ДИСКРЕТНА МОДЕЛЬ БАЗОВИХ ГРУП ОПЕРАЦІЙ ПЕРЕСТАНОВОК КЕРОВАНИХ ІНФОРМАЦІЄЮ ДЛЯ КРИПТОПЕРЕТВОРЕННЯ

Миронюк Т. В.,
старший викладач,
Черкаський державний технологічний університет,
Черкаси, Україна

Ланських Є. В.,
кандидат технічних наук, доцент,
Черкаський державний технологічний університет,
Черкаси, Україна

DISCRETE MODEL OF CORE GROUP PERMUTATIONS WHICH IS MANAGED BY INFORMATION FOR CRYPTOGRAPHIC TRANSFORMATION

Myronyuk T.V.,
Senior Lecturer,
Cherkasy State Technological University,
Cherkasy, Ukraine

Lanskykh Y.V.,
P*h.D., Associate Professor,*
Cherkasy State Technological University,
Cherkasy, Ukraine

Анотація

Криптографічні примітиви мають більш складну структуру, ніж операції для криптоперетворення такі, як додавання за модулем, зсув, перестановка, підстановка та інші. Виявлення нових операцій, здатних для ефективного криптоперетворення, дозволяє вдосконалити криптопримітиви. Вирішення даної задачі знаходиться на межі криптографії, теорії алгоритмів та алгебри логіки.

Виходячи з цього, можна стверджувати, що отримання нових трьохрозрядних операцій перестановок, керованих інформацією може надати нові можливості для розробки нових операцій для криптоперетворення та вдосконалення криптопримітивів.

Задача розробки загальної дискретної моделі отримання базових груп операцій перестановок керованих інформацією на основі мінімізації функцій є актуальною.

Мета роботи – отримання дискретної моделі базових груп операцій перестановок керованих інформацією для криптографічного перетворення.

Методи дослідження - алгебра логіки та булева алгебра.

Основна задача, якій присвячена дана робота, полягає у проведені мінімізації базових операцій та отримані аналітичних залежностей базових операцій на основі першої групи базових операцій криптографічного перетворення.

В результаті мінімізації було визначено модель прямих та обернених базових операцій. Отримано узагальнену дискретну модель базових груп операцій для кодування та декодування інформації.

На основі проведених розрахунків було визначено суть методу синтезу базових операцій криптографічного перетворення, результатом якого є визначені 384 операції криптографічного перетворення для трьохрозрядних елементарних функцій.

Ключові слова: *базова операція, група базових операцій перестановок керована інформацією, дискретна модель, мінімізація операцій, синтез базових операцій, узагальнена дискретну модель базових груп операцій.*

Abstract

Cryptographic primitives have a more complex structure than operations for cryptographic transformation such as addition modulo, shift, permutation, substitution and others. Identifying of new operations, that are able to effective cryptographic transformation, can improve cryptographic primitives. The solution to this problem is on the verge of cryptography, algorithms and theory of algebra of logic.

Therefore, one could argue that getting new permutations three bit operations, managed by information, can provide new opportunities for developing new operations for cryptographic transformation and improving cryptographic primitives.

The task of developing a common pattern of discrete groups of basic operations of permutations, managed by information, based on minimization of functions, is important.

Purpose - to obtain basic models of discrete groups of permutations, managed by operations for cryptographic information transformation.

Methods - algebra of logic and Boolean algebra.

The main task, which this work is devoted to, is to minimize conducted basic operations and analytical dependences basic operations on the basis of the first group of basic operations of cryptographic transformations.

As the result of minimization, direct and inverse model basic operations were determined. Generalized model of discrete groups of basic operations for encoding and decoding information was obtained.

On the basis of the calculations, the essence of the method of synthesis of basic operations of cryptographic transformations was determined; resulting in 384 identified cryptographic operations to convert three bit elementary functions.

Key words: *basic operation, a group of basic operations of permutations controlled information, discrete model, minimization of operations, synthesis of basic operations, basic model generalized discrete group operations*.

Постановка проблеми. Сучасні інформаційні технології сприяють неконтрольованому встановленню інформаційних відносин та впливу на інформаційний простір. Інтернет суттєво змінив методи доступу до інформації та її поширення. Ця мережа порівняно з іншими засобами масової інформації передбачає значні можливості щодо реалізації права особи на вільне збирання, зберігання, використання і поширення інформації. Інтернет надає вільний доступ до накопиченої людством інформації незалежно від відстані й місця зберігання, значно наближаючи до першоджерел.

Це дозволяє широко застосовувати комп'ютерні технології в автоматизованих системах обробки інформації й керування призвело до загострення проблеми захисту інформації, що в свою чергу обумовлює створення нових ефективних засобів захисту інформації, які забезпечать криптографічну стійкість.

Дана стаття присвячена розробці методу синтезу базових груп операцій трьохрозрядних елементарних операцій перестановки керованих інформацією для криптографічного перетворення.

Аналіз публікацій і 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 приведені твердження для елементарних функцій перестановок, керованих інформацією; [4], де для подальшого дослідження визначена група 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; [6], де проведено визначення та аналіз елементарних операцій базової групи операцій перестановок керованих інформацією.

Проте в даних дослідженнях не визначалася суть методу синтезу груп базових операцій перестановок керованих інформацією для криптоперетворення.

Метою даного дослідження є визначення та отримання загальної дискретної моделі базових операцій перестановок керованих інформацією для виконання криптоперетворення.

Виклад основного матеріалу. Для визначення моделі синтезу базових функцій криптографічного перетворення, що входять до базової групи проведемо мінімізацію функцій для операцій кодування та декодування. Для цього функції $F^k \; ma \; F^d$ представимо в наступному вигляді:

$$F_{m,m,m} = \begin{bmatrix} \underline{x_{11}} & x_{12} & x_{13} \\ x_{21} & \underline{x_{22}} & x_{23} \\ x_{31} & x_{32} & \underline{x_{33}} \end{bmatrix}, \qquad (1)$$

де x_{11}, x_{22}, x_{33} – значення першого, другого та третього основних елементів елементарної функції, m – номер елементарної функції криптографічного перетворення.

Щоб отримати базові операції, спробуємо отримати аналітичні залежності базових операцій на основі першої групи базових операцій криптографічного перетворення з таблиці 1[6].

Представимо першу базову групу операцій у вигляді таблиці істинності для операцій кодування F^k у вигляді представленому в таблиці 1.

Таблиця істинності функції кодування F^k

x_{11}	x_{22}	x_{33}	x_{12}	x_{13}	x_{21}	x_{23}	x_{31}	x_{32}
1	0	0	0	1	1	0	1	1
0	1	0	1	1	1	1	1	1
1	0	1	1	1	1	1	1	1
0	0	0	1	0	1	1	1	0
0	1	1	1	0	0	1	1	1
0	0	1	1	1	1	0	0	1
1	1	1	0	1	1	1	0	1
1	1	0	1	1	0	1	1	0

В таблиці 1 визначено модель побудови додаткових елементів $x_{12}, x_{13}, x_{21}, x_{23}, x_{31}, x_{32}$ через основні елементи - x_{11}, x_{22}, x_{33}.

Одним з шляхів отримання залежностей може бути таблиця з подальшим формалізуванням даних таблиці істинності на основі мінімізації за допомогою карти Карно.

Карту Карно для мінімізації відповідно до таблиці 1 представлено у вигляді таблиці 2.

Таблиця 2

Карта Карно для отримання функції кодування F^k

x_{11}	x_{22}	x_{12}		x_{13}		x_{21}		x_{23}		x_{31}		x_{32}	
0	**0**	1	1	0	1	1	1	1	0	1	0	0	1
0	**1**	1	1	1	0	1	0	1	1	1	1	1	1
1	**1**	1	0	1	1	0	1	1	1	1	0	0	1
1	**0**	0	1	1	1	1	1	0	1	1	1	1	1
		0	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**
		x_{33}											

В результаті мінімізації було отримано наступні результати:

$$F_{12} = \bar{x}_{11} \vee x_{22}\bar{x}_{33} \vee \bar{x}_{22}x_{33} = \bar{x}_{11} \vee (x_{22} \oplus x_{33});$$

$$F_{13} = x_{11} \vee x_{22}\bar{x}_{33} \vee \bar{x}_{22}x_{33} = x_{11} \vee (x_{22} \oplus x_{33});$$

$$F_{21} = \bar{x}_{22} \vee \bar{x}_{11}\bar{x}_{33} \vee x_{11}x_{33} = \bar{x}_{22} \vee (x_{11} \equiv x_{33});$$

$$F_{23} = x_{22} \vee \bar{x}_{11}\bar{x}_{33} \vee x_{11}x_{33} = x_{22} \vee (x_{11} \equiv x_{33});$$

$$F_{31} = \bar{x}_{33} \vee \bar{x}_{11}x_{22} \vee x_{11}\bar{x}_{22} = \bar{x}_{33} \vee (x_{11} \oplus x_{22});$$

$$F_{32} = x_{33} \vee \bar{x}_{11}x_{22} \vee x_{11}\bar{x}_{22} = x_{33} \vee (x_{11} \oplus x_{22})$$

Таблиця 5

Синтез базових операцій кодування

x_{11}	$F_{12} = \bar{x}_{11} \vee (x_{22} \oplus x_{33})$	$F_{13} = x_{11} \vee (x_{22} \oplus x_{33})$
$F_{21} = \bar{x}_{22} \vee (x_{11} \equiv x_{33})$	x_{22}	$F_{23} = x_{22} \vee (x_{11} \equiv x_{33})$
$F_{31} = \bar{x}_{33} \vee (x_{11} \oplus x_{22})$	$F_{32} = x_{33} \vee (x_{11} \oplus x_{22})$	x_{33}

Для подальшого дослідження отримання методу синтезу базових операцій кодування, необхідно вивести дискретну модель визначення базових груп операцій для криптоперетворення.

Для цього модифікуємо дискретну модель поєднання матриці перестановок та матриці доповнення представлену за допомогою виразу:

$$F^{k}_{92,46,27} = \begin{vmatrix} \underline{1} & 0 & 1 \\ 1 & \underline{0} & 0 \\ 1 & 1 & \underline{0} \end{vmatrix} \Rightarrow F^{d}_{83,116,78} = \begin{vmatrix} \underline{1} & 1 & 1 \\ 0 & \underline{1} & 1 \\ 1 & 0 & \underline{0} \end{vmatrix}. \quad (2)$$

Для подальшого дослідження замінимо основні та додаткові елементи моделі, відповідними їм елементами приведеними в таблиці 5.

В результаті отримаємо модифіковану матричну дискретну модель наступного вигляду представлену за допомогою виразу 3.

$$F^{k} = \begin{bmatrix} x_{11} & \bar{x}_{11} \vee (x_{22} \oplus x_{33}) & x_{11} \vee (x_{22} \oplus x_{33}) \\ \bar{x}_{22} \vee (x_{11} \equiv x_{33}) & x_{22} & x_{22} \vee (x_{11} \equiv x_{33}) \\ \bar{x}_{33} \vee (x_{11} \oplus x_{22}) & x_{33} \vee (x_{11} \oplus x_{22}) & x_{33} \end{bmatrix} \quad (3)$$

Тепер, відобразимо модифіковану матричну дискретну модель для кодування функцій представлену виразом (3) за допомогою дискретної моделі представлення криптографічних операцій.

Для цього у виразі наведеному нижче

$$F^{k}_{92,46,27} = \begin{vmatrix} x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 \end{vmatrix} \Rightarrow F^{d}_{83,116,78} = \begin{vmatrix} x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 \end{vmatrix} \quad (4)$$

замінимо значення основних та додаткових елементів операції кодування відповідними значеннями з виразу (3).

В результаті було отримано узагальнену дискретну модель базових груп операцій кодування для криптографічного перетворення, яка представлена в наступному вигляді:

$$F^{k} = \begin{bmatrix} (x_1 \equiv (x_{11})) \cdot (x_2 \equiv (\bar{x}_{11} \vee (x_{22} \oplus x_{33}))) \vee \\ \vee (x_1 \equiv (x_{11} \oplus 1)) \cdot (x_3 \equiv (x_{11} \vee (x_{22} \oplus x_{33}))) \\ (x_2 \equiv (x_{22})) \cdot (x_1 \equiv (\bar{x}_{22} \vee (x_{11} \equiv x_{33}))) \vee \\ \vee (x_2 \equiv (x_{22} \oplus 1)) \cdot (x_3 \equiv (x_{22} \vee (x_{11} \equiv x_{33}))) \\ (x_3 \equiv (x_{33})) \cdot (x_1 \equiv (\bar{x}_{33} \vee (x_{11} \oplus x_{22}))) \vee \\ \vee (x_3 \equiv (x_{33} \oplus 1)) \cdot (x_2 \equiv (x_{33} \vee (x_{11} \oplus x_{22}))) \end{bmatrix}. \quad (5)$$

Тепер, перевіримо правильність отриманої дискретної моделі базових груп операцій кодування. Для цього скористаємося таблицею істинності для трьох розрядних функцій.

Підставивши визначені в таблиці істинності значення основних елементів у вираз (5) та виконавши операції рівнозначності, суми по модулю 2 і кон'юнкції отримаємо результат, який представлено у таблиці 6, де x_{11}, x_{22}, x_{33} – значення першого, другого та третього основного елемента елементарної операції, ЕФ1, ЕФ2, ЕФ3 – значення першої, другої та третьої елементарної функції операції криптоперетворення.

Таблиця 6

Таблиця істинності визначення базової групи операцій для кодування F^k для криптоперетворення

x_{11}	x_{22}	x_{33}	Базова група операцій		
			ЕФ1	ЕФ2	ЕФ3
0	0	0	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	$x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
0	0	1	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	$\bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$
0	1	0	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	$x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
0	1	1	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	$\bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$
1	0	0	$x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	$x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
1	0	1	$x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	$x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$
1	1	0	$x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	$\bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
1	1	1	$x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	$x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$\bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$

Отримані в таблиці 6 результати елементарних функцій утворюють першу базову групу операцій отриману внаслідок обчислювального експерименту.

Далі, визначимо спосіб отримання методу синтезу базових операцій криптографічного перетворення для функції декодування. Для цього, представимо результати мінімізації операцій декодування у вигляді таблиці 7.

Таблиця 7 –

Синтез базових операцій декодування

$F_{11} = \bar{x}_{11}x_{22} \vee x_{11}\bar{x}_{33}$	$F_{12} = \bar{x}_{22} \vee (x_{11} \equiv x_{33})$	$F_{13} = \bar{x}_{33} \vee (x_{11} \oplus x_{22})$
$F_{21} = \bar{x}_{11} \vee (x_{22} \oplus x_{33})$	$F_{22} = x_{11}\bar{x}_{22} \vee x_{22}x_{33}$	$F_{23} = x_{33} \vee (x_{11} \oplus x_{22})$
$F_{31} = x_{11} \vee (x_{22} \oplus x_{33})$	$F_{32} = x_{22} \vee (x_{11} \equiv x_{33})$	$F_{33} = \bar{x}_{11}\bar{x}_{33} \vee x_{22}x_{33}$

Для подальшого дослідження методу синтезу базових операцій декодування, модифікуємо дискретну модель операції декодування представлену за допомогою виразу (2). Для цього замінимо основні та додаткові елементи моделі, відповідними їм елементами приведеними в таблиці 7.

В результаті отримаємо дискретну модель функцій декодування для першої групи базових операцій в наступному вигляді:

$$F^d = \begin{bmatrix} \bar{x}_{11}x_{22} \vee x_{11}\bar{x}_{33} & \bar{x}_{22} \vee (x_{11} \equiv x_{33}) & \bar{x}_{33} \vee (x_{11} \oplus x_{22}) \\ \bar{x}_{11} \vee (x_{22} \oplus x_{33}) & x_{11}\bar{x}_{22} \vee x_{22}x_{33} & x_{33} \vee (x_{11} \oplus x_{22}) \\ x_{11} \vee (x_{22} \oplus x_{33}) & x_{22} \vee (x_{11} \equiv x_{33}) & \bar{x}_{11}\bar{x}_{33} \vee x_{22}x_{33} \end{bmatrix}. \quad (6)$$

Тепер для подальшої перевірки представимо отриманий вираз (6) для декодування функцій за допомогою дискретної моделі представлення криптографічних операцій. При цьому, замінимо у виразі (4) значення основних та додаткових елементів операцій криптоперетворення функцій декодування відповідними їм значеннями представленими в таблиці 7.

$$F^d = \begin{bmatrix} \left(x_1 \equiv \left(x_{11}x_{22} \vee \bar{x}_{11}x_{33}\right)\right)\cdot\left(x_2 \equiv \left(x_{22} \vee \left(x_{11} \equiv x_{33}\right)\right)\right)\vee \\ \vee\left(x_1 \equiv \left(\left(\bar{x}_{11}x_{22} \vee x_{11}\bar{x}_{33}\right)\oplus 1\right)\right)\cdot\left(x_3 \equiv \left(\bar{x}_{33} \vee \left(x_{11} \oplus x_{22}\right)\right)\right) \\ \left(x_2 \equiv \left(x_{11}\bar{x}_{22} \vee x_{22}x_{33}\right)\right)\cdot\left(x_1 \equiv \left(\bar{x}_{11} \vee \left(x_{22} \oplus x_{33}\right)\right)\right)\vee \\ \vee\left(x_2 \equiv \left(\left(x_{11}\bar{x}_{22} \vee x_{22}x_{33}\right)\oplus 1\right)\right)\cdot\left(x_3 \equiv \left(x_{33} \vee \left(x_{11} \oplus x_{22}\right)\right)\right) \\ \left(x_3 \equiv \left(\bar{x}_{11}\bar{x}_{33} \vee x_{22}x_{33}\right)\right)\cdot\left(x_1 \equiv \left(x_{11} \vee \left(x_{22} \oplus x_{33}\right)\right)\right)\vee \\ \vee\left(x_3 \equiv \left(\left(\bar{x}_{11}\bar{x}_{33} \vee x_{22}x_{33}\right)\oplus 1\right)\right)\cdot\left(x_2 \equiv \left(x_{22} \vee \left(x_{11} \equiv x_{33}\right)\right)\right) \end{bmatrix} \quad (7)$$

Далі необхідно перевірити правильність отриманої дискретної моделі базових груп операцій декодування. Для цього, скористаємося таблицею істинності для трьох розрядних функцій.

Підставивши визначені в таблиці істинності значення основних елементів у вираз (7) та виконавши операції рівнозначності, суми по модулю 2 і кон'юнкції отримаємо результат, який представлено у таблиці 8.

Отримані в таблиці 8 результати елементарних функцій утворюють першу базову групу операцій декодування отриману внаслідок обчислювального експерименту.

Дослідивши отримані моделі функцій кодування та декодування представлені виразами (5) та (7) можна зробити висновок, що суть методу синтезу базових операцій криптографічного перетворення полягає в змінні значень $x_{11}, x_{22}, x_{33} \in [0,1]$, що дає змогу отримати вісім базових операцій криптографічного перетворення для кодування та декодування функцій.

Таблиця 8

Таблиця істинності визначення базової групи операцій для декодування F^d для криптоперетворення

x_{11}	x_{22}	x_{33}	Базова група операцій		
			ЕФ1	ЕФ2	ЕФ3
0	0	0	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	$\bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$
0	0	1	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	$x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
0	1	0	$x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	$x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$
0	1	1	$x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	$x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$\bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$
1	0	0	$x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	$\bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
1	0	1	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	$x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
1	1	0	$x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	$x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	$x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
1	1	1	$\bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	$\bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	$x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$

Визначивши суть методу синтезу базових операцій криптографічного перетворення, можна зробити висновок, що синтез операцій криптографічного перетворення на основі отриманих дискретних моделей полягає в наступному:

1. Синтезі всіх базових операцій криптографічного перетворення;
2. Для кожної отриманої операції необхідно зробити перестановку, що збільшить їх кількість в 6 разів;
3. Для збільшення кількості операцій необхідно використати операції інверсій, що збільшить кількість операцій перетворення ще у 8 разів.

Результатом обчислювального експерименту є 384 операції криптографічного перетворення для трьохрозрядних елементарних функцій.

Висновки. Отже, результатом роботи є проведена мінімізація базових операцій та отримані аналітичні залежності базових операцій на основі першої групи базових операцій криптографічного перетворення.

В результаті мінімізації було визначено модель прямих та обернених базових операцій. Отримано узагальнену дискретну модель базових груп операцій для кодування та декодування інформації.

На основі проведених розрахунків було визначено суть методу синтезу базових операцій криптографічного перетворення, результатом якого є визначені 384 операції криптографічного перетворення для трьохрозрядних елементарних функцій.

Перелік посилань

1. Віра Бабенко, Ольга Мельник, Руслан Мельник. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації // 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 // ІІ Міжнародна науково-практична конференція «Інформаційні технології в освіті, науці й техніці» (ІТОНТ-2014), 24- 26 квітня: зб. тез. доп. — Черкаси : ЧДТУ, 2014. — С. 147-148

4. Рудницький В. М. Синтез елементарних функцій перестановок, керованих інформацією / В.М. Рудницький, Т. В. Миронюк, О.Г. Мельник, В.П. Щербина // Безпека інформації том 20, №3. – Київ: НАУ, 2014. – С. 242-247

5. Криптографическое кодирование: коллективная монография / Под ред. В.Н. Рудницкого, В.Я. Мильчевича. – Харьков : Изд-во «Щедрая усадьба плюс», 2014. – 240 с.

6. Миронюк Т. В. Визначення елементарних операцій базової групи перестановок керованих інформацією / Т. В. Миронюк // Вісник Черкаського державного технологічного університету. – 2016. – Випуск №2. – С. 100-105.

References

1. Vera Babenko Olga Melnyk Ruslan Melnik.(2013). Classification of three digit basic functions for cryptographic transformation of information // Security of Information, (1(19)), pp. 56-59. (in Ukr.).

2. S.V. Rudnytskyy. (2012). The cryptographic transformation of information based of three digit logical functions / S.V. Rudnytskyy, R.P Melnyk, O. V. Veretelnyk // Vector Science Togliatti state-owned university, (4 (22)), - pp. 119-122.

3. Myronyuk T.V. Synthesis permutations of elementary functions controlled by the information / T.V. Myronyuk, O.H. Melnyk // Conference proceedings of II International Scaintifical-Practical Conference “Information Technologies in Education, Science and Technology” (ITEST-2014): Cherkasy, April 24-26, 2014, - 2 volumes.- Cherkasy: ChSTU, 2014. – pp. 147-148. (in Ukr.).

4. Rudnytskyy V., Melnyk O., Scherbyna V., Myronyuk T. Synthesis of elementary transposition functions controlled by information // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 242-247. (in Ukr.).

5. The cryptographic coding: collective monograph / Ed. V.N. Rudnicki, V.Y. Milchevich. - Kharkov: Publishing house "Schedraya usadba plus", 2014. – 240 pp. (in Rus.)

6. Myronyuk T.V. Definition of elementary operations of core group permutations which is managed by information / T.V. Myronyuk // Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitety. 2016. No. 2. P. 100-105. (Ukr)

АНАЛІЗ ЕФЕКТИВНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП’ЮТЕРНИХ СИСТЕМАХ

Стрембіцький Р.Г.,
магістрант,
Черкаський державний технологічний університет,
Черкаси, Україна

Кобильник О.Б.
магістрант,
Черкаський державний технологічний університет,
Черкаси, Україна

ANALYSIS OF THE EFFECTIVE METHOD OF PROTECTING INFORMATION IN COMPUTER SYSTEMS

Strembitskyi R.G.,
undergraduate,
Cherkassy State Technological University,
Cherkassy, Ukraine

Kobylnyk O.B.,
undergraduate,
Cherkassy State Technological University,
Cherkassy, Ukraine

Анотація

В статті проведено дослідження та аналіз найбільш дієвих методів захисту комп’ютерних систем від несанкціонованого доступу та крадіжки інформації. Такими методами захисту вважаються: міжмережевий екран (Firewall, брандмауер), аркуші доступу (access-lists), NAT (Network Address Translation),