УДК 003.26:004.056.55

Т. В. Миронюк, *старший викладач*
Черкаський державний технологічний університет,
б-р Шевченка, 460, м. Черкаси, 18006, Україна
e-mail: tanjamiron85@gmail.com

ВИЗНАЧЕННЯ ЕЛЕМЕНТАРНИХ ОПЕРАЦІЙ БАЗОВОЇ ГРУПИ ПЕРЕСТАНОВОК, КЕРОВАНИХ ІНФОРМАЦІЄЮ

В статті представлені результати дослідження базових операцій криптоперетворення, що утворюють базову групу операцій перестановок, керованих інформацією. За результатами проведеного обчислювального експерименту було отримано базову групу операцій перестановок, керованих інформацією, та побудовано для неї дискретні моделі представлення операцій. У ході аналізу одержаних результатів експерименту виявлено залежності для основних елементів операцій та визначено, що базову групу операцій криптографічного перетворення можуть утворювати лише ті операції криптографічного перетворення, в яких значення основних елементів по діагоналі дорівнює 2^3 варіантам.

Ключові слова: *базова операція, група базових операцій перестановок, керована інформацією, дискретна модель, матриця інверсії, матриця доповнення, основний елемент.*

Постановка проблеми. Протягом багатьох років криптографія слугувала виключно військовим цілям. Сьогодні звичайні користувачі отримали можливість звертатися до засобів, які дозволяють їм захистити себе від несанкціонованого доступу до конфіденційної інформації, застосовуючи методи комп'ютерної криптографії.

Захист інформації за допомогою шифрування є одним із найнадійніших шляхів вирішення її безпеки, оскільки зашифрована інформація стає доступною лише для того, хто знає, як її розшифрувати, і абсолютно безглуздою для несанкціонованого користувача.

У цій статті обмежимося дослідженням синтезу лише однієї базової групи трирозрядних елементарних операцій перестановки, керованих інформацією, для криптографічного перетворення.

Аналіз останніх досліджень. Серед останніх досліджень і публікацій варто виділити: [1], де проведено класифікацію трирозрядних елементарних функцій для криптографічного перетворення інформації; [2], де проведено синтез множин моделей спеціалізованих трирозрядних логічних функцій і здійснено групування моделей трирозрядних логічних функцій для криптографічного перетворення за обраними критеріями; [3], де виведено твердження для елементарних функцій перестановок, керованих інформацією; [4], де для подальшого дослідження визначено групу елементарних функцій мінімальної складності; [5], де отримано визначення для прямих та інверсних елементарних функцій, керованих інформацією, визначено базові операції та базові групи операцій для криптографічного перетворення.

Проте в цих дослідженнях не вивчалася можливість практичної реалізації базових операцій перестановок, керованих інформацією.

Метою дослідження є визначення та аналіз елементарних операцій базової групи операцій перестановок, керованих інформацією.

Виклад основного матеріалу. Для виділення та отримання з визначених базовими операцій криптографічного перетворення базових груп скористаємося обчислювальним експериментом.

Для цього наведемо як приклад експериментально отриману базову групу операцій криптоперетворення для кодування та декодування функцій у вигляді табл. 1.

Представлена в табл. 1 група операцій є прикладом базової групи операцій криптографічного перетворення для кодування та декодування, визначеної внаслідок обчислювального експерименту.

Повна множина базових груп операцій криптографічного перетворення, визначених внаслідок обчислювального експерименту, які утворюють математичну групу операцій, становить 764 базові групи операцій.

Таблиця 1

Базова група операцій криптографічного перетворення

Група операцій									
	кодування	92 46 27	53 71 27	83 29 39	58 29 78	58 116 39	53 46 114	92 71 114	83 116 78
	декодування	83 116 78	83 29 39	53 71 27	53 46 114	92 71 114	58 29 78	58 116 39	92 46 27

Кожна визначена базова група операцій криптографічного перетворення має свій порядковий номер, а елементарні операції для кодування та декодування, що відповідають базовим групам операцій, позначені кодами функцій [4].

Для подальших досліджень трирозрядних операцій криптографічного перетворення представимо основні елементарні функції у такому вигляді [6]:

$f_m^{(1)}(x_1, x_2, x_3)$, $f_m^{(2)}(x_1, x_2, x_3)$, $f_m^{(3)}(x_1, x_2, x_3)$ – це функції перетворення першого, другого та третього розряду інформації відповідно, що являють собою дискретні логічні функції; m – це код функції перетворення, що застосовується; x_1, x_2, x_3 – значення першого, другого, третього розрядів інформації відповідно.

Відомо, що $x_1, x_2, x_3 \in \{0;1\}$, а відповідно і значення дискретних логічних функцій

$$f_m^{(1)}, f_m^{(2)}, f_m^{(3)} \in \{0;1\}.$$

Оскільки операції криптографічного перетворення синтезуються на основі вибраних елементарних функцій, то їх можна представити у вигляді композиції відповідних функцій перетворення:

$$F_{1,2,3} = \left(f_m^{(1)}, f_m^{(2)}, f_m^{(3)}\right).$$

Звідси випливає, що елементарні функції $f_m^{(1)}, f_m^{(2)}, f_m^{(3)}$ утворюють операцію криптографічного перетворення.

Виконавши дослідження операцій криптографічного перетворення, з яких утворюється базова група операцій криптографічного перетворення, було визначено, що множину елементарних функцій, які утворюють операції, можливо використовувати як для перетворення, так і для оберненого перетворення відповідно. Надалі будемо називати такі відповідні пари криптографічною операцією перетворення F^k та криптографічною операцією оберненого перетворення F^d інформації відповідно.

Представимо, відповідно до визначених позначень, базові групи операцій криптографічного перетворення в явному вигляді.

Розглянемо представлену в табл. 1, визначену внаслідок обчислювального експерименту групу операцій криптоперетворення в такому вигляді:

1. $F^k_{92,46,27} = (f^{(1)}_{92}, f^{(2)}_{46}, f^{(3)}_{27}) \Rightarrow F^d_{83,116,78} = (f^{(1)}_{83}, f^{(2)}_{116}, f^{(3)}_{78})$
2. $F^k_{53,71,27} = (f^{(1)}_{53}, f^{(2)}_{71}, f^{(3)}_{27}) \Rightarrow F^d_{83,29,39} = (f^{(1)}_{83}, f^{(2)}_{29}, f^{(3)}_{39})$
3. $F^k_{83,29,39} = (f^{(1)}_{83}, f^{(2)}_{29}, f^{(3)}_{39}) \Rightarrow F^d_{53,71,27} = (f^{(1)}_{53}, f^{(2)}_{71}, f^{(3)}_{27})$
4. $F^k_{58,29,78} = (f^{(1)}_{58}, f^{(2)}_{29}, f^{(3)}_{78}) \Rightarrow F^d_{53,46,114} = (f^{(1)}_{53}, f^{(2)}_{46}, f^{(3)}_{114})$
5. $F^k_{58,116,39} = (f^{(1)}_{58}, f^{(2)}_{116}, f^{(3)}_{39}) \Rightarrow F^d_{92,71,114} = (f^{(1)}_{92}, f^{(2)}_{71}, f^{(3)}_{114})$
6. $F^k_{53,46,114} = (f^{(1)}_{53}, f^{(2)}_{46}, f^{(3)}_{114}) \Rightarrow F^d_{58,29,78} = (f^{(1)}_{58}, f^{(2)}_{29}, f^{(3)}_{78})$

7. $F^k_{92,71,114} = (f^{(1)}_{92}, f^{(2)}_{71}, f^{(3)}_{114}) \Rightarrow F^d_{58,116,39} = (f^{(1)}_{58}, f^{(2)}_{116}, f^{(3)}_{39})$
8. $F^k_{83,116,78} = (f^{(1)}_{83}, f^{(2)}_{116}, f^{(3)}_{78}) \Rightarrow F^d_{92,46,27} = (f^{(1)}_{92}, f^{(2)}_{46}, f^{(3)}_{27})$

Якщо розписати кожну елементарну функцію операції, то отримаємо дискретну модель представлення криптографічних операцій, що матиме такий вигляд:

$$F^k_{92,46,27} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix} \Rightarrow F^d_{83,116,78} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}, \quad (1)$$

$$F^k_{53,71,27} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix} \Rightarrow F^d_{83,29,39} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}, \quad (2)$$

$$F^k_{83,29,39} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix} \Rightarrow F^d_{53,71,27} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix}, \quad (3)$$

$$F^k_{58,29,78} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix} \Rightarrow F^d_{53,46,114} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}, \quad (4)$$

$$F^k_{58,116,39} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix} \Rightarrow F^d_{92,71,114} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}, \quad (5)$$

$$F^k_{53,46,114} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix} \Rightarrow F^d_{58,29,78} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix}, \quad (6)$$

$$F^k_{92,71,114} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix} \Rightarrow F^d_{58,116,39} = \begin{bmatrix} \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 \end{bmatrix}, \quad (7)$$

$$F^k_{83,116,78} = \begin{bmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{bmatrix} \Rightarrow F^d_{92,46,27} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{bmatrix}. \quad (8)$$

Однак для визначення базових груп операцій криптографічного перетворення представлені за допомогою такої дискретної моделі елементарні операції є складними для розуміння. Тому, представимо визначені операції криптографічного перетворення за допомогою дискретної моделі, яка утворюється поєднанням матриць перестановки й доповнення. Значення основного розряду інформації елементарної функції для такого типу дискретної моделі визначається за станом, в якому він знаходиться в першому розряді елементарної функції.

Для подальшого дослідження представимо групу операцій для криптоперетворення за допомогою дискретної моделі, що представляється у вигляді поєднання двох матриць (матриці перестановок та матриці доповнення).

$$F^k_{92,46,27} = \begin{bmatrix} \underline{1}\ 0\ 1 \\ 1\ \underline{0}\ 0 \\ 1\ 1\ \underline{0} \end{bmatrix} \Rightarrow F^d_{83,116,78} = \begin{bmatrix} \underline{1}\ 1\ 1 \\ 0\ \underline{1}\ 1 \\ 1\ 0\ \underline{0} \end{bmatrix}, \quad (9)$$

$$F^k_{53,71,27} = \begin{bmatrix} \underline{0}\ 1\ 1 \\ 1\ \underline{1}\ 1 \\ 1\ 1\ \underline{0} \end{bmatrix} \Rightarrow F^d_{83,29,39} = \begin{bmatrix} \underline{1}\ 1\ 1 \\ 1\ \underline{0}\ 1 \\ 1\ 1\ \underline{1} \end{bmatrix}, \quad (10)$$

$$F^k_{83,29,39} = \begin{bmatrix} \underline{1}\ 1\ 1 \\ 1\ \underline{0}\ 1 \\ 1\ 1\ \underline{1} \end{bmatrix} \Rightarrow F^d_{53,71,27} = \begin{bmatrix} \underline{0}\ 1\ 1 \\ 1\ \underline{1}\ 1 \\ 1\ 1\ \underline{0} \end{bmatrix}, \quad (11)$$

$$F^k_{58,29,78} = \begin{bmatrix} \underline{0}\ 1\ 0 \\ 1\ \underline{0}\ 1 \\ 1\ 0\ \underline{0} \end{bmatrix} \Rightarrow F^d_{53,46,114} = \begin{bmatrix} \underline{0}\ 1\ 1 \\ 1\ 0\ 0 \\ 0\ 1\ \underline{1} \end{bmatrix}, \quad (12)$$

$$F^k_{58,116,39} = \begin{bmatrix} \underline{0}\ 1\ 0 \\ 0\ \underline{1}\ 1 \\ 1\ 1\ \underline{1} \end{bmatrix} \Rightarrow F^d_{92,71,114} = \begin{bmatrix} \underline{1}\ 0\ 1 \\ 1\ \underline{1}\ 1 \\ 0\ 1\ \underline{1} \end{bmatrix}, \quad (13)$$

$$F^k_{53,46,114} = \begin{bmatrix} \underline{0}\ 1\ 1 \\ 1\ \underline{0}\ 0 \\ 0\ 1\ \underline{1} \end{bmatrix} \Rightarrow F^d_{58,29,78} = \begin{bmatrix} \underline{0}\ 1\ 0 \\ 1\ \underline{0}\ 1 \\ 1\ 0\ \underline{0} \end{bmatrix}, \quad (14)$$

$$F^k_{92,71,114} = \begin{bmatrix} \underline{1}\ 0\ 1 \\ 1\ \underline{1}\ 1 \\ 0\ 1\ \underline{1} \end{bmatrix} \Rightarrow F^d_{58,116,39} = \begin{bmatrix} \underline{0}\ 1\ 0 \\ 0\ \underline{1}\ 1 \\ 1\ 1\ \underline{1} \end{bmatrix}, \quad (15)$$

$$F^k_{83,116,78} = \begin{bmatrix} \underline{1}\ 1\ 1 \\ 0\ \underline{1}\ 1 \\ 1\ 0\ \underline{0} \end{bmatrix} \Rightarrow F^d_{92,46,27} = \begin{bmatrix} \underline{1}\ 0\ 1 \\ 1\ \underline{0}\ 0 \\ 1\ 1\ \underline{0} \end{bmatrix}, \quad (16)$$

де $\underline{0}$ *або* $\underline{1}$ – значення основного елемента елементарної операції в прямому або інверсному значенні; 0 або 1 – значення додаткового елемента елементарної операції, який знаходиться в прямому значенні, що позначено «1», або інверсному значенні, що відповідає «0».

Розглянувши базову групу операцій криптографічного перетворення, представлену вище у вигляді дискретної моделі, було визначено наступні залежності для основних елементів операцій:

$$F^k_{92,46,27} = x_1 = 1, x_2 = 0, x_3 = 0 \Rightarrow F^d_{83,116,78} = x_1 = 1, x_2 = 1, x_3 = 0,$$

$$F^k_{53,71,27} = x_1 = 0, x_2 = 1, x_3 = 0 \Rightarrow F^d_{83,29,39} = x_1 = 1, x_2 = 0, x_3 = 1,$$

$$F^k_{83,29,39} = x_1 = 1, x_2 = 0, x_3 = 1 \Rightarrow F^d_{53,71,27} = x_1 = 0, x_2 = 1, x_3 = 0,$$

$$F^k_{58,29,78} = x_1 = 0, x_2 = 0, x_3 = 0 \Rightarrow F^d_{53,46,114} = x_1 = 0, x_2 = 0, x_3 = 1,$$

$$F^k_{58,116,39} = x_1 = 0, x_2 = 1, x_3 = 1 \Rightarrow F^d_{92,71,114} = x_1 = 1, x_2 = 1, x_3 = 1,$$

$$F^k_{53,46,114} = x_1 = 0, x_2 = 0, x_3 = 1 \Rightarrow F^d_{58,29,78} = x_1 = 0, x_2 = 0, x_3 = 0,$$

$$F^k_{92,71,114} = x_1 = 1, x_2 = 1, x_3 = 1 \Rightarrow F^d_{58,116,39} = x_1 = 0, x_2 = 1, x_3 = 1,$$

$$F^k_{83,116,78} = x_1 = 1, x_2 = 1, x_3 = 0 \Rightarrow F^d_{92,46,27} = x_1 = 1, x_2 = 0, x_3 = 0.$$

Дослідивши отримані залежності, можна зробити висновок, що значення по діагоналі основних елементів операцій криптографічного перетворення, які входять до досліджуваної групи, утворює вісім варіантів операцій, тобто 2^3 варіантів. Звідси можна зробити припущення, що базову групу операцій криптографічного перетворення можуть утворювати лише ті операції криптографічного перетворення, в яких значення основних елементів по діагоналі дорівнює 2^3 варіантам.

Висновки. За результатами проведеного обчислювального експерименту визначено базові операції, що входять до базової групи операцій перестановок, керованих інформацією.

В результаті представлення групи базових операцій у вигляді дискретних моделей було визначено залежності для основних елементів операцій.

У ході аналізу одержаних результатів було виявлено, що базову групу операцій криптографічного перетворення можуть утворювати лише ті операції криптографічного перетворення, в яких значення основних елементів по діагоналі дорівнює 2^3 варіантам.

Список літератури

1. Бабенко В. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / В. Бабенко, О. Мельник, Р. Мельник. // Безпека інформації. – 2013. – Т. 19, № 1. – С. 56–59.
2. Рудницкий С. В. Криптографическое преобразование информации на основе трехразрядных логических функций / С. В. Рудницкий, Р. П. Мельник, В. В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4 (22). – С. 119–122.
3. Миронюк Т. В. Синтез елементарних функцій перестановок, керованих інформацією / Т. В. Миронюк, О. Г. Мельник // Інформаційні технології в освіті, науці й техніці (ІТОНТ-2014) : зб. тез. доп. ІІ Міжнар. наук.-практ. конф., (Черкаси, 24-26 квітня). – Черкаси : ЧДТУ, 2014. – С. 147–148.
4. Синтез елементарних функцій перестановок, керованих інформацією / В. М. Рудницький, Т. В. Миронюк, О. Г. Мельник, В. П. Щербина // Безпека інформації. – Т. 20, № 3. – К. : НАУ, 2014. – С. 242–247.
5. Криптографическое кодирование : [колл. монография] / под ред. В. Н. Рудницкого, В. Я. Мильчевича. – Харьков : Изд-во «Щедрая усадьба плюс», 2014. – 240 с.
6. Бабенко В. Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В. Г. Бабенко, Р. П. Мельник, С. В. Рудницький // Системи управління, навігації та зв'язку : зб. наук. праць. – Вип. 1 (21), т. 2. – К. : Центр. наук.-досл. ін-т навігації і управл., 2012. – С. 170–173.

References

1. Babenko, V., Melnyk, O. and Melnik, R. (2013) Classification of three digit basic functions for cryptographic transformation of information. *Bezpeka informatsiyi*, 19 (1), pp. 56–59 [in Ukrainian].
2. Rudnytskyy, S. V., Melnyk, R. P. and Veretelnyk, O. V. (2012) Cryptographic transformation of information based of three digit logical functions. *Vektor nauki Toliattinskogo gosudarstvennogo universiteta*, 4 (22), pp. 119–122 [in Russian].
3. Myronyuk, T. V. and Melnyk, O. H. (2014) Synthesis of permutations elementary functions controlled by information. *Informatsijni tehnologiyi v osviti, nautsi j tehnitsi (ITONT-2014)*: conf. proceedings of the II Internat. scient.-pract. conf. (Cherkasy, April 24-26).- Cherkasy: ChDTU, pp. 147–148 [in Ukrainian].
4. Rudnytskyy, V. M., Myronyuk, T. V., Melnyk, O. H. and Scherbyna, V. P. (2014) Synthesis of elementary transposition functions controlled by information. *Bezpeka informatsiyi*, 20 (3), pp. 242–247 [in Ukrainian].
5. Cryptographic coding: collective monograph (2014). In: V. N. Rudnicki, V. Ya. Milchevich. Kharkov: Izd-vo "Schedraya usadba plus", 240 p. [in Russian].
6. Babenko, V. G., Melnyk, R. P. and Rudnytskyy, S. V. (2012). Investigation of recording of three digit cryptographic operations. *Systemy upravlinnya, navigatsiyi ta zvyazku:* collection of scientific works, 1 (21), pp. 170–173 [in Ukrainian].

T. V. Myronyuk, *senior lecturer*
Cherkasy State Technological University,
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
e-mail: tanjamiron85@gmail.com

DEFINITION OF ELEMENTARY OPERATIONS OF CORE GROUP PERMUTATIONS, CONTROLLED BY INFORMATION

Introduction. *Over the years, cryptography served to only military targets. Today ordinary users have the opportunity to use tools that allow them to protect themselves from unauthorized access to confidential information using methods of computer cryptography.*

Data protection with the use of encryption is one of the most reliable ways to address its security as encrypted information is available only for those who know how to decipher it.

The purpose of scientific work. *The objective of this research is to identify and analyze elementary operations which consist of basic operations of permutations, controlled by information.*

Formulation of the problem. *In modern printed editions special attention is given to the use of three digit matrix operations of cryptographic transformations and based on these algorithms resources for information protection. However, in these studies, no analysis of the operations of permutations, controlled by information, is performed for encoding and decoding of the information.*

Summary of the main part. *The article presents the results of research of basic cryptographic operations that form the core group of permutations operations, controlled by information. After the results of numerical experiment the core group of permutations operations, controlled by information, is received and discrete models of operations representation are constructed. During the analysis of the results of the experiment dependences for basic elements of operations are revealed.*

Conclusions. *It is determined that the core group of cryptographic transformation operations can be formed only by those cryptographic transformation operations in which the value of the main elements diagonally is equal to 2^3 options.*

Keywords: *basic operation, group of basic operations of permutations, controlled by information, discrete model, inversion matrix, addition matrix, main element.*

Рецензенти: С .В. Голуб, д.т.н., професор,
В. М. Рудницький, д.т.н., професор