UDC 004.056.55:004.312.2 DOI: https://doi.org/10.32782/1995-0519.2022.1.14

IMPROVING THE CRYPTOGRAPHIC PROTECTION OF CONFIDENTIAL INFORMATION IN THE MANAGEMENT OF CIVIL PROTECTION FORCES AND MEANS

Ruslan Melnyk
PhD, Associate Professor,
Associate Professor at Department of Techniques and Means of Civil Defence
Cherkasy Institute of Fire Safety named after Chornobyl Heroes of National University of Civil Defence of Ukraine, 8/1 Onoprienko str., Cherkasy, Ukraine, 18034, melnyk.chipb@gmail.com;
ORCID: 0000-0002-5622-5642

Olga Melnyk
PhD, Senior Researcher,
Associate Professor at Department of Management in Sphere of Civil Defence
Cherkasy Institute of Fire Safety named after Chornobyl Heroes of National University of Civil Defence of Ukraine, 8/1, Onoprienko str., Cherkasy, Ukraine, 18034, melnyk.olja.2014@gmail.com;
ORCID: 0000-0002-9671-108X

The study is devoted to improving the cryptographic protection of confidential information in the management of forces and means of civil protection, based on the use of advanced matrix cryptographic transformation operations. A new group of cryptographic transformation operations has been identified, which will improve the quality of information protection systems of SES of Ukraine. A method for the synthesis of elementary functions of extended matrix transformation by introducing logical constraint conditions that provide nonlinearity of transformation is developed, which made it possible to obtain a complete set of operations of extended matrix transformation. Methods for the synthesis of cryptographic information transformation operations based on extended matrix transformation have been developed. The algorithm of formation of sequence of pseudo-random numbers on the basis of the expanded matrix cryptographic transformation and the algorithm of formation of sequence which combines matrix and extended matrix cryptographic transformation is developed.

Key words: confidential information, prevention of emergencies, cryptographic protection, three-bit logic functions, matrix cryptographic transformation, advanced matrix cryptographic transformation.

INTRODUCTION. Ensuring the protection of the population and territories in case of threats and emergencies is an integral part of state national security policy. Prevention of emergencies, their rapid elimination with the least optimal involvement of forces and means of civil protection is of particular importance for the physical and moral condition of the population and the economy of the country. In any case, all these strategic and tactical actions of State Emergency Service of Ukraine (SES of Ukraine) are accompanied by complex information processes. The exchange of information is carried out in order to prevent emergencies, minimize their consequences and organize a coordinated response of civil protection forces to emergencies and dangerous events. Most information processes in the management of forces and means in emergencies are confidential. The efficiency, reliability and confidentiality of information is of paramount importance for human security and national security in general.

Requirements for the level of information protection in the structure of the SES of Ukraine began to grow with the increase in the number of hacker attacks. Unauthorized access to information processed and circulating at information facilities and in information, telecommunication and information-telecommunication systems of the SES of Ukraine, as well as leakage of information through technical channels occupy a special place for its dangerous consequences among threats that may lead to disclosure of information.

Ensuring sustainable and reliable operation of telecommunication networks and system-wide servers in peacetime and in special periods is the main task of cyber security in SES of Ukraine [1]. Ensuring cybersecurity is one of the priorities in Ukraine's national security system [2].

Today, among the many methods of information protection, cryptographic methods have a special place [3]. Unlike others, these methods are based only on the properties of the information itself

and do not use the properties of its material media, the features of the nodes of its processing, transmission and storage.

ANALYSIS OF LITERATURE DATA AND PROBLEM STATEMENT. Particular attention in publications on this topic is paid to the mathematical foundations of methods of information security theory, cryptography, digital steganography, as well as the peculiarities of their implementation and application [4–6].

Recent research and publications include: [7], where it was researched the operations of the information's strict stable cryptographic coding based on their models' synthesis when changing the amount of two operands' bits; [8], where algorithms for the use of information-driven permutation operations to develop them in both software and hardware cryptographic information security, and [9], where a prototype was selected and the cryptographic information security module was improved. This module fixes information about the user ID, session ID, sending time, message length and serial number, as well as uses a new session key generation procedure for encryption. It allows to ensure the data confidentiality and integrity in information-communication systems and networks.

Scientific work [10] is devoted to the development of modern methods of information protection and analytical systems of civil protection of SES of Ukraine and the Centers for Security of Citizens in decentralization for reliable and rapid management, coordination.

However, insufficient attention has been paid to the study of the possibility of using advanced matrix cryptographic transformation operations to protect the confidential information of SES of Ukraine.

THE PURPOSE AND OBJECTIVES OF THE STUDY. The purpose of this study is to improve the cryptographic protection of confidential information in the management of forces and means of civil protection, based on the use of advanced matrix cryptographic transformation operations to protect confidential information.

To achieve this goal it is necessary to solve the following tasks:

– based on the analysis of existing methods and means of information protection and the results of a computational experiment to identify a new group of cryptographic transformation operations that will improve the quality of information security systems;

– to develop a method for the synthesis of elementary functions of an extended matrix transformation;

– to develop methods of synthesis of operations of cryptographic transformation of information on the basis of the extended matrix transformation;

– to develop an algorithm for the formation of a sequence of pseudo-random numbers based on advanced matrix cryptographic transformation and a sequence generation algorithm that combines matrix and advanced matrix cryptographic transformation.

MAIN PART. One of the ways to increase the efficiency of information protection in the information and telecommunication system of SES of Ukraine is the introduction of cryptographic transformation operations.

To conduct a study on the synthesis of cryptographic transformation operations, three-bit logic functions were chosen, the effectiveness of which has been proven in [11].

The concept of elementary cryptocurrency functions is introduced for a subset of synthesized functions. Basic cryptocurrency functions are: $f_1^{(1)}(x_1, x_2, ..., x_N)$, $f_2^{(2)}(x_1, x_2, ..., x_N)$, $f_m^{(N)}(x_1, x_2, ..., x_N)$ – conversion functions of the first, second and N category of information, respectively. Each function displays the rule-dependence of the converted bit value on all N initial values of information bits.

Cryptographic transformation operations are built on the basis of elementary functions.

For example,

$$F^k_{30,57,106} = \left(f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}\right) \Rightarrow F^d_{45,54,106} = \left(f^{(1)}_{45}, f^{(2)}_{54}, f^{(3)}_{106}\right),$$

$$F^k_{30,89,108} = \left(f^{(1)}_{30}, f^{(2)}_{89}, f^{(3)}_{108}\right) \Rightarrow F^d_{45,106,54} = \left(f^{(1)}_{45}, f^{(2)}_{106}, f^{(3)}_{54}\right),$$

where $f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}$ – elementary functions of the 1st, 2nd, 3rd category, respectively; sub-indices – numbers of elementary functions that correspond to the decimal value of the result of their execution; $F^k_{30,57,106}$, $F^d_{45,54,106}$ – cryptographic transformation operations, where k is direct and d is inverse cryptographic transformation.

It is expedient to single out a group of elementary functions that are not sufficiently studied to date – these are the elementary functions of the extended matrix transformation. This group of functions includes:

Direct functions
$f_{30} = x_1 \cdot \overline{x}_2 \vee x_1 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot x_3$,
$f_{54} = \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3$,
$f_{57} = \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3$,

$f_{75} = x_1 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3$,
$f_{86} = \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$,
$f_{89} = \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3$,
$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3$,
$f_{101} = x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3$,
$f_{106} = x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3$,
$f_{108} = x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3$,
$f_{120} = \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3$,
$f_{210} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$,
Inverse functions
$f_{225} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot x_3$,
$f_{201} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$,
$f_{198} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$,
$f_{86} = \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$,
$f_{169} = \overline{x}_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \cdot x_3$,
$f_{166} = \overline{x}_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3$,
$f_{156} = x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot x_3$,
$f_{154} = x_1 \cdot \overline{x}_3 \vee \overline{x}_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot x_2 \cdot x_3$,
$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3$,
$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3$,
$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3$,
$f_{210} = \overline{x}_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$.

The method of synthesis of elementary functions of extended matrix transformation is developed and formalized. The general expression for obtaining the elementary functions of cryptographic transformation will look like: $f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \overline{\hat{x}}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l$, where $\hat{x}_i$ – variables that can take direct or inverse values.

Further research was aimed at formalizing the synthesis of extended matrix cryptographic transformation operations.

The rules for obtaining a direct elementary function will be formalized by an expression:

$$f = x_i \oplus \left(\hat{x}_j \cdot \hat{x}_l\right)$$

provided: $i \in [1,2,3]$; $j \in [1,2,3]$; $l \in [1,2,3]$; $i \neq j \neq l$, where $\hat{x}$ – any value of the argument.

The first elementary function should be the function of extended matrix transformation on the basis of x_1:

$$f = x_1 \oplus \left(\hat{x}_2 \cdot \hat{x}_3\right). \quad (1)$$

The second function based on x_2 has an inverse value in the second term x_3 the second term of the first function. x_1 can acquire any value.

Based on this, the second elementary function will have a representation:

$$f = x_2 \oplus \left(\hat{x}_1 \cdot \overline{\hat{x}}_3\right). \quad (2)$$

The third function based on x_3 has an inverse value in the second term x_1 to the second term x_1 the second function, x_2 acquires an inverse value x_2 the second term of the first elementary function.

Based on this, the third elementary function will have a representation:

$$f = x_3 \oplus \left(\overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2\right). \quad (3)$$

Based on the expressions (1), (2), (3), the cryptographic transformation operation during the synthesis, starting from the first elementary function, will be presented:

$$\boldsymbol{F}^k = \begin{bmatrix} x_1 \oplus \left(\hat{x}_2 \cdot \hat{x}_3\right) \\ x_2 \oplus \left(\hat{x}_1 \cdot \overline{\hat{x}}_3\right) \\ x_3 \oplus \left(\overline{\hat{x}}_1 \cdot \overline{\hat{x}}_2\right) \end{bmatrix}. \quad (4)$$

We have developed a method for synthesizing operations of extended matrix transformation, which is written by the following rules:

1. Synthesis of a set of operations of extended matrix transformation based on expression (4).
2. Expanding the set of operations by removing the add-on from one or two operations.
3. Delete repetitive operations.
4. Expanding the set of operations by permuting bits in each operation.
5. Expanding the group of operations by introducing the inversion of elementary functions.

Consider the implementation of this method by example.

According to expression (4), 8 operations of extended matrix cryptographic transformation will be obtained:

– operation 1 $\boldsymbol{F}^k_{30,57,149} = \begin{bmatrix} x_1 \oplus \left(x_2 \cdot x_3\right) \\ x_2 \oplus \left(x_1 \cdot \overline{x}_3\right) \\ x_3 \oplus \left(\overline{x}_1 \cdot \overline{x}_2\right) \end{bmatrix}$;

– operation 2 $\boldsymbol{F}^k_{30,147,89} = \begin{bmatrix} x_1 \oplus \left(x_2 \cdot x_3\right) \\ x_2 \oplus \left(\overline{x}_1 \cdot \overline{x}_3\right) \\ x_3 \oplus \left(x_1 \cdot \overline{x}_2\right) \end{bmatrix}$;

– operation 3 $$F^{k}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

– operation 4 $$F^{k}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix};$$

– operation 5 $$F^{k}_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix};$$

– operation 6 $$F^{k}_{75,147,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix};$$

– operation 7 $$F^{k}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix};$$

– operation 8 $$F^{k}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix}.$$

Studies have shown that it was difficult to synthesize the inverse cryptographic transformation operation on the basis of the used forms of representation of elementary functions. Therefore, a tabular form of presentation was proposed for further research.

$$F^{k}_{45,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +\,1\,0 \\ -\,+\,- \\ -\,-\,+ \end{bmatrix};$$

$$F^{d}_{45,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +\,1\,0 \\ -\,+\,- \\ -\,-\,+ \end{bmatrix};$$

$$F^{k}_{45,85,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix} = \begin{bmatrix} +\,1\,0 \\ -\,-\,+ \\ -\,+\,- \end{bmatrix};$$

$$F^{d}_{75,85,51} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix} = \begin{bmatrix} +\,0\,1 \\ -\,-\,+ \\ -\,+\,- \end{bmatrix};$$

$$F^{k}_{57,85,30} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} = \begin{bmatrix} 1\,+\,0 \\ -\,-\,+ \\ +\,1\,1 \end{bmatrix};$$

$$F^{k}_{149,30,57} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} 0\,0\,+ \\ +\,1\,1 \\ 1\,+\,0 \end{bmatrix};$$

$$F^{k}_{149,30,57} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} 0\,0\,+ \\ +\,1\,1 \\ 1\,+\,0 \end{bmatrix};$$

$$F^{d}_{54,101,135} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} 1+1 \\ 0\,1\,+ \\ +\,0\,0 \end{bmatrix}.$$

Presentation of synthesis results using tabular extended matrix representation provided detection and study of dependences of nonlinear operations of extended matrix transformation.

As a result of the synthesis, 42 basic cryptographic transformation operations based on the extended matrix representation were obtained. The number of basic operations coincides with the number of operations obtained on the basis of computational experiment and operations synthesized on the basis of elementary functions of extended matrix transformation by substitution method.

It should be noted that the synthesis of cryptographic transformation operations based on the operation model by the exception method simplifies the synthesis process by using a formalized model of the transformation operation.

The concept of extended matrix transformation is theoretically based on the experimentally proven fact that the operations of matrix cryptographic transformation and extended matrix cryptographic transformation do not form a group of cryptographic transformation operations. As a result, re-conversion of information by operations from another group of cryptographic operations provides increased cryptographic stability of the transformation.

Based on the proposed concept to ensure high cryptographic stability, advanced matrix cryptographic transformation operations are used in conjunction with matrix cryptographic transformation operations, and provide preliminary or subsequent data processing. The use of advanced matrix cryptographic transformation operations before and after matrix transformation operations is inefficient, as their reuse does not increase cryptographic stability.

On the basis of the formed method of protection of information resources on the basis of extended matrix operations of cryptographic transformation [10] we will develop the algorithm of formation of sequence for check of matrix sensor (on the basis of RANDOM) with the help of NIST-STS software package (testing technique, which is most common among developers of cryptographic means of information protection), which is presented

in Fig. 1. To assess the quality of the transformation of any data, we will develop an algorithm for implementing the method of information protection based on advanced matrix operations of cryptographic transformation, which combines matrix and advanced matrix cryptographic transformation. This algorithm is presented in Fig. 2. The test results showed that the method of information protection based on advanced matrix operations of cryptographic transformation has passed a comprehensive control of the NIST-STS method.

CONCLUSION. The paper solves an important scientific and technical problem of improving the cryptographic protection of confidential information in the management of forces and means of civil protection based on the use of new operations of cryptographic transformation:

1. As a result of the analysis of existing methods and means of information protection and results of computational experiment the group of logical operations which will provide expansion of set

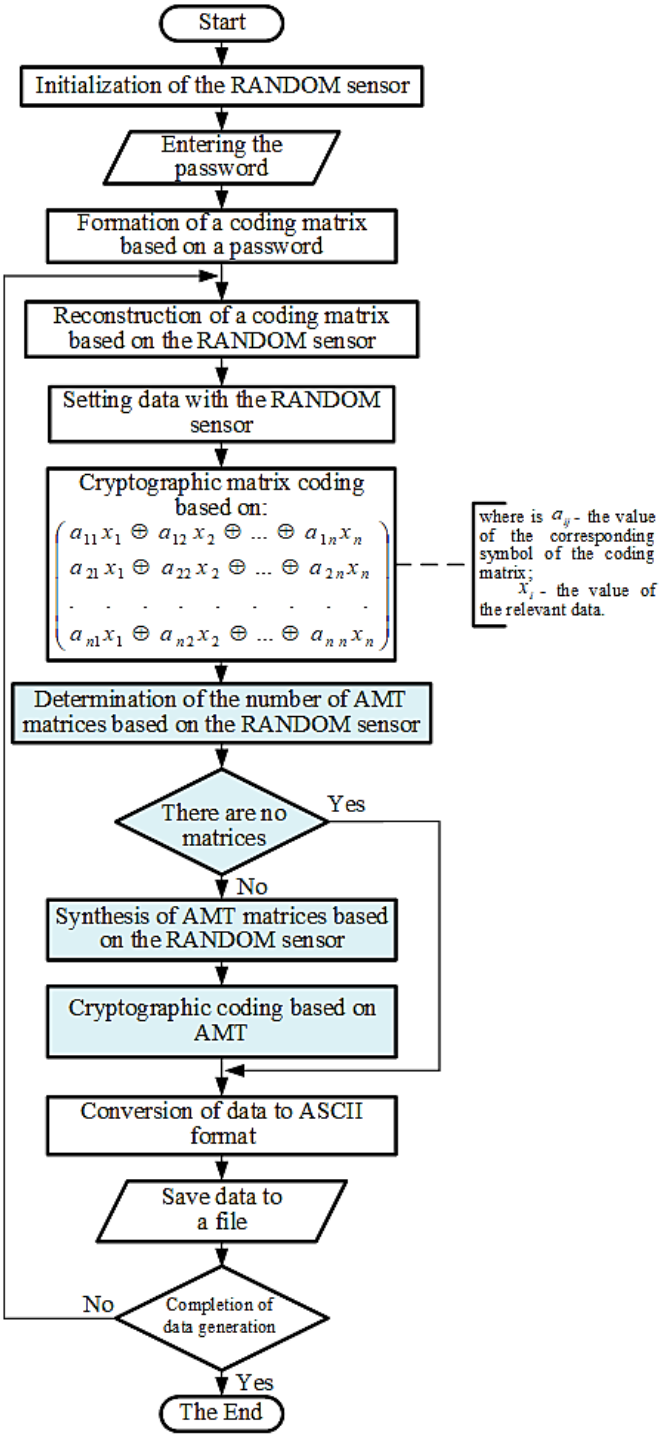

Figure 1 – Algorithm for forming a sequence of pseudo-random numbers based on extended matrix cryptographic transformation

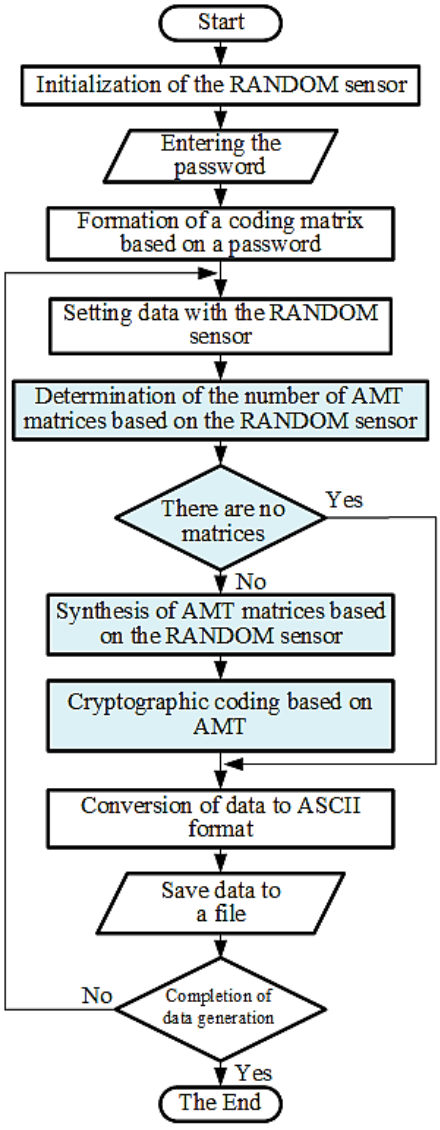

Figure 2 – Algorithm for forming a sequence, which combines matrix and advanced matrix cryptographic transformations

of operations of cryptographic transformation for increase of quality of cryptoalgorithms is defined. Improving of cryptographic stability of information security systems is based on the fact that the operations of extended matrix transformation do not form one group with other operations.

2. A method for the synthesis of elementary functions of extended matrix transformation by introducing logical constraint conditions that provide nonlinearity of transformation is developed, which made it possible to obtain a complete set of operations of extended matrix transformation.

3. Methods for the synthesis of cryptographic information transformation operations based on extended matrix transformation have been developed.

4. An algorithm for the formation of a sequence of pseudo-random numbers based on advanced matrix cryptographic transformation and a sequence generation algorithm that combines matrix and advanced matrix cryptographic transformation has been developed.

REFERENCES

1. Pro zatverdzhennia Polozhennia z orhanizatsii zakhodiv zabezpechennia kiberbezpeky v DSNS : nakaz DSNS Ukrainy vid 01.10.2020 r. № 533. [in Ukrainian]

2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14.05.2021 r. "Pro Stratehiiu kiberbezpeky Ukrainy" : Ukaz Prezydenta Ukrainy vid 26.08.2021 p. № 447/2021. [in Ukrainian]

3. Oppliger, R. Cryptography 101: From Theory to Practice. Artech (2021).

4. Ella Hassanien, Mohamed Elhoseny, Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments. Springer Nature Switzerland AG (2019).

5. Rajeshwaran, K., A nil Kumar, K. Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function, 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, pp. 1–6, doi: 10.1109/ICECCT.2019.8869146

6. Robert Ciesla, Encryption for Organizations and Individuals. Apress, Berkeley, CA. HELSINKI, Finland (2020).

7. Jancarczyk, D., Rudnytskyi, V., Breus, R., Pustovit, M., Veselska, O., & Ziubina, R. Two-Operand Operations of Strict Stable Cryptographic Coding with Different Operands' Bits. In 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). 2020, September, pp. 1–8.

8. Babenko, V., Myronyuk, T., Kryvous, H. Alhorytmy zastosuvannia operatsii perestanovok, kerovanykh informatsiieiu, dlia realizatsii kryptoperetvorennia informatsii. Visnyk Cherkaskogo derzhavnogo tekhnologichnogo universytetu, no. 3, 2021, pp. 44–58 [in Ukrainian]. doi: 10.24025/2306-4412.3.2021.247252

9. Gnatyuk, S., Smirnova, T., Berdibayev, R., Burmak, Y., Ospanova, D. Udoskonalenyi modul kryptohrafichnoho zakhystu informatsii v suchasnykh informatsiino-komunikatsiinykh systemakh ta merezhakh. Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika". 2021. T. 2 (14), pp. 176–185 [in Ukrainian]. doi: 10.28925/2663-4023.2021.14.176185

10. Melnyk, O., Melnyk, R. Rozroblennia metodu zakhystu informatsii informatsiino-analitychnykh system dlia zdiisnennia upravlinnia sylamy ta zasobamy tsyvilnoho zakhystu v umovakh detsentralizatsii. Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky. T. 32 (71). Part 1. № 2, 2021, pp. 188–193. [in Ukrainian]

11. Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii, V. Rudnytskyi, ed. Kharkiv, Ukraine : DISA PLIUS, 2018. [in Ukrainian]

УДОСКОНАЛЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УПРАВЛІННІ СИЛАМИ І ЗАСОБАМИ ЦИВІЛЬНОГО ЗАХИСТУ

Руслан Мельник
кандидат технічних наук, доцент,
доцент кафедри техніки та засобів цивільного захисту
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, вул. Онопрієнка, 8/1, Черкаси, Україна, 18034, melnyk.chipb@gmail.com;
ORCID: 0000-0002-5622-5642

Ольга Мельник
кандидат технічних наук, старший науковий співробітник,
доцент кафедри управління у сфері цивільного захисту
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України, вул. Онопрієнка, 8/1, Черкаси, Україна, 18034, melnyk.olja.2014@gmail.com;
ORCID: 0000-0002-9671-108X

Дослідження присвячено удосконаленню криптографічного захисту конфіденційної інформації в управлінні силами і засобами цивільного захисту на основі використання розвинутих матричних операцій криптографічного перетворення. Визначено нову групу операцій криптографічного перетворення, яка покращить якість систем захисту інформації ДСНС України. Розроблено метод синтезу елементарних функцій розширеного матричного перетворення шляхом введення логічних обмежень, що забезпечують нелінійність перетворення, що дозволило отримати повний набір операцій розширеного матричного перетворення. Розроблено методи синтезу операцій перетворення криптографічної інформації на основі розширеного матричного перетворення. Розроблено алгоритм формування послідовності псевдовипадкових чисел на основі розширеного матричного криптографічного перетворення та алгоритм формування послідовності, який поєднує матричне та розширене матричне криптографічне перетворення.

Ключові слова: конфіденційна інформація, запобігання надзвичайним ситуаціям, криптографічний захист, трирозрядні логічні функції, матричне криптографічне перетворення, розширене матричне криптографічне перетворення.

ЛІТЕРАТУРА

1. Про затвердження Положення з організації заходів забезпечення кібербезпеки в ДСНС : наказ ДСНС України від 01.10.2020 року № 533.

2. Про рішення Ради національної безпеки і оборони України від 14.05.2021 року. «Про стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021.

3. Oppliger R. Cryptography 101: From Theory to Practice. Artech (2021).

4. Ella Hassanien, Mohamed Elhoseny, Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments. Springer Nature Switzerland AG (2019).

5. Rajeshwaran K., A nil Kumar K. Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function, 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, pp. 1–6, doi: 10.1109/ICECCT.2019.8869146

6. Robert Ciesla, Encryption for Organizations and Individuals. Apress, Berkeley, CA. HELSINKI, Finland (2020).

7. Jancarczyk D., Rudnytskyi V., Breus R., Pustovit M., Veselska O., & Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding with Different Operands' Bits. In 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). 2020, September, pp. 1–8.

8. Бабенко В., Миронюк Т., Кривоус Г. Алгоритми застосування операції перестановок, керованих інформацією, для реалізації криптоперетворення інформації. *Вісник Черкаського державного технологічного університету.* Вип. 3. 2021. С. 44–58. doi: 10.24025/2306-4412.3.2021.247252

9. Гнатюк С. О., Смірнова Т. В., Бердибаєв Р. Ш., Бурмак Ю. А., Оспанова Д. М. Удосконалений модуль криптографічного захисту інформації в сучасних інформаційно-комунікаційних системах та мережах. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2021. Т. 2 (14). С. 176–185. doi: 10.28925/2663-4023.2021.14.176185

10. Мельник О., Мельник Р. Розроблення методу захисту інформації інформаційно-аналітичних систем для здійснення управління силами та засобами цивільного захисту в умовах децентралізації. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки.* Т. 32 (71). Частина 1. № 2, 2021. С. 188–193.

11. Рудницький В. Криптографічне кодування: обробка та захист інформації. 2018. Харків, Україна : ДІСА ПЛЮС.

Стаття надійшла 24.03.2022