DOI 10.31891/2307-5732-2020-281-1-225-229
УДК 004.056

І.О. РОЗЛОМІЙ
Черкаський національний університет імені Богдана Хмельницького

МЕТОДИ ПІДСИЛЕННЯ ХЕШ-ФУНКЦІЇ ПАРОЛЮ ПРИ АВТОРИЗАЦІЇ КОРИСТУВАЧІВ

Парольна аутентифікація є одним із способів захисту ідентифікаційних даних користувачів. В статті проведений аналіз основних методів аутентифікації. Доступ до більшості інформаційних систем та web-додатків передбачає використання персональних даних – логіну, паролю. Зазвичай, паролі в базі даних зберігаються в вигляді хеш-функції. В зв'язку з цим, актуальним є завдання розробки методів підсилення хеш-функції паролю при авторизації користувачів. В статті розглянуті методи підсилення хеш-функції паролю на основі n-разового хешування та salt-hashing. Особлива увага в статті зосереджена на розробці методів підсилення хеш-функції паролю із застосуванням операцій матричного криптографічного перетворення. Розроблені методи дозволять підвищити надійність паролю користувача за рахунок збільшення кількості операцій обчислення хеш-функції паролю. В результаті побудовано схему розроблених методів з покроковим алгоритмом їх реалізації.

Ключові слова: *ідентифікація користувача, авторизація, аутентифікація, хеш-функція, пароль, матричне криптографічне перетворення.*

I.O. ROZLOMII
Cherkassy Bogdan Khmelnytsky National University

METHODS OF INCREASING THE PASSWORD HASH FUNCTION AT USER AUTHORIZATION

Effective use of web resources is only possible if there are reliable means of protecting the user authentication data. Password authentication is one way to protect user credentials. The simplicity of implementation and logical clarity of operating principles make password authentication systems the most popular. Although there are many threats to this authorization scheme (password picking, traffic analysis, re-authentication request), it is used in most information systems. The basic methods of authentication were analyzed in the article. The access to most information systems and web-applications involves the use of personal data - login, password. Typically, passwords are stored in the database as a hash function. In this regard, it is urgent to develop methods to enhance the password hash function when authorizing users. Methods of password hash enhancement based on n-time hashing and salt-hashing were discussed in the article. Particular attention focuses on the development of methods to enhance the password hash function using matrix cryptographic transformation operations in the article. Two approaches to enhance the password hash function based on the use of matrix cryptographic transformation operations are proposed. The first approach is based that on the entered password calculate the operation of matrix cryptographic transformation, then calculate hash. Another approach is to first calculate the password hash function, followed by the use of matrix cryptographic transformation operations. The developed methods will allow to increase the reliability of the user's password by increasing the number of operations of calculating the password hash function. As a result, the scheme of the developed methods with a step-by-step algorithm of their realization is constructed.

Keywords: *user identification, authorization, authentication, hash function, password, matrix cryptographic transformation.*

Вступ. Простота реалізації та функціонування систем парольної аутентифікації роблять їх досить популярними. Паролі тривалий час вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити достатній для більшості організацій рівень безпеки. Існує велика кількість загроз даній схемі авторизації – підбір пароля, аналіз трафіка, повторний запит аутентифікації та інші. Попри загрози, ця схема використовується в більшості інформаційних системах, а завдання захисту від перелічених загроз зазвичай вирішуються за допомогою криптографічного захисту.

Зараз використовуються два основні методи аутентифікації користувачів. Один з них – з однонаправленою передачею інформації від клієнта до сервера, інший – технологія «запит – відповідь». Однонаправлена схема передбачає передачу від клієнта до сервера власного ідентифікатора і пароля, які сервер порівнює з тими, які містяться в його базі даних. За результатом порівняння приймається рішення про те, що користувач є тим, за кого себе видає [1]. Для того, щоб протистояти пасивному перехопленню пароля, при передачі мережею, застосовується хешування пароля.

Розробка алгоритмів, інструментів та методів авторизації користувачів в інформаційних системах та інтернет-додатках з використанням хеш-функцій необхідна як для активного, так і для пасивного захисту ідентифікаційних даних користувачів.

Аналіз останніх досліджень та публікацій. Велика кількість публікацій присвячена питанням аутентифікації. Особливої уваги заслуговує серія статей Сабанова А.Г., в яких закладені не лише теоретичні основи аутентифікації, а і описані особливості аутентифікації при доступі до хмарних сервісів, аутентифікація при електронному обміні документами, проведені дослідження надійності віддаленої аутентифікації та інше [2, 3]. Варто також відмітити роботу Власенка А.В., в котрій розглянуто алгоритми, інструменти та методи авторизації користувачів в web-додатках з використанням хеш-функцій [4].

Виділення невирішених раніше частин загальної проблеми. Зважаючи на існуючі наукові здобутки та напрацювання в області аутентифікації користувачів, залишаються питання для подальшого вирішення. Численні дослідження показують ефективність використання операцій матричного криптографічного перетворення в системах електронного цифрового підпису, цифрового водяного знаку, хешуванні та інших механізмах захисту інформації. Проте, дотепер мало уваги приділялося розробці

методів підсилення хеш-функції паролю, на основі операцій матричних криптографічних перетворень зокрема.

Формулювання мети дослідження. Метою дослідження є розробка методів підсилення хеш-функції паролю шляхом здійснення *n*-разового хешування, використання salt-значення та на основі операцій матричного криптографічного перетворення паролю.

Виклад основного матеріалу дослідження й обґрунтування отриманих результатів. Основна більшість атак в сучасних інформаційних системах та веб-додатках пов'язана з авторизацією користувача. Після введення користувачем даних, система перевіряє його логін та пароль. Дані авторизації не зберігаються в чистому вигляді, пароль, як правило зберігається в захешованому вигляді.

Аутентифікація – це основа безпеки будь-якої системи, що полягає в перевірці достовірності даних про користувача сервером [5]. Вона не є тотожною ідентифікації і авторизації. Ці три терміни є елементами захисту інформації. Перша стадія – ідентифікація. Під час ідентифікації відбувається розпізнання інформації про користувача шляхом присвоєння йому унікальних міток: ідентифікаторів, паролів. Ідентифікація дозволяє суб'єкту – користувачу, процесу чи іншому апаратно-програмному компоненту назвати себе. Друга стадія аутентифікації – процес перевірки достовірності інформації про користувача. І остання стадія авторизації – перевірка прав користувача і визначення можливості доступу [6]. Найпоширенішим видом аутентифікації є парольна аутентифікація. Майже кожна інформаційна система вимагає, щоб на початку сеансу роботи користувач ідентифікував себе. Зазвичай, користувач вводить логін та пароль. Під час аутентифікації відбувається порівняння пароля, який ввів користувач з тим, який зберігається в базі даних. Аутентифікація може проходити за одноразовими та багаторазовими паролями [7]. Багаторазовий пароль задає користувач, а система зберігає його в базі даних. Він є однаковим для кожної сесії. До такого пароля відносяться PIN-коди, слова, цифри, графічні ключі. Одноразові паролі – різні для кожної сесії, наприклад можуть надходити SMS-повідомлення з кодом. Для перевірки даних авторизації необхідно порівняти значення обчисленого хешу введеного паролю з тим, що зберігається в базі даних інтернет-додатку, як показано на рис. 1.

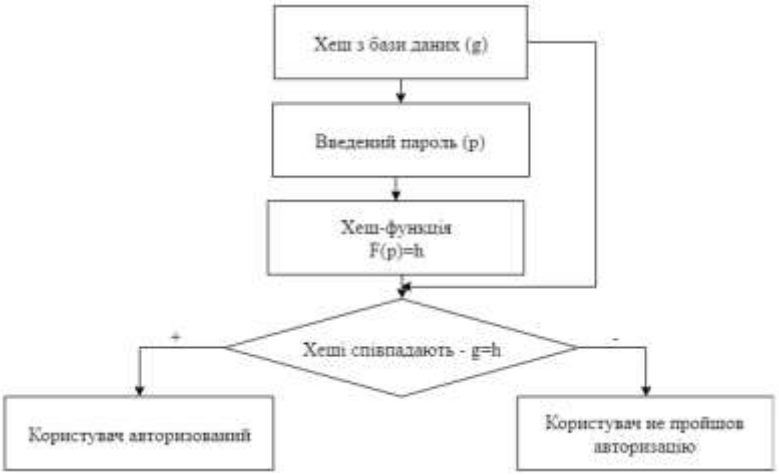

Рис. 1. Простий алгоритм авторизації користувача

Оскільки, паролі в базі даних зберігаються в вигляді хеш-функції, тому зупинимось на базових властивостях хеш-функцій. Хеш-функція може бути як криптографічною, так і не криптографічною. Відмінність криптографічної хеш-функції від інших хеш-функцій полягає в наступному:

- стійкість до колізій першого роду – для будь-якого повідомлення *P* неможливо в реальному часі підібрати будь-яке інше повідомлення *Q*, для якого хеш-функція *F*(*P*)=*F*(*Q*);
- стійкість до колізій другого роду – неможливо в реальному часі підібрати пару повідомлень (*P*, *P*'), які мають однаковий хеш;
- необоротність – для установленого значення хеш-функції *A* неможливо в реальному часі знайти блок даних *X,* хеш-функція якого *F*(*X*)=*A*.

Процес хешування паролю може виконуватись з використанням будь-якого алгоритму. Наприклад, можна використати алгоритм хешування, представлений в статті [8]. При виборі алгоритму хешування важливо звертати увагу на хеш-функції, які стійкі до колізій. Наприклад, алгоритм MD5 не актуальний з 2013 року, а алгоритм bcrypt/scrypt залишається актуальним [9]. Пароль можна підібрати за його хешем, володіючи алгоритмом хешування. Існує багато баз даних, де паролі співставлені з їх хешами. Тому, зловмисникам можна ускладнити завдання підбору пароля за його хешем, використовуючи подвійний хеш або використати salt-hashing. Salt-hashing або «сіль» – спосіб хешування, в якому до пароля додається набір символів одноманітного формату з хешованим паролем, що задається випадковим алгоритмом, який можна змінювати раз в заданий період для підвищення криптографічної стійкості [10].

В криптографії «сіль» – це набір випадкових даних, який використовується в якості додаткового вихідного сигналу в односторонній функції. Вона використовується для захисту паролів в базі даних. Раніше

пароль зберігався в незашифрованому вигляді в системі, але з часом були розроблені додаткові заходи безпеки для захисту пароля. «Сіль» є одним з таких методів. «Сіль» генерується випадковим чином для кожного пароля. Як вже було зазначено, з метою підвищення криптографічної стійкості потрібно з певною періодичністю змінювати алгоритм генерації salt-значення. Зазвичай, пароль і «сіль» об'єднуються і оброблюються криптографічною хеш-функцією, а отриманий результат зберігається в базі даних. Хешування допускає подальшу аутентифікацію без збереження, а отже і без ризику незашифрованого пароля в разі проникнення до сховища даних аутентифікації. На рис. 2 показаний алгоритм з врахуванням запропонованих додаткових інструментів підсилення хешу.

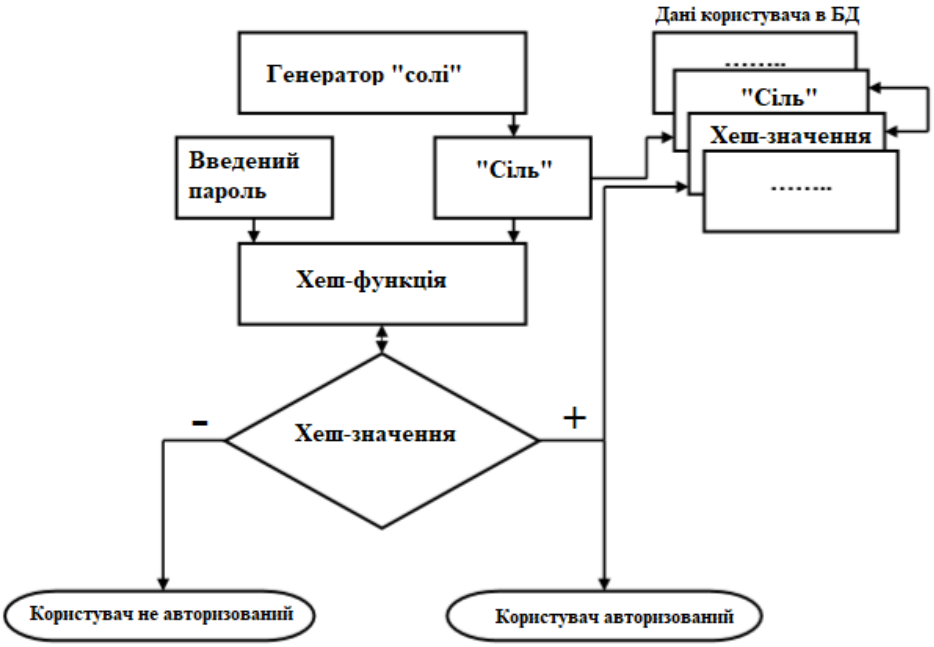

Рис. 2. Ускладнений алгоритм підсилення хеш-функції паролю

Значення «солі» генерується випадковим чином і може мати будь-яку довжину. Salt-значення додається до незашифрованого пароля, а потім результат хешується. Значення «солі» і результат хешування зберігаються.

Також, крім salt-hashing і багаторазового хешування паролю можна використовувати і інші додаткові інструменти: залежний хеш – залежить від унікальної змінної, наприклад, логіну; змішувати значення хешу; інтелектуальний хеш – хеш змінює алгоритм залежно від довжини і значень.

Ще одним зі способів підсилення хеш-функції паролю є використання операцій матричного криптографічного перетворення, рис. 3. Як видно з рис. 3, над паролем користувача спочатку виконується матричне криптографічне перетворення, а вже потім обчислюється значення хеш-функції. Матричні алгоритми придатні для обернених перетворень, якщо при цьому виконується умова невиродженості матриці, тобто:

1) відсутні нульові рядки і стовпці в матриці;

2) додавання рядків і стовпців матриці не дорівнюватиме нулю.

В загальному вигляді операції криптографічного перетворення, побудовані на основі додавання за модулем два, описуються такою моделлю (1) [11]:

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

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

Для виконання операції матричного криптографічного перетворення необхідно задати двійкову матрицю, наприклад, скориставшись генератором матриць і задавши умову $\det(A) \neq 0$.

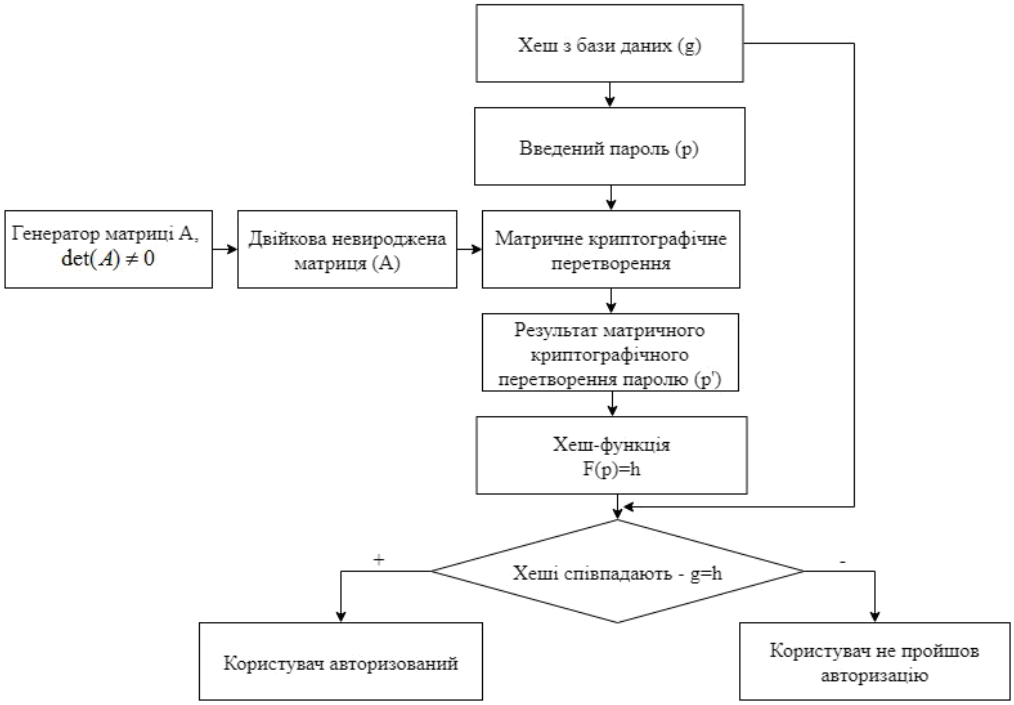

Рис. 3. Ускладнений алгоритм авторизації користувача за рахунок здійснення матричного криптографічного перетворення паролю

На рис. 4 показаний ще один спосіб підсилення хеш-функції пароля. Як видно з рис. 4, хеш пароля підсилений тим, що після обчислення хеш-функції над результатом виконується матричне криптографічне перетворення хешу.

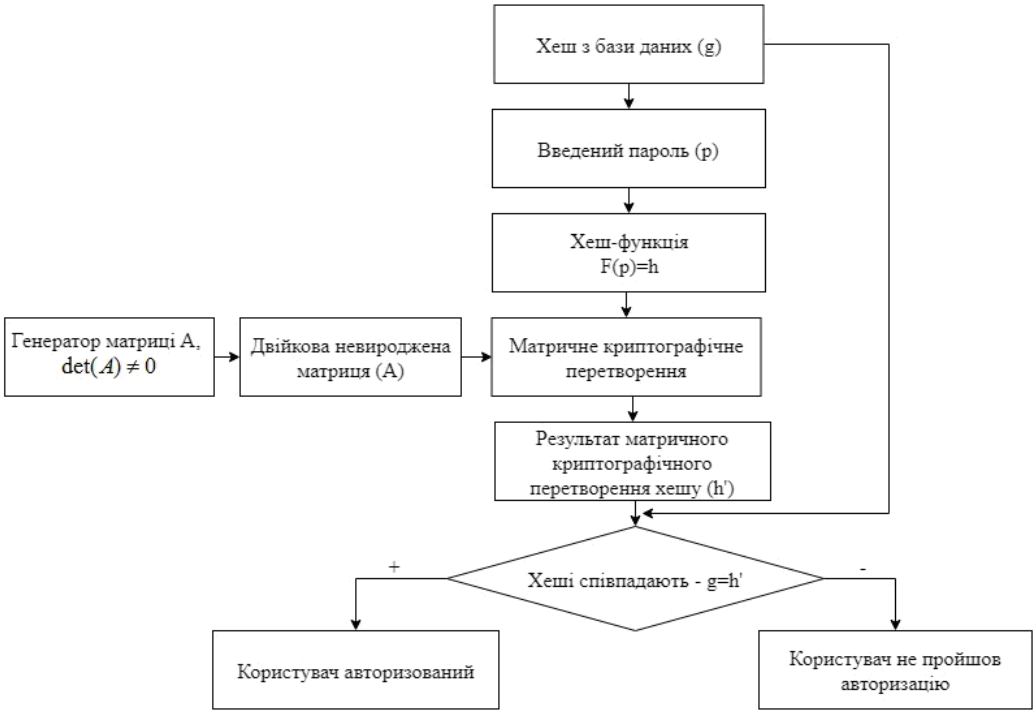

Рис. 4. Ускладнений алгоритм авторизації користувача за рахунок здійснення матричного криптографічного перетворення хешу

Висновки. Політика безпеки сучасних веб-додатків передбачає забезпечення надійної авторизації користувачів інформаційної системи. В зв'язку з цим дослідження методів аутентифікації користувачів не втрачають своєї актуальності. Найпоширенішим способом аутентифікації є парольна аутентифікація, тому доречною є розробка методів підсилення хеш-функції паролю. Таким чином, розроблено методи підсилення хеш-функції паролю шляхом здійснення n-разового хешування та з додаванням ентропії, використовуючи

інструмент salt-значення. Також в статті запропоновані алгоритми авторизації користувача, які включають операцію матричного криптографічного перетворення пароля та його хеш-значення, що ускладнює процес обчислення хеш-функції паролю і відповідно підвищує його надійність.

Література

1. Паутов П.А. Проблема аутентификации в многоуровневых приложениях. Прикладная дискретная математика. 2008. № 2. С. 87–90.

2. Сабанов А.Г. Методы исследования надежности удаленной аутентификации. Электросвязь. 2013. № 4. С. 263–267.

3. Сабанов А.Г. Аутентификация при электронном обмене документами. Доклады Томского государственного университета систем управления и радиоэлектроникию 2011. № 2. С. 263–266.

4. Власенко А.В., Дзьобан П.И., Тимченко М.В. Разработка алгоритмов, инструментов и методов авторизации пользователей в web-приложениях с использованием хеш-функций. Вестник АГУ. 2015. № 4(171). С. 144–150.

5. Рацеев С.М. Об оптимальных кодах аутентификации. Системы и средства информатики. 2013. № 1(23). С. 53–57.

6. Алешников С.И., Демин С.А., Федоров С.Б. Проблемы информационной безопасности организации (предприятия) и пути их решения. Вестник Балтийского федерального университета им. И. Канта. 2013. № 1. С. 147–154.

7. Євсеєв С.П., Томашевський Б. П. Дослідження загроз методів двофакторної аутентифікації. Прогресивні інформаційні технології. Радіоелектроніка, інформатика, управління. 2015. № 1. С. 52–59.

8. Розломій І.О. Методи обчислення хеш-функції електронного документу на основі матричних криптографічних перетворень. Вісник ЧДТУ. Технічні науки. 2016. № 4. С. 88–94.

9. Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. Universitet Shan'don. Kitajskaja Akademija Nauk. Universitet Shanhaj Dzjaoton. 2004.

10. Веденьев Л.Т., Афанасьев А.А., Афанасьев А.Н. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие для вузов. Гриф УМО МО РФ. 2-е изд. 2012. 552 с.

11. Рудницький В.М., Бабенко В.Г., Рудницький С.В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. Збірник наукових праць Харківського університету Повітряних Сил. 2012. № 4(33). С. 198–200.

References

1. Pautov, P.A. (2008) The problem of authentication in multilevel applications. Applied Discrete Mathematics, 2, pp. 87–90.

2. Sabanov, A.G. (2013) Remote authentication reliability research methods. Telecommunication, 4, pp. 263-267.

3. Sabanov, A.G. (2011) Authentication in electronic document exchange. Reports of the Tomsk State University of Control Systems and Radio Electronics, 2, pp. 263-266.

4. Vlasenko, A.V., Dziuban, P.I. and Timchenko, M.V. (2015) Development of algorithms, tools and methods for user authorization in web applications using hash functions. ASU Newsletter, №4 (171), pp. 144–150.

5. Ratseev, S. M. (2013) On optimal authentication codes, Systems and Means of Informatics, 1 (23), pp. 53–57.

6. Aleshnikov, S.I., Demin, S.A. and Fedorov, S.B. (2013) Problems of information security of the organization (enterprise) and ways of their solution. Bulletin of the Kant Baltic Federal University, 1, pp. 147–154.

7. Evseev, S. P. and Tomashevskyy, B. P. (2015) Two-factor authentication methods threats analysis. Progressiv informatics technologies. Radio Electronics, Computer Science, Control, 1, pp. 52–59.

8. Rozlomii, I.O. (2016) Methods for calculating the hash function of an electronic document based on matrix cryptographic transformations. Bulletin of CSTU. Engineering sciences, №4, pp. 88–94.

9. Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu (2004) Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. Universitet Shan'don. Kitajskaja Akademija Nauk. Universitet Shanhaj Dzjaoton.

10. Vedenyev, L.T., Afanasyev, A.A. and Afanasyev, A.N. (2012) Authentication. Theory and practice of provision of secure access to information resources: a manual for higher schools. The 2nd ed. 552 pp.

11. Rudnitsky, V.M., Babenko, V.G. and Rudnitsky, S.V. (2012) Method of synthesis of matrix models of operations of cryptographic coding and decoding of information. Proceedings of Kharkiv University of the Air Force, №4 (33), pp. 198–200.

Рецензія/Peer review : 2.1.2020 р. Надрукована/Printed : 14.2.2020 р.
Рецензент: д.т.н., проф. Рудницький В.М.