КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.401409
UDK 004.056

Olga Hryshchuk
Senior Researcher, Graduate student of the Department of
Information Protection at the National Aviation University
National University of Defense of Ukraine, Research Laboratory of
Information Security Management of the Research Department of the
Problems of Development and Implementation of Strategic Communications of the
Institute of Strategic Communications, Kyiv, Ukraine
ORCID ID: 0000-0001-6957-4748
Ol.Hry@i.ua

MATHEMATICAL MODEL OF A SYMMETRICAL CRYPTOGRAPHIC SYSTEM FOR THE PROTECTION OF SPEECH INFORMATION BASED ON DIFFERENTIAL TRANSFORMATIONS

Abstract. Among known cryptographic systems, in practice, symmetric cryptographic systems are most often used to protect speech information. Such systems, when encrypting speech information, implement stream encryption of outgoing traffic. At the same time, the rapid development of quantum and post-quantum technologies, methods and means of cryptanalysis determines the urgent need for their further development. One of the promising approaches, which is not sufficiently covered in the professional literature today, is considered to be an approach based on the methods of integral cryptography. According to the basic principles of integral cryptography, a mathematical model in the form of an integral Fredholm equation of the first kind can be used as the basis of a cryptographic algorithm for a symmetric cryptographic system of speech information protection. The main difference and at the same time the advantage of cryptographic systems based on Fredholm integral equations of the first kind is their guaranteed theoretical and practical cryptographic stability. The guaranteed theoretical cryptographic stability and speed of such a symmetric cryptographic system is provided by the application of the method of differential transformations of Academician of the National Academy of Sciences of Ukraine G. Pukhov. Practical crypto-resistance is ensured by the practical unsolvability of the inverse incorrect decryption problem. It is suggested to use the regularization method of Professor A. Tikhonov to decipher the cyphergram obtained from speech information. Thus, the proposed mathematical model of a symmetric cryptographic system based on differential transformations is a further development of modern information technologies for cryptographic protection of speech information in Ukraine.

Keywords: mathematical model; symmetric cryptographic system; speech information; differential transformations; Fredholm integral equation of the first kind.

INTRODUCTION

The confidentiality of speech information that circulates in the communication systems of critical infrastructure is constantly under threat [1]. This is due to a number of technological innovations that have taken place in the world recently. This is the improvement of the performance of modern processors, the increase in the sophistication of cyber-attack tactics and the significant (many times) increase in the number of cyber incidents, the rapid development of quantum technologies, etc. [2]. As a result, for the fourth year in a row, the encryption key of the asymmetric cryptographic algorithm RSA-240 with a length of 795 bits has been compromised [3]. Considering the fact that until recently this cryptographic algorithm was considered one of the most reliable from the security point of view, it is possible that the keys to the best symmetric cryptographic algorithms AES-256 and others. can also be compromised.

Thus, today in practice there is an acute problem of ensuring the confidentiality of speech information circulating in communication systems. From a scientific point of view, in order to solve it, the existing cryptographic systems used for this need to be improved. Therefore, the first step on the way to solving a scientific problem, which has significant applied and at the same time scientific value, should be the further development of mathematical models of cryptographic systems for the protection of speech information.

ANALYSIS OF THE PROBLEM

Cryptography as a component of cryptological science has a clear, established over the years and built-up hierarchical system of knowledge about information encryption and decryption algorithms [4]. Currently used asymmetric [5] and symmetric [6] cryptographic algorithms in cryptographic systems of information and communication systems and their components—communication systems, are already practically implemented in the form of cryptographic protocols. From literary sources [4] it was known that the most common security protocols are IPSec, SSH and SRTP. Their main purpose is to ensure confidentiality and protection of information from its reproduction [7].

In addition to the above-mentioned protocols, there are other protocols for the encrypted transmission of speech information sent in the form of VoIP traffic. For example, for the transmission of service information, such a protocol is the TLS-protocol [4]. Its main purpose is the implementation of the procedure for encrypting subscriber numbers and user names, for example, in systems of military assignment at the tactical level [8].

Each of the protocols analyzed above is based on one or another mathematical model of the cryptographic system. For example, in [9] a cryptographic algorithm based on Turmites or the so-called Langton ant is proposed. The mathematical model based on it ensures the stability of the cryptographic algorithm to differential cryptanalysis, which is its significant advantage over the closest analogue—the cryptographic algorithm proposed by Zhang Yong [10]. At the same time, the impossibility of its use in real-time communication systems, which include communication systems in which speech information circulates, significantly hinders its practical application.

In [11], [12], a thorough analysis of known approaches to building mathematical models of cryptographic systems was carried out, in particular, their advantages and disadvantages were given. Thus, based on [12], the most promising cryptographic systems are systems based on mathematical models of dynamic chaos theory, mathematical models of information theory and cognitive theory, models of quantum and post-quantum cryptography, algorithms based on DNA and integral cryptography. At the same time, the mathematical model of the cryptographic system based on integral cryptography, as stated in [12] and [13], provides guaranteed theoretical and practical cryptoresistance, which is of significant practical and scientific interest.

PURPOSE OF THE RESEARCH

The purpose of the article is to develop a mathematical model of a symmetric cryptographic system for protecting speech information based on differential transformations to test the hypothesis about the possibility of creating guaranteed stable cryptosystems.

MAIN RESULTS

Integral cryptography, which is proposed to be the basis of the developed mathematical model of the speech information protection cryptographic system, is based on the application of Fredholm's integral equations of the first kind to perform cryptographic transformations. One of the main advantages of integral cryptography is the guaranteed theoretical and practical cryptoresistance, which is ensured by incorrectness according to J. Hadamard [14]. The class of such problems is practically unsolvable without the use of special regularization methods [15]. It is this property that opens wide prospects for cryptographic protection of speech information in special information and communication systems of critical purpose and their applications.

Based on the above, it is possible to formulate a *working hypothesis* of the research—the use of integral cryptography methods can ensure the theoretical and practical cryptographic stability of symmetric cryptographic systems for the protection of speech information. However, based on [16], *the following requirements must be met* for this:

- the mathematical model must be adequate. The adequacy of the model will determine the degree of its closeness to known symmetric cryptographic systems built according to the classical scheme;
- theoretical cryptoresistance should be ensured by reducing to a combinatorial complexity problem, depending on the number of differential spectrum discretes, which are taken into account during the generation of the encryption key and, accordingly, the differential spectrum of speech information;
- practical cryptoresistance (accuracy of the model) should be specified by the regularization parameter, which determines the accuracy of solving the inverse incorrect problem of decoding speech information;
- the mathematical model should have a low level of structural and functional complexity, which should bring it as close as possible to practical implementation;
- "softness" of the mathematical model to the initial parameters, which will allow it to meet the requirements listed above without changes in its structure and functionality.

The following *basic assumptions and constraints* are adopted when creating the model.

Assumption: encryption key K is kept secret by both participants in the exchange of speech information. As a model of speech information I harmonic mathematical models can be used, which are described by functional dependencies in which the parameters of speech information change over time [17]. Guaranteed theoretical and practical cryptoresistance means the resistance of a cipher to cryptanalysis.

Constraints. When developing a cryptographic system for protecting speech information, one key K must be used, that is, the cryptographic system should be classified as a symmetric cryptographic system. Guaranteed theoretical and practical cryptoresistance is limited to the class of inverse ill-posed problems. To decipher encrypted speech information I, known methods of regularization of incorrect problems should be used.

Based on the proposed requirements based on accepted constrains and assumptions, the formalized presentation of the developed mathematical model of a symmetric cryptographic system based on differential transformations can be reduced to the implementation of a system of two basic procedures related to encryption and decryption of speech information.

Based on the main provisions of the theory of communication in secret systems by K. Shannon [18], *the encryption procedure can be formalized as follows*:

let the sender A have to transmit through an unprotected communication channel some voice message — speech information $z(s)$ to the recipient B. Speech information $z(s)$ are raw data to be encrypted by sender A and decrypted by receiver B, respectively. Taking into account [17] the mathematical model of speech information $z(s)$ in a general form can be represented by an expression of the form

$$h(t) = A_m \cos\left(2\pi f_m t + \varphi_m(t) + \varphi_m\right), \tag{1}$$

where A_m — amplitude, V; f_m — cyclic frequency, Hz; t — voice message transmission time, s; $\varphi_m(t)$ — phase function, rad/s, φ_m — initial phase, rad.

An encryption procedure performed by sender A with respect to speech information transmitted over an open communication channel $z(s)$ according to the basic provisions of integral cryptography consists in solving a direct problem. Such a problem can generally be described by Fredholm's integral equation of the first kind

$$\int_a^b K(x,s)\, z(s)\, ds = u(x), \tag{2}$$

where $K(x,s)$ — secret key (the kernel of the Fredholm integral equation of the first kind); $z(s)$ — speech information to be encrypted and decrypted (source data); $u(x)$ — encrypted data (ciphergram), which are transmitted over an open channel from the sender A to the recipient B (Fig. 1).

Remark 1. In expression (2), the limits of integration are finite and meet the inequality conditions $a \le x$, $s \le b$. In this case, the secret key and encrypted data satisfy the conditions

$$\begin{cases} K(x,s) \in C(a \le x,\ s \le b); \\ u(x) \in C([a,b]). \end{cases}$$

Remark 1. It is assumed that there is a closed (secure) key exchange channel between sender A and receiver B.

To preserve the speed of cryptographic transformations in the system (Fig. 1), it is proposed to use the method of differential transformations by Academician of the National Academy of Sciences of Ukraine H. Pukhov [19]. One of its multiple advantages is the possibility of obtaining a mathematical model of the differential spectrum of speech information in an analytical form without losing the accuracy of the original model, since there is no methodological error in the method. Another advantage of the method, in contrast to other operator methods, such as Laplace, is the ability to perform direct and inverse differential transformations in real time, which is so important for stream ciphers. Reducing the original mathematical model to simple arithmetic operations on its differential spectra significantly simplifies the hardware and software implementation of speech information cryptographic protection means.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

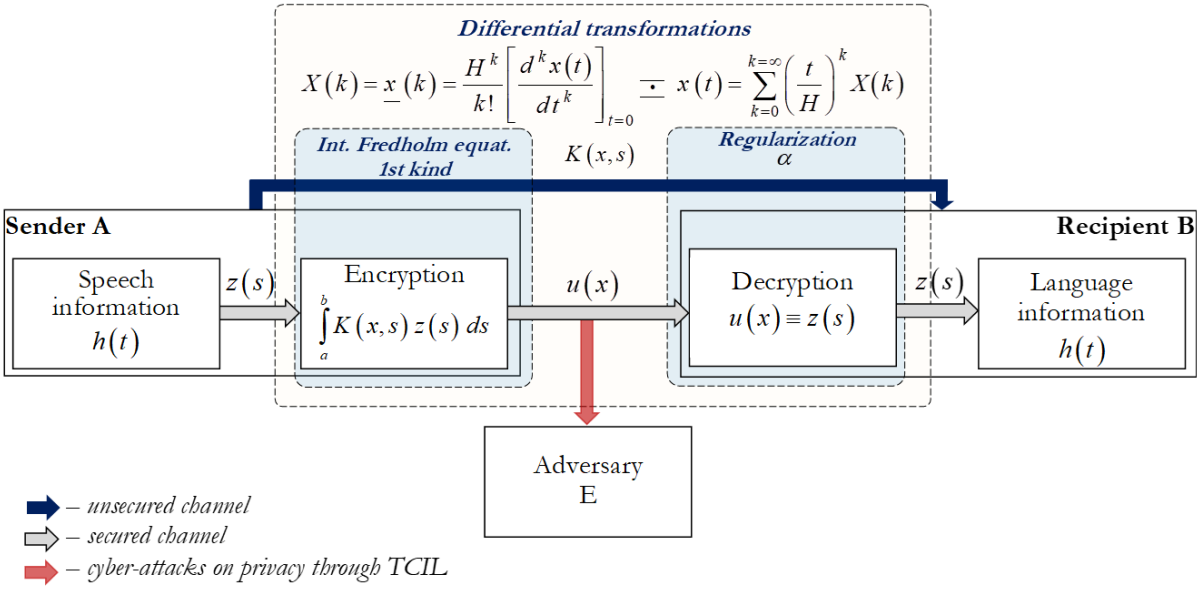

Fig. 1. Structural diagram of a symmetric cryptographic system for protecting speech information based on differential transformations

According to [19], differential transformations involve the presentation of the original mathematical model $x(t)$ by a Taylor power series centered at a point $t=0$. The direct and, accordingly, the inverse transformation have the form [19]:

$$X(k)=\underline{x}(k)=\frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \quad \overline{\cdot}$$
$$\overline{\cdot}\; x(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \qquad (3)$$

where $x(t)$ — the original, which is continuous, infinitely differentiable, and bounded together with all its derivatives by a function of the real argument t; $X(k)$ and $\underline{x}(k)$ — equivalent designations of the differential image of the original describing the discrete (lattice) function of the integer argument $k=0,1,2,\ldots$; H — scale constant, which has the dimension of the argument t and is often chosen as an equal segment $0\le t\le H$, on which the function $x(t)$ is considered; $\overline{\cdot}$ — symbol of correspondence between the original $x(t)$ and its differential image $X(k)=\underline{x}(k)$. According to (3), direct transformation allows according to the original $x(t)$ to find the image $X(k)$, and the reverse transformation (to the right of the symbol $\overline{\cdot}$) allows by image $X(k)$ to get the original $x(t)$. Differential images $X(k)$ are called differential *T-spectra*, and the values of the *T-function* $X(k)$, for specific values of the argument k — the discretes.

The decryption procedure (the inverse of the incorrect task), which is carried out by the recipient B, involves receiving encrypted data $u(x)$ from the sender A in the form of a differential spectrum $X(k)$ (3). The task of receiver B is to decipher the differential spectrum based on the regularization method. As such a method, from the set of all known methods of

regularization of incorrect problems, it is proposed to use the regularization method of Professor A. Tikhonov [15]. Its main advantage is the ability to accurately restore the original mathematical model of speech information according to its differential spectrum by solving the reversed inverse problem using the regularization parameter.

In its formalized form, the decoding procedure is reduced to solving the inverse incorrect problem (2)

$$u(x) = \lim_{\alpha \to 0} u_\alpha(x), \tag{4}$$

where $u_\alpha(x)$ — decoded speech information with accuracy up to the regularization parameter α.

At the same time

$$u_\alpha(x) = \frac{1}{\alpha} u(x) - \int_a^b K(x,s)\, z_\alpha(s)\, ds,$$

where $z_\alpha(s)$ — speech information to be encrypted (output data) with precision up to the regularization parameter α.

In practice, adversary E does not stop trying to carry out cyber-attacks on protected speech information through technical channels of information leakage (Fig. 1). In case of hacking of the crypto algorithm (selection of the secret key $K(x,s)$) and the regularization parameter α the adversary will gain unauthorized access to speech information, violating its confidentiality property.

Thus, the mathematical model of a symmetric cryptographic system based on differential transformations is described by a system of equations ***for encryption***

$$\begin{cases} h(t) = A_m \cos\left(2\pi f_m t + \varphi_m(t) + \varphi_m\right); \\ \int_a^b K(x,s)\, z(s)\, ds = u(x); \\ X(k) = \dfrac{H^k}{k!}\left[\dfrac{d^k x(t)}{dt^k}\right]_{t=0}, \end{cases} \tag{5}$$

where $h(t) \equiv z(s)$, $x(t) \equiv u(x)$ ***and decoding speech information***

$$\begin{cases} u(x) = \lim\limits_{\alpha \to 0} u_\alpha(x); \\ x(t) = \sum\limits_{k=0}^{k=\infty} \left(\dfrac{t}{H}\right)^k X(k), \end{cases} \tag{6}$$

where $u(x) \equiv x(t)$, $u_\alpha(x) \equiv X(k)$.

Analysis of the mathematical model (5), (6) shows that, according to it, the principle of operation of the proposed cryptosystem is reduced to the solution of the direct (correct) problem — the encryption procedure and the inverse (incorrect) problem — the decryption procedure. It also follows from the model that it is built according to the classical model of a symmetric cryptographic system. The difference between the models manifests itself at the level of the applied encryption and decryption procedures. Therefore, the observance of the classical principle of building symmetric cryptographic systems allows to claim that the ideas laid down in its basis fully confirm the working hypothesis of the research, and therefore, the proposed cryptographic system is capable of providing theoretical and practical cryptographic resistance. Based on this, model (5), (6) is adequate.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

In the article, the mathematical model of a symmetric cryptographic system for the protection of speech information was further developed, which differs from the known ones in that it uses a cryptographic algorithm for encryption and decryption of speech information based on the Fredholm integral equation of the first kind and differential transformations, which, due to the incorrectness of the solution of the inverse problem (cryptanalysis problem), provide guaranteed theoretical and practical crypto-resistance.

In the following studies, it is planned to develop an encryption protocol based on the proposed model.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Toledano, S. A. (2024). *Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches.* Birmingham: Packt Publishing.
2. Huiqin, X. (2024). Quantum Truncated Differential and Boomerang Attack. *Symmetry, 16(9),* 1–27.
3. Boudot, F. (2020). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. *Advances in Cryptology – CRYPTO 2020*, 62–91.
4. Schneier, B. (2003). *Applied cryptography. Protocols, algorithms, source texts in C language*. Triumph.
5. Usmonov, M. (2021). Asymmetric Cryptosystems. *International Journal of Academic Engineering Research, 5(1),* 6–9.
6. Deep, G. M. (2024). *Keys and Symmetric Cryptography.* Techsar Pvt. Ltd.
7. Kizza, J. M. (2024). Computer Network Security Protocols. *Guide to Computer Network Security. Springer,* 409–441.
8. Marković, M. R. (2024). Analysis of packet switching in VoIP telephony at the command post of tactical level units. Military technical courier, 72(1), 409–434.
9. Merzlykin, P. V. (2018). Cryptographic algorithm based on the system of tyurmites. *Actual issues of ensuring cyber security and information protection: collection of theses of reports IV International. science and practice conf,* 86–92.
10. Yong, Z. A. (2017). Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm. *Chinese Journal of Electronics, 26(5),* 1022–1031.
11. Gorbenko, I. (2017). Study of the possibility of using and advantages of post-quantum algorithms depending on the conditions of application. *East European Journal of Advanced Technologies, 2(9(86)),* 21–32.
12. Hryshchuk, R. V. (2019). Generalized model of the Fredholm cryptosystem. *Cybersecurity: education, science, technology, 4,* 14–23.
13. Bronshpak, G. (2014). New generation cryptography: Integral equations as an alternative to algebraic methodology. *Applied Electronics, 3,* 337–349.
14. Okhrimenko, M. G. (2008). *Methods of solving incorrectly set problems.* Center for Educational Literature.
15. Tikhonov, A. N. (1979). *Methods for solving ill-posed problems.* Science: Main editorial office of physical and mathematical literature.
16. Pavlenko, P. M. (2017). *Mathematical modeling of systems and processes.* NAU.
17. Korchenko, O. (2022). Comparative analysis of mathematical models of speech information. *Information security, 28(2),* 48–56.
18. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal,* 656–715.
19. Pukhov, G. E. (1986). *Differential transformations and mathematical modeling of physical processes: monograph.* Nauk. dumka.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Грищук Ольга Михайлівна
старший науковий співробітник, аспірантка кафедри засобів захисту інформації Національного авіаційного університету
Національний університет оборони України, науково-дослідна лабораторія управління інформаційною безпекою науково-дослідного відділу проблем розвитку та впровадження стратегічних комунікацій
Інститут стратегічних комунікацій, Київ, Україна
ORCID ID: 0000-0001-6957-4748
Ol.Hry@i.ua

МАТЕМАТИЧНА МОДЕЛЬ СИМТЕРИЧНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ

Анотація. Серед відомих криптографічних систем на практиці для захисту мовної інформації найчастіше застосовуються симетричні криптографічні системи. Такі системи при шифруванні мовної інформації реалізовують потокове шифрування вихідного трафіку. Разом з тим стрімкий розвиток квантових та постквантових технологій, методів та засобів криптоаналізу зумовлює нагальну потребу їх подальшого розвитку. Одним з перспективних підходів, який на сьогодні достатньо мало висвітлений у фаховій літературі, вважається підхід, що ґрунтується на методах інтегральної криптографії. Згідно з базовими основами інтегральної криптографії в основу криптоалгоритму для симетричної криптографічної системи захисту мовної інформації може бути покладено математичну модель у вигляді інтегрального рівняння Фредгольма першого роду. Головною відмінністю та одночасно перевагою криптографічних систем на основі інтегральних рівнянь Фредгольма першого роду є забезпечення ними гарантованої теоретичної та практичної криптостійкості. Гарантована теоретична криптостійкість та швидкодія симетричної такої криптографічної системи забезпечується застосуванням методу диференціальних перетворень академіка НАН України Г. Пухова. Практична криптостійкість забезпечується практичною нерозв'язністю оберненої некоректної задачі дешифрування. Для розшифрування шифрограми одержаної з мовної інформації пропонується скористатися методом регуляризації професора А. Тихонова. Таким чином, запропонована математична модель симетричної криптографічної системи на основі диференціальних перетворень є подальшим розвитком сучасних інформаційних технологій криптографічного захисту мовної інформації в Україні.

Ключові слова: математична модель; симетрична криптографічна система; мовна інформація; диференціальні перетворення; інтегральне рівняння Фредгольма першого роду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Toledano, S. A. (2024). *Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches.* Birmingham: Packt Publishing.
2. Huiqin, X. (2024). Quantum Truncated Differential and Boomerang Attack. *Symmetry, 16(9),* 1–27.
3. Boudot, F. (2020). Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. *Advances in Cryptology – CRYPTO 2020,* 62–91.
4. Schneier, B. (2003). *Applied cryptography. Protocols, algorithms, source texts in C language*. Triumph.
5. Usmonov, M. (2021). Asymmetric Cryptosystems. *International Journal of Academic Engineering Research, 5(1),* 6–9.
6. Deep, G. M. (2024). *Keys and Symmetric Cryptography.* Techsar Pvt. Ltd.
7. Kizza, J. M. (2024). Computer Network Security Protocols. *Guide to Computer Network Security. Springer,* 409–441.
8. Marković, M. R. (2024). Analysis of packet switching in VoIP telephony at the command post of tactical level units. Military technical courier, 72(1), 409–434.

9. Merzlykin, P. V. (2018). Cryptographic algorithm based on the system of tyurmites. *Actual issues of ensuring cyber security and information protection: collection of theses of reports IV International. science and practice conf*, 86–92.
10. Yong, Z. A. (2017). Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm. *Chinese Journal of Electronics, 26(5),* 1022–1031.
11. Gorbenko, I. (2017). Study of the possibility of using and advantages of post-quantum algorithms depending on the conditions of application. *East European Journal of Advanced Technologies, 2(9(86)),* 21–32.
12. Hryshchuk, R. V. (2019). Generalized model of the Fredholm cryptosystem. *Cybersecurity: education, science, technology, 4,* 14–23.
13. Bronshpak, G. (2014). New generation cryptography: Integral equations as an alternative to algebraic methodology. *Applied Electronics, 3,* 337–349.
14. Okhrimenko, M. G. (2008). *Methods of solving incorrectly set problems.* Center for Educational Literature.
15. Tikhonov, A. N. (1979). *Methods for solving ill-posed problems.* Science: Main editorial office of physical and mathematical literature.
16. Pavlenko, P. M. (2017). *Mathematical modeling of systems and processes.* NAU.
17. Korchenko, O. (2022). Comparative analysis of mathematical models of speech information. *Information security, 28(2),* 48–56.
18. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal,* 656–715.
19. Pukhov, G. E. (1986). *Differential transformations and mathematical modeling of physical processes: monograph.* Nauk. dumka.