УДК 004.056.55:004.312.2

С. В. Сисоєнко[1], *асистент*
кафедри інформаційної безпеки та комп'ютерної інженерії,
e-mail: s.sysoienko@gmail.com,
О. Г. Мельник[2], *к.т.н., ст. наук. співробітник,*
доцент кафедри будівельних конструкцій,
e-mail: melnyk.olja.2014@gmail.com,
М. О. Пустовіт[2], *старший викладач*
кафедри техніки та засобів цивільного захисту,
e-mail: m.pustovit@gmail.com.
[1] Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2] Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України
вул. Онопрієнка, 8, м. Черкаси, 18034, Україна

СИНТЕЗ ОПЕРАЦІЙ ОБЕРНЕНОГО ГРУПОВОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Одним із способів удосконалення існуючих та побудови нових систем захисту інформації є пошук та використання нових функцій криптографічного перетворення інформації. На сьогодні не достатньо вивчені операції оберненого групового матричного криптографічного перетворення інформації, що можуть застосовуватися для реалізації криптографічного кодування даних. В роботі досліджено можливість синтезу операцій оберненого перетворення на основі пошуку обернених групових та не групових дворозрядних операцій. Шляхом перебору даних перетворень знайдено алгоритм побудови оберненого групового криптографічного перетворення. За результатами досліджень формалізовано модель прямого та оберненого двохоперандного групового криптографічного перетворення. Запропонована модель забезпечує спрощення знаходження оберненого криптографічного перетворення, тому що для її реалізації необхідно знайти три обернених двохоперандних перетворення замість одного оберненого чотирьохоперандного перетворення.

Ключові слова: *криптографічне перетворення інформації, пряма та обернена операція, операція матричного перетворення, групові операції, коректність операції.*

Актуальність дослідження. З кожним днем об'єм інформації, що обертається в телекомунікаційних мережах, збільшується в геометричній прогресії. При цьому вона потребує все більш кращого захисту від несанкціонованого доступу, що може призвести до її спотворення або викрадення [1]. Захист даних за допомогою методів криптографічного захисту інформації – одне з можливих рішень проблеми безпеки інформації [2].

Актуальним питанням сьогодення є вдосконалення існуючих та пошук нових функцій криптографічного перетворення інформації, що дозволять покращити властивості самих криптоалгоритмів та підвищити стійкість систем захисту інформації.

Вищевикладене зумовило актуальність досліджень, спрямованих на більш детальне дослідження операцій оберненого групового матричного криптографічного перетворення інформації, що можуть застосовуватися для реалізації криптографічного кодування даних.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень і публікацій варто виділити наукові праці, в яких досліджувався метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення [3-5]; в яких розглядалося питання підвищення якості псевдовипадкової послідовності [6, 7]; в яких доведено, що використання матричних операцій криптографічного перетворення в поєднанні з груповими операціями криптографічного перетворення забезпечує підвищення якості шифрування (отриманої псевдовипадкової послідовності), а також забезпечує можливість розшифрування інформації, тому що забезпечує використання умови отримання невироджено-

го перетворення [8], та роботу, в якій було вивчено питання підвищення стійкості комп'ютерних криптографічних алгоритмів за рахунок використання операцій криптоперетворення та алгоритмів криптографічного перетворення двох блоків змінних [9].

Проте в даних дослідженнях не достатньо вивчено питання щодо можливості синтезу операцій оберненого перетворення на основі пошуку обернених групових та не групових дворозрядних операцій.

Мета статті полягає в дослідженні можливості побудови оберненого групового криптографічного перетворення, якщо відоме пряме групове перетворення, та формалізації моделі прямого та оберненого двохоперандного групового криптографічного перетворення.

Виклад основного матеріалу. Дослідимо можливість побудови оберненого групового криптографічного перетворення, якщо відоме пряме групове перетворення.

В [9] для перевірки невиродженості результатів виконання групових операцій криптографічного перетворення інформації використовували метод синтезу матричних операцій оберненого криптографічного перетворення.

Проте при використанні дворозрядних групових операцій відповідно до розглянутих прикладів необхідно знаходити чотирирозрядну матрицю оберненого перетворення. Дослідимо можливість синтезу операцій оберненого перетворення на основі пошуку обернених групових та не групових дворозрядних операцій. Знаходження даних закономірностей приведе до значного зменшення обчислювальної складності розшифрування інформації.

Для побудови оберненого групового криптографічного перетворення, якщо відоме пряме групове перетворення, використаємо прямі та обернені групові й не групові перетворення. Шляхом перебору даних перетворень знайдемо алгоритм побудови оберненого групового криптографічного перетворення, якщо він існує.

При проведенні досліджень необхідно розглянути наступні випадки:

1. Пряма та обернена групова операція співпадають, пряма та обернена не групові операції співпадають.

2. Пряма та обернена групова операція співпадають, пряма та обернена не групові операції не співпадають.

3. Пряма та обернена групова операція не співпадають, пряма та обернена не групові операції співпадають.

4. Пряма та обернена групова операція не співпадають, пряма та обернена не групові операції не співпадають.

Розглянемо перший випадок, коли пряма та обернена групова операція співпадають, пряма та обернена не групові операції співпадають.

Нехай $G = G_{3,6}^k = G_{3,6}^d$,

$F_1 = F_2 = F_{3,6}^k = F_{3,6}^d$, тоді:

$$G_{3,6}^k = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{3,6}^k(z_1) \\ F_{3,6}^k(z_1) \oplus F_{3,6}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1.1} \\ z_{1.1} \oplus z_{1.2} \\ z_{1.1} \oplus z_{2.1} \\ z_{1.1} \oplus z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \end{bmatrix}.$$

Тоді

$$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{3,6}^d(w_1) \\ F_{3,6}^d(w_1) \oplus F_{3,6}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1.1} \\ w_{1.1} \oplus w_{1.2} \\ w_{1.1} \oplus w_{2.1} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G_{3,6}^d = \begin{bmatrix} w_{1.1} \\ w_{1.1} \oplus w_{1.2} \\ w_{1.1} \oplus w_{2.1} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \end{bmatrix} =$$

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

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

Так як підтверджено коректність оберненої операції, то будуть справедливими наступні твердження.

Якщо $G^k_{3,6}=\begin{bmatrix}F^k_{3,6}(z_1)\\ F^k_{3,6}(z_1)\oplus F^k_{3,6}(z_2)\end{bmatrix}$, то $G^d_{3,6}=\begin{bmatrix}F^d_{3,6}(w_1)\\ F^d_{3,6}(w_1)\oplus F^d_{3,6}(w_2)\end{bmatrix}$

або $G^d_{3,6}=\left(G^k_{3,6}=\begin{bmatrix}F^k_{3,6}(z_1)\\ F^k_{3,6}(z_1)\oplus F^k_{3,6}(z_2)\end{bmatrix}\right)$,

або $G^d_{3,6}=\left(G^k_{3,6}=\begin{bmatrix}F^d_{3,6}(w_1)\\ F^d_{3,6}(w_1)\oplus F^d_{3,6}(w_2)\end{bmatrix}\right)$,

або $G^d_{3,6}=\left(G^d_{3,6}=\begin{bmatrix}F^d_{3,6}(w_1)\\ F^k_{3,6}(z_1)\oplus F^k_{3,6}(z_2)\end{bmatrix}\right)$,

або $G^d_{3,6}=\left(G^d_{3,6}=\begin{bmatrix}F^k_{3,6}(z_1)\\ F^k_{3,6}(z_1)\oplus F^k_{3,6}(z_2)\end{bmatrix}\right)$,

або і т.п.

Виходячи з отриманого результату, можна констатувати, що при співпаданні прямого та оберненого перетворення для декодування інформації необхідно брати обернені (прямі) операції криптоперетворення та обернені (прямі) групові операції перетворення.

Нехай $G=G^k_{6,5}=G^d_{6,5}$, $F_1=F_2=F^k_{6,5}=F^d_{6,5}$.

$$G^k_{6,5}=\begin{bmatrix}F_1\oplus F_2\\ F_2\end{bmatrix}=\begin{bmatrix}F^k_{6,5}(z_1)\oplus F^k_{6,5}(z_2)\\ F^k_{6,5}(z_2)\end{bmatrix}=$$

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

Тоді

$$G^d_{6,5}=\begin{bmatrix}F_1\oplus F_2\\ F_2\end{bmatrix}=\begin{bmatrix}F^k_{6,5}(w_1)\oplus F^k_{6,5}(w_2)\\ F^k_{6,5}(w_2)\end{bmatrix}=$$

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

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G^d_{6,5}=\begin{bmatrix}w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2}\\ w_{1.2}\oplus w_{2.2}\\ w_{2.1}\oplus w_{2.2}\\ w_{2.2}\end{bmatrix}=$$

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

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

Перевірка даного факту на повній множині симетричних операцій підтвердила коректність зробленого висновку.

Нехай $G=G^k_{6,5}=G^d_{6,5}$, $F_1=F^k_{6,5}=F^d_{6,5}$, $F_2=F^k_{3,6}=F^d_{3,6}$.

Тоді

$$G^k_{6,5}=\begin{bmatrix}F_1\oplus F_2\\ F_2\end{bmatrix}=\begin{bmatrix}F^k_{6,5}(z_1)\oplus F^k_{3,6}(z_2)\\ F^k_{3,6}(z_2)\end{bmatrix}=\begin{bmatrix}z_{1.1}\oplus z_{1.2}\oplus z_{2.1}\\ z_{1.2}\oplus z_{2.1}\oplus z_{2.2}\\ z_{2.1}\\ z_{2.1}\oplus z_{2.2}\end{bmatrix}.$$

Тоді

$$G^d_{6,5}=\begin{bmatrix}F_1\oplus F_2\\ F_2\end{bmatrix}=\begin{bmatrix}F^d_{6,5}(w_1)\oplus F^d_{3,6}(w_2)\\ F^d_{3,6}(w_2)\end{bmatrix}=\begin{bmatrix}w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\\ w_{1.2}\oplus w_{2.1}\oplus w_{2.2}\\ w_{2.1}\\ w_{2.1}\oplus w_{2.2}\end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G^d_{6,5}=\begin{bmatrix}w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\\ w_{1.2}\oplus w_{2.1}\oplus w_{2.2}\\ w_{2.1}\\ w_{2.1}\oplus w_{2.2}\end{bmatrix}=$$

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

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

Обернене перетворення побудовано за умови

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{6,5}^d(w_1) \oplus F_{3,6}^d(w_2) \\ F_{6,5}^d(w_1) \end{bmatrix} \right) \text{ не коректне.}$$

Отриманий не коректний результат можна розглядати як виняток з правила, робити висновок про хибність даного підходу можна лише тоді, коли буде повторно виявлено не коректність даного підходу.

Розглянемо другий випадок коли пряма та обернена групова операція співпадають, пряма та обернена не групові операції не співпадають.

Нехай $G = G_{3,6}^k = G_{3,6}^d$, $F_1 = F_{5,6}^k \neq F_{6,3}^d$,

$F_2 = F_{6,5}^k = F_{6,5}^d$.

$$G_{3,6}^k = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^k(z_2) \end{bmatrix} = \begin{bmatrix} z_{1.2} \\ z_{1.1} \oplus z_{1.2} \\ z_{1.2} \oplus z_{2.1} \oplus z_{2.2} \\ z_{1.1} \oplus z_{1.2} \oplus z_{2.2} \end{bmatrix}.$$

Тоді

$$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{6,3}^d(w_1) \\ F_{6,3}^d(w_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1.1} \oplus w_{1.2} \\ w_{1.1} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.1} \oplus w_{2.2} \end{bmatrix}.$$

Підставивши результати прямого перетворення в операцію оберненого перетворення, отримаємо:

$$G_{3,6}^d = \begin{bmatrix} w_{1.1} \oplus w_{1.2} \\ w_{1.1} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.1} \oplus w_{2.2} \end{bmatrix} =$$

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

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

Обернене перетворення побудовано за умови

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{6,3}^d(w_1) \\ F_{6,3}^d(w_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} \right) \text{ не коректне.}$$

Розглянемо можливість побудови оберненого групового перетворення на основі використання прямих і обернених перетворень. Так як $G_{3,6}^d = G_{3,6}^k$, то необхідно розглянути:

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} \right).$$

$$G_{3,6}^d = \begin{bmatrix} F_1 \\ F_1 \oplus F_2 \end{bmatrix} = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} = \begin{bmatrix} w_{1.2} \\ w_{1.1} \oplus w_{1.2} \\ w_{1.2} \oplus w_{2.1} \oplus w_{2.2} \\ w_{1.1} \oplus w_{1.2} \oplus w_{2.2} \end{bmatrix} =$$

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

Обернене перетворення не коректне.

Дослідження можливості побудови оберненого групового перетворення на основі використання прямих і обернених перетворень для випадків:

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{6,3}^d(w_1) \\ F_{5,6}^k(z_1) \oplus F_{6,5}^k(z_2) \end{bmatrix} \right) \text{ та}$$

$$G_{3,6}^d = \left(G_{3,6}^d = \begin{bmatrix} F_{5,6}^k(z_1) \\ F_{6,3}^d(w_1) \oplus F_{6,5}^d(w_2) \end{bmatrix} \right),$$

також показали їх некоректність. Шляхом перебору прямих та обернених групових і не групових перетворень побудувати обернене групове криптографічне перетворення для всіх випадків не вдалося.

Спробуємо для відомого групового криптографічного перетворення по аналогії з [10] знайти обернене перетворення і привести його до оберненого групового криптографічного перетворення.

Якщо $G = G_{3,6}^k = G_{3,6}^d$, $F_1 = F_{6,5}^k = F_{6,5}^d$, $F_2 = F_{5,6}^k \neq F_{6,3}^d$.

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

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

Тоді

$$G_{3,6}^d=\begin{bmatrix} w_{1.1}\oplus w_{1.2} \\ w_{1.2} \\ w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2} \\ w_{1.1}\oplus w_{2.1} \end{bmatrix}=\begin{bmatrix} F_{6,5}^d(w_1) \\ F_{6,3}^d(w_1)\oplus F_{6,3}^d(w_2) \end{bmatrix}=$$

$$=\begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1)\oplus F_2^d(w_2) \end{bmatrix}.$$

Перевіримо коректність отриманого оберненого перетворення:

$$G_{3,6}^d=\begin{bmatrix} F_1^d(w_1) \\ F_2^d(w_1)\oplus F_2^d(w_2) \end{bmatrix}=\begin{bmatrix} w_{1.1}\oplus w_{1.2} \\ w_{1.2} \\ w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2} \\ w_{1.1}\oplus w_{2.1} \end{bmatrix}=$$

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

Обернене перетворення отримано коректно.

Перевірка обернених перетворень для випадків:

1) $G=G_{3,6}^k=G_{3,6}^d$, $F_1=F_{5,6}^k\neq F_{6,3}^d$, $F_2=F_{6,5}^k=F_{6,5}^d$;

2) $G=G_{3,6}^k=G_{3,6}^d$, $F_1=F_{5,6}^k\neq F_{6,3}^d$, $F_2=F_{6,3}^k\neq F_{5,6}^d$ також показала їх коректність.

Розглянемо третій випадок, коли пряма та обернена групова операція не співпадають, пряма та обернена не групові операції співпадають.

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

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

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

Тоді

$$G_{6,3}^d=\begin{bmatrix} w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2} \\ w_{1.2}\oplus w_{2.2} \\ w_{1.1} \\ w_{1.1}\oplus w_{1.2} \end{bmatrix}=\begin{bmatrix} F_{6,5}^d(w_1)\oplus F_{6,5}^d(w_2) \\ F_{3,6}^d(w_1) \end{bmatrix}=$$

$$=\begin{bmatrix} F_1^d(w_1)\oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix}.$$

Перевіримо коректність отриманого оберненого перетворення:

$$G_{6,3}^d=\begin{bmatrix} F_1^d(w_1)\oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix}=\begin{bmatrix} w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2} \\ w_{1.2}\oplus w_{2.2} \\ w_{1.1} \\ w_{1.1}\oplus w_{1.2} \end{bmatrix}=$$

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

Обернене перетворення отримано коректно.

Перевірка оберненого перетворення для випадку: $G=G_{6,3}^k\neq G_{5,6}^d$, $F_1=F_{3,6}^k=F_{3,6}^d$, $F_2=F_{6,5}^k=F_{6,5}^d$ також показала його коректність.

Розглянемо четвертий випадок, коли пряма та обернена групова операція не співпадають, пряма та обернена не групові операції не співпадають.

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

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

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

Тоді

$$G_{6,3}^d=\begin{bmatrix} w_{1.2}\oplus w_{2.2} \\ w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2} \\ w_{1.1}\oplus w_{1.2} \\ w_{1.1} \end{bmatrix}=\begin{bmatrix} F_{5,6}^d(w_1)\oplus F_{5,6}^d(w_2) \\ F_{6,3}^d(w_1) \end{bmatrix}=$$

$$=\begin{bmatrix} F_1^d(w_1)\oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix}.$$

Перевіримо коректність отриманого оберненого перетворення:

$$G_{6,3}^d=\begin{bmatrix} F_1^d(w_1)\oplus F_1^d(w_2) \\ F_2^d(w_1) \end{bmatrix}=\begin{bmatrix} w_{1.2}\oplus w_{2.2} \\ w_{1.1}\oplus w_{1.2}\oplus w_{2.1}\oplus w_{2.2} \\ w_{1.1}\oplus w_{1.2} \\ w_{1.1} \end{bmatrix}=$$

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

Обернене перетворення отримано коректно.

Дослідження оберненого перетворення для випадку: $G = G^k_{5,6} \neq G^d_{6,3}$, $F_1 = F^k_{5,6} \neq F^d_{6,3}$, $F_2 = F^k_{6,3} \neq F^d_{5,6}$ також показало його коректність.

Отримані результати дозволяють узагальнити результати дослідження та формалізувати модель прямого та оберненого двохоперандного групового криптографічного перетворення.

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

тоді $G^d = \begin{pmatrix} b_{11}F_1^d(w_{1+k}) \oplus b_{12}F_1^d(w_{2+k}) \\ b_{21}F_2^d(w_{1+k}) \oplus b_{22}F_2^d(w_{2+k}) \end{pmatrix}$,

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 не групових двохоперандних криптографічних перетворень; F_i^d – операції обернених не групових двохоперандних криптографічних перетворень; $\oplus$ – операція «сума за mod 2»; k – коефіцієнт вибору аргумента функції: $w_i = \begin{cases} w_i & якщо \quad k = 0 \\ w_j & якщо \quad k = 1 \end{cases}$ за умови, що $j \neq i$. I, j – номер аргументу, а коефіцієнт визначено з: $k = \begin{cases} 0 & якщо \quad G^k = G^d \\ 1 & якщо \quad G^k \neq G^d \end{cases}$.

Висновок. Запропонована модель забезпечує спрощення знаходження оберненого криптографічного перетворення, тому що для її реалізації необхідно знайти три обернених двохоперандних перетворення замість одного оберненого чотирьохоперандного перетворення.

Список літератури

1. Богуш В. М., Юдін О. К. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.
2. Рудницкий В. Н., Мильчевич В. Я., Бабенко В. Г., Мельник Р. П., Рудницкий С. В., Мельник О. Г. Криптографическое кодирование: методы и средства реализации (часть 2) : монография. Краснодар, 2014. 224 с.
3. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. *Захист інформації: наук.-практ. журнал.* 2012. № 3 (56). С. 50–56.
4. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.
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. Фауре Е. В., Сисоєнко С. В., Миронюк Т.В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. *Системи управління, навігації та зв'язку.* 2015. № 4 (36). С. 85–87.
7. Рудницький В. М., Фауре Е. В., Сисоєнко С. В. Оцінка якості псевдовипадкових послідовностей на основі додавання за модулем. *Вісник інженерної академії України*. 2016. № 3. С. 219–221.
8. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: монография / под общ. ред. В. М. Безрука, В. В. Баранника. Харьков: Лидер, 2017. 600 с.
9. Сисоєнко С. В., Мельник О. Г. Використання операцій та алгоритмів криптоперетворення двох блоків змінних в криптографії. *Інноваційні тенденції сьогодення в сфері природничих, гуманітарних та точних наук:* мат-ли міжнар. наук.-практ. конф. (17 жовтня 2017 р.). Івано-Франківськ, 2017. С. 47–49.
10. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил.* 2012. Вип. 4 (33), С. 198–200.

References

1. Bogush, V. M. and Yudin, O. K. (2005) Information security of the state. Kyiv : MK-Pres, 432 p. [in Ukrainian].
2. Rudnytskyy, V. N., Mylchevych, V. Y., Babenko, V. G., Melnyk, R. P., Rudnytskyy, S. V. and Melnyk, O. G. (2014) Cryptographic coding: methods and means of realization (part 2): monograph. Krasnodar, 224 p. [in Russian].
3. Rudnytskyy, V. M., Babenko, V. G. and Rudnytskyy, S. V. (2012) Method of synthesis of matrix models of operations of cryptographic information reencoding. *Zaxyst informaciyi: nauk.-prakt. zhurnal,* No. 3 (56), pp. 50–56 [in Ukrainian].
4. Rudnytskyy, V. M., Babenko, V. G. and Rudnytskyy, S. V. (2012) Method of synthesis of matrix models of operations of cryptographic encoding and decoding of information. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl,* No. 4 (33), pp. 198–200 [in Ukra-inian].
5. Babenko, V. G. and Rudnytskyy, S. V. (2012) Realization of the method of information protection on the basis of matrix operations of cryptographic transformation. *Systemy obrobky informatsii,* No. 9 (107), pp. 130–139 [in Ukrainian].
6. Faure, E. V., Sysoyenko, S. V. and Myronyuk, T. V. (2015) Synthesis and analysis of pseudorandom sequences based on cryptographic transformation operations. *Systemy upravlinnya, navihatsiyi ta zvyazku,* No. 4 (36), pp. 85–87 [in Ukrainian].
7. Rudnytskyy, V. M., Faure, E. V. and Sysoyenko, S. V. (2016) Assessing the quality of pseudorandom sequences based on the addition of a module. *Visnyk inzhenernoyi akademiyi Ukrayiny,* No. 3, pp. 219–221 [in Ukrainian].
8. High technology in infocommunications: information processing, cybersecurity, information struggle: monograph / pod obshchey red. V. M. Bezruka, V. V. Barannyka. Kharkov: Lyder, 2017, 600 p. [in Ukrainian].
9. Sysoyenko, S. V. and Melnyk, O. G. (2017) Using of the operations and algorithms of cryptographic transformation of two blocks of variables in cryptography. *Innovatsiyni tendentsiyi sohodennya v sferi pryrodnychykh, humanitarnykh ta tochnykh nauk:* mat-ly mizhnar. nauk.-prakt. konf., (17 zhovtnya 2017 r.). Ivano-Frankivsk, pp. 47–49 [in Ukrainian].
10. Rudnytskyy, V. M., Babenko, V. G. and Rudnytskyy, S. V. (2012) Method of synthesis of matrix models of operations of cryptographic encoding and decoding of information. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitryanykh Syl*, No. 4 (33), pp. 198–200 [in Ukrainian].

S. V. Sysoyenko,
Department of Information Security and Computer Engineering, Assistant
e-mail: s.sysoienko@gmail.com,
O. G. Melnyk, *Ph.D., Senior Researcher,*
Department of Building Constructions, Associate professor,
e-mail: melnyk.olja.2014@gmail.com
M. O. Pustovit,
Department of Engineering and Civil Defense Equipment, Senior lecturer,
e-mail: m.pustovit@gmail.com.
[1] Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine
[2] Cherkasy Institute of Fire Safety named after
Chornobyl Heroes of National University of Civil Protection of Ukraine,
Onoprienko Str., 8, Cherkasy, 18034, Ukraine

SYNTHESIS OF OPERATIONS OF REVERSE GROUP MATRIX CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION

One way to improve existing and build new information security systems is to find and use new functions of cryptographic transformation of information. At present, operations of inverse group ma-

trix cryptographic transformation of information, which can be used to implement cryptographic data coding, are not sufficiently studied. The possibility of synthesizing inverse transformation operations based on the search for inverse group and non-group two-bit operations is investigated. By looking through the transformation data, an algorithm for constructing an inverse group cryptographic transformation was found. Based on the research results, the model of direct and inverse two-operand group cryptographic transformation is formalized. The proposed model provides a simplification of finding the reverse cryptographic transformation, since for its implementation it is necessary to find three inverse two-operand transformations instead of one inverse four-operand transformation.

Keywords: *cryptographic transformation of information, direct and reverse operation, operation of matrix transformation, group operations, correctness of operation.*

Рецензенти: Рудницький В. М., д.т.н., професор,
Кириченко О. В., д.т.н., с.н.с.