УДК 621.391

# РЕАЛІЗАЦІЯ МЕТОДУ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

**Миронець І.В.,**
**Рудницький В.М.,** *д.т.н, професор,*
Черкаський державний технологічний університет

*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.*

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

*This article is devoted to solving a problem of access efficiency to confidential information resources. One of the most effective solution of this problem is the usage of specialized logic functions that provide information processing efficiency and improve security and cryptoresistability of information processing systems.*

***Key words:*** *confidential information resources, efficiency access, cryptography, information security decoding function, specialized logic functions.*

**Актуальність теми.** Одним із найважливіших показників зміни способу життя в XXI столітті є розвиток та використання прогресивних інформаційних технологій у всіх сферах соціального життя та діяльності, рівень виробництва та споживання суспільством інформаційних продуктів та послуг. У цьому аспекті особливого значення набувають комп'ютерні мережі. У свою чергу організація мереж обумовлює витрати на комп'ютерну техніку і впливає на швидкість і зручність роботи з інформацією. До однієї і тієї ж інформації можуть звертатися декілька людей, а потім передавати мережею результати своєї роботи. Прогрес технічних засобів в останні роки і збільшення обсягів інформації зумовлюють необхідність швидкого і зручного способу її пошуку та обробки.

Розвиток автоматизованих інформаційних систем (АІС) призвів до їх впровадження в різних сферах людської діяльності. Як наслідок цього відбулося ускладнення самих систем і розширення кола їх користувачів. У сучасних умовах актуалізується і одночасно ускладнюється проблема оперативності доступу до конфіденційної інформації, адже несанкціоноване спотворення, копіювання, знищення інформації зачіпає не тільки процеси, що стосуються сфери державного управління, але й інтереси фізичних осіб. Як наслідок, зростає відповідальність за ухвалення точних і відповідальних рішень у ситуаціях, коли навіть окремі помилки здатні призвести до тяжких наслідків у сфері економіки, фінансів, екології та ін. [1].

Таким чином, можна констатувати, що актуальність проблеми підвищення оперативності доступу до конфіденційних інформаційних ресурсів може розглядатися в трьох аспектах, які обумовлені тенденціями світового розвитку суспільства, економіки, а також науки і техніки.

**Аналіз останніх джерел досліджень і публікацій.** Технічною базою для створення умов розвитку систем доступу до конфіденційних інформаційних ресурсів стали досягнення інформатики і обчислювальної техніки, мікроелектроніки, телекомунікацій тощо.

Важливий вклад у розвиток криптології та захисту інформації зробили такі вітчизняні та зарубіжні науковці, як І.Д. Горбенко, В.А. Мухачев, В.А. Хорошко, А.А. Молдовян, Ю.В. Кузнецов, О.Г. Корченко, Г.Ф. Конахович, Б. Шнайер, М. Хеллман, Ч.Г. Беннет, Ж. Брассар та ін.

В тому числі, наприклад, В.М. Сидельніков і С.О. Шестаков внесли пропозицію використання ряду варіантів схем на основі теоретико-кодових конструкцій, застосовуючи швидкі алгоритми декодування. Б.В. Березін, П.В. Дорошкевич досліджували

схеми електронно-цифрового підпису на основі симетричних алгоритмів. А.Н. Фіонов, Б.Я. Рябко виклали основні підходи і методи сучасної криптографії для вирішення задач, які виникають при обробці, зберіганні і передачі інформації [2, 3, 4].

Проте 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.

Одним із шляхів оперативності доступу до конфіденційних інформаційних ресурсів є використання спеціалізованих логічних функцій.

Методологія даного підходу розглянута в літературі [5]. Проте в цій роботі розглядається перекодування інформації на основі спеціалізованих логічних функцій лише за допомогою перестановок та інверсій.

Основна **мета** даної статті полягає у підвищенні оперативності доступу до конфіденційних інформаційних ресурсів за рахунок розширення набору функцій перекодування.

**Основний матеріал дослідження**. Основна сутність методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів полягає в наступному [5]: якщо справедливі такі 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.

В роботі [5] було проведено дослідження з метою визначення $y = f^*(x)$, при відомих $y = f_1(x)$ та $y = f_3(x)$, а також використовувалося векторне представлення функцій кодування – декодування:

$$\mathbf{r}_F\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix}.$$

Для проведення дослідження обмежимося спеціалізованими логічними функціями, які можна отримати на основі перестановок, інверсій та заміщень [5]:

$$\mathbf{r}_{F_9} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}, \ \mathbf{r}_{F_{10}} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix},$$

$$\mathbf{r}_{F_{11}} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}, \ \mathbf{r}_{F_{12}} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix},$$

$$\mathbf{r}_{F_{13}} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}, \ \mathbf{r}_{F_{14}} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{pmatrix},$$

$$\mathbf{r}_{F_{15}} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}, \ \mathbf{r}_{F_{16}} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}.$$

Для коректності доведення 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 [5].

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 $\mathbf{r}_{F_{13}} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}$, а вихідна функція кодування – як $\mathbf{r}_{F_9} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$, то функція перекодування матиме вигляд $\mathbf{r}_{F_4} = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix}$.

*Доведення:* Маємо отримати структуру перетворення:

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_4}=\begin{pmatrix}x_1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}$$

Тому нехай маємо

$$\mathbf{r}_{F_{13}}\begin{pmatrix}x_1\\ x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}=\begin{pmatrix}Y_1\\ Y_2\end{pmatrix},$$

тоді

$$\mathbf{r}_{F_4}\begin{pmatrix}Y_1\\ Y_2\end{pmatrix}=\begin{pmatrix}Y_1\\ Y_2\oplus 1\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\oplus 1\end{pmatrix}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 0\end{pmatrix}=$$
$$=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}=\mathbf{r}_{F_9}\begin{pmatrix}x_1\\ x_2\end{pmatrix}.$$

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 $\mathbf{r}_{F_1}=\begin{pmatrix}x_1\\ x_2\end{pmatrix}$ одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}.$$

2) Якщо як функція перекодування використовується $\mathbf{r}_{F_2}=\begin{pmatrix}x_2\\ x_1\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}.$$

3) Якщо як функція перекодування використовується $\mathbf{r}_{F_3}=\begin{pmatrix}x_1\oplus 1\\ x_2\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}.$$

4) Якщо як функція перекодування використовується $\mathbf{r}_{F_4}=\begin{pmatrix}x_1\\ x_2\oplus 1\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}.$$

5) Якщо як функція перекодування використовується $\mathbf{r}_{F_5}=\begin{pmatrix}x_1\oplus 1\\ x_2\oplus 1\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}.$$

6) Якщо як функція перекодування використовується $\mathbf{r}_{F_6}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus 1\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

7) Якщо як функція перекодування використовується $\mathbf{r}_{F_7}=\begin{pmatrix}x_2\\ x_1\oplus 1\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}.$$

8) Якщо як функція перекодування використовується $\mathbf{r}_{F_8}=\begin{pmatrix}x_2\oplus 1\\ x_1\end{pmatrix}$, одержимо:

$$\mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{13}}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_{10}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{14}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{pmatrix}\to \mathbf{r}_{F_{12}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix},$$

$$\mathbf{r}_{F_{15}}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to \mathbf{r}_{F_9}=\begin{pmatrix}x_1\oplus x_2\\ x_2\end{pmatrix},$$

$$\mathbf{r}_{F_{16}}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to \mathbf{r}_{F_{11}}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}.$$

Повна множина варіантів перекодування на основі спеціалізованих логічних функцій

визначає 64 функції перекодування. Доведення коректності даних функцій є аналогічним до представлених. [5]

**Висновки.** Запропонований метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів доводить доцільність використання спеціалізованих логічних функцій для оперативності доступу до конфіденційних інформаційних ресурсів. Причому, розширення кількості спеціалізованих логічних функцій дозволяє підвищити захищеність конфіденційної інформації. Також даний підхід створює теоретичну базу для подальших досліджень направлених на доведення доцільності використання спеціалізованих логічних функцій будь-якої складності.

## ЛІТЕРАТУРА


1. Бабенко В.Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій: Дис. канд. техн. наук: 05.13.21. – Черкаси, 2009. – 166 с.
2. Бабенко В.Г. Вибір наборів кодів команд для підвищення надійності та швидкодії систем захисту інформації // Захист інформації з обмеженим доступом та автоматизація її обробки: матеріали наук.-техн. конф. студентів та аспірантів, 12-13 лютого 2009 р.: зб. тез доп. – К.: НАУ, 2009. – С. 5–6.
3. Колесник В.Д. Курс теории информации / В.Д. Колесник, Г.Ш. Полтырев. – М.: Наука, 1982. – 416 с.
4. Жельников В. Криптография от папируса до компьютера / В. Жельников. – М.: ABF, 1996. – 335 с.
5. Миронець І.В., Рудницький В.М., Бабенко В.Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів // Системи обробки інформації: зб. наук. пр. – Х.: Харк. ун-т повітряних сил ім. Івана Кожедуба, 2010. – Вип. 5(86). – С. 15–19.



**Миронець І.В.,** аспірант кафедри системного програмування Черкаського державного технологічного університету.

**Рудницький В.М.,** д.т.н., професор, завідувач кафедри системного програмування Черкаського державного технологічного університету.