УДК 621.391

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

Черкаський державний технологічний університет, Черкаси

МЕТОДОЛОГІЯ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Дана стаття присвячена вирішенню проблеми оперативності доступу до конфіденційних інформаційних ресурсів. Одним із найефективніших рішень даної задачі є використання спеціалізованих логічних функцій, які забезпечують оперативність обробки інформації та підвищують захищеність і криптостійкість систем обробки інформації. Розробка принципів, методів і алгоритмів синтезу наборів спеціалізованих логічних функцій, придатних для криптографічного перетворення інформації, згідно запропонованого підходу ґрунтується на положеннях теорії логіки, криптографії, комп'ютерного моделювання та математичного апарату теорії інформації, систем числення, методів дискретної математики.

Ключові слова: *конфіденційні інформаційні ресурси, оперативність доступу, криптографія, криптосистема, захист інформації, функція перекодування, спеціалізовані логічні функції.*

Вступ

Постановка проблеми. Інформацію сьогодні слід розглядати як стратегічний продукт. Здатність суспільства та його інституцій збирати, обробляти, аналізувати, систематизувати та накопичувати інформацію, забезпечувати свободу інформаційного обміну є важливою передумовою соціального та технологічного прогресу, чинником національної безпеки, однією з основ успішної внутрішньої та зовнішньої політики. Інформаційна сфера має системоутворюючий характер і впливає практично на всі галузі суспільних відносин.

Обчислювальна та комунікаційна техніка, телекомунікаційні мережі, бази і банки даних та знань, інформаційні технології, система інформаційно-аналітичних центрів різного рівня, виробництво технічних засобів інформатизації, системи науково-дослідних установ та підготовки висококваліфікованих фахівців є складовими національної інформаційної інфраструктури і основними чинниками, що забезпечують економічне піднесення. Як показує досвід інших країн, інформатизація сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, розвитку наукоємних виробництв та високих технологій, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства.

На сьогодні системи накопичення і оброблення інформації та реалізація доступу до них з використанням мережних технологій (Internet, Intranet) швидко розвиваються і комерціалізуються. Крім традиційних послуг обміну інформацією (електронна пошта, ftp) і найбільш популярної – доступ до інформаційних ресурсів (Web), активно розвивається розподілене оброблення даних, корпоративні мережі, електронна комерція, реклама. У всіх галузях суспільно-економічного життя запорукою успіху є володіння первинною достовірною інформацією та її професійна аналітична обробка.

Серед найважливіших напрямів фундаментальних досліджень в галузі природничих, технічних і гуманітарних наук за 2009-2013 роки затвердженими постановою Президії Національної академії наук України від 25.02.09 № 55 велика увага приділяється розробці методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії, розробці методів підвищення продуктивності систем криптографії, формуванню наукових інформаційних ресурсів.

Виходячи з цього можна сформулювати проблему наукового дослідження, яка полягає в підвищенні оперативності передачі конфіденційної інформації зі спеціалізованих бібліотек віддаленим користувачам.

Дослідження проблеми захисту інформації здійснюється як у напряму розкриття сутності явища щодо порушення конфіденційності та цілісності інформації, так і в напряму розробки практичних методів її захисту. Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється більшою вартістю, однак їй властиві і переваги: висока продуктивність, простота, захищеність і т.д. Програмна реалізація більш практична, припускає гнучкість у використанні [1 – 3].

Аналіз останніх досліджень і публікацій. Криптографія є одним із найбільш потужних засобів забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регуляторів безпеки [4, 5].

Для вирішення проблеми оперативності доступу до конфіденційних інформаційних ресурсів розг-

лядаються заходи законодавчого, адміністративного, процедурного і програмно-технічного рівня. В сфері інформаційної безпеки важливі не скільки окремі рішення (закони, навчальні курси, програмно-технічні вироби), що знаходяться на сучасному рівні, стільки механізми генерації нових рішень, які дозволяють, як мінімум, адекватно реагувати на загрози інформаційної безпеки або передбачувати нові загрози і вміти їм протистояти [6].

Мета статті полягає у доведенні справедливості використання спеціалізованих логічних функцій для забезпечення оперативності доступу до конфіденційних інформаційних ресурсів.

Основний матеріал

Оперативність обробки інформації в криптографічних системах або їх швидкодія, залежить від ряду додаткових характеристик: швидкість/час обробки блоку даних VB, tB; швидкість/час отримання ключа VK, tK; швидкість/час перетворення даних VD.

Так як у будь-якій криптографічній системі інформація обробляється на основі реалізованого алгоритму криптографічних перетворень деякими блоками із використанням ключа, що генерується для кожного блоку окремо, швидкість обробки блоку визначається як сума швидкості отримання ключа для даного блоку та швидкості реалізації криптографічних перетворень над даним блоком інформації. В силу лінійності дана функціональна залежність описується наступним чином: VB = VK + VD. Так як VK << VD, то одним із напрямів підвищення якості криптосистем може бути розробка методів криптографічного перетворення, які забезпечать збільшення E за рахунок збільшення LB при постійному S та несуттєвому збільшенні CR та VB [1, 2, 9].

Наведемо необхідні для викладення матеріалу визначення.

Прямою функцією називається функція операндами якої не є константи (x_1).

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

Функція називається *простою*, якщо вона залежить лише від одного аргументу.

Функція називається *складною*, якщо вона залежить від декількох аргументів складених по модулю.

Правильно розміщеною функцією називається функція, номер якої співпадає з номером одного із аргументів.

Неправильно розміщеною функцією називається функція, номер якої не співпадає з номером аргументів.

Вхідною функцією кодування називається функція, якою закодована інформація в базі даних інформаційних ресурсів.

Вихідною функцією кодування називається функція, якою закодована інформація інформаційних ресурсів для користувача.

Функцією перекодування називається функція, яка забезпечує перекодування інформації із вхідної функції у вихідну функцію.

Структура системи доступу до конфіденційних інформаційних ресурсів зображена на рис. 1.

Рис. 1. Система доступу до конфіденційних інформаційних ресурсів

Підвищення швидкодії робочої системи можливе за рахунок модернізації блоків 2 і 3 структури, тобто замінити ці етапи етапом перекодування, що забезпечить зменшення часу на обробку інформації і розкриття інформації перед підготовкою передачі користувачеві.

Одним із найбільш ефективних вирішенням даної задачі є використання спеціалізованих логічних функцій, які забезпечують оперативність обробки інформації та підвищують захищеність і криптостійкість систем [4].

Сутність методології підвищення оперативності доступу до конфіденційних інформаційних ресурсів полягає в наступному.

Нехай справедливі функції перетворення інформації: $y = f_1(x)$, $y = f_2(x)$, такі що $f_1(f_2(x)) = y$. Також нехай справедливими є функції: $y = f_3(x)$, $y = f_4(x)$, такі що $f_3(f_4(x)) = y$. Тоді існує функція $y = f^*(x)$, яка забезпечує перетворення інформації:

$$y = f_1(f^*(x)) = f_3(x).$$

Іншими словами: існує спеціалізована логічна функція $y = f^*(x)$, яка забезпечує перекодування із однієї функції в іншу без етапу розкодування інформації.

Наступні дослідження проводилися з метою визначення $y = f^*(x)$, при відомих $y = f_1(x)$ та $y = f_3(x)$.

За результатами досліджень отримано логічні функції, які можуть бути використані в системах

захисту інформації на етапі криптографічного додавання [7, 8].

У процесі синтезу спеціалізованих логічних функцій використовується математичний апарат теорії інформації, систем числення, методів дискретної математики. Розробка принципів, методів і алгоритмів синтезу наборів спеціалізованих логічних функцій, придатних для криптографічного перетворення інформації, згідно запропонованого підходу базується на положеннях теорії логіки, криптографії та комп'ютерного моделювання [9].

Один із варіантів синтезу спеціалізованих логічних функцій двох змінних для криптографії полягає у використанні операцій перестановок, інверсій та заміщень простих логічних функцій складними.

Для доведення коректності використаємо векторне представлення функцій кодування – декодування

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

Для здійснення переходу до векторного представлення нам необхідно з математичних моделей пристроїв кодування-декодування виключити операцію рівнозначності. Для цього скористаємось виразами [9]:

$$f = (f \oplus 0), \quad \overline{f} = (f \oplus 1).$$

Для проведення дослідження обмежимося лише спеціалізованими логічними функціями, які можна отримати лише на основі перестановок та інверсій – це 8 спеціалізованих функцій [7 – 9]:

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

$$\vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix}; \quad \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}; \quad \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};$$

$$\vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}; \quad \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Розглянемо більш детально взаємне перетворення спеціалізованих логічних функцій, яке може бути використано для підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Якщо вхідна функція кодування представлена як $\vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}$, а вихідна функція кодування - як $\vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}$, то функція перекодування матиме вигляд $\vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}$.

Доведення: Маємо отримати структуру перетворення:

$$\vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}.$$

Тому нехай маємо $\vec{F}_7\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix}$, тоді $\vec{F}_3\begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} Y_1 \oplus 1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} = F_6\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, що й треба було довести.

Якщо вхідна функція кодування представлена як $\vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}$, а вихідна функція кодування - як $\vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}$, то функція перекодування матиме вигляд $\vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}$.

Доведення: Маємо отримати структуру перетворення:

$$\vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Тому нехай маємо $\vec{F}_3\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix}$, тоді:

$$\vec{F}_6\begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} Y_2 \oplus 1 \\ Y_1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \oplus 1 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 0 \end{pmatrix} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} = F_8\begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

що й треба було довести.

На основі аналогічних доведень для повної множини варіантів перекодування структуруємо отримані функції за їхнім виглядом, що дозволить зменшити обсяг матеріалу та полегшить простоту його сприймання:

1). Якщо як функція перекодування використовується $\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ одержимо:

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

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}; \ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}; \ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}; \ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

2). Якщо як функція перекодування використовується $\vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$, одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix}.$$

3). Якщо як функція перекодування використовується $\vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}$ одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}.$$

4). Якщо як функція перекодування використовується $\vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix}$ одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}.$$

5). Якщо як функція перекодування використовується $\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}$ одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}.$$

6). Якщо як функція перекодування використовується $\vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}$ одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}.$$

7). Якщо як функція перекодування використовується $\vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}$ одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

8). Якщо як функція перекодування використовується $\vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}$ одержимо:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix};\ \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix};\ \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix};\ \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix};\ \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix};\ \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}.$$

Повна множина варіантів перекодування на основі спеціалізованих логічних функцій визначає 64 функції перекодування. Доведення коректності даних функцій є аналогічним до представлених.

Розглянутий матеріал доводить доцільність використання спеціалізованих логічних функцій для забезпечення оперативності доступу до конфіденційних інформаційних ресурсів.

Висновки

Запропонована методологія побудови систем доступу до конфіденційних інформаційних ресурсів дозволяє:

1) зменшити час доступу до конфіденційних інформаційних ресурсів за рахунок заміни етапів декодування та кодування у форматі користувача на етап перекодування;

2) підвищити конфіденційність збереження інформації за рахунок обмеження доступу технічних працівників електронних бібліотек до конфіденційних інформаційних ресурсів;

3) даний підхід дозволяє використовувати для побудови систем захисту конфіденційних інформаційних ресурсів будь-які спеціалізовані логічні функції придатні для криптографії.

Список літератури

1. *Безбогов А.А. Криптографическая защита информации: учебное пособие / А.А. Безбогов, А.Я. Яковлев, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.*
2. *Фергюссон Н. Практическая криптография: пер. с англ. / Нильс Фергюссон, Брюс Шнайер – М.: Торговый дом «Вильямс», 2005. – 424 с.*
3. *Brassard G. Modern Cryptography: a Tutorial / G. Brassard. – Springer-Verlang, 1988.*
4. *Миронець І.В. Технологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів / І.В. Миронець // Інтегровані комп'ютерні технології в машинобудуванні ІКТМ 2009: міжнародна науково-технічна конференція – Х., 2009. – Т. 2. – С. 184.*
5. *Карпов В.Е. Основы операционных систем: курс лекций, учебное пособие [Электронный ресурс] / В.Е. Карпов, К.А. Коньков. – 2004. – 632 с. – Режим доступа к учебному пособию: http:/intuit.ru.*
6. *Безбогов А.А. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.Я. Яковлев, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.*
7. *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*
8. *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.*
9. *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.*

Надійшла до редколегії 30.04.2010

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

МЕТОДОЛОГИЯ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ

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

Данная статья посвящена решению проблемы оперативности доступа к конфиденциальным информационным ресурсам. Одним из наиболее эффективных решений данной задачи является использование специализированных логических функций, обеспечивающих оперативность обработки информации и повышают защищенность и криптостойкость систем обработки информации. Разработка принципов, методов и алгоритмов синтеза наборов специализированных логических функций, пригодных для криптографического преобразования информации, согласно предложенного подхода базируется на положениях теории логики, криптографии, компьютерного моделирования и математического аппарата теории информации, систем счисления, методов дискретной математики.

Ключевые слова: *конфиденциальные информационные ресурсы, оперативность доступа, криптография, криптосистема, защита информации, функция перекодировки, специализированные логические функции.*

METHODOLOGY OF EXPEDITING ACCESS TO CONFIDENTIAL INFORMATION RESOURCES

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

This article is devoted to solving a problem of o-line access to confidential information resources. One of the most effective solution of this problem is using specialized logic functions that provide information processing efficiency and improve a security and cryptographic of information processing systems. According to the proposed approach the development principles, methods and algorithms of synthesis of specialized logic functions sets suitable for cryptographic transformation of data is based on the provisions of the theory of logic, cryptography, computer simulation and mathematical apparatus of information theory, number systems, methods of discrete mathematics.

Keywords: *confidential information resources, online access, cryptography, cryptosystem, information security, function transcode, specialized logic functions.*