Таблиця 2

Імовірності появи символьних помилок при використанні методів завадостійкого кодування

Назва коду	**Відносна швидкість,** $R=m/n$	**Надлишковість коду,** $K=k/n$	Pc, **при** $E_c / N_0 = 2дБ$	Pc, **при** $E_c / N_0 = 10дБ$
ЛУ-код	0,985	0,015	2,35754e-2	4,53007e-6
Код Хемінга	0,994	0,006	2,30765e-2	4,12292e-6
ЛХ-код	0,966	0,034	2,46663e-2	5,52712e-6
CRC-32	0,985	0,015	2,35754e-2	4,53007e-6
CRC-64	0.97	0,03	2,44323e-2	5,30035e-6
БЧХ	0,799	0,201	3,69093e-2	3,20076e-5
Матричний код	0,955	0,045	2,53221e-2	6,20224e-6
ЛМ-код	0,886	0,114	2,98806e-2	1,27961e-5

Таким чином, показано, що при використанні коду умовних лишків відбувається зменшення ймовірностей появи символьних помилок та подальше повне усунення спотворень у інформаційному повідомленні з умов появи багатократних помилок, що підвищує ефективність та надійність функціонування ІКСМ з умов збільшення вірогідності інформаційного потоку даних, без втрат якості. Тобто, відбувається зменшення ймовірність появи символьних помилок та повне усунення спотворень у інформаційному повідомленні.

Використання даного коду дозволяє виявляти та виправляти багатократні помилки та усувати спотворення. Також, відбувається підвищення швидкості передачі даних, збільшення вірогідного потоку даних, економія смуги частот ІКСМ.

ЛІТЕРАТУРА

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Пер. с англ. – М.: Изд. дом Вильямс, 2004. – 1104 с.

2. Юдін О.К. Кодування в інформаційно-комунікаційних мережах – Монографія. К.: Книжкове видавництво НАУ, 2007. – 302 с.

3. Василенко В.С. Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об’єктів в умовах природних впливів / В.С. Василенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. –2006. – Вип. 2 (13) – С. 144 −159.

4. Пат. 67988 Україна, МПК H03M 13/00 Спосіб забезпечення цілісності інформації на базі завадостійкого коду умовних лишків/ Василенко В.С., Василенко М.Ю., Чунарьов А.В.; заявник та патентовласник Нац. авіац. ун-т. – u201110207; заявл. 19.08.2011; опубл.12.03.2012, Бюл. №. 5 – 4 с.

5. Чунарьов А.В. Забезпечення цілісності інформаційних ресурсів на базі методів завадостійкого кодування/ А.В.Чунарьов, М.Ю.Василенко // Наукоємні технології: наук.-техн. конф. студентів та молодих учених (Київ, 11–12 листопада 2011 р.) – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2011. – С.11.

Надійшла: 27.07.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 004.056.55:004.312.2

Рудницький В.М., Бабенко В.Г., Рудницький С.В.

МЕТОД СИНТЕЗУ МАТРИЧНИХ МОДЕЛЕЙ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕКОДУВАННЯ ІНФОРМАЦІЇ

У роботі запропонований математичний апарат, який покладений в основу розробки методу синтезу матричних моделей операцій криптографічного перекодування інформації на основі заданих вхідної та вихідної операцій криптографічного кодування.

Ключові слова: матрична модель, операція криптографічного перекодування, матриця перекодування.

Постановка проблеми у загальному вигляді та її зв'язок із важливими практичними завданнями. У даний час основними засобами захисту інформації в системах і мережах є криптографічні засоби, що реалізують різноманітні методи шифрування. Але

існуючі засоби шифрування не завжди задовольняють вимогам продуктивності, особливо при застосуванні у високошвидкісних комп'ютерних системах. Усе це обумовлює актуальність розробки методів шифрування інформації, які б забезпечували побудову шифрів, стійких до зламу, і створення високопродуктивних засобів шифрування для систем захисту інформації.

Відомі наукові праці, в яких доведено, що для забезпечення криптостійкості блокових шифрів потрібно використовувати перетворення на основі спеціальних логічних функцій, що називають бент-функціями. З цього випливають задачі наукового обґрунтування можливості синтезу спеціальних логічних функцій, стійких до лінійного і диференційного криптоаналізу, розробки методів блокового і потокового шифрування та алгоритмів і програмних засобів, що їх реалізують. Таким чином, усе сказане обумовлює актуальність задачі розробки методів синтезу спеціалізованих логічних операцій, що можуть використовуватись в якості криптографічних примітивів.

Аналіз останніх досліджень і публікацій показав, що особливу увагу привертають [1, 2], в яких одержано модель синтезу групи операцій перекодування на базі групи трьохрозрядних логічних операцій, що забезпечують криптографічне перетворення без врахування інверсій відповідно до матричного представлення вхідної та вихідної логічних операцій. У [3] був запропонований метод синтезу базових операцій криптографічного перетворення на основі заміщення однієї або декількох елементарних функцій зі збереженням інформативності. Крім цього, існують публікації присвячені питанням синтезу криптографічних примітивів на основі булевих функцій перетворення, проте не існує математичного апарату для побудови операцій перекодування інформації, а також відсутні методи знаходження матриці перекодування за допомою заданих матриць кодування. Саме тому вирішення даної задачі є необхідним як в теоретичному так і практичному аспекті.

Мета статті полягає у розробці методу синтезу матричних моделей операцій криптографічного перекодування інформації.

Основна частина. Основною задачею, яка вирішується, є знаходження операцій перекодування, які формуються з визначеного набору логічних операцій за допомогою операції композиція, для двох заданих операцій кодування, тобто дослідження функціональних залежностей між синтезованими операціями кодування, при чому операція перекодування теж повинна належати множині операцій кодування.

Якщо процес перекодування видозмінити так, щоб при застосуванні операції криптографічного перетворення над даними, які закодовані першим користувачем, безпосередньо одержували дані, які закодовані другим користувачем, без необхідності реалізації процесу декодування для повторного кодування. Звідси виходить, що дійсно застосування операції перекодування зменшує кількість перетворень, що потрібно виконати : $x_i^{**} = F_{перекод}(x_i^*) = F_{код2}(F_{декод}(F_{код1}(x_i)))$, де $x_i^* = F_{код1}(x_i),\ x_i = F_{декод}(x_i^*),\quad x_i^{**} = F_{код2}(x_i)$, де, в свою чергу, $F_{k1,}\, F_{k2,} F_{decoda}, F_p$ – операція криптографічного перетворення за допомогою коду 1, операція криптографічного перетворення за допомогою коду 2, операція криптографічного декодування для інформації перетвореної за допомогою коду 1 та операція криптографічного перекодування відповідно, при чому $x_i \in \{0;1\}$ – розряди інформації, $i = 1..n$, де n – кількість розрядів інформації, що беруть участь в криптоперетворенні.

У загальному вигляді операції криптографічного кодування побудовані на основі додавання за модулем два будуть описані наступною моделлю:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \oplus b_2 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix}, \qquad (1)$$

де $a_{ij}, b_i, x_i \in [0;1];\ \ i = 1..n;$ де n – кількість розрядів інформації, що беруть участь в процесі перетворення, $x_1..x_n$ – операнди-розряди інформації відповідно; a_{ij} – коефіцієнти матриці кодування; b_i – ознака наявності групи операцій інверсії; $\oplus$ – операція "сума за модулем 2".

$$\vec{F}_{k1} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n \end{pmatrix}, \tag{2}$$

Для спрощення отримання математичної моделі побудови операцій перекодування ми розглядали поєднання логічних операцій без врахування інверсії.

Якщо операції криптографічного кодування без врахування групи операцій інверсії ($b_i = 0$) задані виразами:

$$\vec{F}_{k2} = \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{nn}x_n \end{pmatrix}, \tag{3}$$

де $\vec{F}_{k1}, \vec{F}_{k2}$ – вхідна та вихідна операція криптографічного кодування відповідно, $a_{ij}, c_{ij}, x_i \in \{0;1\};\ \ i = 1..n;$ де n – кількість розрядів інформації, що беруть участь в процесі перетворення, $x_1..x_n$ – операнди-розряди інформації відповідно; a_{ij}, c_{ij} – коефіцієнти вхідної та вихідної матриці кодування відповідно; $\oplus$ – операція "сума за модулем 2".

Тоді операція криптографічного перекодування буде задана виразом:

$$\vec{F}_p = \begin{pmatrix} d_{11}y_1 \oplus d_{12}y_2 \oplus ... \oplus d_{1n}y_n \\ d_{21}y_1 \oplus d_{22}y_2 \oplus ... \oplus d_{2n}y_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ d_{n1}y_1 \oplus d_{n2}y_2 \oplus ... \oplus d_{nn}y_n \end{pmatrix}, \tag{4}$$

де $\vec{F}_p$, – операція криптографічного перекодування, $d_{ij}, y_i \in \{0;1\},\ i = 1..n;$ де n – кількість розрядів інформації, що беруть участь в процесі перетворення, $y_1...y_n$ – операнди-розряди інформації відповідно; d_{ij} – коефіцієнти матриці перекодування; $\oplus$ – операція "сума за модулем 2".

Наведемо детальний опис процесу знаходження операції (матриці) перекодування [4].

$$\vec{F}_p = \begin{pmatrix} d_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \\ \oplus d_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ d_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \\ \oplus d_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ d_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \\ \oplus d_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \end{pmatrix} = \tag{5}$$

$$= \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{nn}x_n \end{pmatrix}.$$

Цей процес можна представити у вигляді таких етапів:

1. Знайдемо перший рядок матриці перекодування.

Так як $d_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \oplus d_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) = c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n$, тоді d_{1i} є рішенням системи рівнянь:

$$\begin{cases} d_{11}a_{11} \oplus d_{12}a_{21} \oplus ... \oplus d_{1n}a_{n1} = c_{11} \\ d_{11}a_{12} \oplus d_{12}a_{22} \oplus ... \oplus d_{1n}a_{n2} = c_{12} \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{11}a_{1n} \oplus d_{12}a_{2n} \oplus ... \oplus d_{1n}a_{n\,n} = c_{1n} \end{cases}.$$

2. Знайдемо другий рядок матриці перекодування.

Так як $d_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \oplus d_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) = c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n$, тоді d_{2i} є рішенням системи рівнянь:

$$\begin{cases} d_{21}a_{11} \oplus d_{22}a_{21} \oplus ... \oplus d_{2n}a_{n1} = c_{21} \\ d_{21}a_{12} \oplus d_{22}a_{22} \oplus ... \oplus d_{2n}a_{n2} = c_{22} \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{21}a_{1n} \oplus d_{22}a_{2n} \oplus ... \oplus d_{2n}a_{n\,n} = c_{2n} \end{cases}.$$

3. Знайдемо n-ий рядок матриці перекодування.

Так як $d_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \oplus d_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) = c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{n\,n}x_n$, тоді d_{ni} є рішенням системи рівнянь:

$$\begin{cases} d_{n1}a_{11} \oplus d_{n2}a_{21} \oplus ... \oplus d_{nn}a_{n1} = c_{n1} \\ d_{n1}a_{12} \oplus d_{n2}a_{22} \oplus ... \oplus d_{nn}a_{n2} = c_{n2} \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{n1}a_{1n} \oplus d_{n2}a_{2n} \oplus ... \oplus d_{nn}a_{n\,n} = c_{nn} \end{cases}.$$

Приклад 1. Якщо перша операція криптографічного кодування задана матрицею (вхідна матриця) $\vec{F}_{k1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, а друга операція криптографічного кодування задана матрицею (вихідна матриця) $\vec{F}_{k2} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, тоді підставивши значення матриць в вираз (5) отримаємо: $\vec{F}_p = \begin{pmatrix} d_{11}x_1 \oplus d_{12}x_1 \oplus d_{12}x_2 \\ d_{21}x_1 \oplus d_{22}x_1 \oplus d_{22}x_2. \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$.

Для знаходження першого рядка матриці перекодування розв'яжемо систему рівнянь:

$$\begin{cases} d_{11} \oplus d_{12} = 1 \\ d_{12} = 1. \end{cases} = \begin{cases} d_{11} = 0 \\ d_{12} = 1. \end{cases}$$

Для знаходження другого рядка матриці перекодування розв'яжемо систему рівнянь:

$$\begin{cases} d_{21} \oplus d_{22} = 1 \\ d_{22} = 0. \end{cases} = \begin{cases} b_{21} = 1 \\ b_{22} = 0. \end{cases}$$

Отримана операція криптографічного перекодування буде задана матрицею $\vec{F}_p = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Приклад 2. Якщо перша операція криптографічного кодування задана матрицею (вхідна матриця) $\vec{F}_{k1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, а друга операція криптографічного кодування задана матрицею (вихідна матриця) $\vec{F}_{k2} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, тоді підставивши значення матриць в в вираз (5) отримаємо:

$$\vec{F}_p = \begin{pmatrix} d_{11}x_1 \oplus d_{11}x_3 \oplus d_{12}x_1 \oplus d_{12}x_2 \oplus d_{13}x_2 \\ d_{21}x_1 \oplus d_{21}x_3 \oplus d_{22}x_1 \oplus d_{22}x_2 \oplus d_{23}x_2 \\ d_{31}x_1 \oplus d_{31}x_3 \oplus d_{32}x_1 \oplus d_{32}x_2 \oplus d_{33}x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \end{pmatrix}.$$

Для знаходження першого рядка матриці перекодування розв’яжемо систему рівнянь:

$$\begin{cases} d_{11} \oplus d_{12} = 0 \\ d_{12} \oplus d_{13} = 1 \\ d_{11} = 0 \end{cases} = \begin{cases} d_{11} = 0 \\ d_{12} = 0. \\ d_{13} = 1 \end{cases}$$

Для знаходження другого рядка матриці перекодування розв’яжемо систему рівнянь:

$$\begin{cases} d_{21} \oplus d_{22} = 1 \\ d_{22} \oplus d_{23} = 1 \\ d_{21} = 1 \end{cases} = \begin{cases} d_{21} = 1 \\ d_{22} = 0. \\ d_{23} = 1 \end{cases}$$

Для знаходження третього рядка матриці перекодування розв’яжемо систему рівнянь:

$$\begin{cases} d_{31} \oplus d_{32} = 0 \\ d_{32} \oplus d_{33} = 1 \\ d_{31} = 1 \end{cases} = \begin{cases} d_{31} = 1 \\ d_{32} = 1. \\ d_{33} = 0 \end{cases}$$

Отримана операція криптографічного перекодування буде задана матрицею

$$\vec{F}_p = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Приклад 3. Якщо перша операція криптографічного кодування задана матрицею (вхідна матриця) $\vec{F}_{k1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, а друга операція криптографічного кодування задана

матрицею (вихідна матриця) $\vec{F}_{k2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$, тоді підставивши значення матриць в вираз (5) отримаємо:

$$\vec{F}_p = \begin{pmatrix} d_{11}x_1 \oplus d_{11}x_3 \oplus d_{11}x_4 \oplus d_{12}x_1 \oplus d_{12}x_2 \oplus d_{12}x_4 \oplus d_{13}x_1 \oplus d_{13}x_4 \oplus d_{14}x_2 \oplus d_{14}x_3 \oplus d_{14}x_4 \\ d_{21}x_1 \oplus d_{21}x_3 \oplus d_{21}x_4 \oplus d_{22}x_1 \oplus d_{22}x_2 \oplus d_{22}x_4 \oplus d_{23}x_1 \oplus d_{23}x_4 \oplus d_{24}x_2 \oplus d_{24}x_3 \oplus d_{24}x_4 \\ d_{31}x_1 \oplus d_{31}x_3 \oplus d_{31}x_4 \oplus d_{32}x_1 \oplus d_{32}x_2 \oplus d_{32}x_4 \oplus d_{33}x_1 \oplus d_{33}x_4 \oplus d_{34}x_2 \oplus d_{34}x_3 \oplus d_{34}x_4 \end{pmatrix} =$$

$$= \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_4 \\ x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_4 \end{pmatrix}.$$

Для знаходження першого рядка матриці перекодування розв'яжемо систему рівнянь:

$$\begin{cases} d_{11} \oplus d_{12} \oplus d_{13} = 1 \\ d_{12} \oplus d_{14} = 1 \\ d_{11} \oplus d_{14} = 1 \\ d_{11} \oplus d_{12} \oplus d_{13} \oplus d_{14} = 1 \end{cases} = \begin{cases} d_{11} = 1 \\ d_{12} = 1 \\ d_{13} = 1 \\ d_{14} = 0 \end{cases}.$$

Для знаходження другого рядка матриці перекодування розв'яжемо систему рівнянь:

$$\begin{cases} d_{21} \oplus d_{22} \oplus d_{23} = 0 \\ d_{22} \oplus d_{24} = 1 \\ d_{21} \oplus d_{24} = 0 \\ d_{21} \oplus d_{22} \oplus d_{23} \oplus d_{24} = 1 \end{cases} = \begin{cases} d_{21} = 1 \\ d_{22} = 0 \\ d_{23} = 1 \\ d_{24} = 1 \end{cases}.$$

Для знаходження третього рядка матриці перекодування розв'яжемо систему рівнянь:

$$\begin{cases} d_{31} \oplus d_{32} \oplus d_{33} = 1 \\ d_{32} \oplus d_{34} = 0 \\ d_{31} \oplus d_{34} = 1 \\ d_{31} \oplus d_{32} \oplus d_{33} \oplus d_{34} = 0 \end{cases} = \begin{cases} d_{31} = 0 \\ d_{32} = 1 \\ d_{33} = 0 \\ d_{34} = 1 \end{cases}.$$

Для знаходження четвертого рядка матриці перекодування розв'яжемо систему рівнянь:

$$\begin{cases} d_{41} \oplus d_{42} \oplus d_{43} = 1 \\ d_{42} \oplus d_{44} = 1 \\ d_{41} \oplus d_{44} = 1 \\ d_{41} \oplus d_{42} \oplus d_{43} \oplus d_{44} = 1 \end{cases} = \begin{cases} d_{41} = 1 \\ d_{42} = 1 \\ d_{43} = 0 \\ d_{44} = 0 \end{cases}.$$

Отримана операція криптографічного перекодування буде задана матрицею

$$\vec{F}_p = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

У результаті проведення досліджень було одержано математичну модель синтезу групи операцій перекодування на базі групи двох, трьох та чотирьохрозрядних логічних

операцій, що забезпечують криптографічне перетворення, без врахування інверсій відповідно до матричного представлення вхідної та вихідної логічних операцій.

Висновки. У даній роботі запропоновано спосіб побудови математичної моделі матриці перекодування з відомих вхідної та вихідної матриць кодування на основі операції суми за модулем два.

У дослідженні запропонований математичний апарат, який покладений в основу розробки методу синтезу матричних моделей операцій криптографічного перекодування інформації. До того ж, на прикладах моделей матриць двох, трьох та чотирьохрозрядних операцій криптографічного перетворення інформації підтверджена коректність застосування запропонованого методу.

ЛІТЕРАТУРА

1. Бабенко В.Г. Синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення / В.Г. Бабенко, С.В. Рудницький // Моделирование, идентификация, синтез систем управления // Сб. тезисов пятнадцатой Международной научно-технической конференции. 9-16 сентября 2012.Донецк: Изд. института прикладной математики и механики НАН Украины, 2012. . – С.190-191.

2. Бабенко В.Г. Дослідження групи трьохрозрядних криптографічних операцій / В.Г. Бабенко, С.В. Рудницький // Восьма наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба "Новітні технології – для захисту повітряного простору": Тези доповідей: 18-19 квітня 2012 року. – Харків: ХУПС ім. І. Кожедуба, 2012. – С.218.

3. Голуб С.В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С.В. Голуб, В.Г. Бабенко, С.В. Рудницький // Зб. наук. пр. «Системи обробки інформації». – Харків: ХУПС ім. І. Кожедуба. – 2012. – Випуск 3(101). – Том 1. – С. 119-122.

4. Ф.Р. Гантмахер. Теория матриц. М.: Наука. – 1966. – 576 стр.

Надійшла:

Рецензент: д.т.н., професор Хорошко В.О.

УДК 681.5.62:5(045)

Покидько Л.Н., Пепа Ю.В.

МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ ПОДВИЖНЫМ ИСТОЧНИКОМ ТЕПЛОВОГО ВОЗДЕЙСТВИЯ НА ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ

Рассмотрена структурная схема управления перемещением и мощностью подвижного лазерного источника излучения. Построены модели объекта с учетом теплового поля и предложен метод программного управления подвижным источником теплового воздействия.

Ключевые слова: модель, системы, управление, модули.

Аналитического моделирования нелинейных систем управления лазерным излучением и систем обработки информации о температурном поле защищаемых объектов как развернутой теории, которую можно было бы без ограничений применять на практике, как правило, не существует. Редкие системы, описываемые нелинейными моделями, удается подвергнуть традиционному анализу, который позволил бы аналитическим путем получать прогноз поведения технических систем обработки информации, описываемых нелинейными типовыми математическими моделями.

Известны два основных направления материального моделирования нелинейных систем - физическое и формальное с помощью вычислительных устройств. Они широко отражены в работах П.А. Алабужева, В.А. Штоффа, И.Б. Новика, Н.А. Уёмова и др.

Применение мощных электронно-лучевых и лазерных установок в системах нападения на защищаемые объекты привело к появлению систем управления с подвижными источниками воздействия на объект (плавка, сварка, термообработка, напыление пленок в вакууме). Подвижный источник обеспечивает создание определенного температурного поля для получения заданных свойств объекта.