UDC 519.6: 004.421.5
DOI https://doi.org/10.32782/2521-6643-2026-1-71.3

Pasichnyk V. A., Candidate of Physical and Mathematical Sciences, Associate Professor, Principal Developer of Software Engineering and Digital Transformation Company Luxoft
ORCID: 0000-0001-9434-563X

Pasichnyk A. N., Doctor of Physical and Mathematical Sciences, Professor, Professor at the Department of Mathematical Modelling and System Analysis Dniprosky State Technical University
ORCID: 0000-0002-8561-1374

Riabenko. V. I., Higher Education Applicant at the Department of Mathematical Modelling and System Analysis Dniprosky State Technical University
ORCID: 0009-0004-8723-8819

MATHEMATICAL MODELS AND ALGORITHMS OF CRYPTOGRAPHIC DATA PROTECTION IN DISTRIBUTED INFORMATION SYSTEMS

In modern conditions, information networks and data processing and transmission centers are a determining factor in the effective functioning of management systems of state institutions, financial and industrial organizations, energy and communications enterprises, transport and logistics infrastructure. Accordingly, the increase in the number of such centers and the number of different communication lines between them significantly increases the risks of unauthorized access to confidential information, ensuring data security and integrity. Therefore, the study of the problem of information security is of great importance for preventing and countering phishing attacks, which are constantly exposed to both individual enterprise networks and national networks.

The paper analyzes mathematical models that describe the process of information protection using cryptographic data encryption algorithms. The practical application of the algorithms of the given substitution, the Vigenère cipher, and self-synchronizing stream ciphers is considered. To increase the stability of the ciphertext, a modification of the Vigenère algorithm is proposed using separate unified alphabet tables for the text and the encryption/decryption key. Recommendations are developed for the use of the considered crypto algorithms to ensure effective protection of information systems from intentional or accidental interference. To increase the efficiency of the use of crypto algorithms, the feasibility of the integrated use of symmetric and asymmetric encryption methods to use their positive qualities, such as the speed of processing secret keys and the security of their transmission, is indicated. Promising directions for the development of information security systems using cryptographic algorithms are identified.

Key words: *information systems, crypto algorithms; data encryption; authentication; access control.*

Пасічник В. А., Пасічник А. М., Рябенко В. І. Математичні моделі та алгоритми криптографічного захисту даних в розподілених інформаційних системах

В сучасних умовах інформаційні мережі та центри обробки і передачі даних є визначальним фактором ефективного функціонування систем управління державними інституціями, фінансовими і промисловими організаціями, підприємствами енергетичного сектору і зв'язку, транспортною та логістичною інфраструктурою. Відповідно збільшення чисельності таких центрів і кількості різних ліній зв'язку між ними значно підвищує ризики несанкціонованого доступу до конфіденційної інформації, забезпечення безпеки та цілісності даних. Тому дослідження проблеми інформаційної безпеки має важливе значення для упередження та протидії фішинговим атакам, яким постійно піддаються як окремі мережі підприємств, так і національні мережі в цілому.

У роботі проведено аналіз математичних моделей, які описують процес захисту інформації за допомогою криптографічних алгоритмів шифрування даних. Розглянуто питання практичного застосування алгоритмів заданої підстановки, шифру Віженера та потокових шифрів, що самосихронізуються. Для підвищення стійкості шифротексту запропоновано модифікацію алгоритму Віженера з використанням окремих уніфікованих таблиць алфавітів для тексту і ключа шифрування/дешифрування.

Розроблено рекомендації щодо застосування розглянутих криптоалгоритмів для забезпечення ефективного захисту інформаційних систем від навмисного чи випадкового втручання. Для підвищення ефективності застосування криптоалгоритмів вказано на доцільність комплексного застосування методів симетричного і асиметричного

© V. A. Pasichnyk, A. N. Pasichnyk, V. I. Riabenko, 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

шифрування для використання їх позитивних якостей, таких як швидкість обробки секретних ключів та безпеки їх передачі. Визначені перспективні напрями розвитку систем інформаційної безпеки з використанням криптографічних алгоритмів.

Ключові слова: *інформаційні системи, криптоалгоритми; шифрування даних; автентифікація; управління доступом.*

Formulation of the problem. The use of information and communication technologies is one of the most important levers of economic development of society. In modern conditions, information networks implement the processing and transmission of large volumes of data that ensure the management of state institutions, financial and industrial organizations, energy sector enterprises, transport and logistics infrastructure, special-purpose control and communication systems. According to expert estimates, the total volume of data processed and transmitted in computer networks increases almost an order of magnitude annually. The effectiveness of the functioning of such information systems involves the use of a distributed architecture that combines a large number of computer centers located at a considerable distance. Accordingly, the increase in the number of such centers and the number of different communication lines between them significantly increases the risks of unauthorized access to confidential information, ensuring data security and integrity [1, 2]. Therefore, the issues of protecting computer networks and systems from unauthorized access in modern conditions have become particularly important, and the problems of improving and determining the effectiveness of information protection methods are quite relevant and require further development.

Analysis of recent research and publications. Currently, one of the most effective approaches to data protection in information systems is cryptographic methods that are based on the properties of the information itself and do not use the properties of its material carriers, the features of computer centers for its processing, transmission and storage technologies. Therefore, various aspects of the study of the problems of the development of cryptology and cryptographic analysis are actively investigated in numerous scientific works.

Thus, the conceptual principles of information security, national interests in the information sphere, the strategy for the development and formation of a single information space, threats to the security of the state and its citizens in the information sphere, the system for ensuring information security in Ukraine, the features of the functioning and functions of its subjects are systematized in the textbook [1]. The work [2] presents the results of the unification of practical approaches and standards, which are proven and agreed methods for implementing cybersecurity for a wide range of technical developments in the field of computerized systems, information networks and computer architecture.

The article [3] considers the problem of increasing the security of Web resources with stable cryptographic algorithms based on random number generators that take into account the features of user behavior in distributed information systems of collective access. During the study, a random number generation algorithm was developed that uses pre-prepared tables containing verified irrelevant numbers. An algorithm for the operation of a table generator for the software implementation of an encryption system was proposed.

The work [4] is devoted to the problems of information protection at critical infrastructure facilities. It is shown that in order to ensure the reliability of the functioning and protection of such facilities from cyber threats, it is necessary to ensure the implementation of the latest strategies and approaches in this area using innovative technologies of artificial intelligence, cryptography, machine learning, blockchain, and others.

The results of the analysis of the problems of developing an information security system and protecting information systems from intentional or accidental interference are given in the publication [5]. Directions for improving information security technologies are determined, taking into account real and potential threats, as well as the basic principles of its provision.

In [6], a methodology for identifying information security violations of a cyber-physical system of a wind generator is presented, taking into account the analysis of statistical indicators of dispersion, asymmetry and kurtosis of the input parameter “power” collected by the system sensors. An algorithm for formalizing the process of identifying falsified data in the information flow of a cyber-physical system and detecting information security violations using methods for analyzing the corresponding statistical indicators is proposed.

In [7], several cryptographic algorithms were proposed to implement access to authorization centers – the Diffie–Hellman key exchange protocol, the DSA algorithm for creating a digital signature of data required for the above protocol, as well as the AES algorithm with different encryption modes for authentication and symmetric data encryption. It is shown that this choice of protocols is explained by the mutual compensation of the problematic areas of these protocols. Thus, the AES algorithm uses an encryption key that is the same for two recipients, since it is used both for encryption and decryption of data. Accordingly, to prevent unauthorized access, a protocol for creating a shared key with the recipient is used, the authentication of which is provided by the DSA algorithm.

The possibilities of using technical systems of interconnected computing devices, mechanical and digital machines (IoT) for data protection of information and telecommunication networks are analyzed in the article [8]. The limitation of the power cycle, memory and data processing of such systems is shown, which complicates the implementation of reliable network security. Based on the analysis of known encryption algorithms: RSA,

Vernam cipher, El-Gamal scheme, a prototype of the IoT system was presented using limited devices and a software implementation of the Vernam cipher, which ensured its high cryptographic stability.

In the work [9], a study of models and algorithms of information security systems of corporate telecommunication networks was conducted. According to the results of the analysis, the identified problematic issues of protecting such networks are related to the need to improve the guest Wi-Fi system connection models and password manager operation algorithms that allow implementing a secure architecture through additional user authentication with its audit within the corporate network perimeter, while protecting credentials from external influence and implementing the "Zero Trust" principle ("never trust, always verify").

The purpose of the article. The purpose of this article is to study mathematical models of complex protection and ensuring the security and reliability of data transmission in computer systems and networks using algorithms of given substitution, Vigenère cipher and self-synchronizing stream ciphers. Identification and justification of promising directions for improving methods of cryptographic encryption and information protection.

Presenting main material. At this stage, the main features of the development of information technologies can be characterized as follows:

– access to certain data allows you to control significant material and financial values, and the value of information began to increase rapidly;

– continuous growth in volumes and a wide range of computer processing of information, which is no longer limited to text data;

– the complexity of the nature of information interactions poses new tasks for cryptography, such as signing an electronic document and delivering an electronic document "against receipt";

– the subjects of information processes are now not only people, but also the software systems they create;

– the power of modern computers provides new opportunities for both cipher developers and analysts to break these ciphers.

The above conditions have given new impetus to the development of practical cryptography on mathematical methods for ensuring the confidentiality, integrity and authenticity of information in the following areas:

– firstly, stable ciphers with secret symmetric and asymmetric keys have been developed, designed to perform the classic task of ensuring the secrecy and integrity of transmitted or stored data;

– secondly, methods have been created for solving new, non-traditional problems in the field of information protection, the most famous of which are the problems of signing a digital document and open key distribution.

It should be noted that data can be encrypted both during storage and during transmission using:

– with symmetric encryption, only one key, and everyone uses the same secret key;

– with asymmetric encryption of several keys: one "public key" for encryption, and another "private key" for decryption.

To effectively protect different types of data, it is advisable to use different types of crypto algorithms. A crypto algorithm is an algorithm for implementing a mathematical model of data transformation (encryption) and key generation to ensure access only to authorized users. The use of effective encryption algorithms and secure keys is important for protecting information and preventing unauthorized access to it by attackers. A cryptographic protocol defines a set of cryptographic schemes for data transformation, rules and procedures for key management, including their development and distribution. A cryptographic transformation with a known key k can be represented by the transformation function F, which is defined as follows:

$$y = F(x, k) + x, \tag{1}$$

where x – elements of the original text; k – encryption key; y – elements of the cryptogram.

Let's consider modifications of well-known algorithms: simple substitution, Vigenère cipher, Playfair cipher, and the stream encryption algorithm. We will also consider an algorithm that allows you to encrypt and decrypt data using the proposed crypto algorithms using different data tables.

Simple substitution cipher. This is the simplest encryption method, also called monoalphabetic substitution. The key is a permuted alphabet, the letters of which replace the letters of the regular alphabet of the source text. For example, each letter is replaced by the letter that is 3 positions after it: A®D, B®E, etc. Then the text ABC is replaced by DEF. All monoalphabetic substitutions can be represented in the following form:

$$Y = (a x_i + b) \bmod g, \tag{2}$$

where a – some constant decimal coefficient; b – shift coefficient; g – number of letters of the alphabet used ($g = 33$ for the Ukrainian alphabet, $g = 27$ for the Latin alphabet); x_i – code of the i-th character of the plaintext (sequential number in the alphabet); $i = 1, \ldots, n$; n – number of letters of the alphabet used.

The main disadvantage of the considered method is that the statistical properties of the plaintext (frequency of letter repetition) are also preserved in the ciphertext.

Vigenère cipher. A Vigenère cipher is a polyalphabetic encryption algorithm that uses a keyword to shift each letter of the plaintext according to a Vigenère table according to the following formula:

$$y_i = (x_i + k_j) \bmod g, \quad (3)$$

where k_j – code of the j-th character of the key, as which a word or phrase of the main alphabet is used.

Let us consider an example of data encryption according to the given model (3), using the encoding of letters of the Ukrainian alphabet, table 1.

Table 1

Encryption algorithm using alphabet letter code

Letter	A	B	C	D	E	F	G	H	I
Code	01	02	03	04	05	06	07	08	09
Letter	J	K	L	M	N	O	P	Q	R
Code	10	11	12	13	14	15	16	17	18
Letter	S	T	U	V	W	X	Y	Z	gap
Code	19	20	21	22	23	24	25	26	27

We assume that the original plain text TECHNOLOGY and the substitution of the Vigenère cipher are given, table 2.

Table 2

Encryption algorithm using alphabet letter code

T	***E***	***C***	***H***	***N***	***O***	***L***	***O***	***G***	***Y***
A	L	G	R	I	T	M	A	L	G

The results of encryption of the original data given in Table 2 using the Vigenère cipher (3) are presented in table 3.

Table 3

Algorithm for encrypting the original data with a given key

$Y_1 = (20 + 0l) \bmod 27 = 21 \Rightarrow U$;	$Y_6 = (15 + 20) \bmod 27 = 08 \Rightarrow H$;
$Y_2 = (05 + 12) \bmod 27 = 17 \Rightarrow Q$;	$Y_7 = (12 + 13) \bmod 27 = 25 \Rightarrow Y$;
$Y_3 = (03 + 07) \bmod 27 = 10 \Rightarrow J$;	$Y_8 = (17 + 01) \bmod 27 = 18 \Rightarrow R$;
$Y_4 = (08 + 18) \bmod 27 = 26 \Rightarrow Z$;	$Y_9 = (07 + 12) \bmod 27 = 19 \Rightarrow S$;
$Y_5 = (14 + 09) \bmod 27 = 23 \Rightarrow W$;	$Y_{10} = (25 + 07) \bmod 27 = 05 \Rightarrow E$.

Thus, the resulting cryptogram of encrypting the source text using the Viginer algorithm will have the form given in table 4.

Table 4

Ciphertext from a fixed code letter to an alphabet

U	*Q*	*J*	*Z*	*W*	*H*	*Y*	*R*	*S*	*E*

It is also possible to use modifications of the Vigenère cipher – Beaufort ciphers, which have the following formulas:

$$y_i = (k_i - x_i) \bmod g, \quad (4)$$

$$y_i = (x_i - k_i) \bmod g. \quad (5)$$

Homophonic replacement of one character in the ciphertext makes it like a few characters in the ciphertext. This method is used to twist statistical power into the text.

To increase the strength of the Vigenère cipher, it is recommended to introduce the following modification of its algorithm:

$$y_{ij} = (x_i + k_j) \min(\bmod g, \bmod q), \quad (6)$$

where x_i – i-th code of the symbol hidden in the text; k_j – code of the j-th symbol of the key, the role of which is matched with letters from the table of keys, which has a size – q.

Stream ciphers. Ciphers of this type have recently become popular due to their high speed. They convert plaintext into ciphertext one bit per operation. The keystream generator, also called a rolling key generator, produces

a stream of bits: $k_1, k_2, k_3, \ldots, k_i$. This keystream and the plaintext bitstream $p_1, p_2, p_3, \ldots, p_i$ undergo surgery XOR (exclusively or) to produce the ciphertext bitstream:

$$c_i = p_i \wedge k_i. \tag{7}$$

During decryption, an XOR operation is performed on the ciphertext bits and the same key stream to recover the plaintext bits:

$$p_i = c_i \wedge k_i. \tag{8}$$

The security of the system is entirely dependent on the power of the key flow generator. The key stream generator creates a bit stream that is like a drop-in stream but is determinative and can be created without delay once decrypted, fig. 1. It is necessary to ensure that the closer the output of the generator to the key flow is to the output, then more time will be required for the evil cipher.

For all stream ciphers, keys are verified. The output of the key stream generator is the key function. Now, if you remove the plaintext/ciphertext pair, you can only read messages that are encrypted with the same key. Stream ciphers are especially useful for encrypting continuous streams of communication traffic, such as a channel that connects two computers.

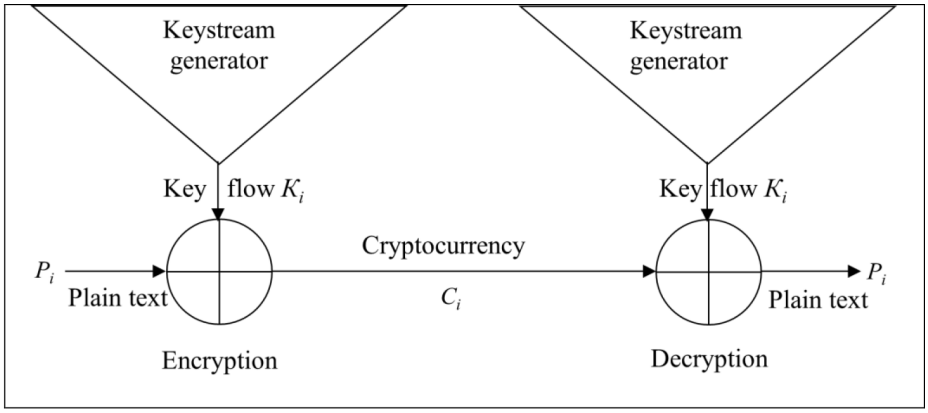

Fig. 1. Algorithm for implementing streaming data encryption

The key flow generator consists of three main parts. The internal mill describes the flow mill of the key flow generator. Two key stream generators with the same key and the same internal host produce the same key streams. The internal output function generates a bit to the key stream. The function of attacking the internal stun generates a new internal stun.

Let's also look at the algorithm for implementing the symmetric stream cipher RC4, which is related to ciphers that are self-synchronizing. This cryptographic algorithm is called a ciphertext autokey. In stream ciphers that are self-synchronizing, the flow of keys is a function of a fixed number of leading bits in the ciphertext, fig. 2.

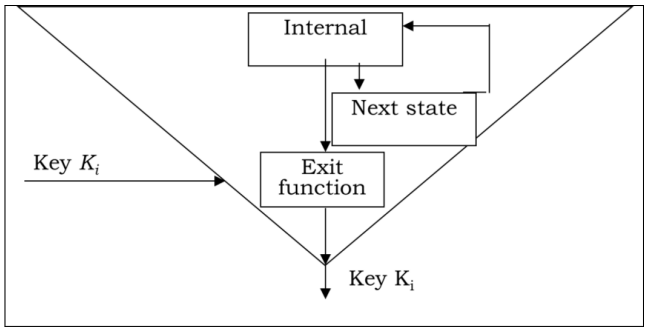

Fig. 2. Algorithm for implementing a key stream generator

A stream cipher that is self-synchronizing is shown in fig. 3. The internal structure is the function of the forward *n* bits of the ciphertext. It is a cryptographically complex output function that uses the internal machine to generate bets to the key stream.

The fragments of the internal system are entirely contained in the front n symbols of the ciphertext, the decryption generator of the key stream is automatically synchronized with the encryption generator of the key stream that has received the n bits of the ciphertext. In intelligent implementations of this mode, skin notification begins

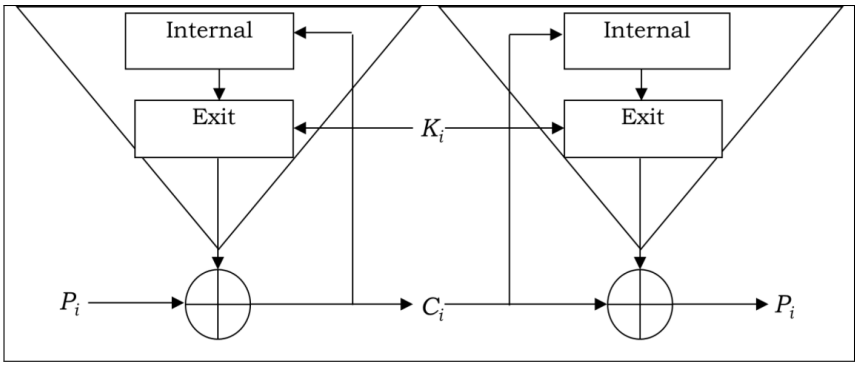

Fig. 3. Schematic of a self-synchronizing key stream generator

with a drop-down heading of up to n bits. This header is encrypted, transmitted and then decrypted. Decryption will be correct after these n bits, as long as the key stream generators are synchronized.

The main advantage of the use of streaming crypto algorithms, which are self-synchronizing, is the speed of their work. The weakness of such algorithms is the widening of the cuts. For each ciphertext bit encoded at the time of transmission, the key stream decryption generator shows *n* incorrect bits to the key stream. Therefore, each incorrect bit ciphertext is given *n* replies to the open text until the zipped bits stop flowing into the internal system.

Conclusions. The results of the analysis show that encryption and data protection are important components of information systems protection, ensuring information confidentiality and preserving data integrity in the face of growing cyber threats. The use of modern computer technology and mathematical methods allows to significantly increase the efficiency of the application of models and algorithms of cryptographic data protection.

Modern crypto algorithms provide ample opportunities for modification to dynamically respond to the emergence of new cyber threats when using limited computing resources. Thus, in the work to increase the stability of the ciphertext, a modification of the Vigenère algorithm using separate unified alphabet tables for the text and the encryption key was proposed. It is also necessary to take into account that despite the expediency of separate application of symmetric and asymmetric encryption methods when ensuring certain types of information protection, in information and computing networks it is advisable to use a combination of both approaches for the comprehensive use of their positive qualities, such as the speed of processing secret keys and the security of their transmission.

Bibliography:

1. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. та ін. Інформаційна безпека: підручник. Київ : В-во Ліра. К, 2021. 412 с.

2. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley, 2019. 800 p.

3. Салієва О., Карпінець В., Грицак А., Павловський П., Бондаренко І. Підвищення стійкості криптографічних алгоритмів у багатокористувацьких WEB-ресурсах на основі генераторів випадкових чисел, що враховують ентропію поведінки користувача. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2023. В. 1. С. 167–173.

4. Машталяр Я. Русланівна., Козачок В. А., Бржевська З. М. Богданов О. М. Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2023. № 2(22). С. 156–167.

5. Плєхова Г. А., Костікова М. В. Актуальні проблеми інформаційної безпеки. *Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті* : мат. Всеукр. наук.-практ. Internet-конф. Харків : ХНАДУ. 2022. С. 68–73.

6. Фурсов І. І., Шматко О. В. Аналіз статистичних показників дисперсії, асиметрії та ексцесу при визначенні порушень інформаційної безпеки кіберфізичних систем вітрових генераторів. *Radioelectronic and Computer Systems*. 2021, №. 4(100). С. 132–144.

7. Бачинський Р. В., Купецький А. В. Система криптографічного захисту bluetooth зв'язку між пристроєм інтернету речей та мобільним обчислювальним пристроєм. Серія: Інформаційні системи та мережі. *Вісник НУ «Львівська політехніка»*. 2018. № 887. С. 18–24.

8. Черненко Р. М., Рябчун О. П., Ворохоб М. В., Аносов А. О., Козачок В. А. Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. *Кібербезпека: освіта, наука, техніка*. 2021. № 3(11). С. 124–135.

9. Pasichnyk V., Pasichnyk A. Methods and algorithms for increasing reliability and level security of corporate telecommunications networks. *Математичне моделювання*. К. : ДДТУ. 2025. № 2(53). С. 30–37.

References:

1. Ostroukhov, V. V., Prysiazhniuk, M. M., Farmahei, O. I., Chekhovska, M. M. ta in. (2021). Informatsiina bezpeka: pidruchnyk [Information Security: A Textbook]. Kyiv: V-vo Lira. 412 s.

2. Stallings, W. (2019). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley, 800 p.

3. Saliieva, O., Karpinets, V., Hrytsak, A., Pavlovskyi, P., Bondarenko, I. (2023). Pidvyshchennia stiikosti kryptohrafichnykh alhorytmiv u bahatokorystuvatskykh WEB-resursakh na osnovi heneratoriv vypadkovykh chysel, shcho vrakhovuiut entropiiu povedinky korystuvacha [Increasing the stability of cryptographic algorithms in multi-user WEB resources based on random number generators that take into account the entropy of user behavior]. *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh*. V. 1. S. 167–173.

4. Mashtaliar, Ya. R.., Kozachok, V. A., Brzhevska, Z. M. Bohdanov, O. M. (2023). Doslidzhennia rozvytku ta innovatsii kiberzakhystu na obiektakh krytychnoi infrastruktury [Research into the development and innovation of cyber protection at critical infrastructure facilities]. *Kiberbezpeka: osvita, nauka, tekhnika*. №.2(22). S. 156–167.

5. Pliekhova, H. A., Kostikova, M. V. (2022). Aktualni problemy informatsiinoi bezpeky [Current problems of information security]. *Modeliuvannia ta informatsiini tekhnolohii v nautsi, tekhnitsi, kiberbezpetsi ta osviti* : mat. Vseukr. nauk.-prakt. Internet-konf. Kharkiv : KhNADU. S. 68–73.

6. Fursov, I. I., Shmatko, O. V. (2021). Analiz statystychnykh pokaznykiv dyspersii, asymetrii ta ekstsesu pry vyznachenni porushen informatsiinoi bezpeky kiberfizychnykh system vitrovykh heneratoriv [Analysis of statistical indicators of dispersion, asymmetry and kurtosis in determining information security violations of cyber-physical systems of wind generators]. *Radioelectronic and Computer Systems*. №. 4(100). S.132–144.

7. Bachynskyi, R. V., & Kupetskyi, A. V. (2018). Systema kryptohrafichnoho zakhystu bluetooth zviazku mizh prystroiem internetu rechei ta mobilnym obchysliuvalnym prystroiem [System of cryptographic protection of bluetooth communication between an Internet of Things device and a mobile computing device]. Seriia: Informatsiini systemy ta merezhi. *Visnyk NU "Lvivska politekhnika"*. № 887. S. 18–24.

8. Chernenko, R. M., Riabchun, O. P., Vorokhob, M. V., Anosov, A. O., Kozachok, V. A. (2021). Pidvyshchennia rivnia zakhyshchenosti system merezhi internetu rechei za rakhunok shyfruvannia danykh na prystroiakh z obmezhenymy obchysliuvalnymy resursamy [Increasing the security level of IoT systems by encrypting data on devices with limited computing resources]. *Kiberbezpeka: osvita, nauka, tekhnika*. № 3(11). S. 124–135.

9. Pasichnyk, V., Pasichnyk, A. (2025). Methods and algorithms for increasing reliability and level security of corporate telecommunications networks. *Matematychne modeliuvannia*. K. : DDTU. № 2(53). S. 30–37.

Дата першого надходження статті до видання: 30.11.2025
Дата прийняття статті до друку після рецензування: 22.12.2025
Дата публікації (оприлюднення) статті 27.01.2026