Захист інформації

УДК 003.26:004.056.55

В.Г. Бабенко[1], С.В. Рудницький[2]

[1]*Одеська національна академія зв'язку ім. О.С. Попова, Одеса*
[2]*Черкаський державний технологічний університет, Черкаси*

РЕАЛІЗАЦІЯ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МАТРИЧНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

В статті розроблено метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення та структурна схема його застосування. Проведений синтез функціональних схем для реалізації елементарних функцій та операцій матричного криптографічного перетворення інформації на основі суми за модулем два. Проведено розробку алгоритмів застосування операцій матричного криптографічного перетворення та оцінка статистичних властивостей результатів криптографічного перетворення на їх основі.

Ключові слова: *матричні операції, криптографічне перетворення, оцінка статистичних властивостей, статичний портрет.*

Постановка проблеми

Нині відбувається глобальний перехід до інформаційного суспільства, розвиток якого нерозривно пов'язаний з інтенсифікацією інформаційних процесів, необхідністю збору, обробки і передавання величезних обсягів інформації. Інформатизація зачепила всі сфери діяльності людини в цілому: державне управління, фінанси, економіку, освіту, виробництво та ін.

Як наслідок розвиток інформаційних ресурсів нерозривно пов'язаний з їх інформаційною безпекою.

Одним з найбільш дієвих засобів захисту інформаційно-телекомунікаційних систем є використання методів та засобів криптографії.

На сьогоднішній день одним із перспективних напрямів розвитку криптографії є використання розширеного спектру операцій криптографічного перетворення для вдосконалення існуючих та побудови нових криптоалгоритмів.

В проаналізованих нами сучасних дослідженнях запропоновано ряд нових операцій криптографічного перетворення на основі булевих функцій (криптографічне перетворення). Проте залишається цілий ряд задач і проблем, зокрема побудова операцій криптографічного перетворення над великою кількістю змінних, розробка методів використання операцій криптографічного пертворення в алгоритмах та інші.

Вирішення поставлених задач забезпечить підвищення якості та ефективності систем інформаційної безпеки.

Аналіз останніх досліджень і публікацій. В роботах [1, 2] запропонований метод синтезу базових операцій криптографічного перетворення на основі заміщення однієї або декількох елементарних функцій зі збереженням інформативності, описані етапи синтезу трьохрозрядних операцій криптографічного перетворення на основі операції додавання за модулем два. Показано залежність порядку застосування логічних операцій криптографічного перетворення для процесу прямого та оберненого перетворення інформації. Отримано математичні моделі функцій взаємного перетворення.

В [3] проведена розробка та реалізація пристроїв криптографічного взаємного перетворення інформації з метою застосування методу підвищення оперативності доступу до конфіденційної інформації в системах захисту інформації на основі спеціалізованих логічних функцій.

Проте залишається невирішеним задача застосування синтезованих матричний операцій криптографічного перетворення для захисту інформаційних ресурсів.

Метою статті є формулювання методу захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення, розробка структурної схеми його застосування. Синтез функціональних схем для реалізації операцій матричного криптографічного перетворення інформації на основі суми за модулем два. Розробка алгоритмів застосування операцій матричного криптографічного перетворення та оцінка статистичних властивостей результатів криптографічного перетворення на їх основі.

Структура системи захисту інформації на основі матричних операцій криптографічного перетворення

В [4, 5] були розроблені методи синтезу матричних операцій прямого, оберненого та взаємного криптографічного перетворення інформації. На основі проведених досліджень були сформовані обмеження до існування прямих та обернених операцій (матриць):

Обмеження 1. Матриця повинна бути невиродженою: відсутні нульові рядки, чи нульові стовбці, тобто $\sum_{j=1}^{n} a_{ij} > 0$ або $\sum_{i=1}^{n} a_{ij} > 0$;

Обмеження 2. У матриці відсутні однакові рядки: $\sum_{j=1}^{n} (a_{ij} \oplus a_{lj}) > 0$;

Обмеження 3. Сума по модулю два двох чи декількох рядків не повторює існуючий рядок матриці:

$$\sum_{j=1}^{n} (a_{ij} \oplus a_{lj} \oplus a_{hj} \oplus \ldots \oplus a_{uj}) > 0 .$$

Відповідність цим вимогам забезпечує наявність розв'язку виразу (1) і як наслідок існування для кожної прямої операції (матриці) перетворення оберненої операції (матриці).

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n); \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n); \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n). \end{pmatrix} = \quad (1)$$

$$= \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ \ldots & \ldots & \ldots & \\ & & & a_{n\,n}x_n \end{pmatrix}.$$

Отримані в попередніх дослідженнях [4, 5] результати дозволяють сформулювати метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення:

1. На основі даних пароля сформулювати первинну не вироджену матрицю криптографічного прямого перетворення.

Для виконання обмежень 1-3 до існування прямих та обернених операцій (матриць) перетворення, які забезпечують існування не виродженої матриці. Синтез матриці проводиться на основі послідовного додавання за модулем два рядків матриці. Кількість доданків для синтезу кожного рядка матриці, а також номера доданків (рядків) визначаються паролем.

При закінченні даних пароля формування матриці продовжується на основі псевдовипадкової послідовності.

Якщо при побудові первинної матриці пароль не вичерпано, то він використовується для корекції матриці прямого перетворення на наступних циклах роботи, а в іншому випадку використовується псевдовипадкова послідовність.

2. Корекція матриці криптографічного прямого перетворення на основі псевдовипадкової послідовності (або даних паролю).

3. Перевірка правильності синтезу матриці криптографічного прямого перетворення.

3.1. Шляхом вирішення відповідних систем рівнянь для розв'язку виразу (1) побудувати матрицю криптографічного оберненого перетворення.

3.2. Шляхом вирішення відповідних систем рівнянь побудувати матрицю криптографічного взаємного перетворення, що відповідає розв'язку виразу (2).

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

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

Наявність рішень системи рівнянь пунктів 3.1-3.2 підтверджують правильність проведення корекції матриці криптографічного прямого перетворення, так як для вироджених матриць дані системи рівнянь не мають розв'язків.

4. Криптографічне перетворення інформації на основі матриць прямого, оберненого та взаємного криптографічного перетворення в залежності від поставлених задач.

5. Перехід до наступного циклу криптографічного перетворення (пункту 2) при наявності вхідної інформації.

Структурна схема реалізації методу захисту інформаційних ресурсів на основі матричних операцій криптографічного пертворення представлена на рис. 1.

Рис. 1. Структурна схема реалізації методу захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення

Синтез функціональних схем реалізації матричних операцій криптографічного перетворення

Блок виконання криптографічного перетворення (рис. 1) реалізує операцію матричного криптографічного перетворення. В загальному виді операції криптографічного перетворення побудовані на основі додавання за модулем два описуються моделлю (3).

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \oplus b_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix}, \qquad (3)$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1 \ldots x_n$ - операнди відповідно; $\oplus$ – операція "сума за модулем 2".

Операція криптографічного перетворення будується із елементарних функцій матричного криптографічного перетворення. В загальному вигляді елементарна функція матричного криптографічного перетворення відповідно до виразу (3) без врахування функцій групи інверсій матиме вигляд:

$$f = a_{i1}x_1 \oplus a_{i2}x_2 \oplus \ldots \oplus a_{i\,n}x_n \ . \qquad (4)$$

Реалізувати дану елементарну функцію можливо на основі послідовного з'єднання операцій додавання за модулем два та логічного множення кожного з доданків на значення елементів рядка матриці перетворення.

Функціональна схема пристрою реалізації елементарної функції матричного криптографічного перетворення представлена на рис. 2, де a_{ij} –відповідне значення матриці перетворення, x_j – відповідне значення даних.

Пристрій працює наступним чином: при подачі на входи (x_j) відповідних значень блоку даних та значень і-го рядка матриці криптографічного перетворення (a_{ij}) на виході пристрою (Y_i) буде встановлено значення результату виконання елементарної функції відповідно до виразу (4).

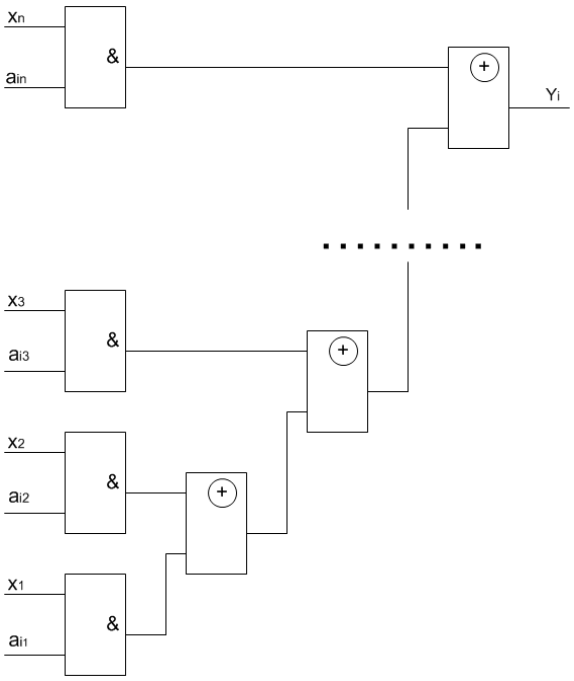

Рис. 2. Функціональна схема реалізації елементарної функції матричного криптографічного перетворення

Даний пристрій реалізує повний набір елементарних функцій матричного криптографічного перетворення.

Операція прямого (оберненого) криптографічного перетворення, яка включає в себе матричну операцію криптографічного перетворення та операцію інверсії (3), може бути реалізована на основі пристрою матричного прямого та оберненого криптографічного перетворення, функціональна схема якого представлена на рис. 3.

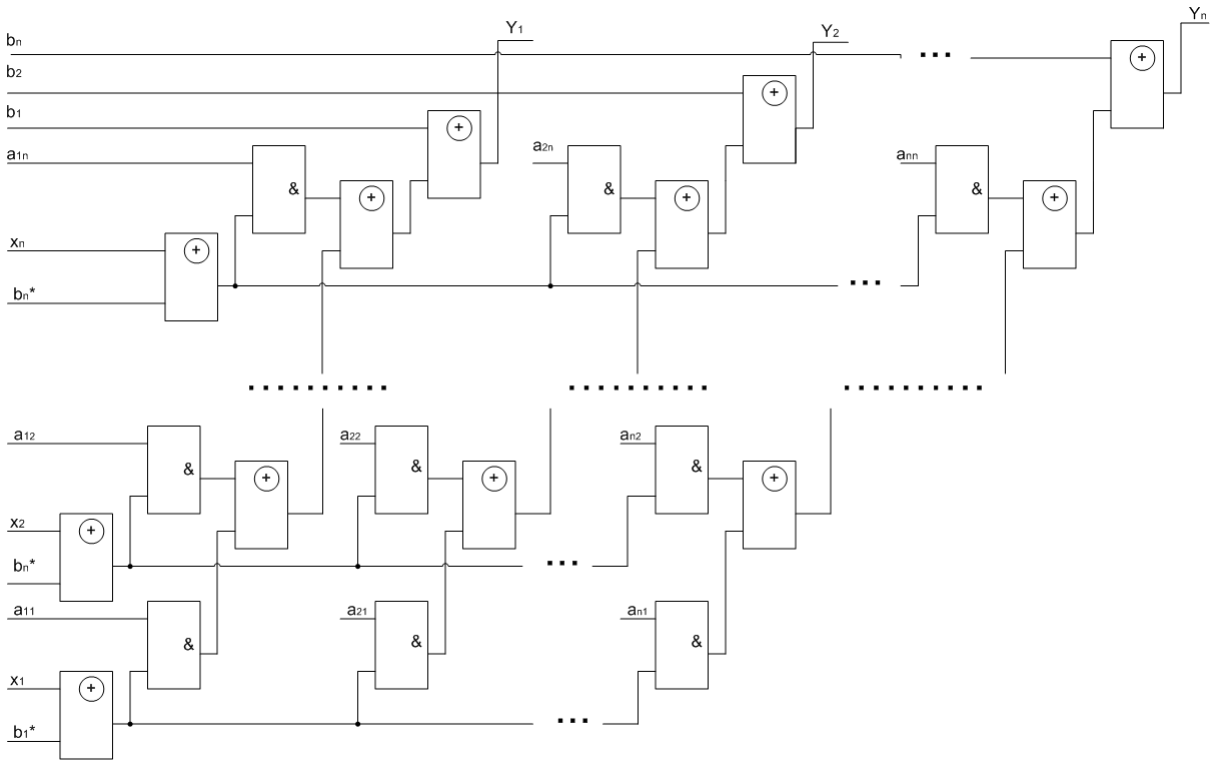

Рис. 3. Функціональна схема реалізації операції матричного криптографічного перетворення

Пристрій працює наступним чином: при подачі на входи (x_j) відповідних значень блоку даних, значень матриці прямого (оберненого) криптографічного перетворення (a_{ij}) та значень інверсій (b_i- для прямого перетворення, b_i^* - для оберненого перетворення) на виході пристрою (Y_i) буде встановлено значення результату виконання операції прямого (оберненого) криптографічного перетворення, або взаємного перетворення відповідно до виразу (3).

Даний пристрій реалізує повну множину операцій матричного криптографічного перетворення.

Оцінка статистичних властивостей результатів криптографічного перетворення

В 1999 р. спеціалістами NIST (Національний інститут стандартів и технологій (НИСТ) США), в рамках проекту AES (Advanced Encryption Standard) був розроблений набор статистичних тестів «NIST STS» (NIST Statistical Test Suite) [6] і запропонована методика проведення статистичного тестування ПВП (ГПВП), орієнтованих на використання в задачах криптографічного захисту інформації, яка, на погляд фахівців в даній області в наш час найкраще відповідає вимогам усіх зацікавлених сторін.

Пакет NIST STS містить 15 статистичних тестів, які розроблені для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини. Ці тести основані на різних статистичних властивостях притаманних лише випадковим послідовностям.

В основі статистичного тесту лежить перевірка деякої нульової гіпотези H_0 такої, що досліджувана послідовність — випадкова. Також передбачена альтернативна гіпотеза H_A, що припускає досліджувану послідовність не випадковою. Таким чином, після перевірки згенерованої послідовності, для кожного тесту робиться висновок щодо відхилення, або прийняття нульової гіпотези H_0.

Для кожного тесту обирається адекватна статистика випадковості, на підставі якої далі відхиляється або приймається гіпотеза H_0. Така статистика, відповідно припущенню на випадковість, володіє деяким розподілом випадкових значень. Теоретично розподіл статистики для нульової гіпотези розраховується із застосуванням математичних методів. Далі із такого зразкового розподілу визначається критичне значення. По проведенні тесту розраховується значення тестової статистики, яке порівнюється із критичним значенням. При перевищенні тестового критичного значення над еталонним, відхиляється нульова гіпотеза випадковості H_0. В іншому випадку робиться висновок про прийняття нульової гіпотези. Для здійснення тестувань були обрані такі параметри:

1) довжина послідовності, що тестується $n = 10^6$ біт;

2) кількість послідовностей, що тестується $m = 100$;

3) рівень значущості $\alpha = 0{,}01$.

4) кількість тестів $q = 189$.

Таким чином, обсяг вибірки, що тестується, склав $N = 10^6 \times 100 = 10^8$ біт, кількість тестів (q) для

різних довжин $q = 189$. Отже, статистичний портрет ПВП містить 18900 значень імовірності *P*.

В ідеальному випадку при $m = 100$ і $\alpha = 0{,}01$ у ході тестування може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту має складати 99%. Але це занадто жорстке правило. Тому застосовується правило на основі довірчого інтервалу. Нижня межа дорівнює 0,96015.

Перевіримо на основі пакету тестів NIST STS метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення.

Розроблений метод використовує для вибору матриць криптографічного перетворення генератор псевдовипадкової послідовності. Виберемо в якості генератора ПВП, реалізований мовою високого рівня програмування генератор ПВП на основі функції RANDOM.

Алгоритм формування ПВП на основі RANDOM для перевірки програмним пакетом NIST STS представлено на рис. 4.

Статичний портрет програмної реалізації генератора ПВП на основі стандартної функції (RANDOM) зображено на рис. 5.

Зведені результати тестування генератора ПВП на основі RANDOM представлені в табл. 1.

В табл. 2 наведено тести пакету NIST STS, в яких коефіцієнт проходження генератора ПВП на основі RANDOM менше 0,96015, тобто дані тести не пройдені.

Як видно з результатів, генератор RANDOM не пройшов комплексний контроль за методикою NIST STS.

Застосуємо метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення для покращення характеристик ПВП, яка генерується RANDOM. Для вирішення задачі на основі генератора ПВП на кожному циклі криптографічного перетворення коректуємо матрицю перетворення та перетворюємо вихідні дані генератора.

Статичний портрет програмної реалізації матричного генератора зображено на рис. 6. Алгоритм формування послідовності для перевірки матричного генератора (на основі RANDOM) програмним пакетом NIST-STS представлено на рис. 7.

Зведені результати тестування матричного генератора (на основі RANDOM) програмним пакетом NIST-STS представлені в табл. 3.

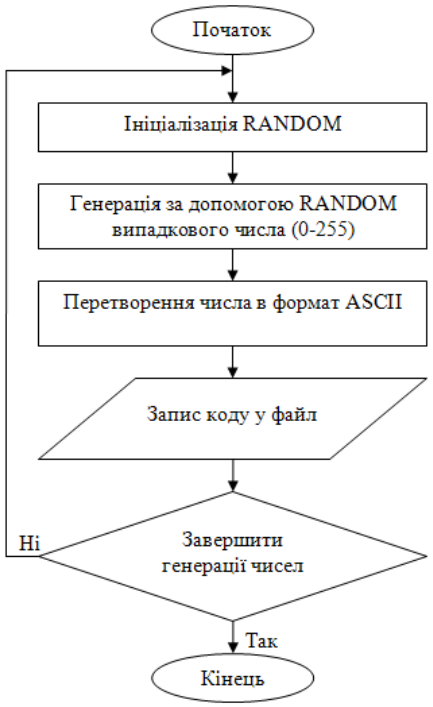

Рис. 4. Алгоритм формування послідовності для перевірки ПВП на основі RANDOM програмним пакетом NIST-STS

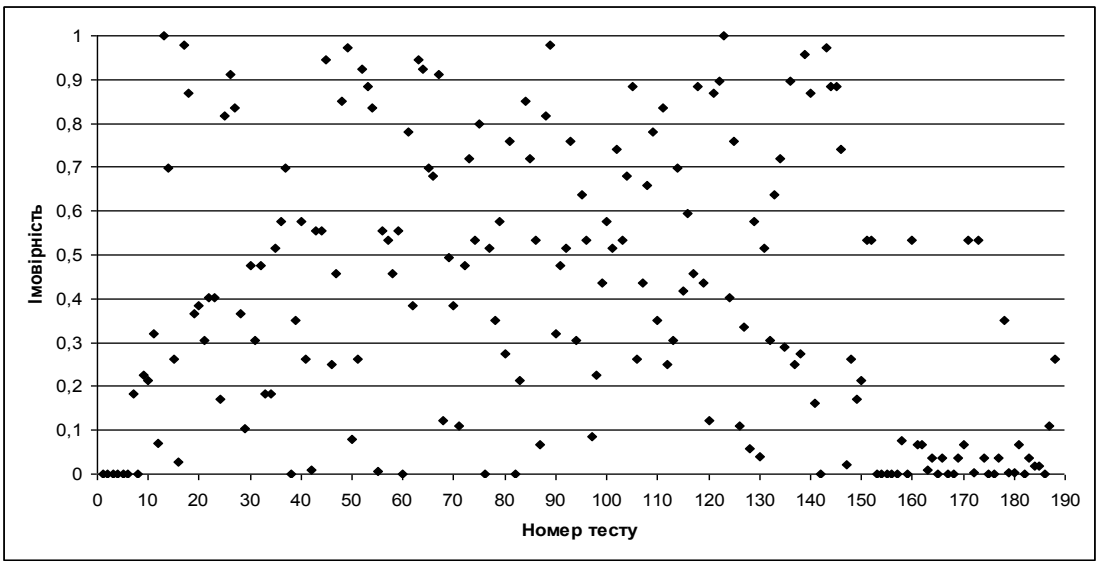

Рис. 5. Статистичний портрет програмної реалізації ПВП на основі RANDOM

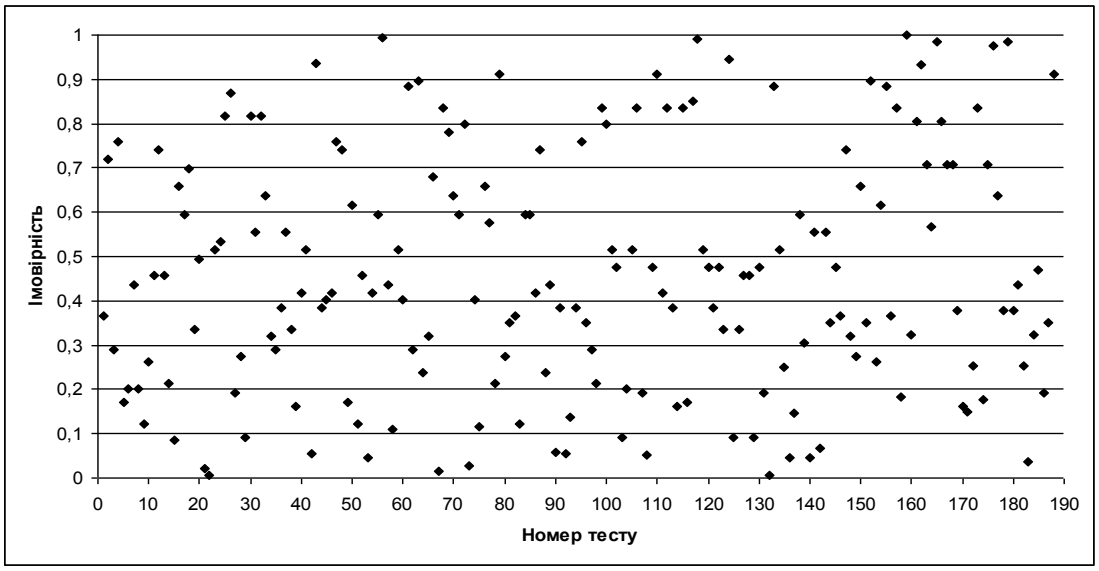

Рис. 6. Статистичний портрет програмної реалізації матричного датчика

Таблиця 1

Зведені результати
тестування датчика RANDOM

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
RANDOM	113 (59,8 %)	170 (89,9%)

Таблиця 2

Тести пакету NIST STS,
в яких коефіцієнт проходження
датчика RANDOM менше 0,96015

Номер	STATISTICAL TEST
1. .	Frequency
2.	BlockFrequency
3.	CumulativeSums
4.	CumulativeSums
5.	Runs
6.	LongestRun
7.	NonOverlappingTemplate
8.	OverlappingTemplate
9.	ApproximateEntropy
10.	Serial

Як видно з результатів, генератор ПВП, реалізований на базі матричного генератора на основі стандартної функції RANDOM, пройшов комплексний контроль за методикою NIST STS.

Спираючись на результати проведеного обчислювального експерименту, був розроблений алгоритм формування псевдовипадкової послідовності на основі операцій матричного перетворення числової або текстової інформації.

Алгоритм реалізації матричного криптографічного перетворення, результатом якого є псевдовипадкова послідовність для аналізу тестами NIST STS представлена на рис. 8.

Таблиця 3

Зведені результати
тестування датчика RANDOM

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Матричний датчик на основі RANDOM	150 (79,4%)	189 (100%)

Так як тести NIST STS направлені на виявлення статистичних закономірностей в псевдовипадкових послідовностях, перевіримо можливість виявлення таких закономірностей на невипадковій монотонно зростаючій послідовності з циклом повторення 64 байти, в яку записані коди чисел 64, 65, 66, …, 128.

Зведені результати тестування матричного кодування невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти програмним пакетом NIST-STS представлені в табл. 4.

Як видно з результатів, послідовність, яка досліджувалась, пройшла комплексний контроль за методикою NIST STS.

Перевіримо можливість виявлення статичних властивостей результатів матричного криптографічного кодування невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти, в яку записані коди чисел 0, 1, 2, …, 255.

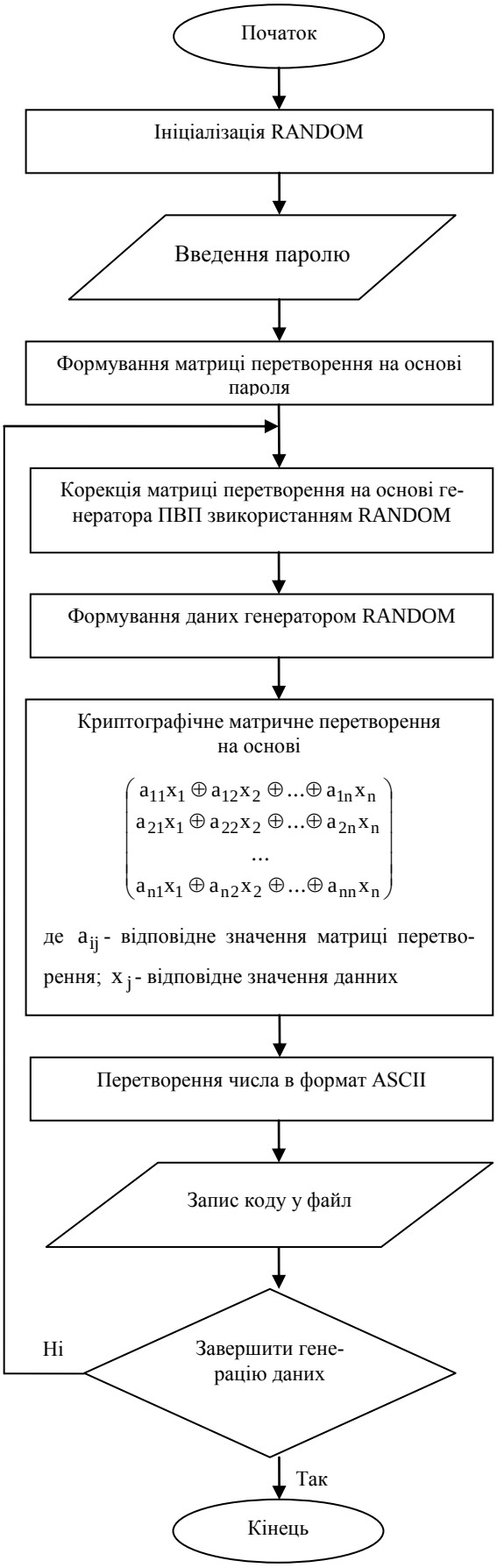

Рис. 7. Алгоритм формування послідовності для перевірки матричного генератора (на основі RANDOM) програмним пакетом NIST-STS

Таблиця 4

Зведені результати тестування матричного кодування невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Матричне криптографічне кодування	129 (68,3%)	189 (100%)

Зведені результати тестування матричного кодування невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти програмним пакетом NIST-STS представлені в табл. 5.

Таблиця 5

Зведені результати тестування матричного кодування невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Матричне криптографічне кодування	136 (71,9%)	188 (99,5%)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS, так як не був пройдений 1 тест:

```
---------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND
THE PROPORTION OF PASSING SEQUENCES
---------------------------------------------------------------------------
  generator is <KOD_CHT1.bin>
---------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION
---------------------------------------------------------------------------
18   5  10  12  13   7  10   8   8   9 0.213309   0.9500 *
STATISTICAL TEST
NonOverlappingTemplate
```

Для забезпечення проходження даного тесту проведемо обчислювальний експеримент, додавши в алгоритм криптографічного матричного кодування (рис. 8) додатковий блок криптографічне кодування групою операцій інверсії результатів матричного кодування.

Статичний портрет програмної реалізації алгоритму модифікованого матричного кодування невипадкової монотонно зростаючої послідовності з циклом повторення розміром 256 байтів зображено на рис. 9.

Рис 8. Алгоритм формування послідовності на основі операцій матричного перетворення

Зведені результати тестування матричного кодування за модифікованим алгоритмом невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти програмним пакетом NIST-STS представлені в табл. 6.

Таблиця 6

Зведені результати тестування даних за модифікованим алгоритмом матричного перетворення

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Модифіковане матричне криптографічне перетворення	132 (69,8%)	189 (100%)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

Перевіримо статистичні властивості результатів матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів, а саме художньої літератури в текстовому форматі.

Статичний портрет програмної реалізації алгоритму модифікованого матричного криптографічного перетворення тестового файлу зображено на рис. 10.

Зведені результати тестування матричного криптографічного перетворення за модифікованим алгоритмом текстового файлу програмним пакетом NIST-STS представлені в табл. 7.

Таблиця 7

Зведені результати тестування даних за модифікованим алгоритмом матричного перетворення текстового файлу

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Модифіковане матричне криптографічне перетворення	129 (68,3%)	189 (100%)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

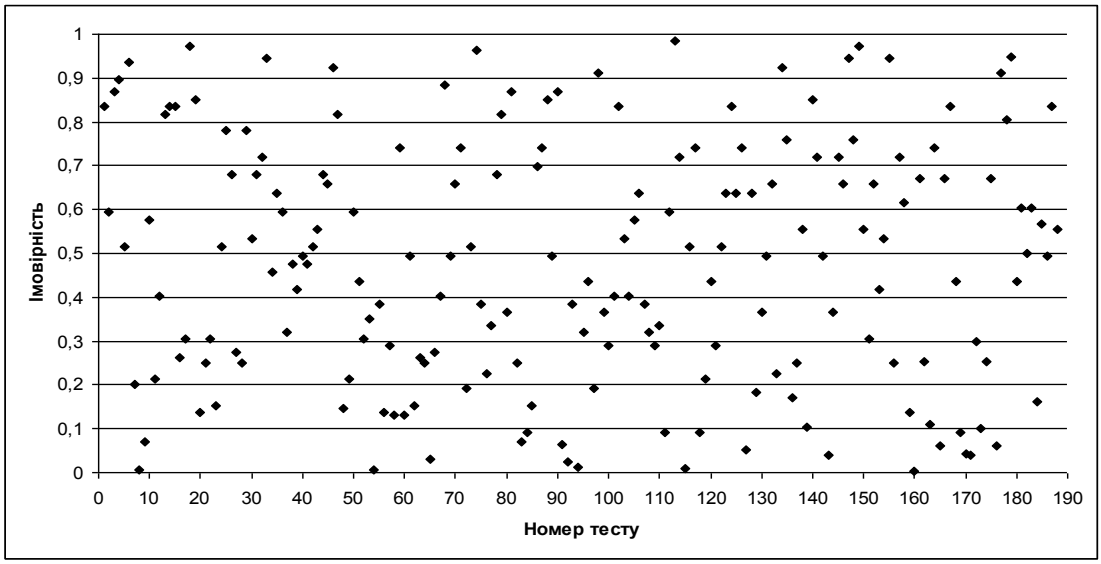

Рис. 9. Статистичний портрет програмної реалізації алгоритму модифікованого матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти

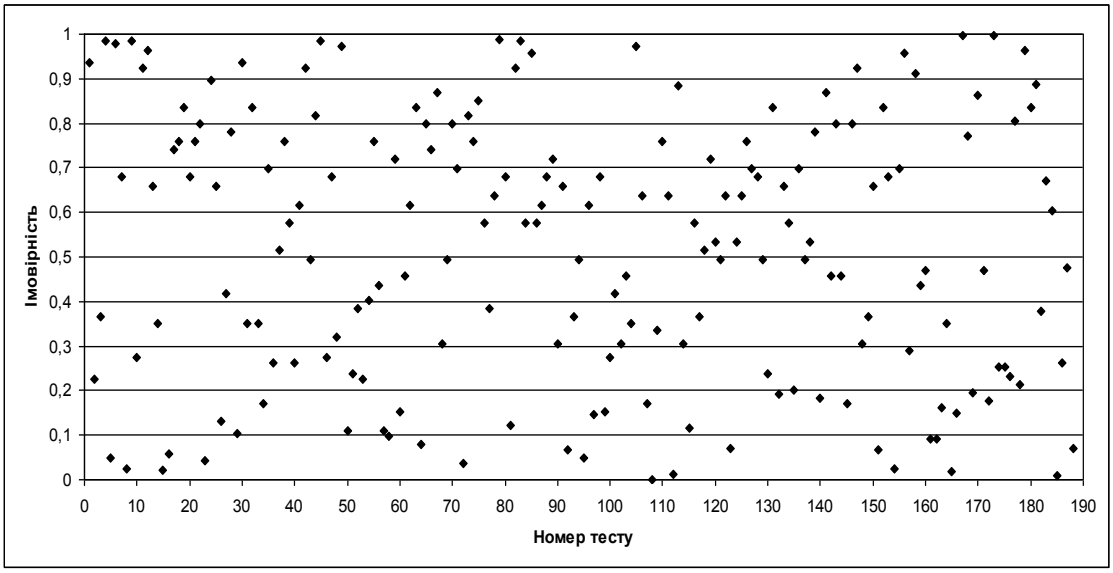

Рис. 10. Статистичний портрет програмної реалізації алгоритму модифікованого матричного криптографічного перетворення тестового файлу.

Підвищити швидкість роботи системи захисту інформації на основі матричних операцій криптографічного перетворення за модулем два можливо за рахунок розпаралелення процесу виконання перетворення. Один з варіантів реалізації алгоритму з паралельним виконанням матричного криптограмфічного перетворення наведено на рис. 11.

Розроблені методи та засоби криптографічного пертворення забезпечують вирішення важливої науково-технічної задачі підвищення якості функціонування систем захисту інформаційних ресурсів на основі матричного криптографічного перетворення.

Висновки

В статті на основі узагальнення отриманих результатів розроблено метод захисту інформації на основі матричних операцій криптографічного пертворення з використанням операції суми за модулем два.

Запропонована структура системи захисту інформації на основі матричних операцій криптографічного пертворення та розроблені функціональні моделі пристроїв для їх апаратної реалізації.

На основі виконаної програмної реалізації методу захисту інформації проведено тестування згенерованих псевдовипадкових послідовностей програмним пакетом тестів NIST-STS. Аналіз результатів тестування дозволив зробити висновок, що запропонований метод матричного криптографічного пертворення придатний для використовувати в системах криптографічного захисту інформаційних ресурсів.

Рис. 11. Алгоритм з паралельним виконанням матричного криптографічного перетворення

Список літератури

1. *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». – Х.: ХУПС ім. І. Кожедуба. – 2012. – Вип. 3(101). – Т. 1. – С. 119-122.*
2. *Бабенко В.Г. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій / В.Г. Бабенко, С.В. Рудницький // Наук. журн. «Системи озброєння і військова техніка». – Х.: ХУПС ім. І. Кожедуба. – 2012. – Випуск 1(29). – С. 84-87.*
3. *Рудницький В.М. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС ім. І. Кожедуба. – 2011. – Вип. 3(29). – С. 145-150.*
4. *Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС ім. І. Кожедуба. – 2012. – Вип. 4(33). – С. 198-200.*
5. *Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Науково-практичний журнал «Захист інформації» – К.: НАУ. – 2012. – № 3(56). – С. 50-56.*
6. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 (with revisions dated May 15, 2001).*

Надійшла до редколегії 30.10.2012

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

РЕАЛИЗАЦИЯ МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МАТРИЧНЫХ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

В.Г. Бабенко, С.В. Рудницкий

В статье разработан метод защиты информационных ресурсов на основе матричных операций криптографического преобразования и структурная схема его применения. Проведен синтез функциональных схем для реализации элементарных функций и операций матричного криптографического преобразования информации на основе суммы по модулю два. Проведена разработка алгоритмов применения операций матричного криптографического преобразования и оценка статистических свойств результатов криптографического преобразования на их основе.

Ключевые слова: *матричные операции, криптографическое преобразование, оценка статистических свойств, статистический портрет.*

IMPLEMENTATION OF INFORMATION SECURITY METHOD BASED ON CRYPTOGRAPHIC TRANSFORMATION MATRIX OPERATIONS

V.G. Babenko, S.V. Rudnickiy

In the paper was developed a method for protection of information resources on the basis of a cryptographic transformation matrix operations and framework of its application. The synthesis of functional circuits to implement basic functions and operations of cryptographic information transformation matrix based on the sum modulo two. Conducted to develop algorithms using the operations of cryptographic transformation matrix and evaluation of the results of the statistical properties of cryptographic transformations on them.

Keywords: *matrix operations, cryptographic transformation, evaluation of the statistical properties, the statistical portrait.*