Practical Implementation Effectiveness of the Speed Increasing Method of Group Matrix Cryptographic Transformation

Svitlana Sysoienko[1][0000-0002-0009-337X], Iryna Myronets[2][0000-0003-2007-9943], Vira Babenko[3][0000-0003-2039-2841],

Cherkasy State Technological University, Shevchenko str., 460, Cherkasy, 18006, Ukraine

[1]s.sysoienko@gmail.com, [2]irenmir30@gmail.com, [3]verababenko84@gmail.com

Abstract. This material is devoted to the development of the speed increasing method of implementing a group matrix cryptographic transformation based on a generalized mathematical model of a group matrix cryptographic transformation, by reducing the complexity of building and implementing an reverse transformation, which provided a decrease in mathematical complexity and an increase in the speed of cryptographic transformation. On the basis of the mathematical apparatus of block matrices, checked the correctness of the mathematical model for constructing the group matrix of reverse cryptographic transformation.

Keywords: operation results, group operations, speed encryption, cryptographic transformation, block matrices, mathematical model, reverse transformation, cryptographic protection, logical functions.

1 Introduction

The cyber-attack environment, in which cybernetic influence is possible, is cybernetic space (cyberspace). Cyberspace is an artificial electronic environment for the existence of information objects in digital form, formed as a result of the functioning of cybernetic computer control and information processing systems and provides users with access to computing and information resources of the systems, the development of electronic computing products, the exchange of electronic messages information images in real time to enter into a relationship (to interact) on the sharing of computing and information resources (the provision of information services, conducting e-commerce, etc.) [1].

Ensuring the confidentiality, integrity, significance of information, protection from illegal actions of users is the basis for the functioning of modern computer systems [2-9]. One of the ways to combat cybercrime is to use cryptography.

Addressing the problem of the processing and protection of personal information of users placed in cyberspace is provided both at the national and international levels [10-13]. The problem of protecting confidential information requires continuous improvement of the quality and effectiveness of information security systems, improvement of new and existing methods and algorithms using cryptographic methods and information protection tools, methods and means of pseudorandom sequences forming and assessing their quality in connection with the constant increase in cyber attacks on computer systems [2, 14-20].

The problem of evaluating the cryptographic stability of information security systems is very relevant today, since there is a large number of a cryptographic algorithm [21], and there is the task of improving existing and building new effective information security systems and increasing the overall level of confidentiality of transmitted information.

2 Formal problem statement

In the course of the previous [22] the study obtained a generalized mathematical model for the direct and reverse group matrix cryptographic transformation:

$$G = \begin{bmatrix} a_{11}F_1\ (z_1) \oplus a_{12}F_2\ (z_2) \oplus \ldots \oplus a_{1k}F_k\ (z_k) \\ a_{21}F_1\ (z_1) \oplus a_{22}F_2\ (z_2) \oplus \ldots \oplus a_{2k}F_k\ (z_k) \\ \ldots\ldots\ldots\ \ \ldots\ldots\ldots\ \ \ldots\ldots\ldots\ \ \ldots\ldots\ldots\ \ \ldots\ldots \\ a_{k1}F_1\ (z_1) \oplus a_{k2}F_2\ (z_2) \oplus \ldots \oplus a_{kk}F_k\ (z_k) \end{bmatrix}, \tag{1}$$

where $a_{ij} \in [0,1]$ – the coefficients of the matrix of direct group cryptographic transformation, F_i – operations of non-group cryptographic transformations, $\oplus$ – operation of addition modulo 2, z_i – input data for direct transformation, $i \in \{1...k\}$.

This model contributed to the development of the theory of block matrices adapted to matrix cryptographic transformations. It was the result of the improving model of constructing cryptographic transformation based on the use of two operand operations by introducing a group transform, which made it possible to construct a generalized model of group cryptographic transformation with arbitrary number of operands.

In the course of further research, the speed increasing method of the implementation of group matrix cryptographic transformation [23] was developed and there was a need to evaluate its effectiveness.

3 Literature review

Problems of security and integrity of information in computer systems and networks require special approaches to their solution. In connection with the latest developments in Ukraine and the world, the increasing number of attacks on computer systems need to solve new security information tasks that are facing the relevant specialists.

Ensuring the protection of confidential information about the social, political, economic, military, scientific and technological condition of the state and personal information of national persons is an extremely important task. In the context of increasing the number of threats, there is a need to develop new and improve existing information security systems. In the field of information security, cryptographic protection is one of the promising directions of scientific research both in our country and abroad.

A significant contribution to the improvement of existing and development of new methods and means of cryptographic protection made such foreign and domestic scientists: C. E. Shannon, B Schneier, G Brassard, J. L. Massey, W. Diffie, M. E. Hellman, R. L. Rivest, A. Shamir, N. Koblitz, O. A. Moldovian, M. A. Moldovian, I. D. Gorbenko, V. K. Zadiraka, M. A. Ivanov, A. N. Fionov, V. V. Yashchenko, A. O. Logachev, B. Ya. Riabko, A. M. Oleksiichuk, L. V. Kovalchuk, A. Ya. Biletskyi, O. G. Korchenko and others.

However, due to the development of computer systems, there have always been and will remain unresolved tasks of increasing the level of information security and reducing the time of encryption. The main characteristics of cryptographic systems are the stability, speed and reliability of cryptographic transformations that need to be constantly raised. To date, not all possibilities have been exhausted for improving the stability of cryptographic systems on the basis of the use of logical operations of cryptographic transformation, a significant contribution to the development of which have been made: K. G. Samofalov, V. A. Luzhetskyi, O.V. Dmytryshyn, O. M. Romankevych, R. P. Melnyk and others. Therefore, there is a need for additional research aimed at developing methods for improving the quality of pseudorandom sequences, as well as improving the quality of crypto primitives for streaming and block encryption. An outstanding solution to the problem of increasing the speed and stability of the matrix cryptographic information transformation is the use of group transformations.

4 Evaluating the effectiveness of the speed increasing method of the implementation of group matrix cryptographic transformation

On the basis of the proposed generalized models of group matrix cryptographic transformation [22, 24], which are presented in the following form:

$$G^k = \begin{bmatrix} a_{11}F_1^k(z_1) \oplus a_{12}F_2^k(z_2) \oplus ... \oplus a_{1n}F_n^k(z_n) \\ a_{21}F_1^k(z_1) \oplus a_{22}F_2^k(z_2) \oplus ... \oplus a_{2n}F_n^k(z_n) \\ .... \; .... \; .... \; .... \; ..... \\ a_{n1}F_1^k(z_1) \oplus a_{n2}F_2^k(z_2) \oplus ... \oplus a_{nn}F_n^k(z_n) \end{bmatrix}, \qquad (2)$$

where $a_{ij} \in [0,1]$ – the coefficients of the matrix of direct group cryptographic transformation, F_i^k – operations of non-group two operand cryptographic transformations, $\oplus$ – operation of addition modulo 2, z_i – input data for direct transformation, w_i – input data (results of direct transformation) for reverse transformation, $i \in \{1...n\}$, $j \in \{1..n\}$.

$$G^d = \begin{bmatrix} b_{11}F_1^d(w_1) \oplus b_{12}F_1^d(w_2) \oplus ... \oplus b_{1n}F_1^d(w_n) \\ b_{21}F_2^d(w_1) \oplus b_{22}F_2^d(w_2) \oplus ... \oplus b_{2n}F_2^d(w_n) \\ .... \; .... \; .... \; .... \; ..... \\ b_{n1}F_n^d(w_1) \oplus b_{n2}F_n^d(w_2) \oplus ... \oplus b_{nn}F_n^d(w_n) \end{bmatrix}, \qquad (3)$$

where $b_{ij} \in [0,1]$ – the matrix coefficients of reverse group cryptographic transformation, F_i^d – operations of reverse non-group two operand cryptographic transformations, $i \in \{1...n\}$, $j \in \{1..n\}$.

For practical implementation, the schemes was constructed for the direct (Fig. 1, which implements the proposed model (2)), and the reverse (Fig. 2, which implements the proposed model (3)), group cryptographic information transformations.

It should be noted that a direct and reverse non-group matrix cryptographic transformation is performed in the first round of encryption and decryption. The direct and reverse group matrix transformations are implemented in other rounds of cryptographic transformation.

Taking into account the general technology of the encryption and decryption process with the key (Fig. 3) [25]:

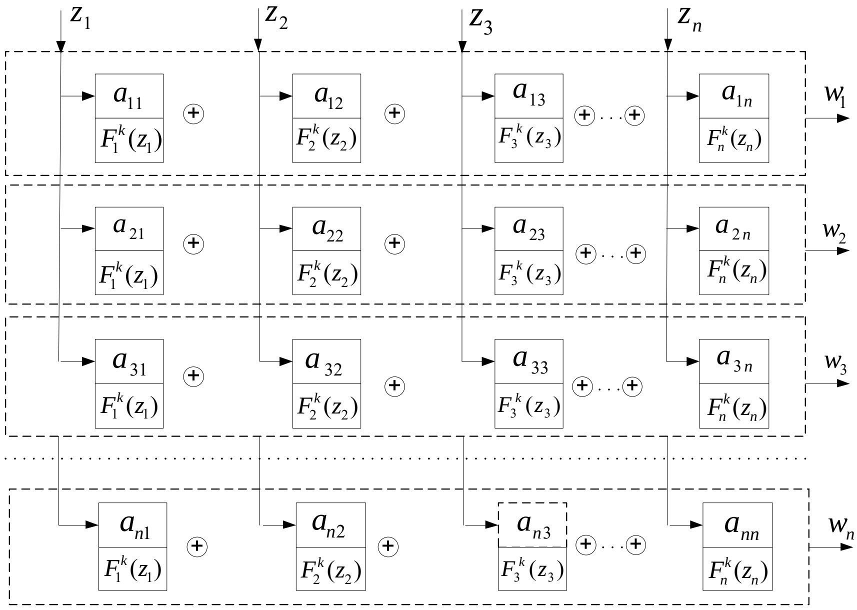

Fig. 1. The block diagram of direct group cryptographic information transformation in the implementation of the model (2)

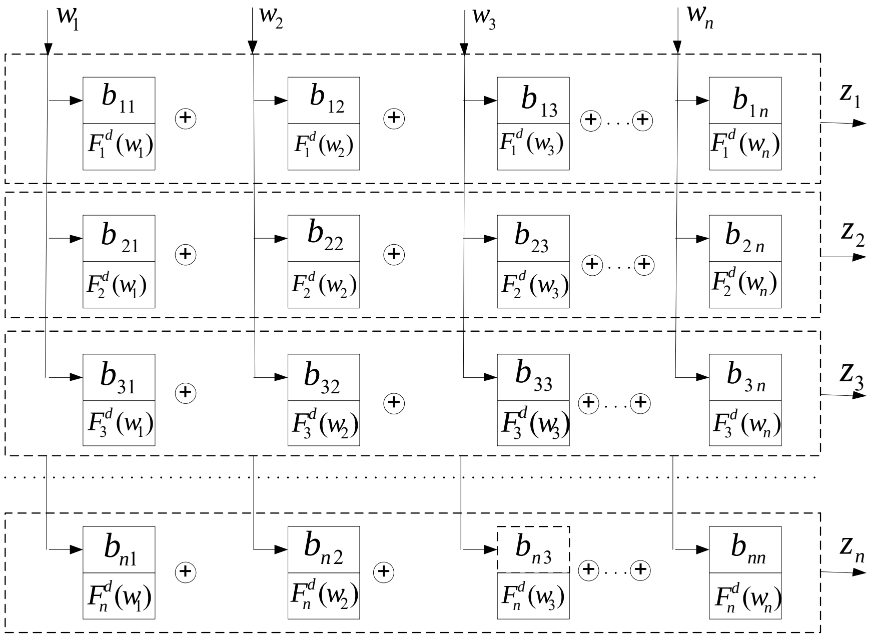

Fig. 2. The block diagram of reverse group cryptographic information transformation for model implementation (3)

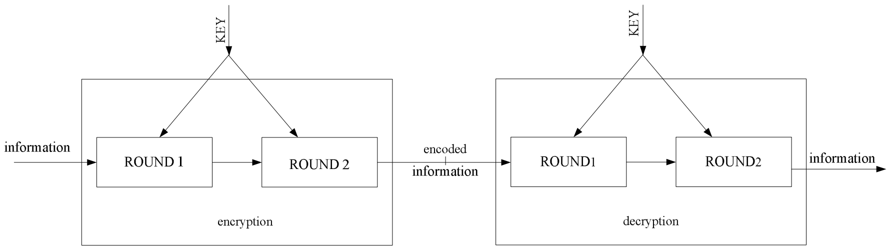

Fig. 3. Encryption and decryption with the key

Consider in more detail two-round hierarchical matrix encryption.

If in a group matrix transformation, n blocks of data are encrypted at the same time for m bits each, then the block diagram of implementing two-round hierarchical matrix encryption can be presented as (Fig. 4):

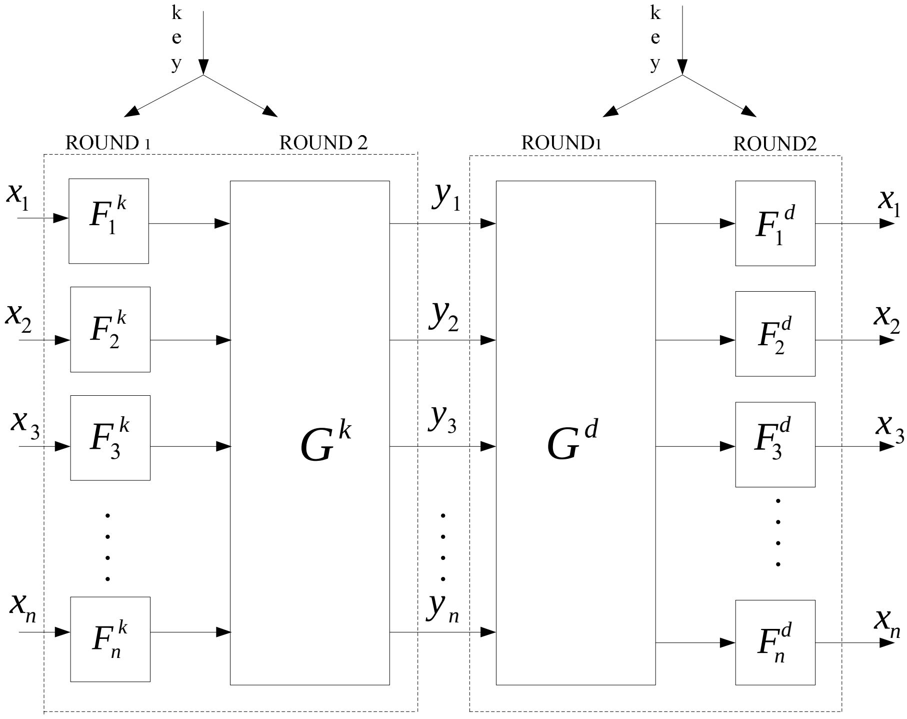

Fig. 4. Block diagram of implementing two-round hierarchical matrix encryption

In accordance with the developed speed increasing method of a group matrix cryptographic transformation, which implements mathematical models (2) and (3), the block diagram of implementing two-round hierarchical matrix encryption can be improved by reducing the elements and blocks of the reverse transform diagram.

The block diagram of implementing the speed increasing method of group matrix cryptographic transformation is presented in Fig. 5.

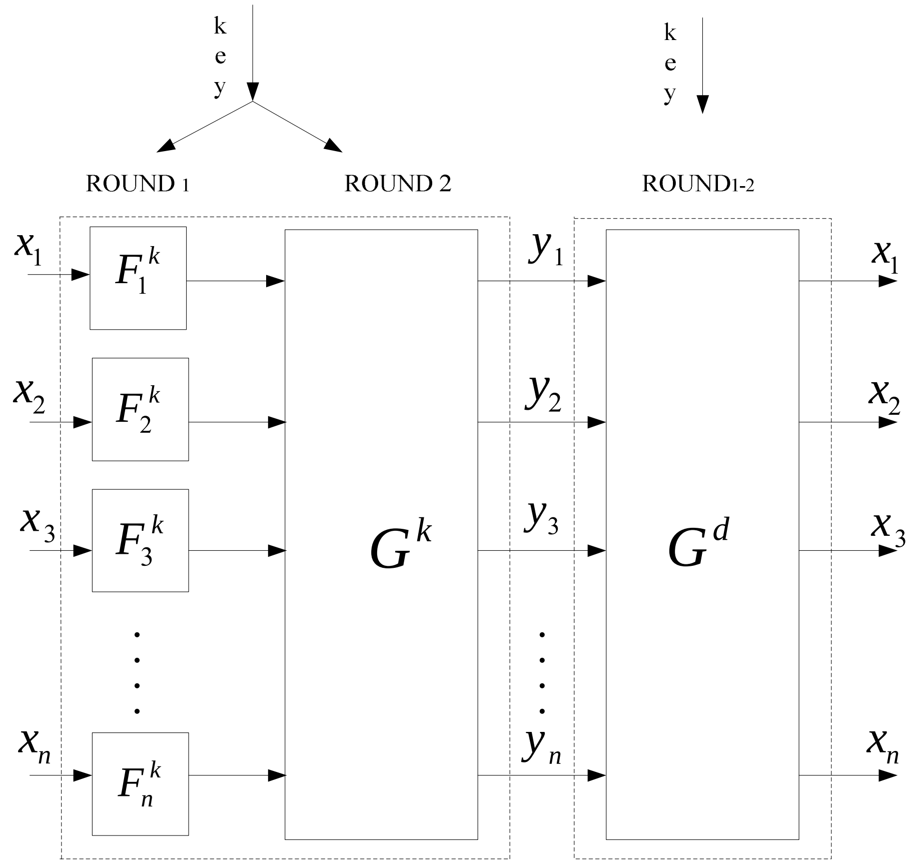

Fig. 5. The block diagram of the speed increasing method of group matrix cryptographic transformation

It should be noted that the block diagram of implementation of the speed increasing method of group matrix cryptographic transformation presented in Fig. 5 provides the implementation of an improved two-round hierarchical matrix encryption. Due to the improvement, which consists of combining two rounds of decryption based on a mathematical model (3), achieved by increasing the speed of the reverse transformation, leading to the reduction of time spent on this transformation.

Let be $t^k_{F_{\max}}$ – the maximal time of non-group direct matrix cryptographic transformation ($t^k_{F_{\max}} = \max\{t^k_{F_1}, t^k_{F_2}, t^k_{F_3}, ..., t^k_{F_n}\}$, $t^k_{F_i}$ – time of non-group direct matrix cryptographic transformation of Fi operation), t_G^k – time of group direct matrix cryptographic transform, $t_{F_{\max}}^d$ – maximum time of non-group reverse matrix cryptographic transformation ($t_{F_{\max}}^d = \max\{t_{F_1}^d, t_{F_2}^d, t_{F_3}^d, ..., t_{F_n}^d\}$, $t_{F_l}^d$ – time of non-group reverse matrix cryptographic transformation Fi operation), t_G^k – the time of group reverse matrix cryptographic transformation. It should be noted that in the general case $t_{F_{\max}}^k = t_{F_{\max}}^d$, and $t_G^k = t_G^d$.

Then the speed of implementation of two-round hierarchical matrix encryption (Fig. 4) will be determined:

$$t_{mp} = t_{F_{\max}}^k + t_G^k + t_{F_{\max}}^d + t_G^d. \tag{4}$$

The speed of implementation of the speed increasing method of group matrix cryptographic encryption (Fig. 5) will be determined:

$$t_{mpg} = t_{F_{\max}}^k + t_G^k + t_{\max}^d + t_{\oplus}, \tag{5}$$

where $t_{\max}^d = \max\{t_{F_{\max}}^d, t_G^d\}$, $t_{\oplus}$ – the implementation time of the addition operation by module, $t_{\max}^d > t_{\oplus}$.

Having analyzed expressions (4) and (5), we can state that:

$$t_{mp} > t_{mpg}. \tag{6}$$

Consequently, implementation of the speed increasing method of group matrix cryptographic encryption provides an increase in the total speed of encryption and decryption of information, both by reducing the complexity of finding the reverse transformation and by combining group and non-group matrix transformations when decoding information.

5 Conclusion

As a result of conducted research, an expression was obtained for calculating the complexity of logical determinants, depending on their order:

$$C_n = [(17 + (n-3) \times 6) \times 4 + 3]n + (n-1) \,,$$

where n>4 – the order of the logical determinant.

In this expression, the complexity is determined by the number of inputs of the logical elements of the functional scheme, which implements the construction of the determinant.

It was proved that the model (2) and (3) provide for reducing the complexity of implementing the matrix transformation from 8 to 33 times, depending on the matrix dimensions.

The proposed hierarchical structure of the group transformation made it possible to make certain changes in the matrix encryption and decryption process, that is, it made it possible to significantly reduce the time for the process of passing the cryptographic matrix transform (Fig. 6):

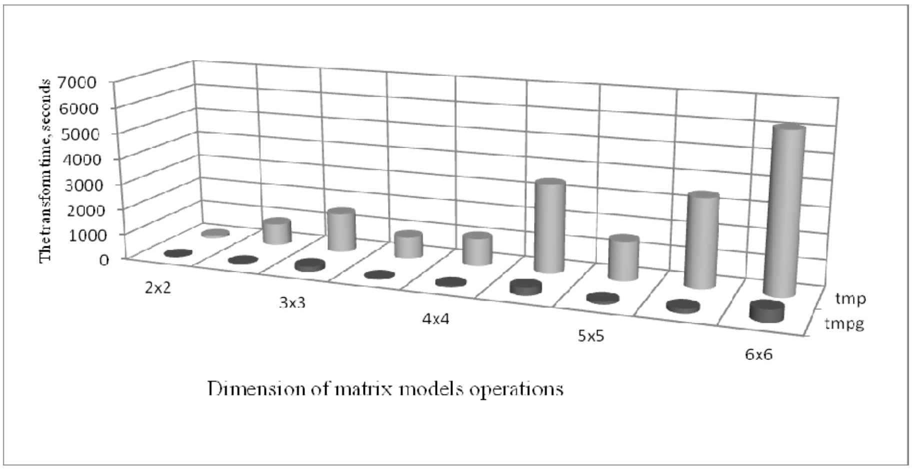

Fig. 6. Time of matrix transformation and group matrix cryptographic transformation

In the classical case, the implementation of group transformation in direct transformation is performed non-group, and then in a group operation, and in the case of inverse transformation, the group is initially performed, and then non-group operations. The spent time goes to all four stages of implementation.

The application of developed models of group matrix cryptographic transformation allows us to combine the stages of reverse group and non-group transformations. According to the results of practical implementation, the implementation of this method provides an increase in speed of 6-8% depending on the matrix dimensions.

References

1. Pogoretsky M. A., Shelomentsev V. P.: The concept of cyberspace as a medium for committing a crime. Information security of a person, a society, a state, vol. 2 (2), pp. 77-81 (2009).
2. Bernet S., Payne S. Cryptography. Official RSA Security Guide. Publishing house «Binom Press», Moscow (2002).
3. Schneier B. Secrets and Lies. Data security in the digital world. Publishing house «Peter», St. Petersburg (2003).
4. Maftyk S. Protection mechanism in computer networks. Publishing house «Myr», Moscow, pp. 126-128 (1993).
5. Zapechnikov S. V., Miloslavskaya N. G., Tolstoy A. I., Ushakov D. V. Threats, vulnerabilities, attacks and approaches to protection. Publishing house «Goryachaya Liniya – Telecom», Moscow, Information security of open systems: in 2 volumes. T. 1. 536 pp. (2006).
6. Shangin V. F. Information security of computer systems and networks. Publishing house «FORUM, INFRA-M,», Moscow (2011).
7. Authentication. Theory and practice of ensuring secure access to information resources. Ed. A. A. Shelupanov, S. L. Gruzdeva, Yu. S. Nakhayev. Publishing house «Goryachaya Liniya –Telecom», Moscow, (2009).
8. Faure E.V., Shvydkyi V.V., Shcherba A.I.: Information integrity control based on the factorial number system. Journal of Baku engineering university. Mathematics and computer science, vol. 1, no. 1, pp. 3-13 (2017).
9. Faure E.V., Shcherba A.I., Kharin A.A.: Factorial code with a given number of inversions. Radio electronics, computer science, control, no. 2, pp. 143-153 (2018). DOI 10.15588/1607-3274-2018-2-16.
10. Marushchak A. I. Information law: regulation of information activities. Publishing house «Skif, KNT», Kiev, (2008).
11. Decree of the President of Ukraine "On the Regulations on the Procedure for Implementing Cryptographic Information Protection in Ukraine" No. 505/98 dated 05.22.1998. [Electronic resource]: Official website of the President of Ukraine. URL: http://www.president.gov.ua /stateauthority/authofstate /prezidlist/ Prezidentadmin.
12. Decree of the President of Ukraine "On Amendments to Paragraph 5 of the Regulations on the Procedure for Implementing Cryptographic Information Protection in Ukraine" No. 333/2008 of April 11, 2008. [Electronic resource]: Official website of the President of Ukraine. URL: http://zakon5.rada.gov.ua/laws/show/333/2008.
13. Order of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine "On Approval of the Regulation on Control over the Operation of the Technical Information Protection System" No. 61 of December 22, 1999 [Electronic resource]: Legislation of Ukraine: Official site of the Verkhovna Rada of Ukraine. URL: http:www. http://zakon2.rada.gov.ua.
14. Rudnytskyi V. M., Myronets I. V., Babenko V. G.: Methodology for increasing the access speed to confidential information resources. Systems of information processing, vol. 5 (86), pp. 15-19 (2010).
15. Moldovian A.A., Moldovian N.A., Sovietov B.Ya. Cryptography: a series of "Textbook for universities. Special literature". Publishing house «Lan», St. Petersburg, (2000).
16. Chernetskyi I. F. Computer Security Technologies: Monograph. Publishing house MEGU, Rivne (2011).

17. Ivanov M. A.: Cryptographic methods for protecting information in computer systems and networks. Publishing house KUDITS-OBRAZ, Moscow (2001).
18. N. Ferguson, B. Schneier: Practical cryptography. Publishing house «Vyliams» (2005).
19. Myronets I. V.: Algorithm of the method of increasing the access speed to confidential information resources. Methods and means of encoding, protection and compaction of information: Proceedings of the Third International scientific-practic. conf. Publishing house VNTU, Vinnytsya. pp. 308 (2011)
20. Faure E.V., Shcherba A.I., and Rudnytskyi V.M.: The method and criterion for quality assessment of random number sequences. Cybernetics and systems analysis, vol. 52, issue 2, pp. 277-284 (2016). DOI: 10.1007/s10559-016-9824-3.
21. Venbo, Mao: Modern cryptography: theory and practice. Publishing house «Vylyams», Moscow (2005).
22. B. Schneider: Applied cryptography. Protocols, Algorithms, and Source Code in C. Publishing house «TRIUMF», Moscow (2002).
23. Sysoienko S. V., Babenko V. G.: Analysis of the complexity of implementation of operations models of group matrix cryptographic transformation. Naukowy i innowacyjny potencjał prezentacji: kolekcja pra naukowych "ΛώξΟΣ" z materiału międzynarodowej naukowo-praktycznej konferencji, Opole, 18 listopada 2018 r. Równe: «Volynsky Oberegi» Publishing House, t. 7, pp. 50-53 (2018).
24. Sysoienko S. V., Myronets I. V., Babenko V. G.: Construction of a generalized mathematical model of group matrix cryptographic transformation. Modern special technics, vol. 4 (55) (in print).
25. Sysoienko S. V.: Evaluation of the speed of group matrix cryptographic transformation. Systems of control, navigation and communication, vol. 1(47), pp. 141–145 (2018).