або верхній ($j \in [0; (n-1)/2-1]$) частині матриці після застосування вертикального спадаючого або зростаючого зсувів визначаються наступним чином:

$$\sum_{i=0}^{n-1} (i \cdot n + j + 1) - \sum_{q=1}^{\frac{n-1}{2}} q + \sum_{q=1}^{n-1-j} q + \sum_{q=n-j}^{\frac{n-1}{2}} (q - n) = \frac{n^2 + 1}{2} \cdot n.$$

Сума елементів, що знаходяться на головній діагоналі матриці, тобто при $j=i$ розраховується наступним чином:

$$\sum_{i=0}^{n-1} (i \cdot n + i + 1) - \sum_{q=1}^{\frac{n-1}{2}} q + \sum_{q=1}^{\frac{n-1}{2}} q = \frac{n^2 + 1}{2} \cdot n.$$

Сума елементів, що лежать на побічній діагоналі матриці, тобто при $j=n-1-i$, при $(n-1)/2$ – парне, обчислюється наступним чином:

$$\sum_{i=0}^{n-1} (i \cdot n + n - i) + \left(\frac{n-1}{2} + 1\right) - \left(\frac{n-1}{2} + 1\right) + \sum_{q=1}^{\frac{n-1}{4}} (q - n) + \sum_{q=1}^{\frac{n-1}{4}} (n - q) = \frac{n^2 + 1}{2} \cdot n.$$

А при непарних значеннях $(n-1)/2$:

$$\sum_{i=0}^{n-1} (i \cdot n + n - i) + \left(\frac{n+1}{2} + 1 \right) - \left(\frac{n+1}{2} + 1 \right) + \sum_{q=1}^{\frac{n+1}{2}} (q - n) + \sum_{q=1}^{\frac{n+1}{2}} (n - q) = \frac{n^2 + 1}{2} \cdot n.$$

Таким чином доведено, що після застосування до початкової матриці А спадаючого або зростаючого вертикального зсуву, суми елементів всіх рядків та діагоналей дорівнюють магичній сумі.

Елементи матриці А після горизонтального зсуву ліворуч визначаються за наступною формулою:

$$j \in [0; n-1]: \begin{cases} i \in \left[0; \frac{n-1}{2}\right], & q \in \left[1; \frac{n-1}{2}\right]: & a_{ji} = (i+q) \cdot n + j + 1 \\ i \in \left[\frac{n+1}{2}; n-1\right], & q \in [1; n-1-i]: & a_{ji} = (i+q) \cdot n + j + 1 \\ i \in \left[\frac{n+1}{2}; n-1\right], & q \in \left[n-i; \frac{n-1}{2}\right]: & a_{ji} = (i+q-n) \cdot n + j + 1 \end{cases} \quad (4)$$

Аналогічно елементи матриці А після горизонтального зсуву праворуч визначаються за наступною формулою:

$$j \in [0; n-1]: \begin{cases} i \in \left[0; \frac{n-1}{2}\right], & q \in \left[1+i; \frac{n-1}{2}\right]: & a_{ji} = (i+n-q) \cdot n + j + 1 \\ i \in \left[0; \frac{n-1}{2}\right], & q \in [1; i]: & a_{ji} = (i-q) \cdot n + j + 1 \\ i \in \left[\frac{n+1}{2}; n-1\right], & q \in \left[1; \frac{n-1}{2}\right]: & a_{ji} = (i-q) \cdot n + j + 1 \end{cases} \quad (5)$$

Згідно формул (4) та (5), суми елементів кожного i -го стовпця у лівій ($i \in [0; (n-1)/2-1]$) або правій ($i \in [(n+1)/2; n-1]$) частині матриці після застосування горизонтального спадаючого або зростаючого зсувів визначаються наступним чином:

$$\sum_{j=0}^{n-1} (i \cdot n + j + 1) + \sum_{q=1}^{\frac{n-1}{2}} q \cdot n - \sum_{q=1}^i q \cdot n + \sum_{q=i+1}^{\frac{n-1}{2}} (n-q) \cdot n = \frac{n^2 + 1}{2} \cdot n.$$

Згідно формул (4) та (5), суми елементів кожного i -го стовпця у правій ($i \in [(n+1)/2; n-1]$) або лівій ($i \in [0; (n-1)/2-1]$) частині матриці після застосування горизонтального спадаючого або зростаючого зсувів визначаються наступним чином:

$$\sum_{j=0}^{n-1} (i \cdot n + j + 1) - \sum_{q=1}^{\frac{n-1}{2}} q \cdot n + \sum_{q=1}^{n-1-i} q \cdot n + \sum_{q=n-i}^{\frac{n-1}{2}} (q-n) \cdot n = \frac{n^2 + 1}{2} \cdot n.$$

Сума елементів, що знаходяться на головній діагоналі матриці, тобто при $i=j$ розраховується наступним чином:

$$\sum_{j=0}^{n-1} (j \cdot n + j + 1) + \sum_{q=1}^{\frac{n-1}{2}} q \cdot n - \sum_{q=1}^{\frac{n-1}{2}} q \cdot n = \frac{n^2 + 1}{2} \cdot n.$$

Сума елементів, що лежать на побічній діагоналі матриці, тобто при $i=n-1-j$ при $(n-1)/2$ – парне, обчислюється наступним чином:

$$\sum_{j=0}^{n-1} ((n-1-j) \cdot n + j + 1) + \left(\frac{n-1}{2} + 1\right) \cdot n - \left(\frac{n-1}{2} + 1\right) \cdot n + \sum_{q=1}^{\frac{n-1}{4}} (n-q) \cdot n + \sum_{q=1}^{\frac{n-1}{4}} (q-n) \cdot n = \frac{n^2 + 1}{2} \cdot n$$

А при непарних значеннях $(n-1)/2$:

$$\sum_{j=0}^{n-1} ((n-1-j) \cdot n + j + 1) + \left(\frac{n+1}{2} + 1\right) \cdot n - \left(\frac{n+1}{2} + 1\right) \cdot n + \sum_{q=1}^{\frac{n+1}{4}} (n-q) \cdot n + \sum_{q=1}^{\frac{n+1}{4}} (q-n) \cdot n = \frac{n^2 + 1}{2} \cdot n$$

Отже, доведено, що після застосування до початкової матриці A спадаючого або зростаючого горизонтального зсуву, суми елементів всіх стовпців та діагоналей дорівнюють магічній сумі. Виходячи з цього цілком очевидно, що після застосування системи зсувів запропонованих у розробленому методі, синтезується магічний квадрат.

Важливим аспектом розробки методу синтезу магічних квадратів виступає порівняльна оцінка його ефективності. Виходячи з поставленої мети в якості оцінки ефективності запропонованого методу використовується обчислювальна складність побудови магічних квадратів.

Обчислювальна складність може бути визначена наступним чином: кожен зсув рядка або стовпця матриці реалізується n операціями. При цьому, кількість зсувів стовпців/рядків, яку передбачає запропонований метод дорівнює $n-1$, оскільки центральний стовпець/рядок лишається незмінним. Таким чином кількість операцій, яку передбачає розроблений метод для зсуву усіх стовпців та рядків становить $2n \cdot (n-1)$. Отже, обчислювальна складність запропонованого методу складає $O(2n \cdot (n-1))$.

При порівнянні запропонованого методу і вже відомих можливо зробити наступні висновки:

9. Обчислювальна складність методу Ейлера становить $O(3n^2)$, таким чином, запропонований спосіб створення є більш ефективним завдяки зменшенню обчислювальної складності більше ніж в 3 рази.

10. Для створення магічного квадрату з використанням методу границь необхідно зробити значно більшу кількість операцій, з цього випливає, що його обчислювальна складність багаторазово перевищує складність створеного методу.

Таким чином, запропонований метод є відносно обчислювально простим та забезпечує синтез кількох унікальних магічних квадратів одного порядку, що робить його ефективним інструментом у вирішенні завдань побудови магічних квадратів.

Висновки. В статті запропоновано та досліджено підхід до збільшення ефективності технології побудови магічних квадратів непарних порядків, за рахунок зменшення обчислювальної складності її комп'ютерної реалізації. Підхід конкретизовано у вигляді формалізованого методу синтезу магічних квадратів непарного порядку.

Базова ідея запропонованого методу полягає використанні заздалегідь заповненої вихідної матриці, над елементами якої здійснюються спеціальні операції зсуву. Приведено математично строгі доведення конструктивності запропонованого методу, тобто того, що розроблена система комбінацій циклічних зсувів утворює магічний квадрат.

Теоретично та експериментально показано, що ефективність запропонованого методу в плані прискорення комп'ютерної реалізації побудови магічних квадратів непарних порядків вища в порівнянні з відомими технологіями.

Література:

1. Yoke H.P. Magic Squares in China / H.P. Yoke // *Encyclopaedia of the History of Science, Technology, and Medicine in Non-Western Cultures*; за наук. ред. Н. Selin. – Dordrecht: Springer, 2008. – С. 1251–1252.
2. Magic Squares and Cubes / W. S. Andrews, P. Carus, L. S. Frierson, C. A. Browne. – Chicago: Open Court, 1917. – 419 с.
3. De las Cuevas G. Quantum magic squares: Dilations and their limitations / G. De las Cuevas, T. Drescher, T. Netzer. // *Journal of Mathematics and Physics*. – 2020. – №61.
4. Grami A. Discrete Mathematics: Essentials and Applications. Amsterdam: Elsevier Science, 2022. – 464 с.
5. Ganapathy G. Add-On Security Model for Public-Key Cryptosystem Based on Magic Square Implementation / G. Ganapathy, K. Mani. // *Тези доповідей World Congress on Engineering and Computer Science Vol I*. – 2009.
6. Pickover C.A. The Zen of Magic Squares, Circles, and Stars: An Exhibition of Surprising Structures Across Dimensions / C.A. Pickover. – Princeton: Princeton University Press, 2002. – 432 с.
7. Jacques S. Magic Squares: Their History and Construction from Ancient Times to Ad 1600. Cham: Springer, 2019. – 313 с.
8. Boyer C. Some notes on the magic squares of squares problem / C. Boyer. // *The Mathematical Intelligencer*. – 2005. – №27. – С. 52–64.
9. Vaithianathan S. Bordered magic squares of odd order / S. Vaithianathan. // *The Mathematical Gazette*. – 1998. – №82. – С. 438–442.

References:

1. Yoke, H.P. (2008). Magic Squares in China. *Encyclopaedia of the History of Science, Technology, and Medicine in Non-Western Cultures* (pp. 1251–1252). H, Selin (Ed.). Dordrecht: Springer.

2. Andrews, W. S., Carus, P., Frierson, L. S., Browne, C. A. (1917). *Magic Squares and Cubes* – Chicago: Open Court.
3. De las Cuevas, G., Drescher, T., Netzer, T. (2020). Quantum magic squares: Dilations and their limitations *Journal of Mathematics and Physics*, 61.
4. Grami, A. (2022). *Discrete Mathematics: Essentials and Applications*. Amsterdam: Elsevier Science.
5. Ganapathy, G. & Mani, K. (2009). Add-On Security Model for Public-Key Cryptosystem Based on Magic Square Implementation. *Proceedings of the World Congress on Engineering and Computer Science Vol I*. San Francisco.
6. Pickover, C. A. (2002). *The Zen of Magic Squares, Circles, and Stars: An Exhibition of Surprising Structures Across Dimensions*. Princeton: Princeton University Press.
7. Jacques, S. (2019). *Magic Squares: Their History and Construction from Ancient Times to Ad 1600*. Cham: Springer.
8. Boyer, C. (2005). Some notes on the magic squares of squares problem. *The Mathematical Intelligencer*, 27, (pp. 52–64). New-York: Springer.
9. Vaithianathan, S. (1998). Bordered magic squares of odd order. *The Mathematical Gazette*, 82, (pp. 438–442). Princeton: Princeton University Press.