УДК 621.391

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

Черкаський державний технологічний університет, Черкаси

ТЕХНОЛОГІЯ ПОБУДОВИ ПРИСТРОЮ РЕАЛІЗАЦІЇ МЕТОДУ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Дана стаття присвячена розробці та реалізації пристроїв криптографічного перекодування інформації з метою застосування методу підвищення оперативності доступу до конфіденційної інформації в системах захисту інформації на основі спеціалізованих логічних функцій. Отримана схема реалізації методу дає змогу використовувати одержані функціональні схеми не лише для перекодування інформації, а й для проведення операцій кодування та декодування. Крім того, одержані технічні рішення забезпечують отримання позитивного ефекту за рахунок обробки кількості інформації, більшої ніж довжина ключової послідовності.

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

Вступ

Постановка проблеми. Довгий час криптографія була прерогативою держави, а криптографічні алгоритми вважалися військовими технологіями. Поширення інформаційних технологій вимусило до необхідності інтеграції в них все більш стійких механізмів безпеки, що неможливо без використання надійних криптографічних алгоритмів і це призводить до того, що криптографія втрачає військовий статус. Внаслідок такої ситуації, до недавнього часу, з причини браку інформації було важко визначити ступінь надійності криптографічних алгоритмів, та, навіть, знайти їх описи. Це призводило до використання різних примітивних методів криптографічного захисту чи до створення абсолютно ненадійних алгоритмів.

На сьогоднішній день існує величезна кількість криптографічних алгоритмів, що відрізняються як своїми загальними характеристиками, так і принципами, на яких базується їх робота. Не всі вони є однаково надійними - серед них є навіть такі, що оформлені як стандарти та при цьому не забезпечують скільки-небудь реального захисту. Насправді ж, створення надійного криптографічного алгоритму – дуже важка задача. Крім того, надійність є відносна річ – багато з раніше розроблених алгоритмів, які вважалися надійними, тепер або ненадійні, або ця надійність викликає великий сумнів. Тому при розробці криптографічного алгоритму необхідно враховувати тенденції розвитку комп'ютерної техніки а також інші фактори, що потенційно можуть знизити його стійкість в майбутньому.

Аналіз останніх досліджень і публікацій. На основі огляду поширених криптографічних систем можливо виділити групу алгоритмів захисту інформації, які реалізують криптографічні перетворення на основі згенерованого ключа [1 – 7].

В автоматизованих системах криптографічного захисту в якості операції криптографічного додавання, як правило, використовується операція додавання за

модулем два, яка реалізується суматором за модулем два. Традиційно розглядається, що суматор виконує операцію додавання за модулем відкритого тексту та ключової послідовності. З іншого боку можна функцію додавання за модулем два можна розглядати як сукупність двох функцій: повторення та інверсія, які виконуються над відкритим текстом, залежно від вхідних бітів ключової послідовності. Таким чином з'являється можливість представити процес роботи суматора як пристрою, який виконує перетворення відкритого тексту в залежності від ключової послідовності.

Даний підхід (рис. 1) можна розглядати як базовий для вдосконалення процесу криптографічного перетворення інформації [8].

Рис. 1. Типова структура процесу криптографічного захисту інформації на основі логічних функцій

Мета статті полягає у дослідженні технології побудови пристрою перекодування інформації на основі реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Основний матеріал

Повний набір визначених логічних функцій перекодування складає 576 функцій [9 – 12]. Проведення досліджень і доведень можливих алгоритмів синтезу функцій перекодування на основі представлень цих функцій, виявилось досить трудомістким і не практичним. Одним із шляхів спрощення аналізу отриманих результатів обчислювального експерименту може бути використання матричного представлення спеціалізованих логічних функцій.

Розглянемо загальний матричний вигляд логічної функції як добуток двох матриць, тоді одержимо:

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix} = \\ = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \\ a_{21}x_1 \oplus a_{22}x_2 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \vec{F}_a \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} * \vec{F}_b^i \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, \quad (1)$$

де $a_{i,j} = \overline{0,1}$, $b_i = \overline{0,1}$, $\oplus$ – сума по модулю два.

Формула (1) дає можливість розглядати базову логічну функцію $\vec{F}_a \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ без врахування інверсії та функцію інверсій $\vec{F}_b^i \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ окремо [1 – 4].

Виходячи з даної гіпотези, вдосконалимо типову структуру криптосистеми, доповнивши її двома новими блоками, а саме блоком формування наборів команд функцій інверсій, що надходить із основного блоку генерації ключової послідовності, та блоком виконання функцій інверсій. Дана структура зображена на рис. 2.

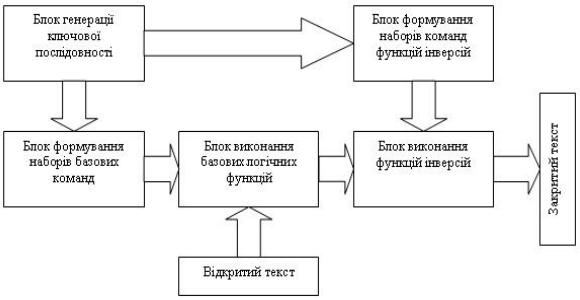

Рис. 2. Вдосконалена структура процесу криптографічного захисту інформації на основі логічних функцій

В основу розробки технології підвищення оперативності доступу до конфіденційних інформаційних ресурсів було покладено метод підвищення швидкодії систем захисту інформації на основі спеціалізованих логічних функцій [22].

Технологія доступу до інформації полягає в наступному (рис. 3). Вдосконалимо дану технологію за рахунок базових та інверсних функцій перекодування (рис. 4). Отримана схема доступу до інформації набуде відображення схематичної реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

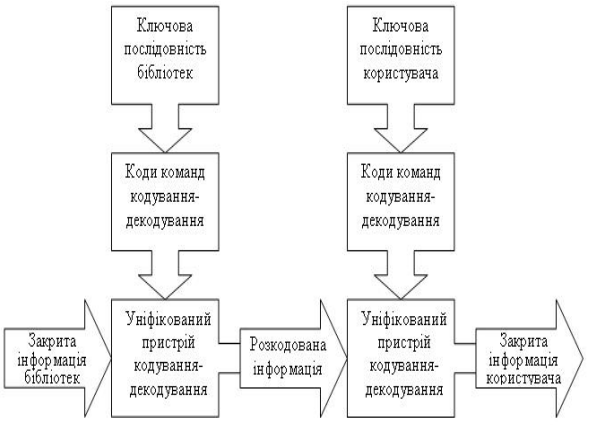

Рис. 3. Структурна схема технології доступу до конфіденційної інформації

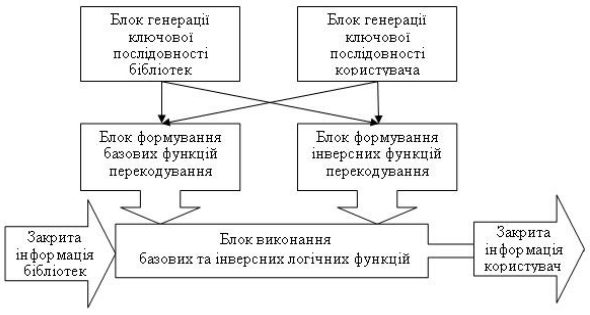

Рис. 4. Технологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів

Так як роботи по дослідженню логічних функцій з можливістю побудови функцій перекодування взагалі раніше не проводились, то для отримання результату, а саме – математичної моделі побудови функцій перекодування, було послідовно розглянуто 5 ідей, на основі яких сформульовано і досліджено підходи вибору наборів логічних функцій. Та лише 5-ий підхід дозволив отримати модель логічної функції перекодування, найбільш повну за описом та найпростішу для математичної та практичної реалізації [11, 12].

В результаті проведення досліджень було одержано модель синтезу функції перекодування без врахування інверсій відповідно матричного представлення вхідної та вихідної логічних функцій [10].

Було досліджено два підходи по синтезу функцій перекодування для повної множини логічних функцій. Але, виходячи із отриманих моделей, було зроблено висновок, що практичне застосування одержаних математичних моделей логічних функцій до повної множини результатів обчислювального експерименту є досить громіздким в обрахунках і не дає можливості побудувати дискретний пристрій придатний для практичної реалізації. Тому було використано другий підхід, який полягає в тому, що перетворення інформації є рознесеним в часі на перетворення базової функції перекодування та функції інверсії [12].

Отримані математичні моделі функцій перекодування дозволили розробити технологію та одержати алгоритм методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів, в основу якого було покладено метод підвищення швидкодії систем захисту інформації на основі спеціалізованих логічних функцій.

Узагальнивши результати, сформулюємо алгоритм реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів:

1. Проаналізувати ключову послідовність бібліотеки, визначити матрицю вхідної логічної функції згідно формули (2), на основі якої виконано кодування інформації:

$$\vec{F}_{Vh} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} * \begin{pmatrix} x_9 \\ x_{10} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_9 \\ x_3 & x_4 & x_{10} \end{pmatrix}. \quad (2)$$

2. Проаналізувати ключову послідовність користувача, визначити матрицю вихідної логічної функції згідно формули (3), на основі якої виконано кодування інформації користувача:

$$\vec{F}_{Vuh} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} * \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_5 & x_6 & x_{11} \\ x_7 & x_8 & x_{12} \end{pmatrix}. \quad (3)$$

3. Виділити базові вхідну $\vec{F}_{Vh}$ та вихідну $\vec{F}_{Vuh}$ матриці із матриць логічних функцій одержаних в пунктах 1 і 2, згідно формул (4):

$$\vec{F}_{Vh} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, \quad \vec{F}_{Vuh} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix},$$

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}. \quad (4)$$

4. На основі виразу (5) отримати базову функцію перекодування інформації:

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) \end{pmatrix}. \quad (5)$$

Для реалізації виразу (5) необхідно за допомогою сигналів управління $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ отримати сигнали управління f_1, f_2, f_3, f_4.

Реалізуємо функцію перекодування у вигляді чотирьох функціональних схем, які синтезують функції f_1, f_2, f_3, f_4. Побудуємо функціональну схему реалізації фрагменту команди першого розряду функції перекодування:

$$f_1 = (x_3 \bar{x}_5 \vee \bar{x}_3 x_5) \vee (x_4 \bar{x}_6 \vee \bar{x}_4 x_6). \quad (6)$$

Комбінаційна схема, яка реалізує функцію f_1, згідно до формули (6), буде мати вигляд наведений на рис. 5.

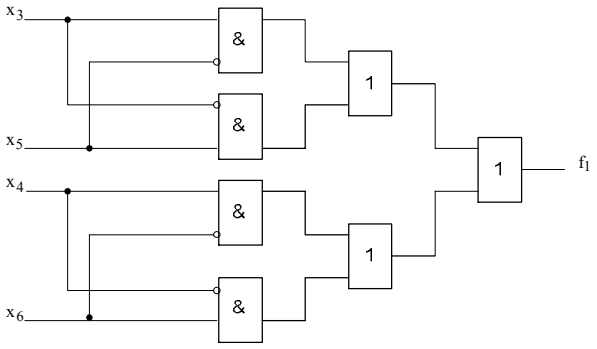

Рис. 5. Комбінаційна схема формування сигналу управління першого розряду функції перекодування

З метою зменшення кількості входів логічних елементів, а також часу, який витрачається на процес криптографічного перетворення та враховуючи формули (5, 6), модернізуємо рис. 5 як показано на рис. 6.

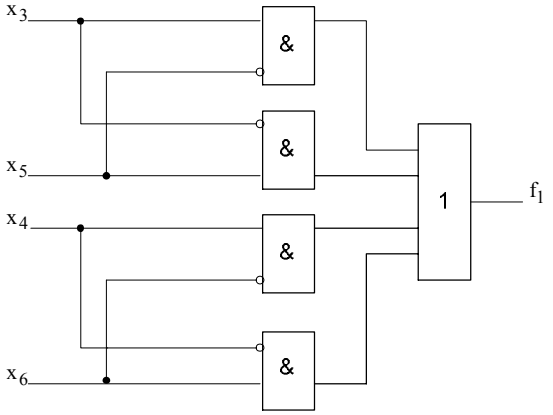

Рис. 6. Удосконалена комбінаційна схема формування сигналу управління першого розряду функції перекодування

Аналогічним способом побудуємо функціональні схеми реалізації фрагментів команди другого,

третього та четвертого f_2, f_3, f_4 розрядів функції перекодування згідно формул (5):

$$f_2 = (x_1\bar{x}_5 \vee \bar{x}_1x_5) \vee (x_2\bar{x}_6 \vee \bar{x}_2x_6); \quad (7)$$

$$f_3 = (x_3\bar{x}_7 \vee \bar{x}_3x_7) \vee (x_4\bar{x}_8 \vee \bar{x}_4x_8); \quad (8)$$

$$f_4 = (x_1\bar{x}_7 \vee \bar{x}_1x_7) \vee (x_2\bar{x}_8 \vee \bar{x}_2x_8). \quad (9)$$

Модернізовані комбінаційні схеми, які реалізують функції f_2, f_3, f_4 згідно до формул (7) – (9), матимуть такий вигляд (рис. 7 – 9).

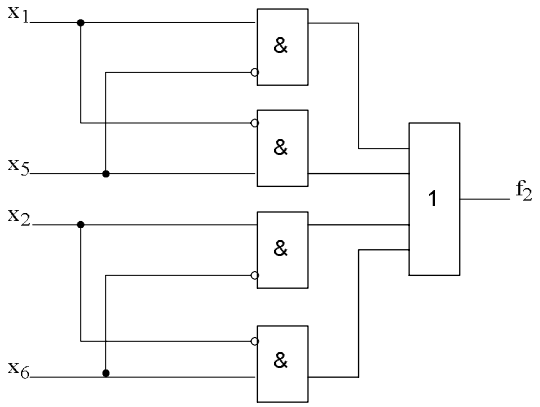

Рис. 7. Удосконалена комбінаційна схема формування сигналу управління другого розряду функції перекодування

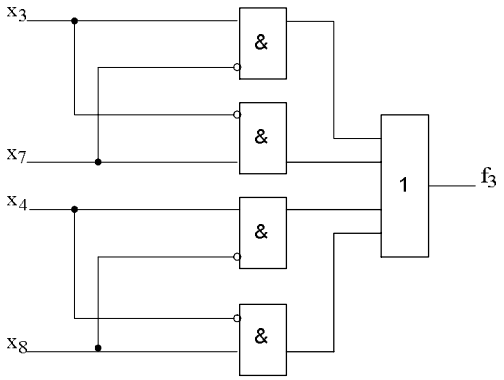

Рис. 8. Удосконалена комбінаційна схема формування сигналу управління третього розряду функції перекодування

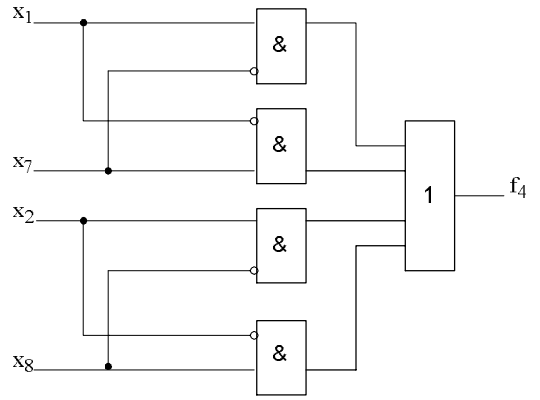

Рис. 9. Удосконалена комбінаційна схема формування сигналу управління четвертого розряду функції перекодування

Виходячи із викладеного матеріалу та беручи до уваги результати досліджень попередніх розділів, побудуємо комбінаційну схему пристрою реалізації базової функції перекодування для методу підвищення оперативності доступу до конфіденційної інформації.

Відповідно до (5), математична модель пристрою реалізації базової функції перекодування матиме наступний вигляд:

$$\begin{aligned} b_1 &= a_1\bar{a}_2f_1 \vee a_1f_1\bar{f}_2 \vee \bar{a}_1a_2f_2 \vee a_2\bar{f}_1f_2; \\ b_2 &= a_1\bar{a}_2f_3 \vee a_1f_3\bar{f}_4 \vee \bar{a}_1a_2f_4 \vee a_2\bar{f}_3f_4. \end{aligned} \quad (10)$$

В даній моделі враховано наступні позначення:

– $\vec{F}_{Vh}\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ – інформація вхідної функції;

– $\vec{F}_{Vuh}\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ – інформація вихідної функції;

– $\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$ – команди функції перекодування.

Комбінаційна схема, яка реалізує модель (10) представлена на рис. 10.

Одержана комбінаційна схема пристрою (рис. 10) забезпечує виконання криптографічного перетворення, що полягає у застосуванні повної множини логічних функцій перекодування. Управління схемою реалізується за допомогою команд управління пристроєм, що надходять на чотири входи управління (f_1, f_2, f_3, f_4 відповідно).

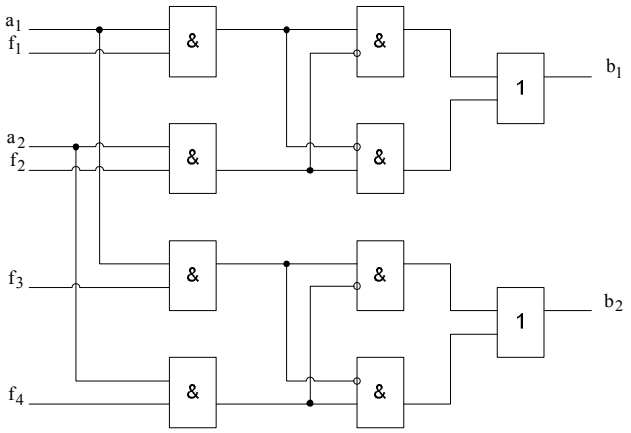

Рис. 10. Комбінаційна схема пристрою реалізації базової функції перекодування

5. Виділити матриці інверсних вхідної $\vec{F}^i_{Vh}$ та вихідної $\vec{F}^i_{Vuh}$ функцій із матриць логічних функцій одержаних в пунктах 1 і 2:

$$\vec{F}^i_{Vh} = \begin{pmatrix} x_9 \\ x_{10} \end{pmatrix}, \quad \vec{F}^i_{Vuh} = \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix}. \quad (11)$$

6. Отримати інверсну функцію перекодування (13) для логічних вхідної $\vec{F}^i_{Vh}$ та вихідної $\vec{F}^i_{Vuh}$ функцій інверсій, враховуючи формулу (12) – загальний

вигляд шуканої функції перекодування для повної множини логічних функцій:

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} * \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix}; \quad (12)$$

$$\vec{F}^{i}_{Pk} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} x_9 \oplus x_{11} \\ x_{10} \oplus x_{12} \end{pmatrix}. \quad (13)$$

Виходячи із викладеного матеріалу побудуємо математичну модель пристрою реалізації функції перекодування інверсій для методу підвищення оперативності доступу до конфіденційної інформації в комп'ютерних системах.

Оскільки входами пристрою виконання функцій перекодування інверсій є виходи пристрою виконання базових функцій перекодування, введемо наступні позначення:

– $\vec{F}_{Vh}\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ – інформація вихідної функції для функції перекодування інверсій;

– $\vec{F}_{Vuh}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ – інформація вихідної функції;

– $\vec{F}^{i}_{Pk} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} x_9 \oplus x_{11} \\ x_{10} \oplus x_{12} \end{pmatrix}$ – команди функції перекодування інверсій.

Відповідно до введених позначень, математична модель пристрою реалізації функції перекодування інверсій матиме наступний вигляд:

$$\begin{aligned} c_1 &= \bar{x}_{10} b_1 \vee x_9 b_1 \bar{b}_2 \vee \bar{x}_9 b_2 \vee x_{10} \bar{b}_1 b_2, \\ c_2 &= \bar{x}_{11} b_2 \vee x_{11} b_1 \bar{b}_2 \vee \bar{x}_{12} b_1 \vee x_{12} \bar{b}_1 b_2. \end{aligned} \quad (14)$$

7. Перекодувати функцію представлену в коді бібліотеки у функцію користувача на основі отриманих моделей за допомогою синтезованих пристроїв.

Отримані технічні рішення дозволяють використовувати одержані комбінаційні схеми не лише для перекодування інформації, а й для проведення операцій кодування та декодування.

На основі комбінаційних схем рис. 5 - 10 технологія перекодування і декодування перекодованої інформації буде мати наступну послідовність:

1. Перекодування:
1.1. Перекодування базової функції.
1.2. Перекодування інверсної функції.
2. Декодування:
2.1. Декодування інверсної функції.
2.2. Декодування базової функції.

Виходячи із викладеного матеріалу, очевидно, що етап перекодування та етап декодування відрізняються послідовністю виконання операцій, причому, якщо зміниться послідовність виконання дій в процесі перекодування, то зміниться послідовність дій і в процесі подальшого декодування інформації.

Виходячи з вище сказаного, структурна схема реалізації технології доступу до інформації на основі методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів в комп'ютерних системах дещо ускладнюється.

Нову структурну схему технології підвищення оперативності доступу до конфіденційних інформаційних ресурсів з використанням та врахуванням результатів проведених досліджень зображено на рис. 11.

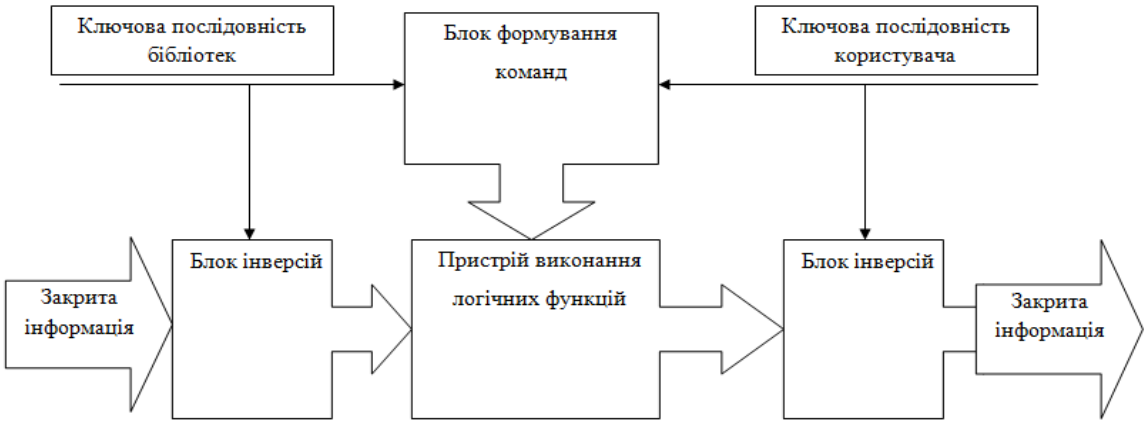

Рис. 11. Структурна схема реалізації технології доступу до інформації на основі методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів в комп'ютерних системах

В даній схемі замінено блок формування інверсій блоком формування інверсій ключової послідовності бібліотек та блоком формування інверсій ключової послідовності користувача, тоді, згідно табл. 4.6, одержимо нові коди сигналів управління інверсних логічних функцій відповідно для кожного з вище названих блоків формування інверсій.

Враховуючи функцію перекодування інверсій (13) та позначення математичних моделей (10) і (14), коди сигналів управління інверсних логічних функцій відповідно для кожного блоків формування інверсій набудуть наступного вигляду:

1) для блоку формування інверсій ключової послідовності бібліотек:

$$f_5^1 = a_1 \oplus x_9, \; f_6^1 = a_2 \oplus x_{10}; \quad (15)$$

2) для блоку формування інверсій ключової послідовності користувача:

$$f_5^2 = a_1 \oplus x_{11},\ f_6^2 = a_2 \oplus x_{12}. \qquad (16)$$

Сумарна складність блоків інверсій описаних виразами (15) та (16) менша складності блоку інверсій на рис. 4, який описується моделлю (14).

Подальше використання одержаних результатів можливе і доцільне при розробці систем інформаційної безпеки й вибору варіантів швидкодіючих та надійних рішень покращення якості функціонування систем захисту інформації.

Висновки

В основу розробки пристрою перекодування інформації покладено метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання логічних функцій для криптографічного перетворення шляхом введення логічних функцій перекодування, що дозволило зменшити час доступу до інформації за рахунок заміни процесу «декодування-кодування».

Отримана схема реалізації методу дає змогу використовувати одержані функціональні схеми не лише для перекодування інформації, а й для проведення операцій кодування та декодування. Крім того, одержані технічні рішення забезпечують отримання позитивного ефекту за рахунок обробки кількості інформації, більшої ніж довжина ключової послідовності.

Список літератури

1. Спосіб шифрування інформації на основі шифру Файстеля / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк,. В.М. Кінзерявий // Вісник інженерної академії України. – 2009. – № 2. – С. 117-121.

2. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК-Пресс, 2003. – 656 с.

3. Рудницький В.М. Синтез математичних моделей пристроїв декодування інформації для криптографічних систем / В.М. Рудницький, В.Г. Бабенко // Системи обробки інформації: зб. наук. пр. – Х.: ХУ ПС, 2009. – Вип. 2 (76). – С. 124-128.

4. Корченко О.Г. Конвейерный криптографический вычислитель реального времени / О.Г. Корченко, А.В. Малофеев, Ю.Е. Хохлачева // Захист інформації: журн. – К.: ДУІКТ, 2010. – Вип. № 2 (47). – С. 30-36.

5. Молдовян А.А. Криптография: учебник для вузов / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. – СПб.: Лань, 2000. – 224 с.

6. Молдовян Н.А. Скоростные блочные шифры / Н.А. Молдовян. – СПб.: СПбГУ, 1998. – 230 с.

7. Нечаев В.И. Элементы криптографии. Основы теории защиты информации / В.И. Нечаев. – М.: Высшая школа, 1999. – 109 с.

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

9. 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.: ХУ ПС, 2010. – Вип. 5 (86). – С. 15-19.

10. 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 «ЦНДІ НіУ», 2010. – Вип. 2 (14). – С. 118-122.

11. Рудницький В.М. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Вісник Черкаського державного технологічного університету. – 2010. – Вип. № 3. – С. 60-65.

12. Рудницький В.М. Дослідження алгоритмів синтезу функцій перекодування / В.М. Рудницький, І.В. Миронець // Вісник Черкаського державного технологічного університету. – 2010. – Вип. № 4. – С. 60-64.

Надійшла до редколегії 24.10.2011

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

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ УСТРОЙСТВА РЕАЛИЗАЦИИ МЕТОДА ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ

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

Данная статья посвящена разработке и реализации устройств криптографического перекодирования информации с целью применения метода повышения оперативности доступа к конфиденциальной информации в системах защиты информации на основе специализированных логических функций. Полученная схема реализации метода позволяет использовать построенные функциональные схемы не только для перекодирования информации, но и для проведения операций кодирования и декодирования. Кроме того, данные технические решения обеспечивают получение положительного эффекта за счет обработки количества информации, большей чем длина ключевой последовательности.

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

TECHNOLOGY OF CONSTRUCTION DEVICE OF IMPLEMENTING THE METHOD OF EXPEDITING ACCESS TO CONFIDENTIAL INFORMATION RESOURCES

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

This article focuses on the development and implementation devices of cryptographic convertion information, in order to apply the method of expediting access to confidential information in the information protect systems based on specialized logical functions. The scheme implementation of the method allows the use of functional circuits built not only for re-encoding of information, but also for encoding and decoding operations. In addition, these solutions provide a receipt of a positive effect due to the amount of information processing, greater than the length of key sequence.

Keywords: *confidential information resources, method of expediting access, cryptographic convertion, re-encoding function.*