УДК 621.391

В.М. Рудницький, І.В. Миронець, В.Г. Бабенко

Черкаський державний технологічний університет, Черкаси

СИСТЕМАТИЗАЦІЯ ПОВНОЇ МНОЖИНИ ЛОГІЧНИХ ФУНКЦІЙ ДЛЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Дана стаття присвячена визначенню та систематизації повної множини логічних функцій для криптографічного перекодування інформації. Одержані логічні функції перекодування можуть знайти практичне застосування для перекодування інформації конфіденційного призначення в криптографічних системах захисту інформації. Разом з раніше відомими методами та засобами вони дадуть змогу в перспективі значно покращити оперативність доступу до віддаленої захищеної інформації.

Ключові слова: *конфіденційні інформаційні ресурси, оперативність доступу, криптографічне перетворення, функція перекодування.*

Вступ

Постановка проблеми. У сфері доступу до конфіденційних інформаційних ресурсів залишається цілий ряд задач і проблем, вирішення яких має важливе науково-технічне і загальнодержавне значення. Однією з таких задач є підвищення оперативності доступу до конфіденційних інформаційних ресурсів та оперативності обробки конфіденційної інформації. Основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають криптографічні методи та засоби захисту інформації. Слід врахувати, що найбільш надійний захист можна забезпечити тільки за допомогою комплексного підходу, тобто рішення задачі має представляти собою сукупність організаційно-технічних та криптографічних заходів.

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, виробленого за певними математичними законами, з метою виключити доступ до даної інформації сторонніх користувачів, а також з метою забезпечення неможливості безконтрольної зміни інформації з боку тих же самих осіб.

Забезпечити конфіденційність інформації користувача дозволить використання спеціалізованих логічних функцій, які можливо використовувати для підвищення оперативності доступу до конфіденційних інформаційних ресурсів [1, 2, 3], на основі виконання операції перекодування. Це дозволяє зменшити час доступу до конфіденційних інформаційних ресурсів за рахунок заміни етапів декодування та кодування у форматі користувача на етап перекодування, а також, підвищити конфіденційність збереження інформації за рахунок обмеження доступу технічних працівників електронних бібліотек до конфіденційних інформаційних ресурсів.

Аналіз останніх досліджень і публікацій. Аналітичний огляд поширених сучасних методів і засобів розвитку нових тенденцій показав, що задача забезпечення оперативності доступу до інформації в комп'ютерних системах та мережах є дуже важливою та актуальною. Вирішення даної задачі є практично необхідним як на сучасному етапі розвитку систем захисту інформації, так і для подальшої перспективи.

Попередніми дослідниками було сформульовано і доведено ряд теорем, які стали теоретичним підґрунтям для побудови моделей пристроїв криптографічного перекодування, була розроблена методика, яка дала змогу спростити процес побудови функцій криптографічного перетворення інформації. Забезпечення конфіденційності інформації при реалізації даної методики базується на забезпеченні криптостійкості стандартними алгоритмами, а також збільшенням кількості перетворень двохрозрядного коду. Було доведено, що метод підвищення оперативності криптографічного перетворення інформації на основі використання запропонованих спеціалізованих логічних функцій для систем захисту інформації дозволяє збільшити швидкість обробки інформації від 1,57 до 2,92 разів залежно від часу отримання ключа та розрядності перетворення [3].

На даний час в доступних джерелах науково-технічної інформації відсутні дані про оперативність доступу до конфіденційних інформаційних ресурсів на основі використання широкого спектру логічних функцій декількох змінних замість операцій криптографічного додавання.

Мета статті полягає у проведенні систематизації логічних функцій, придатних для підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Основний матеріал

Як вже говорилося, одним із найбільш ефективних вирішенням задачі підвищення оперативності доступу до конфіденційних інформаційних ресурсів є використання спеціалізованих логічних функцій, які забезпечують оперативність обробки інформації та під-

вищують захищеність і криптостійкість систем [2, 4].

Результатами обчислювального експерименту по визначенню повної множини логічних функцій, придатних для криптоперетворення, стали 576 функцій перекодування, які дають можливість підвищення оперативності доступу до конфіденційних інформаційних ресурсів. Збільшення кількості спеціалізованих логічних функцій дозволяє підвищити захищеність конфіденційної інформації. Також проведений експеримент створює теоретичну базу для подальших досліджень, направлених на доведення доцільності використання спеціалізованих логічних функцій будь-якої складності.

Для проведення аналізу повної множини логічних функцій перекодування наведемо необхідні означення.

Означення 1. Функція, операндами якої не є константи, називається прямою функцією (x_1).

Означення 2. Функція, яка є оберненою до прямої, називається інвертованою функцією, або, функція, яка містить хоча б один операнд-константу, називається інвертованою функцією $(x_1 \oplus 1)$.

Означення 3. Функція, яка залежить лише від одного аргументу, називається простою.

Означення 4. Функція, яка залежить від декількох аргументів, складених за модулем, називається складною.

Означення 4.1. Функція, утворена заміною першого розряду на суму за модулем першого та другого розрядів, називається складною функцією першого порядку.

Означення 4.2. Функція, утворена заміною другого розряду на суму за модулем першого та другого розрядів, називається складною функцією другого порядку.

Означення 5. Функція, номер якої співпадає з номером одного з аргументів, називається правильно розміщеною функцією.

Означення 6. Функція, номер якої не співпадає з номером аргументів, називається неправильно розміщеною функцією.

Означення 7. Функція, якою закодована інформація в базі даних інформаційних ресурсів, називається вхідною функцією кодування ($\vec{F}_{Vh}$).

Означення 8. Функція, якою закодована інформація інформаційних ресурсів для користувача, називається вихідною функцією кодування ($\vec{F}_{Vuh}$).

Означення 9. Функція, яка забезпечує перекодування інформації із вхідної функції у вихідну, називається функцією перекодування ($\vec{F}_{Pk}$) [1 – 4].

За результатами досліджень отримано логічні функції перекодування, які можуть бути використані в системах захисту інформації на етапі криптографічного додавання [5 – 6].

Для аналізу результатів використаємо векторне представлення функцій перекодування:

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix},$$

де $a_{i,j} = \overline{0,1}$, $b_i = \overline{0,1}$;

$\oplus$ – сума за модулем два [1–2, 4].

Структуровані результати обчислювального експерименту наведено в табл. 1.

Таблиця 1

Структуровані результати обчислювального експерименту

Vh \ Vuh	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	10	20	11	10	11	21	20	21	30	20	31	21	30	31	20	21	10	30	11	31	10	11	30	31
	20	10	20	21	21	11	11	10	20	30	21	31	21	20	31	30	30	10	31	11	31	30	11	10
1	10	20	11	10	11	21	20	21	30	20	31	21	30	31	20	21	10	30	11	31	10	11	30	31
	20	10	20	21	21	11	11	10	20	30	21	31	21	20	31	30	30	10	31	11	31	30	11	10
	20	10	21	20	21	11	10	11	30	10	31	11	30	31	10	11	20	30	21	31	20	21	30	31
2	10	20	10	11	11	21	21	20	10	30	11	31	11	10	31	30	30	20	31	21	31	30	21	20
	11	20	10	11	10	21	20	21	31	20	30	21	31	30	20	21	11	31	10	30	11	10	31	30
3	20	11	20	21	21	10	10	11	20	31	21	30	21	20	30	31	31	11	30	10	30	31	10	11
	10	21	11	10	11	20	21	20	31	21	30	20	31	30	21	20	10	31	11	30	10	11	31	30
4	21	10	21	20	20	11	11	10	21	31	20	30	20	21	30	31	31	10	30	11	30	31	11	10
	11	21	10	11	10	20	21	20	30	21	31	20	30	31	21	20	11	30	10	31	11	10	30	31
5	21	11	21	20	20	10	10	11	21	30	20	31	20	21	31	30	30	11	31	10	31	30	10	11
	21	11	21	11	10	20	20	21	30	11	31	10	30	31	11	10	21	30	20	31	21	20	30	31
6	11	21	11	10	10	20	20	21	11	30	10	31	10	11	31	30	30	21	31	20	31	30	20	21
	20	21	10	20	21	20	11	10	31	10	30	11	31	30	10	11	21	31	20	30	21	20	31	30
7	11	10	21	10	11	20	20	21	10	31	11	30	11	10	30	31	31	21	30	20	30	31	20	21
	21	20	11	21	20	21	10	11	10	31	11	30	10	31	30	11	10	20	31	21	30	20	21	31	30
8	10	11	20	11	10	21	21	20	11	31	10	30	10	11	30	31	31	20	30	21	30	31	21	20
	30	20	31	30	31	21	20	21	10	20	11	21	10	11	20	21	30	10	31	11	30	31	10	11
9	20	30	20	21	21	31	31	30	20	10	21	11	21	20	11	10	10	30	11	31	11	10	31	30
	20	10	31	30	31	11	10	11	20	10	21	11	20	21	10	11	30	20	31	21	30	31	20	21
10	30	10	30	11	11	31	31	30	10	20	11	21	11	10	21	20	20	30	21	31	21	20	31	30
	31	20	21	31	30	21	20	21	11	21	10	20	11	10	21	20	30	11	31	10	30	31	11	10
11	21	30	21	20	20	31	31	30	21	11	20	10	20	21	10	11	11	30	10	31	10	11	31	30
	21	30	11	31	30	11	10	11	21	11	20	10	21	20	11	10	30	21	31	20	30	31	21	20
12	31	11	30	10	10	31	31	30	11	21	10	20	10	11	20	21	21	30	20	31	20	21	31	30
	30	31	21	30	31	20	21	20	10	21	11	20	10	11	21	20	31	10	30	11	31	30	10	11
13	21	31	21	20	20	30	30	31	21	10	20	11	20	21	11	10	10	31	11	30	11	10	30	31
	31	20	30	31	30	21	20	21	11	20	10	21	11	10	20	21	31	11	30	10	31	30	11	10
14	20	31	20	21	21	30	30	31	20	11	21	10	21	20	10	11	11	31	10	30	10	11	30	31
	20	31	10	30	31	30	11	10	21	10	20	11	21	20	10	11	31	21	30	20	31	30	21	20
15	31	10	31	30	31	30	11	10	21	10	21	11	20	21	10	11	21	31	20	30	20	21	30	31
	21	31	11	30	31	30	11	10	20	11	21	10	20	21	11	10	31	20	30	21	31	30	20	21
16	30	11	31	11	10	30	30	31	11	20	10	21	10	11	21	20	20	31	21	30	21	20	30	31
	10	30	11	10	11	31	30	31	20	30	21	31	20	21	30	31	10	20	11	21	10	11	20	21
17	30	10	30	31	31	11	11	10	30	20	31	21	31	30	21	20	20	10	21	11	21	20	11	10
	20	30	21	20	21	31	30	31	10	30	11	31	10	11	30	31	20	10	21	11	20	21	10	11
18	10	30	20	31	31	21	21	20	30	10	31	11	31	30	11	10	10	20	11	21	11	10	21	20
	11	30	10	11	10	31	30	31	21	30	20	31	21	20	30	31	11	21	10	20	11	10	21	20
19	31	11	30	31	31	10	10	11	30	21	31	20	31	30	20	21	21	11	20	10	20	21	10	11
	21	30	20	21	20	31	30	31	11	30	10	31	11	10	30	31	21	11	20	10	21	20	11	10
20	11	30	21	30	31	31	20	20	21	30	11	31	10	31	30	10	11	21	10	20	10	11	20	21
	10	31	11	10	11	30	31	30	21	31	20	30	21	20	31	30	10	21	11	20	10	11	21	20
21	31	10	31	30	30	11	11	10	31	21	30	20	30	31	20	21	21	10	20	11	20	21	11	10
	11	31	10	11	10	30	31	30	20	31	21	30	21	20	31	30	11	20	10	21	11	10	21	20
22	31	11	31	30	30	10	10	11	31	20	30	21	30	31	21	20	20	11	21	10	21	20	10	11
	21	31	20	21	20	30	31	30	10	31	11	30	10	11	31	30	21	10	20	11	21	20	10	11
23	11	21	31	30	30	20	20	21	31	10	30	11	30	31	11	10	10	21	11	20	11	10	20	21
	20	31	21	20	21	30	31	30	11	31	10	30	11	10	31	30	20	11	21	10	20	21	11	10
24	31	20	31	30	30	21	21	20	31	11	30	10	30	31	10	11	11	20	10	21	10	11	21	20

Під час дослідження структурованої таблиці отриманих результатів експерименту (табл. 1) було виявлено, що всі логічні функції перекодування об'єднуються в дев'ять множин, які, в свою чергу, можливо умовно об'єднати в три великі блоки.

Класифікуємо функції перекодування на основі представлення вхідної та вихідної логічної функції.

Введемо необхідні позначення логічних функцій (рис. 1):

1. Проста логічна функція – **Пр** $\vec{F}$ (функції з номерами 1–8).

2. Складна логічна функція – **Ск** $\vec{F}$ (функції з номерами 9–24), причому:

a. складна логічна функція першого порядку – **Ск1** $\vec{F}$ (функції з номерами 9–16);

b. складна логічна функція другого порядку – **Ск2** $\vec{F}$ (функції з номерами 17–24).

Тому, виходячи із представлення логічних функцій (рис. 1) та структурованих результатів обчислювального експерименту (табл. 1), маємо наступну систематизацію по множинам функцій перекодування (табл. 2).

Таблиця 2

Систематизація функцій перекодування

$\vec{F}_{Vuh}$ / $\vec{F}_{Vh}$	**Пр** $\vec{F}_{Vuh}$	**Ск1** $\vec{F}_{Vuh}$	**Ск2** $\vec{F}_{Vuh}$
Пр $\vec{F}_{Vh}$	M_1	M_2	M_3
Ск1 $\vec{F}_{Vh}$	M_4	M_5	M_6
Ск2 $\vec{F}_{Vh}$	M_7	M_8	M_9

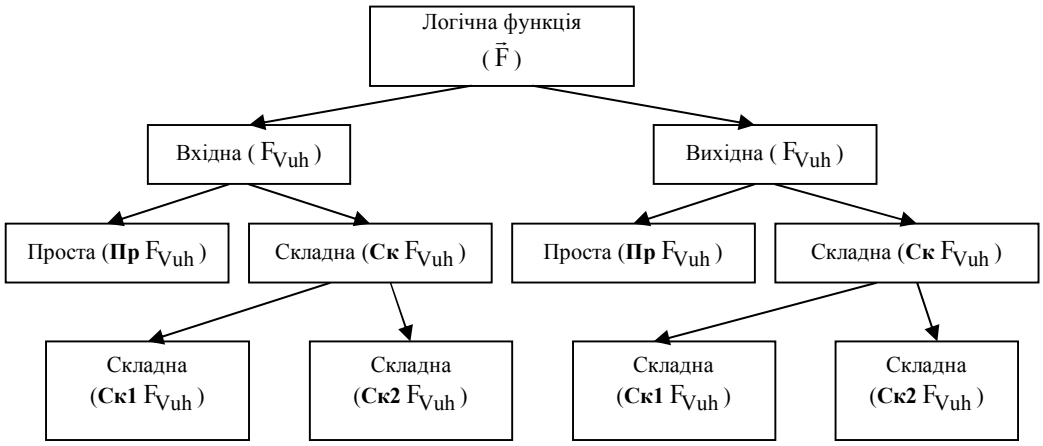

Рис. 1. Представлення логічних функцій

Проведемо нумерацію множин таблиці структурованих результатів зліва-направо та зверху-вниз. Тоді:

1) до першого умовного блоку логічних функцій перекодування (B_1) віднесемо першу (M_1), п'яту (M_5) та дев'яту (M_9) множини таблиці: $B_1 = \{M_1, M_5, M_9\}$;

2) до другого умовного блоку логічних функцій перекодування (B_2) віднесемо другу (M_2), третю (M_3) та шосту (M_6) множини таблиці: $B_2 = \{M_2, M_3, M_6\}$;

3) до третього умовного блоку логічних функцій перекодування (B_3) віднесемо четверту (M_4), сьому (M_7) та восьму (M_8) множини таблиці: $B_3 = \{M_4, M_7, M_8\}$.

Перший блок логічних функцій перекодування B_1 включає в себе лише прості логічні функції, одержані на основі перестановок та інверсій – це 8 спеціалізованих функцій [1 – 2, 7]:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix},\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix},\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix},$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix},\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix},\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix},$$

$$\vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Повна множина варіантів перекодування в кожній множині визначає 64 функції перекодування [4].

Аналогічно представляються множини M_5 та M_9 (рис. 1, табл. 2), враховуючи, що:

– для множини M_5 вхідною є – **Ск1** F_{Vuh}, а вихідною – **Ск1** F_{Vuh};

– для множини M_9 вхідною є – **Ск2** F_{Vuh}, а вихідною – **Ск2** F_{Vuh}.

Ввівши позначення функції перекодування як $\vec{F}_{a.b.c}$, де a – номер блоку, b – номер множини, c – особистий номер логічної функції, одержимо скорочені набори функцій перекодування для кожної із

множин першого блоку:

$$B_1 = \left\{ \begin{array}{l} M_1 = \{\vec{F}_{1.1.1}, \vec{F}_{1.1.2}, \vec{F}_{1.1.3}, \vec{F}_{1.1.4}, \vec{F}_{1.1.5}, \vec{F}_{1.1.6}, \vec{F}_{1.1.7}, \vec{F}_{1.1.8}\}, \\ M_5 = \{\vec{F}_{1.5.1}, \vec{F}_{1.5.2}, \vec{F}_{1.5.3}, \vec{F}_{1.5.4}, \vec{F}_{1.5.5}, \vec{F}_{1.5.6}, \vec{F}_{1.5.7}, \vec{F}_{1.5.8}\}, \\ M_9 = \{\vec{F}_{1.9.1}, \vec{F}_{1.9.2}, \vec{F}_{1.9.3}, \vec{F}_{1.9.4}, \vec{F}_{1.9.5}, \vec{F}_{1.9.6}, \vec{F}_{1.9.7}, \vec{F}_{1.9.8}\} \end{array} \right\}.$$

Другий B_2 та третій B_3 блоки логічних функцій перекодування включають в себе складні логічні функції першого та другого порядків, одержані на основі перестановок та інверсій відповідно першого або другого розрядів і суми за модулем першого та другого розряду - це 16 спеціалізованих функцій:

– складні логічні функції першого порядку **Ск1** $\vec{F}$:

$$\vec{F}_9 = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}, \ \vec{F}_{10} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix},$$

$$\vec{F}_{11} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{12} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}, \ \vec{F}_{13} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}$$

$$\vec{F}_{14} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{pmatrix}, \ \vec{F}_{15} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{16} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix};$$

– складні логічні функції другого порядку **Ск2** $\vec{F}$:

$$\vec{F}_{17} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix}, \ \vec{F}_{18} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix},$$

$$\vec{F}_{19} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}, \ \vec{F}_{20} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{21} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{22} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}, \ \vec{F}_{23} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{24} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Аналізуючи множини M_2, M_3, M_6 (рис. 1, табл. 4) другого умовного блоку B_2 класифікатора, маємо:

– для множини M_2 вхідною функцією є – **Пр** F_{Vuh}, а вихідною - **Ск1** F_{Vuh};

– для множини M_3 вхідною функцією є – **Пр** F_{Vuh}, а вихідною – **Ск2** F_{Vuh};

– для множини M_6 вхідною функцією є – **Ск1** F_{Vuh}, а вихідною – **Ск2** F_{Vuh}.

Аналогічно для множин M_4, M_7, M_8 (рис. 1, табл. 2) третього умовного блоку B_3 класифікатора:

– для множини M_4 вхідною функцією є – **Ск1** F_{Vuh}, а вихідною - **Пр** $\vec{F}_{Vuh}$;

– для множини M_7 вхідною функцією є – **Ск2** F_{Vuh}, а вихідною – **Пр** $\vec{F}_{Vuh}$;

– для множини M_8 вхідною функцією є – **Ск2** F_{Vuh}, а вихідною – **Ск1** F_{Vuh}.

Отже, для другого та третього умовних блоків класифікатора маємо скорочені набори функцій перекодування:

$$B_2 = \left\{ \begin{array}{l} M_2 = \left\{ \begin{array}{l} \vec{F}_{2.2.9}, \ \vec{F}_{2.2.10}, \ \vec{F}_{2.2.11}, \ \vec{F}_{2.2.12}, \ \vec{F}_{2.2.13}, \ \vec{F}_{2.2.14}, \ \vec{F}_{2.2.15}, \ \vec{F}_{2.2.16}, \\ \vec{F}_{2.2.17}, \ \vec{F}_{2.2.18}, \ \vec{F}_{2.2.19}, \ \vec{F}_{2.2.20}, \ \vec{F}_{2.2.21}, \ \vec{F}_{2.2.22}, \ \vec{F}_{2.2.23}, \ \vec{F}_{2.2.24} \end{array} \right\}, \\ M_3 = \left\{ \begin{array}{l} \vec{F}_{2.3.9}, \ \vec{F}_{2.3.10} \ \vec{F}_{2.3.11}, \ \vec{F}_{2.3.12}, \ \vec{F}_{2.3.13}, \ \vec{F}_{2.3.14}, \ \vec{F}_{2.3.15}, \ \vec{F}_{2.3.16}, \\ \vec{F}_{2.3.17}, \ \vec{F}_{2.3.18}, \ \vec{F}_{2.3.19}, \ \vec{F}_{2.3.20}, \ \vec{F}_{2.3.21}, \ \vec{F}_{2.3.22}, \ \vec{F}_{2.3.23}, \ \vec{F}_{2.3.24} \end{array} \right\}, \\ M_6 = \left\{ \begin{array}{l} \vec{F}_{2.6.9}, \ \vec{F}_{2.6.10}, \ \vec{F}_{2.6.11}, \ \vec{F}_{2.6.12}, \ \vec{F}_{2.6.13}, \ \vec{F}_{2.6.14}, \ \vec{F}_{2.6.15}, \ \vec{F}_{2.6.16}, \\ \vec{F}_{2.6.17}, \ \vec{F}_{2.6.18}, \ \vec{F}_{2.6.19}, \ \vec{F}_{2.6.20}, \ \vec{F}_{2.6.21}, \ \vec{F}_{2.6.22}, \ \vec{F}_{2.6.23}, \ \vec{F}_{2.3.24} \end{array} \right\} \end{array} \right\},$$

$$B_3 = \left\{ \begin{array}{l} M_4 = \left\{ \begin{array}{l} \vec{F}_{3.4.9}, \ \vec{F}_{3.4.10}, \ \vec{F}_{3.4.11}, \ \vec{F}_{3.4.12}, \ \vec{F}_{3.4.13}, \ \vec{F}_{3.4.14}, \ \vec{F}_{3.4.15}, \ \vec{F}_{3.4.16}, \\ \vec{F}_{3.4.17}, \ \vec{F}_{3.4.18}, \ \vec{F}_{3.4.19}, \ \vec{F}_{3.4.20}, \ \vec{F}_{3.4.21}, \ \vec{F}_{3.4.22}, \ \vec{F}_{3.4.23}, \ \vec{F}_{3.4.24} \end{array} \right\}, \\ M_7 = \left\{ \begin{array}{l} \vec{F}_{3.7.9}, \ \vec{F}_{3.7.10} \ \vec{F}_{3.7.11}, \ \vec{F}_{3.7.12}, \ \vec{F}_{3.7.13}, \ \vec{F}_{3.7.14}, \ \vec{F}_{3.7.15}, \ \vec{F}_{3.7.16}, \\ \vec{F}_{3.7.17}, \ \vec{F}_{3.7.18}, \ \vec{F}_{3.7.19}, \ \vec{F}_{3.7.20}, \ \vec{F}_{3.7.21}, \ \vec{F}_{3.7.22}, \ \vec{F}_{3.7.23}, \ \vec{F}_{3.7.24} \end{array} \right\}, \\ M_8 = \left\{ \begin{array}{l} \vec{F}_{3.8.9}, \ \vec{F}_{3.8.10}, \ \vec{F}_{3.8.11}, \ \vec{F}_{3.8.12}, \ \vec{F}_{3.8.13}, \ \vec{F}_{3.8.14}, \ \vec{F}_{3.8.15}, \ \vec{F}_{3.8.16}, \\ \vec{F}_{3.8.17}, \ \vec{F}_{3.8.18}, \ \vec{F}_{3.8.19}, \ \vec{F}_{3.8.20}, \ \vec{F}_{3.8.21}, \ \vec{F}_{3.8.22}, \ \vec{F}_{3.8.23}, \ \vec{F}_{3.8.24} \end{array} \right\} \end{array} \right\},$$

Узагальнюючи обгрунтування правильності отриманих функцій перекодування, сформулюємо наступні твердження.

Теорема 1. Якщо вхідна $\vec{F}_{Vh}$ та вихідна $\vec{F}_{Vuh}$ логічні функції кодування мають однакове представлення (рис. 1), то відповідна їм функція перекодування буде простою логічною функцією **Пр** $\vec{F}_{Pk}$ (рис. 2), тобто належатиме одній із множин першого умовного блоку класифікатора $B_1 = \{M_1, M_5, M_9\}$.

Наслідок теореми 1. Якщо вхідна $\vec{F}_{Vh}$ та вихідна $\vec{F}_{Vuh}$ логічні функції кодування мають різне представлення (рис. 2), то відповідна їм функція перекодування буде складною логічною функцією першого **Ск1** $\vec{F}_{Pk}$ або другого **Ск2** $\vec{F}_{Pk}$ порядку, тобто належатиме одній із множин другого або третього умовних блоків класифікатора: $B_2 = \{M_2, M_3, M_6\}$ або $B_3 = \{M_4, M_7, M_8\}$.

Висновки

Шляхом аналізу структурного табличного представлення результатів експерименту було проведено систематизацію спеціалізованих логічних функцій перекодування, яка дала змогу спростити подальший аналіз та виявлення взаємозв'язків між відомими вхідними та вихідними функціями кодування інформації.

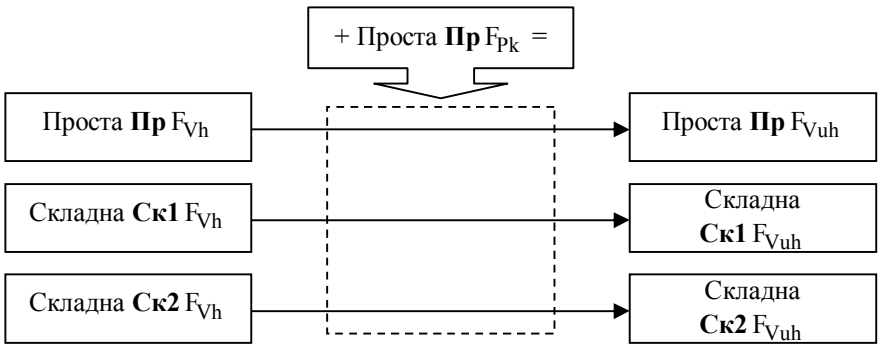

Рис. 2. Практичний результат використання теореми 1

Отримані результати дослідження експериментальних даних на основі їх векторного представлення дозволили сформулювати теорему, які забезпечили достатнє наукове обґрунтування правильності одержаних результатів та коректності використання спеціалізованих логічних функцій для підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Список літератури

1. Рудницький В.М. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Системи управління, навігації та зв'язку: зб. наук. пр. – К.: ДП «Центральний науково-дослідний інститут навігації і управління» Мінпромполітики, 2010. – Вип. 2(14). – С. 118-122.

2. Рудницький В.М. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Вісник Черкаського державного технологічного університету. – 2010. – Вип. 3. – С. 60-65.

3. Бабенко В.Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій: Дис. канд. техн. наук: 05.13.21 / Бабенко Віра Григорівна. – Черкаси, 2009. – 166 с.

4. Рудницький В.М. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Системи обробки інформації: зб. наук. пр. – Х.: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2010. – Вип. 5(86). – С. 15-19.

5. Бабенко В.Г. Алгоритми синтезу логічних функцій для систем захисту інформації / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Інтегровані інформаційні технології та системи (ІІТС-2007). – К.:НАУ, 2007. – С. 46-48.

6. Бабенко В.Г. Результати моделювання логічних функцій для криптографії / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Сучасні інформаційні системи. Проблеми і тенденції розвитку: Зб. матеріалів конференції. – Х.: ХНУРЕ, 2007. – С. 421-422.

7. Миронець І.В. Визначення логічних функцій для криптоперетворення інформації / І.В. Миронець // «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ'2010»: матеріали десятої наук.-техн. конференції молодих вчених, 23-26 листопада 2010 р.: зб. тез доп. – Х.: НАКУ ім. М.Є. Жуковського «Харківський авіаційний інститут» , 2010.

Надійшла до редколегії 18.10.2011

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

СИСТЕМАТИЗАЦИЯ ПОЛНОГО МНОЖЕСТВА ЛОГИЧЕСКИХ ФУНКЦИЙ ДЛЯ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

В.Н. Рудницкий, И.В. Миронец, В.Г. Бабенко

Данная статья посвящена определению и систематизации полного множества логических функций для криптографического перекодирования информации. Полученные логические функции перекодировки могут найти практическое применение для перекодирования информации конфиденциального назначения в криптографических системах защиты информации. Вместе с ранее известными методами и средствами они позволят в перспективе значительно улучшить оперативность доступа к удаленной защищенной информации.

Ключевые слова: *конфиденциальные информационные ресурсы, оперативность доступа, криптографическое преобразование, функция перекодировки.*

SYSTEMATIZATION OF THE FULL SET OF LOGICAL FUNCTIONS OF CRYPTOGRAPHIC DATA CONVERSION

V.N. Rudnitsky, I.V. Mironets, V.G. Babenko

This article is devoted to defining and systemizing a full set of logical functions of cryptographic re-encoding information. The resulting conversion logical functions may find practical application for re-encoding confidential information to the cryptographic information protect systems. Together with previously known methods and means they will eventually greatly improve the efficiency of remote access to protected information.

Keywords*: confidential information resources, efficiency of access, cryptographic data conversion, the conversion function.*