УДК 004.056.2

І. О. Розломій, *аспірантка*
Черкаський національний університет імені Богдана Хмельницького
б-р Шевченка, 81, м. Черкаси, 18000, Україна

МЕТОДИ ОБЧИСЛЕННЯ ХЕШ-ФУНКЦІЇ ЕЛКТРОННОГО ДОКУМЕНТА НА ОСНОВІ МАТРИЧНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Алгоритми електронного цифрового підпису (ЕЦП) та хешування є найефективнішими способами ідентифікації цифрової інформації. Тому перспективним напрямом досліджень є розробка методів обчислення хеш-функції електронного документа (ЕД). У статті розглядається можливість використання матричних криптографічних перетворень для обчислення хеш-функції ЕД. У результаті проведених досліджень було сформовано два алгоритми обчислення хеш-функції ЕД: перший алгоритм базується на послідовному виконанні операції додавання за модулем рядків матриці, другий – ускладнений шляхом введення правил додавання рядків матриці. В роботі показано структурні схеми запропонованих алгоритмів, описано математичні моделі виконання операцій перетворення рядків матриці. Отримані результати дають перспективи для подальшої розробки та вдосконалення алгоритмів хешування.

Ключові слова: *електронний документ, електронний цифровий підпис, цілісність, хеш-функція, криптографічні перетворення, матричні операції.*

Вступ. В наш час інформація стала найбільшою цінністю, найдорожчим продуктом виробництва. ЇЇ роль у сучасному світі є настільки великою, що інформаційна індустрія стала однією з головних галузей сьогодення. Глобальна інформатизація суспільства привела до виникнення нової – електронної – форми ведення документообігу. Електронний документообіг є одним з найголовніших технічних елементів системи електронного урядування, адже саме він забезпечує циркуляцію ЕД, які є основою нової форми взаємодії держави та суспільства. Широке використання електронного документообігу в усіх сферах життя суспільства робить досить актуальною проблему захисту ЕД. Питання захисту ЕД не можуть бути повністю вирішені лише стандартним набором засобів захисту інформації. Тому використання інформаційних технологій привело до розвитку різноманітних методів захисту інформації, серед яких можна виділити кодування та криптографію.

Постановка проблеми. Враховуючи, що сьогодні обсяг даних, які доводиться зберігати, обробляти та передавати мережею, постійно зростає, виникає необхідність їх надійного захисту від основних порушень цілісності. Цілісність є основною властивістю ЕД, яка свідчить про його незмінність і збереження в тому вигляді, в якому він був створений. Основним гарантом цілісності ЕД залишається електронний цифровий підпис (ЕЦП). До цього часу відомо багато способів отримання ЕЦП, досліджено принципи їх побудови, але більшість з них не здатні повною мірою забезпечити надійний захист ЕД. У найпростішому випадку цифровий підпис – це результат виконання хешування. Звідси, очевидною є необхідність розробки алгоритмів обчислення хеш-функції ЕД.

Аналіз останніх досліджень та публікацій. Аналіз наукової літератури доводить актуальність досліджень засобів захисту ЕД. В роботах [1–3] авторами виділені основні аспекти забезпечення інформаційної безпеки ЕД. Використання ЕЦП як основного механізму забезпечення цілісності та автентичності ЕД показані в дослідженнях Т. С. Астахової, О. В. Линника [2–3]. Проте, разом з цим, існують питання, які потребують більш детального дослідження. До теперішнього часу мало уваги приділялося розробці алгоритмів обчислення хеш-функції ЕД, на основі матричних криптографічних перетворень зокрема. Дослідженням операцій прямого й оберненого матричного перетворення займалися такі науковці, як В. А. Лужецький, В. М. Рудницький, В. Г. Бабенко, І. В. Миронець та інші. Але в цих дослідженнях [4–9] не розглядалися пропозиції щодо обчислення матриці хеш-функції електронного документа з заданої ключової

матриці, а також відсутні методи оберненого обчислення з метою виявлення порушень цілісності інформації. Саме тому розв'язання цієї задачі є практично необхідним для подальшої розробки засобів захисту ЕД та виявлення можливих фальсифікацій.

Мета статті – дослідження методів забезпечення цілісності ЕД і розробка алгоритмів використання операцій матричного криптографічного перетворення для обчислення хеш-функції електронного документа.

Основний матеріал. Як свідчать попередні дослідження, основним гарантом авторства ЕД є його головний реквізит – ЕЦП. ЕЦП являє собою контрольну суму бітів, отриману в результаті аналізу ЕД. У найбільш примітивному випадку ЕЦП – це результат обчислення хеш-функції. Хеш-функцію можна використовувати для перетворення довільного вхідного тексту у відповідний формат [10]. Процес обчислення хеш-функції називають хешуванням, а результат виконання – хешем ЕД. Результат обчислення хеш-функції не повинен повторюватися для різних вхідних даних, а ще хеш має бути значно меншого розміру, ніж вхідний ЕД. Також важливою умовою є те, що за допомогою хешу не можна відновити вхідний ЕД.

Зазвичай, результатом хешування є фіксована кількість бітів, що характеризує повністю весь документ. До цього часу в процесі обчислення хеш-функції ЕД не використовувалися матричні криптографічні перетворення.

Матричні алгоритми придатні для обернених перетворень, якщо при цьому виконуються такі умови:

1) відсутні нульові рядки і стовпці в матриці;

2) додавання рядків і стовпців матриці не дорівнюватиме нулю.

Виходячи з цього, можна говорити, що при додаванні рядків і стовпців матриця буде не виродженою [4], візьмемо це за основу.

У загальному вигляді операції криптографічного перетворення, побудовані на основі додавання за модулем два, описуються такою моделлю [5]:

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

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2».

Якщо ключова матриця задана виразом

$$A_k = \begin{pmatrix} a_{11}, a_{12}, ..., a_{1n} \\ a_{21}, a_{22}, ..., a_{2n} \\ . \quad . \quad . \quad . \quad . \\ a_{n1}, a_{n2}, ..., a_{n\,n} \end{pmatrix}, \quad (2)$$

де $a_{ij} \in [0,1];$ – коефіцієнти ключової матриці, тоді матриця хеш-функції ЕД, отримана в результаті криптографічного оберненого перетворення, буде задана виразом

$$A_h = \begin{pmatrix} b_{11}, b_{12}, ..., b_{1n} \\ b_{21}, b_{22}, ..., b_{2n} \\ . \quad . \quad . \quad . \quad . \\ b_{n1}, b_{n2}, ..., b_{n\,n} \end{pmatrix}, \quad (3)$$

де $b_{ij} \in [0;1]$ – коефіцієнти матриці хеш-функції.

Розглянемо докладніше процес обчислення хеш-функції з заданої ключової матриці. Найпростішим способом обчислення є послідовне додавання до одного рядка матриці іншого рядка, вибраного на основі аналізу фрагмента інформації (4).

$$A_h = \begin{pmatrix} b_{11}(a_{11} \oplus a_{21}), b_{12}(a_{12} \oplus a_{22}), ..., b_{1n}(a_{1n} \oplus a_{2n}) \\ b_{21}(a_{21} \oplus a_{n1}), b_{22}(a_{22} \oplus a_{n2}), ..., b_{2n}(a_{2n} \oplus a_{nn}) \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}(a_{n1} \oplus a_{11}), b_{n2}(a_{n2} \oplus a_{12}), ..., b_{n\,n}(a_{nn} \oplus a_{1n}) \end{pmatrix}, \quad (4)$$

Основою для вибору рядка матриці, який буде додаватися до поточного рядка, є фрагмент даних. Інформація, представлена в двійковій формі, розбивається на блоки однакової довжини. Таким чином, сума бітів визначеного блока вказує на рядок, який буде додаватися до поточного рядка. Алгоритм формування хеш-функції електронного документа на основі послідовних операцій матричного перетворення показаний на рис. 1.

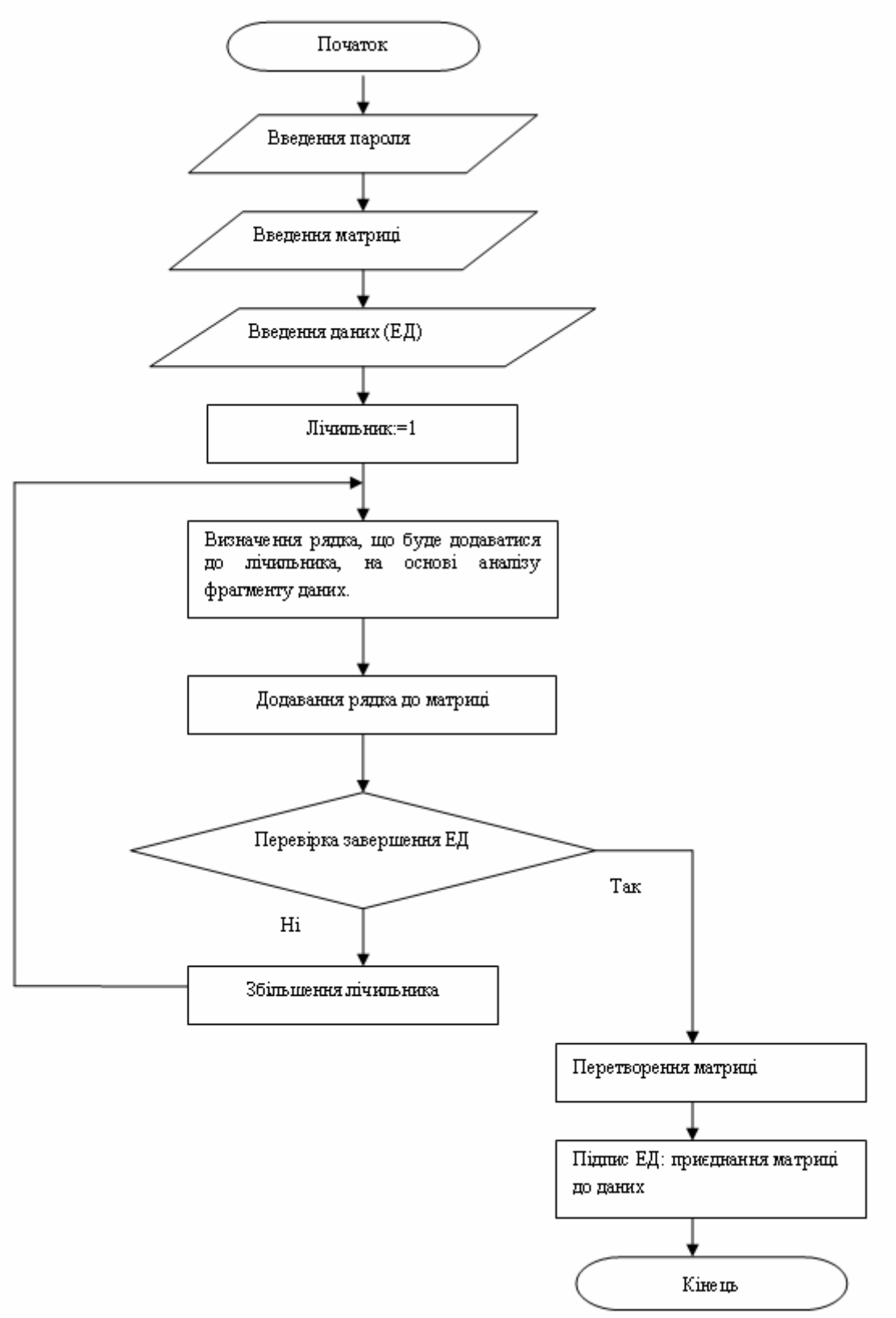

Рис. 1. Алгоритм формування хеш-функції електронного документа на основі послідовних операцій матричного перетворення

З рис. 1 видно, що алгоритм перетворення рядків матриці функціонуватиме до кінця електронного документа, тобто доти, поки послідовно не буде проаналізований

кожний блок інформації. Матриця, отримана в результаті послідовних перетворень, і буде хеш-функцією електронного документа, яка приєднається до нього. При перевірці ЕЦП ця матриця свідчитиме про його цілісність і незмінність.

Результати програмної реалізації алгоритму обчислення хеш-функції електронного документа на основі матричного криптографічного перетворення були оцінені за допомогою статистичних тестів NIST STS.

Ускладнимо алгоритм обчислення хеш-функції ЕД шляхом введення правил додавання рядків матриці. В попередньому варіанті алгоритму поточний рядок змінювався шляхом послідовного додавання випадково обраного іншого рядка, на основі аналізу фрагмента даних. Вдосконалений алгоритм полягає в тому, що один двійковий блок даних вказує на кількість операцій над поточним рядком, наступні блоки визначають, які конкретно рядки будуть додаватися (5).

$$A_h = \begin{pmatrix} b_{11}(a_{11} \oplus a_{21} \oplus a_{n1}), b_{12}(a_{12} \oplus a_{22} \oplus a_{n2}),..., b_{1n}(a_{1n} \oplus a_{2n} \oplus a_{nn}) \\ b_{21}(a_{21} \oplus a_{11} \oplus a_{n1}), b_{22}(a_{22} \oplus a_{21} \oplus a_{n2}),..., b_{2n}(a_{2n} \oplus a_{1n} \oplus a_{nn}) \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}(a_{n1} \oplus a_{11} \oplus a_{21}), b_{n2}(a_{n2} \oplus a_{12} \oplus a_{22}),..., b_{nn}(a_{nn} \oplus a_{1n} \oplus a_{2n}) \end{pmatrix}, \quad (5)$$

Нехай блок, який вказує, скільки разів додаватимемо до поточного рядка, буде керуючим (К), а блоки, які будуть безпосередньо додаватися, – виконуючими (В) (табл. 1).

Таблиця 1

1	2	3	4	5	6	7	8	9	…
К	В	В	К	В	В	К	В	В	…
01	10	11	01	10	00	01	11	10	…

Згідно з табл. 1 правила додавання рядків можна описати такими кроками:

1) перший блок (керуючий) показує, що до першого рядка матриці потрібно додавати два рази;

2) другий блок (виконуючий) вказує, що до першого рядка потрібно додати другий рядок;

3) третій блок (виконуючий) вказує, що до першого рядка потрібно додати третій рядок;

4) четвертий блок (керуючий) показує, що до другого рядка матриці потрібно додавати два рази;

5) п’ятий блок (виконуючий) вказує, що до другого рядка потрібно додати другий рядок – така операція не виконується;

6) шостий блок (виконуючий) вказує, що до другого рядка потрібно додати перший рядок;

7) сьомий блок (керуючий) показує, що до третього рядка матриці потрібно додавати два рази;

8) восьмий блок (виконуючий) вказує, що до третього рядка потрібно додати третій рядок – така операція не виконується;

9) дев’ятий блок (виконуючий) вказує, що до третього рядка потрібно додати другий рядок.

Матричні перетворення триватимуть доти, доки не буде проаналізований весь документ. Запропонований алгоритм вимагає більшої кількості вихідних даних, тому що, на відміну від попереднього алгоритму, де кожний блок визначав рядок, який буде додаватися послідовно, в цьому алгоритмі передбачені керуючі блоки, які вказують на кількість операцій додавання. Вдосконалений алгоритм формування хеш-функції ЕД показаний на рис. 2.

Як і в попередньому алгоритмі, результатом обчислення хеш-функції ЕД буде матриця, яку отримаємо в кінці, після аналізу всього ЕД.

Отримані в обох випадках в результаті процесу хешування контрольні суми – найпростіший спосіб перевірки цілісності ЕД.

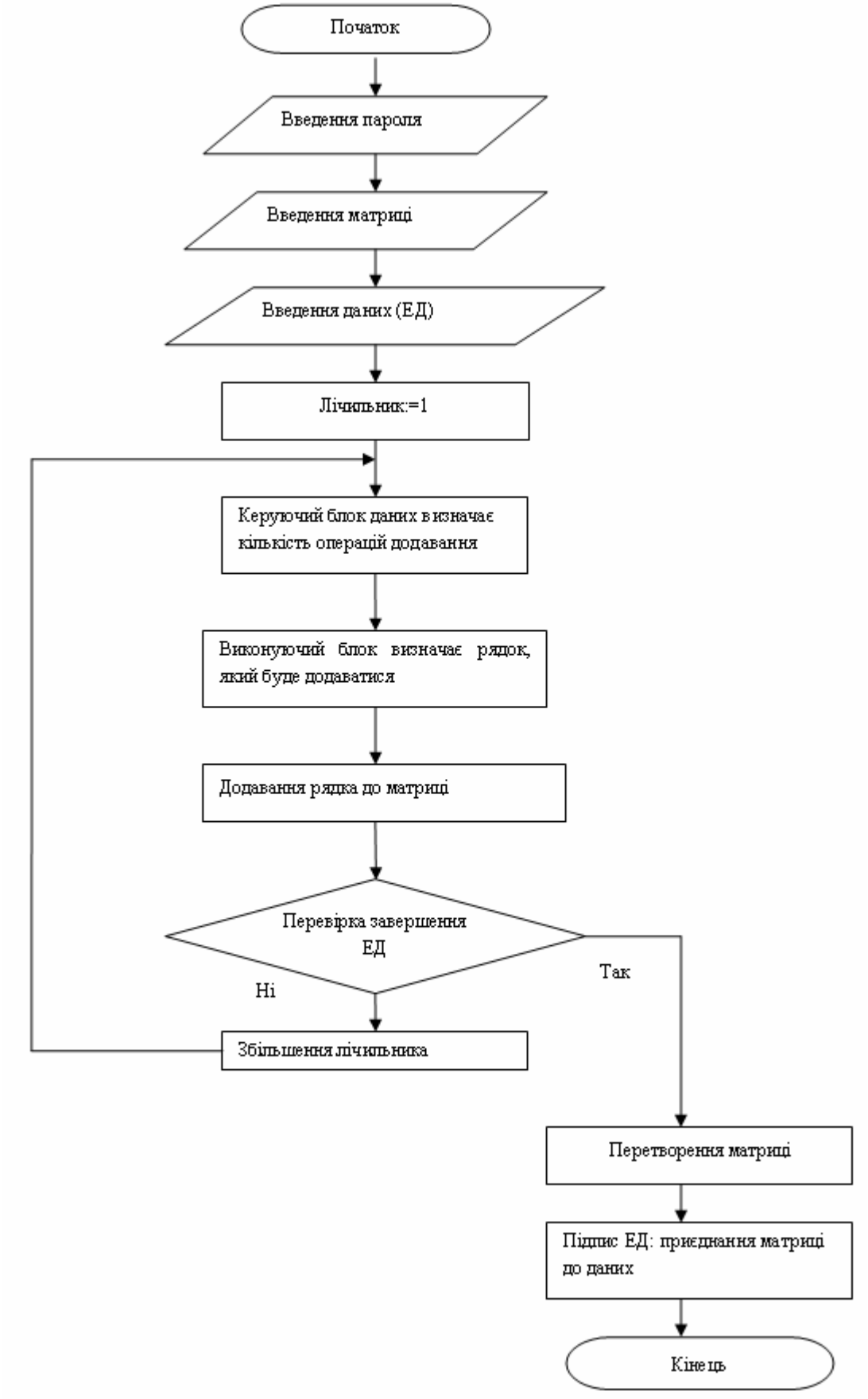

Рис. 2. Вдосконалений алгоритм формування хеш-функції електронного документа

Висновки. Таким чином, у статті досліджено проблему забезпечення цілісності ЕД. У результаті проведених досліджень було сформовано два алгоритми обчислення хеш-функції ЕД. Перший алгоритм базується на послідовному виконанні операції додавання за модулем рядків матриці. Другий алгоритм ускладнений шляхом введення правил додавання рядків матриці. Вдосконалений спосіб обчислення вимагає більшої кількості вхідних даних, тому що вводиться поняття «керуючий та виконуючий блоки», на основі яких відбувається перетворення рядків матриці. Типових алгоритмів обчислення хеш-функції ЕД за допомогою матричних криптографічних перетворень можна побудувати безліч, задаючи нові правила додавання рядків матриці. Все це дасть змогу забезпечити цілісність і автентичність ЕД.

Список літератури

1. Панасенко С. П. Защита электронных документов: целостность и конфиденциальность / С. П. Панасенко // Банки и технологии. – 2000. – № 4. – С. 82–87.
2. Астахова Т. С. Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа / Т. С. Астахова, Е. П. Чадаева // Известия Томского политехнического университета. – 2012. – № 6. – С. 55–61.
3. Линник О. В. Виявлення підробки електронного цифрового підпису для встановлення змін у документі / О. В. Линник // Юридичний науковий електронний журнал. – 2015. – № 2. – С. 209– 211.
4. Криптографическое кодирование: методы и средства реализации (часть 2): [монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко и др.]. – Х. : Щедрая усадьба, 2014. – 224 с.
5. Миронець І. В. Підвищення достовірності процесу матричного криптографічного перетворення / І. В. Миронець // Информационные технологии и системы управления. – 2015. – № 5/6 (25). – С. 52–54.
6. 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. – 2012. – № 4. – С. 198–200.
7. Голуб С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації. – 2012. – № 3 (101). – С. 119–122.
8. Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В. Г. Бабенко, С. В. Рудницький // Системи обробки інформації. – 2012. – № 9 (107). – С. 130–139.
9. Лужецький В. А. Використання операції множення за модулем в симетричних блокових шифрах / В. А. Лужецький, О. В. Дмитришин // Системи обробки інформації. – 2010. – № 5. – С. 9–14.
10. Black J. Black-box analysis of the block-cipher-based hash-function constructions from PGV / J. Black, P. Rogaway, T. Shrimpton // Advances in Cryptology, CRYPTO'02, Lecture Notes in Computer Science, Springer-Verlag, 2002.

References

1. Panasenko, S. P. (2000) The security of digital documents: integrity and confidentiality. *Banki i tehnologiyi*, No. 4, pp. 82–87 [in Russian].
2. Astakhova, T. S. and Chadaeva, E. P. (2012) Electronic digital signature as a factor of ensuring integrity and authenticity of a document. *Izvestiya Tomskogo politechnicheskogo Universiteta*, No. 6, pp. 153–157 [in Russian].
3. Linnik, O. V. (2015) Identifying the fake of electronic digital signature to establish changes in a document. *Yurydychnyy naukovyy elektronnyy zhurnal*, No. 2, pp. 209–211 [in Ukrainian].
4. Rudnitsky, V. N., Milchevich, V. Ja., Babenko, V. G. et al. (2014) Cryptographic coding: methods and means of implementation (Part 2). Kharkov: Schedraya usadba, 224 p. [in Russian].
5. Myronets, I. V. (2015) The increase of reliability of the process of matrix cryptographic transformation. *Informatsionnye technologiyi i sistemy upravleniya*, No. 5/6 (25), pp. 52–54 [in Ukrainian].
6. Rudnitsky, V. M., Babenko? V. G. and Rudnitsky, S. V. (2012) The method for synthesis of matrix models of cryptographic op-

erations of data encoding and decoding. *Zbirnyk naukovyh prats Harkivskoho universytetu Povitryanyh syl*, No. 4, pp. 198–200 [in Ukrainian].
7. Golub, S. V., Babenko, V. G. and Rudnitsky, S. V. (2012) The method for synthesis of cryptographic transformation operations on the basis of addition by modulo two. *Systemy obrobky informatsiyi*, No. 3 (101), pp. 119–122 [in Ukrainian].
8. Babenko, V. G. and Rudnitsky, S. V. (2012) Implementation of information security method based on matrix operations of cryptographic transformation. *Systemy obrobky informatsiyi*, No. 9 (107), pp. 130–139 [in Ukrainian].
9. Luzhetsky, V. A. and Dmytryshyn, A. V. (2010) The use of modular multiplication in symmetric block ciphers. *Systemy obrobky informatsiyi*, No. 5, pp. 9–14 [in Ukrainian].
10. Black, J., Rogaway, P. and Shrimpton T. (2002) Black-box analysis of the block-cipher-based hash-function constructions from PGV. Advances in Cryptology, CRYPTO'02, Lecture Notes in Computer Science, Springer-Verlag.

I. O. Rozlomii, *postgraduate student*
Cherkasy Bogdan Khmelnytskyi National University
Schevchenko blvd, 81, Cherkasy, 18000, Ukraine

METHODS FOR CALCULATING THE HASH FUNCTION OF ELECTRONIC DOCUMENT ON THE BASIS OF MATIX CRYPTOGRAPHIC TRANSFORMATIONS

The widespread use of electronic document management in all areas of society makes a very urgent problem of electronic documents protection. Electronic digital signature and hashing algorithms are the most effective ways to identify digital information. Electronic digital signature is the main guarantee of electronic document's integrity. The result of hashing is the simplest case of electronic digital signature. So promising area of the research consists in the development of methods for calculating the hash function of electronic document.

The aim of the article is to develop algorithms using the matrix of operations of cryptographic transformations to calculate the hash function of electronic document.

To achieve this goal, hash function concept, particularly the process of hashing, has been investigated. The calculation of the hash function of electronic document with the use of matrix cryptographic transformations is examined in the article. Two algorithms for computing the hash function of electronic document are formed as a result of the research. The first algorithm is based on the consistent performance of the operation of addition by matrix lines modulo. The second algorithm is complicated by the introduction of the rules of matrix rows adding. An improved calculation method requires more input data because it introduces the notion of managing and executing blocks, on the basis of which the transformation of matrix lines occurs. In the article block diagrams of the proposed algorithms are shown, mathematical models of operations of matrix lines transformation are described.

The results give the prospects for further development and perfection of hashing algorithms.

Keywords: *electronic document, electronic digital signature, integrity, hash function, cryptographic transformations, matrix operations.*

Рецензенти: В. М. Рудницький, д.т.н., професор,
С. В. Голуб, д.т.н., професор