УДК 004.056.55:004.312.2

Є. В. Ланських, *к.т.н., доцент,*
доцент кафедри інформаційної безпеки та комп'ютерної інженерії
e-mail: yevhenlanskykh@gmail.com
С. В. Сисоєнко, *асистент*
кафедри інформаційної безпеки та комп'ютерної інженерії
e-mail: s.sysoienko@gmail.com
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ДОСЛІДЖЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ДВОХОПЕРАНДНОГО ГРУПОВОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

У статті розглянуто і теоретично обґрунтовано результати перевірки коректності запропонованої математичної моделі побудови прямого та оберненого двохоперандного групового матричного криптографічного перетворення за допомогою математичного апарату теорії блочних матриць. За результатами досліджень встановлена коректність математичної моделі побудови оберненого групового матричного криптографічного перетворення, яка перевірена на повних множинах групових і негрупових операцій. Запропонована модель побудови оберненого групового матричного криптографічного перетворення забезпечує коректний синтез оберненого перетворення при відсутності негрупових операцій на основній діагоналі матриці групової операції. Отримані результати підтверджують коректну побудову оберненого перетворення на основі запропонованої моделі, реалізація якої забезпечує зменшення складності обчислень.

Отриманий результат показав правильність знаходження оберненої матриці за допомогою запропонованої моделі.

Ключові слова: *пряме та обернене криптографічне перетворення, двохоперандні криптографічні перетворення, коректність моделі, матрична операція.*

Актуальність досліджень. Ефективний захист інформації в реальному часі функціонування інформаційно-телекомунікаційних систем неможливий без використання криптографічних методів [1], які забезпечують швидкодію апаратного забезпечення для реалізації шифрування. Захист даних та безпека інформації можливі за допомогою вдосконалення існуючих та пошуку нових методів криптографічного захисту інформації [2].

Одним із шляхів вирішення цієї проблеми є застосування матричних операцій криптографічного перетворення для розробки і вдосконалення криптоалгоритмів.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто виділити [3], де досліджено використання групових операцій криптографічного перетворення, що забезпечують підвищення якості шифрування та можливість розшифрування інформації, і [4], де було розглянуто питання підвищення стійкості комп'ютерних криптографічних алгоритмів за рахунок використання операцій криптоперетворення та алгоритмів криптографічного перетворення двох блоків змінних. В [5] проведено розробку алгоритмів застосування операцій матричного криптографічного перетворення та оцінювання статистичних властивостей результатів криптографічного перетворення на їх основі.

Проте в цих дослідженнях не було сформульовано та математично обґрунтовано правила побудови оберненої операції за допомогою математичного апарату теорії блочних матриць.

Мета статті – дослідження й оцінювання властивостей математичної моделі двохоперандного групового матричного криптографічного перетворення.

Виклад основного матеріалу. В процесі дослідження матричних групових криптографічних перетворень [6–7] було запропоновано формалізовану модель прямого та оберненого двохоперандного групового матричного криптографічного перетворення.

Якщо $G^k = \begin{pmatrix} a_{11}F_1^k(z_1) \oplus a_{12}F_2^k(z_2) \\ a_{21}F_1^k(z_1) \oplus a_{22}F_2^k(z_2) \end{pmatrix}$, (1)

тоді $G^d = \begin{pmatrix} b_{11}F_1^d(w_1) \oplus b_{12}F_1^d(w_2) \\ b_{21}F_2^d(w_1) \oplus b_{22}F_2^d(w_2) \end{pmatrix}$, (2)

де $a_{ij} \in [0,1]$ – коефіцієнти матриці прямого групового криптографічного перетворення, $b_{ij} \in [0,1]$ – коефіцієнти матриці оберненого групового криптографічного перетворення, F_i^k – операції негрупових двохоперандних криптографічних перетворень, F_i^d – операції обернених негрупових двохоперандних криптографічних перетворень; $\oplus$ – операція «сума за mod 2».

Перевіримо коректність запропонованої математичної моделі побудови оберненого групового матричного криптографічного перетворення. Для перевірки коректності скористаємося математичним апаратом теорії блочних матриць [8–10]. Будемо вважати, що перетворення на основі запропонованої моделі (1), (2) є коректним, якщо результат побудови оберненої матриці збігся з оберненою матрицею, побудованою на основі теорії блочних матриць [8-10].

Згідно з даними (табл. 1–2) [4] представимо:

$G^k = G_{6,5}^k$, $F_1^k = F_{6,5}^k$, $F_2^k = F_{5,6}^k$.

Оскільки $G_{6,5}^k \to G_{6,5}^d$, $F_{6,5}^k \to F_{6,5}^d$, $F_{5,6}^k \to F_{6,3}^d$, то відповідно до (1), (2) отримаємо:

для $G_{6,5}^k = \begin{bmatrix} F_1^k(z_1) \oplus F_2^k(z_2) \\ F_2^k(z_2) \end{bmatrix}$ обернене перетворення буде $G_{6,5}^d = \begin{bmatrix} F_1^d(w_1) \oplus F_1^d(w_2) \\ F_2^d(w_2) \end{bmatrix}$.

Для зручності проведення математичних розрахунків приймемо [4]

$z_{1.1}, z_{1.2}, z_{2.1}, z_{2.2} \in \{0,1\}$ – вхідні дані для прямого перетворення:

$$z_1 = \begin{bmatrix} z_{1.1} \\ z_{1.2} \end{bmatrix}, \quad z_2 = \begin{bmatrix} z_{2.1} \\ z_{2.2} \end{bmatrix},$$

та $w_{1.1}, w_{1.2}, w_{2.1}, w_{2.2} \in \{0,1\}$ – вхідні дані (результати прямого перетворення) для оберненого перетворення:

$$w_1 = \begin{bmatrix} w_{1.1} \\ w_{1.2} \end{bmatrix}, \; w_2 = \begin{bmatrix} w_{2.1} \\ w_{2.2} \end{bmatrix}.$$

Таблиця 1

Операції криптографічного перетворення інформації двох блоків змінних

Номер операції	Модель операції	
	Модель операції прямого перетворення	Модель операції оберненого перетворення
1	$F_{6,5}^k = \begin{bmatrix} z_1 \oplus z_2 \\ z_2 \end{bmatrix}$	$F_{6,5}^d = \begin{bmatrix} w_1 \oplus w_2 \\ w_2 \end{bmatrix}$
2	$F_{3,6}^k = \begin{bmatrix} z_1 \\ z_1 \oplus z_2 \end{bmatrix}$	$F_{3,6}^d = \begin{bmatrix} w_1 \\ w_1 \oplus w_2 \end{bmatrix}$
3	$F_{5,6}^k = \begin{bmatrix} z_2 \\ z_1 \oplus z_2 \end{bmatrix}$	$F_{6,3}^d = \begin{bmatrix} w_1 \oplus w_2 \\ w_1 \end{bmatrix}$
4	$F_{6,3}^k = \begin{bmatrix} z_1 \oplus z_2 \\ z_1 \end{bmatrix}$	$F_{5,6}^d = \begin{bmatrix} w_2 \\ w_1 \oplus w_2 \end{bmatrix}$

Таблиця 2

Алгоритм криптографічного перетворення двох блоків змінних

Номер алгоритму	Алгоритми криптографічного перетворення	
	Алгоритм прямого перетворення	Алгоритм оберненого перетворення
1	$G_{6,5}^k = \begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix}$	$G_{6,5}^d = \begin{bmatrix} F_1 \oplus F_2 \\ F_2 \end{bmatrix}$
2	$G_{3,6}^k = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix}$	$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix}$
3	$G_{5,6}^k = \begin{bmatrix} F_2 \\ F_1 \oplus F_2 \end{bmatrix}$	$G_{6,3}^d = \begin{bmatrix} F_1 \oplus F_2 \\ F_1 \end{bmatrix}$
4	$G_{6,3}^k = \begin{bmatrix} F_1 \oplus F_2 \\ F_1 \end{bmatrix}$	$G_{5,6}^d = \begin{bmatrix} F_2 \\ F_1 \oplus F_2 \end{bmatrix}$

Перевіримо правильність отриманого результату, використавши формулу Фробеніуса [8–10].

Умова невиродженості (несингулярності) матриці A є необхідною і достатньою для існування оберненої матриці A^{-1} [8]. Якщо визначник $\det A \neq 0$, то матриця A має обернену A^{-1} [8].

A – невироджена матриця, яка є блочною

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}.$$

Для оберненої матриці [8] A^{-1} виконується рівність:

$$AA^{-1} = A^{-1}A = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix}. \quad (3)$$

Обернена до A матриця – також блочна відповідно до формули Фробеніуса [8], причому

$$A^{-1} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}^{-1} = \\ = \begin{bmatrix} A_{11}^{-1} + FQ^{-1}F' & -FQ^{-1} \\ -Q^{-1}F' & Q^{-1} \end{bmatrix}, \quad (4)$$

де $Q = A_{22} - A_{21}A_{22}^{-1}A_{12}$, $F = A_{11}^{-1}A_{12}$.

Якщо матриця $\begin{bmatrix} A & 0 \\ C & D \end{bmatrix}$ – невироджена з квадратними блоками [9] A і D, то з невиродженості випливає, що $\det A \neq 0$ і $\det D \neq 0$.

Для випадку

$$\begin{bmatrix} A & 0 \\ C & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & 0 \\ -D^{-1}CA^{-1} & D \end{bmatrix}. \quad (5)$$

Аналогічно для випадку

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix}. \quad (6)$$

Для цього випадку представимо матрицю A.

$$G_{6,5}^{k} = \begin{bmatrix} F_1^k(z_1) \oplus F_2^k(z_2) \\ F_2^k(z_2) \end{bmatrix} = \begin{bmatrix} F_{6,5}^k(z_1) \oplus F_{5,6}^k(z_2) \\ F_{5,6}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1.1} \oplus z_{1.2} \oplus z_{2.2} \\ z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \\ z_{2.2} \\ z_{2.1} \oplus z_{2.2} \end{bmatrix}$$

$$G_{6,5}^{k} = A_{6,5} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Обернену матрицю $A_{6,5}^{-1}$ до матриці $A_{6,5}$ знайдемо згідно з випадком (6)

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix}.$$

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \; C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \; D = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Оскільки $-1 \equiv 1 (\mathrm{mod}\, 2)$, $1^{-1} = 1$, то операції додавання, віднімання, множення і ділення за модулем 2 збігаються:

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} (\mathrm{mod}\, 2) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$D^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = -\begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix} (\mathrm{mod}\, 2) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$-A^{-1}B = -\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \\ = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} (\mathrm{mod}\, 2) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$-A^{-1}BD^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Побудуємо обернену матрицю на основі попередніх розрахунків:

$$A_{6,5}^{-1} = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (7)$$

Провівши відповідні математичні обчислення, перевіримо, чи виконується рівність (3) для оберненої матриці [8].

$$A_{6,5}A_{6,5}^{-1} = A_{6,5}^{-1}A_{6,5} = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ця перевірка показала правильність знаходження оберненої матриці.

Порівняємо результат оберненого перетворення $G_{6,5}^{d} = \begin{bmatrix} F_1^{d}(w_1) \oplus F_1^{d}(w_2) \\ F_2^{d}(w_2) \end{bmatrix}$ на основі запропонованої моделі (1), (2) з результатом побудови оберненої матриці, що побудована на основі теорії блочних матриць (7).

$$G_{6,5}^{d} = \begin{bmatrix} F_1^{d}(w_1) \oplus F_1^{d}(w_2) \\ F_2^{d}(w_2) \end{bmatrix} = \begin{bmatrix} F_{6,5}^{d}(w_1) \oplus F_{6,5}^{d}(w_2) \\ F_{6,3}^{d}(w_2) \end{bmatrix} =$$

$$= \begin{bmatrix} w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.2} \oplus w_{2.2} \\ w_{2.1} \oplus w_{2.2} \\ w_{2.1} \end{bmatrix}$$

$$G_{6,5}^{d} = A_{6,5}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad (8)$$

Перетворення на основі запропонованої моделі (1), (2) є коректним, оскільки результати розрахунків (7) та (8) збіглися.

Нехай $G^{k} = G_{5,6}^{k}$, $F_1^{k} = F_{6,5}^{k}$, $F_2^{k} = F_{6,3}^{k}$.

Оскільки $G_{5,6}^{k} \to G_{6,3}^{d}$, $F_{6,5}^{k} \to F_{6,5}^{d}$, $F_{6,3}^{k} \to F_{5,6}^{d}$, то відповідно до (1). (2) отримаємо:

для $G_{5,6}^{k} = \begin{bmatrix} F_2^{k}(z_2) \\ F_1^{k}(z_1) \oplus F_2^{k}(z_2) \end{bmatrix}$ обернене перетворення буде $G_{6,3}^{d} = \begin{bmatrix} F_1^{d}(w_1) \oplus F_1^{d}(w_2) \\ F_2^{d}(w_1) \end{bmatrix}$.

Згідно з даними (табл.1–2) [4] представимо матрицю A.

$$G_{5,6}^{k} = \begin{bmatrix} F_2^{k}(z_2) \\ F_1^{k}(z_1) \oplus F_2^{k}(z_2) \end{bmatrix} = \begin{bmatrix} F_{6,3}^{k}(z_2) \\ F_{6,5}^{k}(z_1) \oplus F_{6,3}^{k}(z_2) \end{bmatrix} =$$

$$= \begin{bmatrix} z_{2.1} \oplus z_{2.2} \\ z_{2.1} \\ z_{1.1} \oplus z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \\ z_{1.2} \oplus z_{2.1} \end{bmatrix}$$

$$G_{5,6}^{k} = A_{5,6} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Для цього випадку згідно з (5), (6) матриця $A_{5,6}$ – вироджена.

А згідно з [8] для існування оберненої матриці A^{-1} потрібно виконання умови невиродженості матриці A.

У випадках обмежень на математичний апарат блочних матриць скористаємося математичним апаратом перевірки коректності синтезованої оберненої матриці. Представимо обернену матрицю на основі запропонованої моделі (1), (2) та перевіримо, чи виконується рівність (3) для оберненої матриці [8].

Результат оберненого перетворення запропонованої моделі (1), (2) буде наступним:

$$G_{6,3}^{d} = \begin{bmatrix} F_1^{d}(w_1) \oplus F_1^{d}(w_2) \\ F_2^{d}(w_1) \end{bmatrix} = \begin{bmatrix} F_{6,5}^{d}(w_1) \oplus F_{6,5}^{d}(w_2) \\ F_{5,6}^{d}(w_1) \end{bmatrix} =$$

$$= \begin{bmatrix} w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.2} \oplus w_{2.2} \\ w_{1.2} \\ w_{1.1} \oplus w_{1.2} \end{bmatrix}$$

$$G_{6,3}^{d} = A_{6,3}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}. \qquad (9)$$

Провівши відповідні математичні обчислення, підставивши у вираз (3) отримані результати, перевіримо, чи виконується рівність для оберненої матриці [8].

$$A_{5,6}A_{6,3}^{-1} = A_{6,3}^{-1}A_{5,6} = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix} =$$

$$= \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Цей результат показав правильність знаходження оберненої матриці за допомогою запропонованої моделі.

Нехай $G^k = G_{3,6}^k$, $F_1^k = F_{3,6}^k$, $F_2^k = F_{5,6}^k$.

Оскільки $G_{3,6}^k \to G_{3,6}^d$, $F_{3,6}^k \to F_{3,6}^d$, $F_{5,6}^k \to F_{6,3}^d$, то відповідно до (1), (2) отримаємо:

для $G_{3,6}^k = \begin{bmatrix} F_1^k(z_1) \\ F_1^k(z_1) \oplus F_2^k(z_2) \end{bmatrix}$ обернене перетворення буде $G_{3,6}^d = \begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1) \oplus F_2^d(w_2) \end{bmatrix}$.

Знайдемо матрицю *A* для цього випадку.

$$G_{3,6}^k = \begin{bmatrix} F_1^k(z_1) \\ F_1^k(z_1) \oplus F_2^k(z_2) \end{bmatrix} =$$

$$\begin{bmatrix} F_{3,6}^k(z_1) \\ F_{3,6}^k(z_1) \oplus F_{5,6}^k(z_2) \end{bmatrix} == \begin{bmatrix} z_{1.1} \\ z_{1.1} \oplus z_{1.2} \\ z_{1.1} \oplus z_{2.2} \\ z_{1.1} \oplus z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \end{bmatrix}$$

$$G_{3,6}^k = A_{3,6} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Обернену матрицю $A_{3,6}^{-1}$ до матриці $A_{3,6}$ знайдемо згідно з випадком (5):

$$\begin{bmatrix} A & 0 \\ C & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & 0 \\ -D^{-1}CA^{-1} & D \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ C = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ D = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Побудуємо обернену матрицю на основі попередніх розрахунків:

$$A_{3,6}^{-1} = \begin{bmatrix} A & 0 \\ C & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & 0 \\ -D^{-1}CA^{-1} & D \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad . \quad (10)$$

Перевіримо виконання рівності (3) для оберненої матриці [8].

$$A_{3,6}A_{3,6}^{-1} = A_{3,6}^{-1}A_{3,6} = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ця перевірка показала правильність знаходження оберненої матриці.

Порівняємо результат оберненого перетворення $G_{3,6}^d = \begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1) \oplus F_2^d(w_2) \end{bmatrix}$ на основі (1), (2) з результатом побудови оберненої матриці, що побудована на основі теорії блочних матриць (10).

$$G_{3,6}^d = \begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1) \oplus F_2^d(w_2) \end{bmatrix} = \begin{bmatrix} F_{3,6}^d(w_1) \\ F_{6,3}^d(w_1) \oplus F_{6,3}^d(w_2) \end{bmatrix} =$$

$$\begin{bmatrix} w_{1.1} \\ w_{1.1} \oplus w_{1.2} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.1} \oplus w_{2.1} \end{bmatrix}$$

$$G_{3,6}^d = A_{3,6}^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad (11)$$

Перетворення на основі (1), (2) є коректним, оскільки результати розрахунків (10) та (11) збіглися.

Нехай $G^k = G_{6,3}^k$, $F_1^k = F_{5,6}^k$, $F_2^k = F_{6,3}^k$.

Оскільки $G^k_{6,3} \to G^d_{5,6}$, $F^k_{5,6} \to F^d_{6,3}$, $F^k_{6,3} \to F^d_{5,6}$, то згідно з (1), (2) отримаємо:

для $G^k_{6,3} = \begin{bmatrix} F^k_1(z_1) \oplus F^k_2(z_2) \\ F^k_1(z_1) \end{bmatrix}$ обернене перетворення буде $G^d_{5,6} = \begin{bmatrix} F^d_1(w_2) \\ F^d_2(w_1) \oplus F^d_2(w_2) \end{bmatrix}$.

Перевіримо коректність побудованого оберненого перетворення.

Згідно з даними (табл. 1–2) [4] представимо матрицю $A_{6,3}$.

$$G^k_{6,3} = \begin{bmatrix} F^k_1(z_1) \oplus F^k_2(z_2) \\ F^k_1(z_1) \end{bmatrix} = \begin{bmatrix} F^k_{5,6}(z_1) \oplus F^k_{6,3}(z_2) \\ F^k_{6,5}(z_1) \end{bmatrix} =$$

$$= \begin{bmatrix} z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \\ z_{1.1} \oplus z_{1.2} \oplus z_{2.1} \\ z_{1.2} \\ z_{1.1} \oplus z_{1.2} \end{bmatrix}$$

$$G^k_{6,3} = A_{6,3} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Для цього випадку згідно з (5), (6) матриця $A_{6,3}$ – вироджена. Для існування оберненої матриці A^{-1} потрібно виконання умови невиродженості матриці A [8].

Представимо обернену матрицю на основі запропонованої моделі та перевіримо, чи виконується рівність (3) для оберненої матриці [8].

Провівши відповідні математичні обчислення, підставивши у вираз (3) отримані результати, перевіримо, чи виконується рівність для оберненої матриці [8].

$$G^d_{5,6} = \begin{bmatrix} F^d_1(w_2) \\ F^d_2(w_1) \oplus F^d_2(w_2) \end{bmatrix} = \begin{bmatrix} F^d_{6,3}(w_2) \\ F^d_{5,6}(w_1) \oplus F^d_{5,6}(w_2) \end{bmatrix} =$$

$$= \begin{bmatrix} w_{2.1} \oplus w_{2.2} \\ w_{2.1} \\ w_{1.2} \oplus w_{2.2} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \end{bmatrix}$$

$$G^d_{5,6} = A_{5,6}{}^{-1} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \qquad (12)$$

$$A_{6,3}A_{5,6}{}^{-1} = A_{5,6}{}^{-1}A_{6,3} = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix} =$$

$$= \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Цей результат показав правильність знаходження оберненої матриці за допомогою запропонованої моделі. Коректність математичної моделі побудови оберненого групового матричного криптографічного перетворення перевірена на повних множинах групових і негрупових операцій (табл. 1, 2) [4].

Слід відзначити, що запропонована модель побудови оберненого групового матричного криптографічного перетворення забезпечує коректний синтез оберненого перетворення при відсутності негрупових операцій на основній діагоналі матриці групової операції. В теорії блочних матриць [8, 9] якщо матриця $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ – невироджена з квадратними блоками A і D, то з її невиродженості випливає, що $\det A \neq 0$ і $\det D \neq 0$, якщо ж навпаки, вважається виродженою і обернене перетворення для цієї матриці побудувати неможливо. Також не виконується рівність $AA^{-1} = A^{-1}A = \begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix}$ для оберненої матриці [8].

Висновок. У статті на основі узагальнення отриманих результатів розглянуто і теоретично обґрунтовано перевірку коректності запропонованої математичної моделі побудови прямого та оберненого двохоперандного групового матричного криптографічного перетворення за допомогою математичного апарату теорії блочних матриць. Знаходження оберненої матриці для двохоперандного групового матричного криптографічного перетворення за допомогою запропонованої моделі забезпечує зменшення складності обчислень.

Список літератури

1. Криптографическое кодирование: кол. монографія / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.
2. Бабенко В. Г., Мельник Р. П., Гончар С.В. Оцінка ефективності використання операцій криптографічного перетворення. *Вісник інженерної академії України.* Вип. 2. Київ, 2014. С. 39–41.
3. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография / под общ. ред. В. М. Без-рука, В. В. Баранника. Харьков: Лидер, 2017. 600 с.
4. Рудницький В. М., Сисоєнко С. В., Мельник О. Г., Пустовіт М. О. Дослідження методу підвищення стійкості комп'ютерних криптографічних алгоритмів. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. № 3. С. 5–10.
5. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації.* 2012. № 9 (107). С. 130–139.
6. Сисоєнко С. В., Мельник О. Г., Пустовіт М. О. Синтез операцій оберненого групового матричного криптографічного перетворення інформації. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2017. № 4. С. 118–125.
7. Сисоєнко С. В., Мельник О. Г. Дослідження операцій оберненого групового матричного криптографічного перетворення інформації. *Наука у контексті сучасних глобалізаційних процесів:* Міжнар. наук.-практ. конф. (19 листопада 2017 р.). Т. 10. Полтава, 2017. С. 44–46.
8. Наконечний С. І., Терещенко Т.О., Романюк Т. П. Економетрія: підручник. Вид. 3-тє, доп. та перероб. Київ: КНЕУ, 2004. 520 с.
9. Фадеев Д. К. Лекции по алгебре: учебное пособие для вузов. Москва: Наука, 1984. 416 с.
10. Гантмахер Ф. Р. Теория матриц. 5-е изд. Москва: Физматлит, 2004. 560 с.

References

1. Cryptographic coding (2014): a collective monograph under the ed. of V. N. Rudnitsky, V. Y. Milcevich. Kharkiv: Schedraya Usadba Plus, 240 p. [in Russian].
2. Babenko, V. G., Melnyk, R. P. and Gonchar, S.V. (2014) Evaluating the effectiveness of using cryptographic transformation operations. *Visnyk inghenernoyi akademiyi Ukrainy,* No. 2. Kyiv, pp. 39–41 [in Ukrainian].
3. High technologies in infocommunications: information processing, cybersecurity, information struggle (2017): monograph under the ed. of V. M. Bezruk, V. V. Barannyk. Kharkov: Lider, 600 p. [in Russian].
4. Rudnitsky, V. M., Sysoenko, S. V., Melnyk, O. G. and Pustovit, M. O. (2017) Investigation of the method of increasing the stability of computer cryptographic algorithms. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky,* No. 3, pp. 5–10 [in Ukrainian].
5. Babenko, V. G. and Rudnitsky, S. V. (2012) Realization of the method of information protection on the basis of matrix operations of cryptographic transformation. *Systemy obrobky informatsiyi,* No. 9 (107), pp. 130–139 [in Ukrainian].
6. Sysoenko, S. V, Melnyk, O. G. and Pustovit, M. O. (2017) Synthesis of operations of inverse group matrix cryptographic information transformation. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu. Seria: Tehnichni nauky,* No. 4, pp. 118–125 [in Ukrainian].
7. Sysoenko, S. V. and Melnyk, O. G. (2017) Investigation of operations of inverse group matrix cryptographic information transformation. *Nauka u konteksti suchasnyh hlobalizatsiynyh procesiv:* Internat. sci.-pract. conf. Vol. 10. Poltava, pp. 44–46 [in Ukrainian].
8. Nakonechny, S. I., Tereshchenko, T. O. and Romanyuk, T. P. (2004) Econometrics. 3rd ed. Kyiv: KNEU, 520 p. [in Ukrainian].
9. Fadeev, D. K. (1984) Lectures on algebra. Moscow: Nauka, 416 p. [in Russian].
10. Gantmacher, F. R. (2004) Theory of matrices. 5th ed. Moscow: Fizmatlit, 560 p. [in Russian].

Ye. V. Lanskykh, *Ph.D., associate professor,*
associate professor of the department of information security and computer engineering
e-mail: yevhenlanskykh@gmail.com,
S. V. Sysoienko, *assistant lecturer*
of the department of information security and computer engineering
e-mail: s.sysoienko@gmail.com,
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

STUDY OF MATHEMATICAL MODEL OF TWO-OPERAND GROUP MATRIX CRYPTOGRAPHIC TRANSFORMATION

The article considers and theoretically substantiates the results of checking the correctness of the proposed mathematical model for constructing a direct and inverse two-operand group matrix cryptographic transformation using mathematical apparatus of block matrix theory. According to the results of the research, the correctness of mathematical model for constructing an inverse group matrix cryptographic transformation has been established, which is tested on complete sets of group and non-group operations. The proposed model for constructing an inverse group matrix cryptographic transformation provides the correct synthesis of inverse transformation in the absence of non-group operations on the main diagonal of the matrix of group operation. The obtained results confirm the correct construction of inverse transformation on the basis of the proposed model, the implementation of which provides a reduction in the complexity of calculations. This result has shown the correctness of finding the inverse matrix with the help of proposed model.

Key words: *direct and inverse cryptographic transformation, two-operand cryptographic transformations, model correctness, matrix operation.*