МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 15, № 1

Volume 15, No. 1

Одеса – 2025
Odesa – 2025

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odesa National Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460Р of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Національного університету «Одеська політехніка»

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: 1, Шевченка пр., Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

Editorial address: 1, Shevchenko Ave., Odesa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

ЗМІСТ/CONTENTS

DOI 10.15276/imms.v15.no1.5
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 5-14

DETECTION OF COVERT CHANNELS IN WEB APPLICATIONS BASED ON UNIMODALITY VIOLATION IN THE WALSH–HADAMARD SPECTRUM

A.I. Dyka

National University "Odesa Law Academy"
23, Fontanska road, Odesa, 65009, Ukraine

This paper presents the theoretical foundations of an innovative method for steganalysis of digital images based on detecting violations of unimodality in the Walsh–Hadamard transform spectrum. The method targets the detection of covert information transmission channels in web applications, particularly in scenarios where users are allowed to upload graphic content. The relevance of this research stems from the increasing use of modern steganographic techniques that are resistant to classical steganalysis methods, thereby posing potential threats of data leakage or the transmission of hidden commands within seemingly legitimate content. The paper formalizes the concept of code-controlled embedding in the spatial domain by selectively affecting individual Walsh–Hadamard transformants. It is shown that such embedding leads to statistically significant deviations from unimodality in the distribution of the corresponding spectral components, which can serve as indicators of hidden activity. Two theoretical propositions are proven: the first describes the expected statistical behavior of Walsh–Hadamard transformants in natural images, while the second demonstrates the emergence of bimodal histograms under steganographic embedding. The theoretical framework is supported by computational experiments across large datasets of real-world images. The findings form a basis for the development of effective detection systems for covert channels in web applications. The proposed approach can be used to generate meaningful features for training artificial intelligence models integrated into automated security testing pipelines, as well as for monitoring uploaded content for the presence of hidden information. The method is format-agnostic and retains effectiveness even under common attack conditions, such as lossy JPEG compression.

Keywords: steganography; Walsh–Hadamard transform; code control; web application security; covert communication channels; unimodality of distribution; digital images; machine learning; steganalysis; information security

1. Introduction and statement of the problem. In the modern software development lifecycle, security testing is critical to identifying vulnerabilities that may lead to unauthorized access, data leakage, or system disruption. From a cybersecurity perspective, testing the security of software components, particularly those exposed to user interaction, is essential for identifying and mitigating threats and covert communication channels [1-3].

For web applications, one of the underexplored but increasingly relevant threats is the use of steganographic methods to covertly transmit information via seemingly legitimate user-uploaded content [4]. While legacy steganographic algorithms were often detectable using classical steganalysis techniques [5], modern methods exhibit high resistance to traditional detection, making them a greater threat in practice.

A notable example is a recently proposed method based on code-controlled embedding, which allows selective modification of spatial regions of an image while maintaining the ability to influence specific frequency components. This makes the approach robust to steganalytic attacks and suitable for use in constrained environments such as mobile devices, IoT systems, and UAVs, where computational resources are limited but reliability and stealth remain important. Research has shown that this method achieves superior resistance to detection compared to popular transform-domain methods, including those based on singular value decomposition (SVD) [6…7].

Prior research [8] demonstrated that the code-controlled embedding method exhibits high robustness against known steganalysis tools such as StegExpose, which failed to reliably detect covert messages even under ideal analysis conditions. Although some statistical signs of embedding were identified, resulting in a preliminary steganalytic approach, its detection accuracy was limited (~80%) and significantly decreased when the embedding density was low or when lossy compression formats were applied.

The very concept of code-controlled embedding presents a major risk for web infrastructure, as it enables the construction of covert communication channels that are resistant to both perceptual and analytical detection. Addressing this threat requires the development of new theoretical and algorithmic foundations for steganalysis, capable of detecting such subtle manipulations.

In this context, the Walsh-Hadamard Transform offers a promising mathematical basis due to its high computational efficiency and clear interpretability of its spectral components. Theoretical analysis and empirical research presented in this paper demonstrate that Walsh-Hadamard Transform domain features can reveal structural changes in image data resulting from code-controlled embedding, particularly through violations of the unimodal distribution of specific transformants. This paper lays a theoretical foundation for future AI-based detection models capable of identifying covert channels in web applications.

The purpose of this paper is to improve the efficiency of detecting covert communication channels based on the code-controlled steganographic method in web applications.

The paper is structured as follows: Section 2 formalizes the concept of code-controlled embedding and presents the core mathematical relationships. Section 3 provides an in-depth analysis of the statistical behavior of Walsh-Hadamard Transform coefficients under steganographic influence and demonstrates the presence of a bimodal distribution that can serve as a detection criterion.

2. General definitions and mathematical foundations of code-controlled steganographic method. One of the important tools for processing digital images in the context of steganography and steganalysis is the two-dimensional Walsh-Hadamard Transform [9]. This orthogonal transform is based on functions that take only the values +1 and −1, and allows you to effectively represent the signal as a sequence of transformants that characterize its frequency components.

Let a digital image block X of size $N \times N$ to be defined. Then the Walsh-Hadamard transform of this block is defined as

$$W_X = H'_N X H'^T_N, \tag{1}$$

where $H'_N = \frac{1}{\sqrt{N}} H_N$, X is a matrix of size $N \times N$, and the Hadamard matrix H_N of order N is given by the Sylvester construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{2}$$

In addition to the two-dimensional Walsh-Hadamard transform, its one-dimensional version is also known, which for a vector Y is given as

$$V = YH_N, \tag{3}$$

at the same time, in [10], a relationship was established between the two-dimensional and one-dimensional versions of the Walsh-Hadamard transform, within the framework of which it was proved that

$$\tilde{W} = \tilde{X} H_{N^2}, \tag{4}$$

where the notation $\tilde{W}$ and $\tilde{X}$ means the representation of the corresponding matrices of size $N \times N$ in the form of a vector of length N^2 by sequential concatenation of the rows of the corresponding matrix, while the calculation of the Walsh-Hadamard transformants is performed with an accuracy of up to the normalization coefficient $1/N$.

Expression (4) became the basis of the concept of code-controlled embedding of additional information, which consists in the fact that the embedding occurs by representing each information bit d_i in the form of a codeword T, which selectively affects one or another transformant of the Walsh-Hadamard transform, which is additively embedded in the corresponding container block

$$\tilde{M} = \tilde{X} + \tilde{T}, \tag{5}$$

then

$$\tilde{W} = \tilde{M} H_{N^2} = (\tilde{X} + \tilde{T}) H_{N^2} = \tilde{X} H_{N^2} + \tilde{T} H_{N^2}. \tag{6}$$

As evident from equation (6), the influence on the Walsh–Hadamard transformants of the container block is entirely determined by the structure of the transformants of the selected codeword. Since the codeword selectively affects a specific Walsh–Hadamard transformant, this enables precise embedding of additional information into that particular transformant.

Let us consider a specific example for the block size 8×8. Let us give a container block for which we find the matrix of the Walsh-Hadamard transformants

$$X = \begin{bmatrix} 93 & 102 & 102 & 106 & 110 & 115 & 116 & 118 \\ 99 & 109 & 102 & 112 & 117 & 114 & 116 & 115 \\ 103 & 114 & 106 & 111 & 121 & 116 & 123 & 111 \\ 113 & 116 & 113 & 115 & 115 & 114 & 121 & 116 \\ 113 & 113 & 115 & 113 & 113 & 109 & 109 & 115 \\ 128 & 111 & 114 & 117 & 114 & 114 & 117 & 116 \\ 126 & 111 & 112 & 116 & 109 & 111 & 128 & 130 \\ 118 & 117 & 110 & 114 & 111 & 107 & 111 & 120 \end{bmatrix};$$

$$W_X = \begin{bmatrix} 7256 & -20 & -64 & 40 & -128 & -40 & 80 & 20 \\ -36 & -4 & -40 & -28 & -68 & 0 & 0 & -8 \\ -102 & -22 & 6 & 2 & -30 & 14 & -74 & -10 \\ -70 & -34 & -6 & -14 & 34 & 18 & -22 & -58 \\ -108 & -48 & 0 & -88 & -156 & -108 & -88 & -20 \\ -44 & -4 & 28 & -8 & -20 & -8 & -20 & 4 \\ -62 & -54 & -54 & 22 & -70 & 14 & 42 & -6 \\ 62 & 26 & -46 & 10 & -10 & 62 & 50 & 62 \end{bmatrix}, \tag{7}$$

as well as the codeword used to target the Walsh–Hadamard transformant (5,1), which belongs to the lower-frequency components and, according to [11], provides the highest robustness against attacks on the embedded message when used for additional data embedding.

$$T=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}. \quad (9)$$

Then, according to equation (6), the resulting steganographic message and its Walsh–Hadamard transform coefficients will take the following form

$$M=\begin{bmatrix} 94 & 103 & 103 & 107 & 111 & 116 & 117 & 119 \\ 100 & 110 & 103 & 113 & 118 & 115 & 117 & 116 \\ 104 & 115 & 107 & 112 & 122 & 117 & 124 & 112 \\ 114 & 117 & 114 & 116 & 116 & 115 & 122 & 117 \\ 112 & 112 & 114 & 112 & 112 & 108 & 108 & 114 \\ 127 & 110 & 113 & 116 & 113 & 113 & 116 & 115 \\ 125 & 110 & 111 & 115 & 108 & 110 & 127 & 129 \\ 117 & 116 & 109 & 113 & 110 & 106 & 110 & 119 \end{bmatrix};$$

$$W_M=\begin{bmatrix} 7256 & -20 & -64 & 40 & -128 & -40 & 80 & 20 \\ -36 & -4 & -40 & -28 & -68 & 0 & 0 & -8 \\ -102 & -22 & 6 & 2 & -30 & 14 & -74 & -10 \\ -70 & -34 & -6 & -14 & 34 & 18 & -22 & -58 \\ -44 & -48 & 0 & -88 & -156 & -108 & -88 & -20 \\ -44 & -4 & 28 & -8 & -20 & -8 & -20 & 4 \\ -62 & -54 & -54 & 22 & -70 & 14 & 42 & -6 \\ 62 & 26 & -46 & 10 & -10 & 62 & 50 & 62 \end{bmatrix}. \quad (10)$$

By comparing expressions (10) and (7), we conclude that the embedding of additional information was performed specifically in the (5,1) Walsh–Hadamard transformant, as it is the only one among all transformants that underwent modification.

3. Analysis of the properties of Walsh-Hadamard transformants of digital images under code-controlled embedding. Detecting steganographic messages requires a more detailed analysis of the patterns to which the container is subjected during the steganographic embedding process. Identifying such patterns, in turn, requires an understanding of the probabilistic and structural characteristics of the Walsh-Hadamard transform coefficients of real images.

Proposition 1. Let there be given a set of matrices W_{X_j} of size $N\times N$ representing the Walsh-Hadamard transformants of image blocks X_j, $j=1,2,...,n$, and each having the form

$$W_{X_j}=\begin{bmatrix} w_{X_j,11} & w_{X_j,12} & \cdots & w_{X_j,1N} \\ w_{X_j,21} & w_{X_j,22} & \cdots & w_{X_j,2N} \\ \vdots & \vdots & \ddots & \vdots \\ w_{X_j,N1} & w_{X_j,N2} & \cdots & w_{X_j,NN} \end{bmatrix}, \quad (11)$$

then the sequence of transformants $u_{kl}=\begin{bmatrix} w_{X_1,kl} & w_{X_2,kl} & \dots & w_{X_n,kl} \end{bmatrix}$ has zero mathematical expectation $\mathrm{E}[u_{kl}]=0$ for all k,l except $k=l=1$.

Proof. To prove Proposition 1, we note that according to (4) each matrix W_{X_j} can be represented as a vector of transformants $W_{X_j}=X_jH_{N^2}=[w_{X_1,11} \quad w_{X_1,12} \quad \dots \quad w_{NN}]$, of the Walsh-Hadamard transform, thus each coefficient $w_{X_1,kl}$ obtained by multiplying the

corresponding vector X formed by successive concatenation of the rows of the block matrix X by the corresponding row of the Walsh-Hadamard matrix H_{N^2}, which by construction is a Walsh function h_g of length N^2. Then we can write the corresponding coefficient $w_{X_j,kl}$ as

$$w_{X_j,kl} = \sum_{\alpha=1}^{N^2} h_{g,\alpha} x_\alpha \ . \tag{12}$$

In other words, since the intensity values x_α of the pixels of an arbitrary image do not depend on the elements of the Walsh functions $h_{g,\alpha}$, the mathematical expectation $\mathrm{E}[w_{X_j,kl}]$ for each $w_{X_j,kl}$ will be defined as

$$\mathrm{E}[w_{X_j,kl}] = \mathrm{E}[h_{g,\alpha} x_\alpha] = \mathrm{E}[h_{g,\alpha}]\mathrm{E}[x_\alpha] \ . \tag{13}$$

Since by their construction the Walsh functions are balanced for any $g \neq 1$, then $\sum_{\alpha=1}^{N^2} h_{g,\alpha} = 0$, and therefore the product $\mathrm{E}[w_{X_j,kl}] = 0$.

Given that $\mathrm{E}[w_{X_j,kl}] = 0$ for $\forall k,l$ except $k = l = 1$, i.e. when $g \neq 1$, we obtain $\mathrm{E}[u_{kl}] = 0$ for any k,l except $k = l = 1$, which proves the conditions of Proposition 1.

Computational experiment 1.

To practically verify the conditions of Proposition 1, we will perform the following computational experiment. For a sample of 500 images from the NRCS database [12], we will form a vector for blocks of size 4×4, 8×8, 16×16, after which we will find the average value of the vector u_{kl} elements for all values k,l according to the block size.

The results of the computational experiment for blocks of sizes 4×4 and 8×8 are shown in Table 1.

Empirically constructed average values of the transformants of the Walsh-Hadamard transform

Table 1.

Block size 4×4				
k/l	1	2	3	4
1	$1.8\cdot10^3$	0	0	0
2	0.1	0	0	0
3	0.4	0	0	0
4	0	0	0	0

Block size 8×8								
k/l	1	2	3	4	5	6	7	8
1	$7.3\cdot10^3$	0	0	0.2	-0.2	0	0	0
2	0.7	0	0	0.1	0	0	0	0
3	1.7	0	0	0	0	0	0	0
4	0.3	0	0	0.2	0	0	0	0
5	3.0	0.2	0	-0.1	0	-0.1	0	-0.1
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Note that for blocks of size 16×16 the average value of the element $(1,1)$ is equal to $2.9\cdot10^4$, while other values in the computational experiment are practically equal to 0.

Analysis of the data in Table 1 leads to practical confirmation of Proposition 1, because the average values of the transformants of the Walsh-Hadamard transform when averaging over blocks are indeed close to 0 in practice, except for the case of values $k=l=1$.

Note that the standard deviation and dispersion of vector u_{kl} values in practice depend very much on the specific image and its structure, which, in our opinion, sets a number of restrictions on their generalization and limits their application in practice for detecting steganographic messages.

For greater clarity, let us form histograms of the distribution of vector u_{15} and u_{51} element values for the size of the blocks 8×8 (Fig. 1).

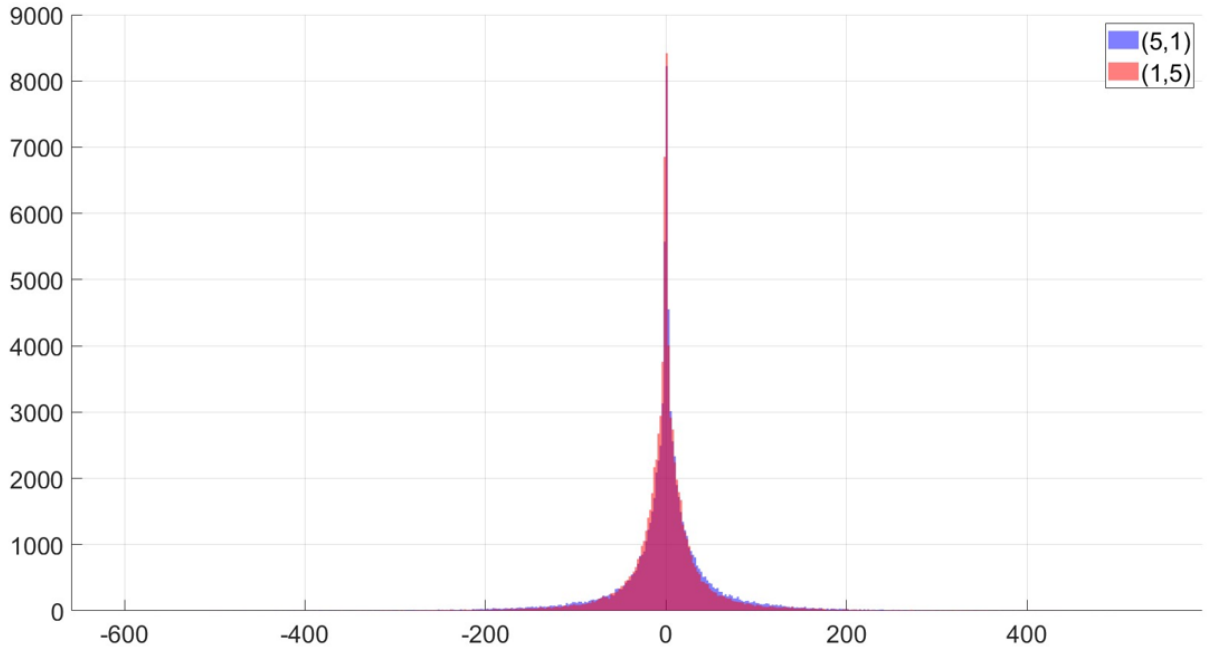


Fig. 1. — Histogram of the distribution of element values for vectors u_{15} and u_{51}

Let us research the effect of steganographic transformation using the code-controlled method with embedding additional information on the statistical characteristics of vectors u_{kl}.

According to conditions (6) of using the code-controlled steganographic method with codewords that selectively affect a given transformant, the Walsh-Hadamard transform leads to a change in its value in each block by the value of N^2.

Proposition 2. The histogram of the distribution of vectors u_{kl}, in which additional information was embedded using the code-controlled steganographic method with codewords based on Walsh functions, will have a bimodal character with maxima at points $\pm N^2$.

Proof. To prove Proposition 2, we note that one of the important components of the steganographic system is the precoder, the function of which is to form a sequence $\{d_j\}$ using analog-to-digital conversion operations (if necessary), effective coding, noise-resistant coding of information, and encryption. The use of high-quality encryption algorithms leads to a uniform distribution of symbols "0" and "1" in the sequence $\{d_j\}$. Therefore, in the context of using the steganographic method with code control, we will assume that the distribution of symbols in the sequence $\{d_j\}$ is uniform.

Taking into account the above, from a statistical point of view, steganographic message vectors u'_{kl} can be represented as

$$u'_{kl} = \begin{cases} u'_{kl} + N^2, \text{ with probability } 0.5; \\ u'_{kl} - N^2, \text{ with probability } 0.5. \end{cases} \quad (14)$$

Since, according to the conditions of Proposition 1, the probability density $f_{u_{kl}}$ has a maximum (since the random variable u_{kl} is distributed according to a symmetric unimodal distribution, which is confirmed by the obtained empirical data for a given sample of images, the maximum of the probability density $f_{u_{kl}}$ will coincide with its mathematical expectation) at point 0.

Then the probability density $f_{u_{kl}}(u_{kl} - N^2)$ has a maximum at $u_{kl} - N^2 = 0,$, i.e. at $u_{kl} = N^2$. Similarly, $f_{u_{kl}}(u_{kl} + N^2)$ will have a maximum at $u_{kl} + N^2 = 0$, i.e. at $u_{kl} = N^2$. Therefore, $f_{u'_{kl}}$ will have two maxima: at points $-N$ and N, since both terms contribute their maxima independently.

The above proves the conditions of Proposition 2.

Fig. 2 shows the u_{51} distribution histograms for the original image, as well as the steganographic message for the transformant of the Walsh-Hadamard transform (5,1), into which additional information was embedded using the corresponding codeword (9) of size 8×8.

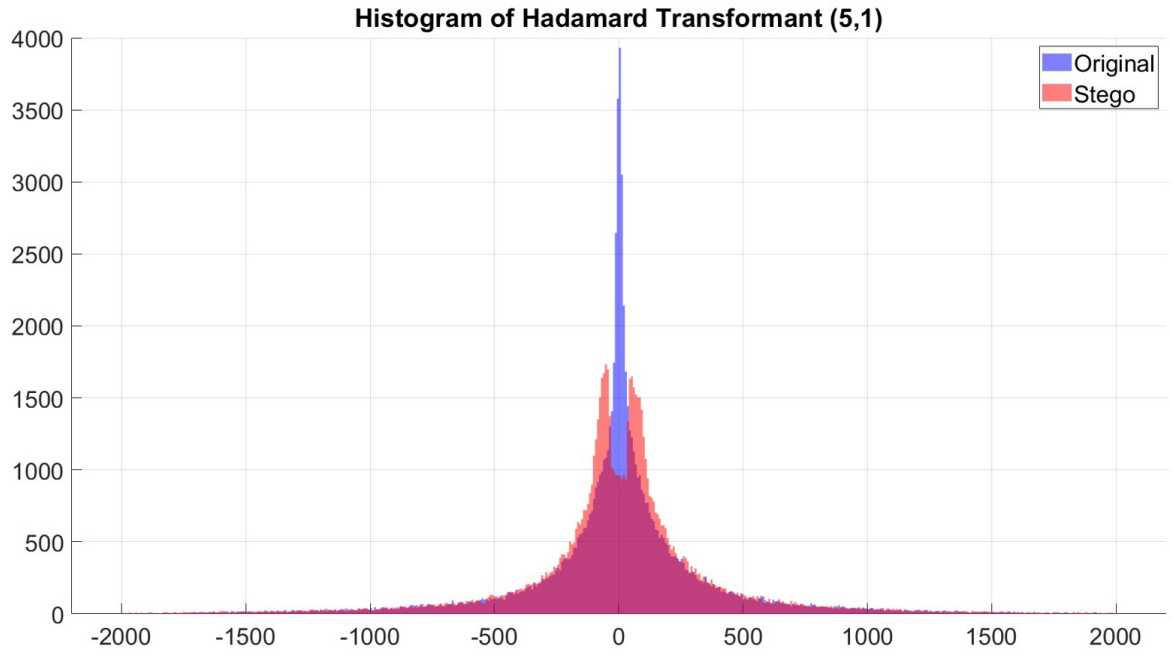


Fig. 2. — Histogram of distribution of u_{51} for the original image and u'_{51} for the steganographic message

The analysis of the data in Fig. 2 confirms the conditions of Proposition 2: for a steganographic message, unlike the original image, the distribution of the transformant of the Walsh-Hadamard transform, which has undergone the embedding of additional information, is bimodal with maxima in the values $\pm N = \pm 64$, which confirms that the size of the block in which the embedding occurred is indeed $N = 8$.

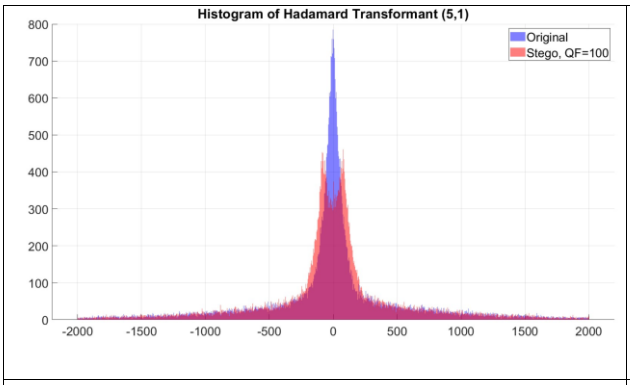
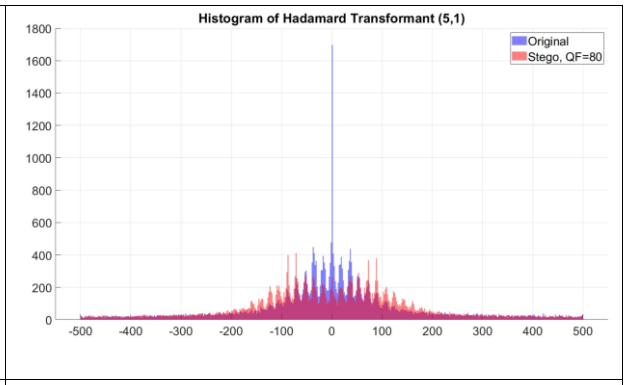
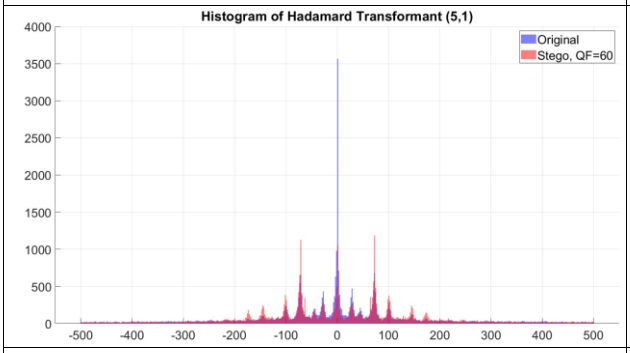
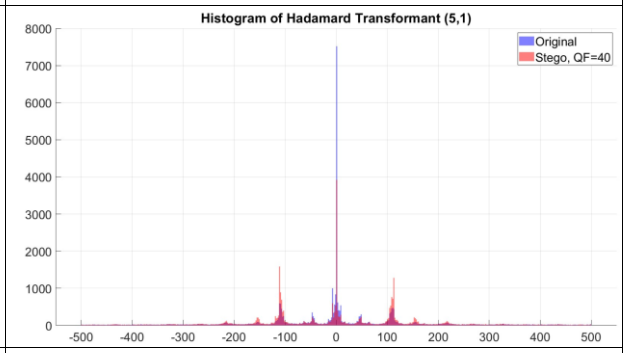
Obviously, taking into account the conditions of Proposition 2, this type of deviation of the histogram of the distribution of vectors u_{kl} from the classical unimodal probability distribution is a sign of the use of a steganographic method with code control for embedding additional information into a given transformant of the Walsh-Hadamard transform.

An important factor influencing the practical applicability of Proposition 2 for detecting the embedding of additional information embedded using the code-controlled steganographic method is its robustness under disruptive conditions, in particular, compression attacks, which are among the most common forms of attacks targeting embedded messages. Experimental data [6] confirm the resilience of this method to such attacks.

Table 2 shows the histograms of steganographic message vectors u'_{51} that were subjected to compression attacks against the embedded message with different values of the quality factor $QF = \{100, 80, 60, 40, 20\}$.

Histograms of steganographic message vectors u'_{51} for different QF compression levels

Table 2.

	
QF=100	*QF*=80
	
QF=60	*QF*=40

Analysis of the data presented in Table 2 leads to the conclusion that, although image compression leads to multimodality of the distribution of the Walsh-Hadamard transformants, we see that for the steganographic message it remains noticeable due to a significantly higher concentration of the Walsh-Hadamard transform values in the side lobes of the histogram, while for the original images this concentration remains significant near the zero value. This makes it possible to detect the embedding of additional information using the steganographic method with code control using the conditions of Proposition 2, even after a compression attack against the embedded message.

Conclusions. The paper proposes the theoretical foundations of the steganalysis method, which is based on the detection of a violation of the unimodality of the distribution of the Walsh-Hadamard transformants in images to which code-controlled steganographic embedding has been applied. It is shown that such a feature allows us to formalize the criterion for the presence of embedded information, which can be used for the automated detection of covert channels in web applications.

The obtained analytical statements are confirmed by computational experiments that demonstrate the high sensitivity of transformants histograms to the fact of embedding. In particular, it was established that selective embedding leads to the formation of bimodal distributions, which is a reliable sign of hidden influence.

The proposed approach has practical significance for web application protection systems that allow users to upload images. The theoretical framework developed in this paper can be used as a basis for training artificial intelligence models capable of detecting atypical patterns in image transformants that signal the presence of hidden messages.

Integrating such analysis into content monitoring will increase the level of information security of web-based systems, complementing classic vulnerability detection methods with mechanisms for controlling covert data transmission channels.

References

1. Trofymenko O., Dyka A., Loboda Y. Analysis of vulnerabilities and security problems of web applications. System technologies. 2023. Vol. 3, No. 146. P. 25-37.
2. Kranthi A. G. et al. Securing web apps: Analysis to understand common vulnerabilities, attack scenarios, and protective measures. ICCDE 2024. P. 64.
3. Mohammed A. et al. Security of web applications: Threats, vulnerabilities, and protection methods. International Journal of Computer Science & Network Security. 2021. Vol. 21, No. 8. P. 167-176.
4. Othman N. A. et al. Image Steganography Using Web Application. Journal of Computing Research and Innovation. 2023. Vol. 8, No. 2. P. 1-11.
5. Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions. IEEE Access. 2020. No. 8. P. 166589-166611.
6. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130.
7. Kobozeva A.A., Sokolov A.V. Steganographic Method with Code Control of Information Embedding Based on Multi-level Code Words. Radioelectronics and Communications Systems. Vol. 66, No. 4. P. 173-189.
8. Lanovska O.O., Sokolov A.V. Steganalysis of a method with code-controlled information embedding in the Walsh-Hadamard transform domain. Informatics and mathematical methods in simulation. 2024. V.1. No 4. P.1-12
9. Beer T. Walsh transforms. American Journal of Physics. 1981. Vol. 49, No. 5. P.466-472.
10. Kobozeva A.A., Sokolov A.V. The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain. 2022. Problemele Energeticii Regionale 54 (2). P. 84-100.
11. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications.* 2018. 40. P. 217-235.
12. Natural Resources Conservation Service (NRCS) // United States Department of Agriculture. URL: https://www.nrcs.usda.gov

A.I. Dyka

ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ У ВЕБ-ЗАСТОСУНКАХ НА ОСНОВІ АНАЛІЗУ ПОРУШЕНЬ ОДНОМОДАЛЬНОСТІ СПЕКТРА УОЛША-АДАМАРА

А.І. Дика

Національний університет «Одеська юридична академія»
23, Фонтанська дорога, м.Одеса, 65009, Україна

У цій статті представлено теоретичні основи нового методу стеганоаналізу цифрових зображень, заснованого на виявленні порушень унімодальності в спектрі перетворення Уолша-Адамара. Метод спрямований на виявлення прихованих каналів передачі інформації у веб-застосунках, зокрема в сценаріях, де користувачам дозволено завантажувати графічний контент. Актуальність цього дослідження пов'язана зі зростаючим використанням сучасних стеганографічних методів, стійких до класичних методів стеганоаналізу, що створює потенційні загрози витоку даних або передачі прихованих команд у межах, здавалося б, легітимного контенту. У статті формалізовано концепцію кодового управління вбудовуванням в просторовій області шляхом вибіркового впливу на окремі трансформанти перетворення Уолша-Адамара. Показано, що таке вбудовування призводить до статистично значущих відхилень від унімодальності в розподілі відповідних спектральних компонентів, які можуть служити індикаторами прихованої активності. Доведено два теоретичні твердження: перше описує очікувану статистичну поведінку коефіцієнтів перетворення Уолша-Адамара в природних зображеннях, а друге демонструє появу бімодальних гістограм при стеганографічному вбудовуванні. Теоретичну основу підтверджують обчислювальні експерименти на великих наборах даних реальних зображень. Отримані результати формують основу для розробки ефективних систем виявлення прихованих каналів у веб-застосунках. Запропонований підхід може бути використаний для створення значущих ознак для навчання моделей штучного інтелекту, інтегрованих в автоматизовані конвеєри тестування безпеки, а також для моніторингу завантаженого контенту на наявність прихованої інформації. Метод не залежить від формату та зберігає ефективність навіть за поширених умов атаки, таких як стиснення JPEG з втратами.

Ключові слова: стеганографія; перетворення Уолша-Адамара; кодове управління; безпека веб-застосунків; приховані канали зв'язку; унімодальність розподілу; цифрові зображення; машинне навчання; стеганоаналіз; інформаційна безпека.

DOI 10.15276/imms.v15.no1.15
UDC 004.932+004.4’2+004.272.2

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 15-23

ACCELERATION OF IMAGE PROCESSING ALGORITHMS USING SIMD TECHNOLOGY

O.O. Zhulkovskyi[1], H.Ya. Vokhmianin[1],
I.I. Zhulkovska[2], Yu.V. Ulianovska[2], E.A. Riabovolenko[2]

[1]Dniprovsky State Technical University
Dniprobudivska str., 2, Kamianske city, 51918, Ukraine
[2]University of Customs and Finance
2/4, Volodymyr Vernadskyi str., Dnipro, 49000, Ukraine
Email: olalzh@ukr.net

A rational choice of computing platform and software optimization that considers the specifics of processor architecture can significantly reduce the time of complex computations, improve overall system performance, and ensure efficient scalability when processing large amounts of data. This study addresses the problem of accelerating computational image processing algorithms, specifically the Gaussian smoothing algorithm, using SIMD data-level parallelism technology. The Gaussian smoothing algorithm, which is commonly used to reduce noise and remove small image details, is characterized by high computational complexity due to the need to perform numerous arithmetic operations on each pixel. In this regard, the optimization of such algorithms is a relevant task, and SIMD technology offers the potential for parallel data processing using extended processor instructions, thereby significantly enhancing computational performance. The aim of this study is to enhance the efficiency of the Gaussian smoothing algorithm through SIMD-based computation optimization. Two variants of the software implementation of the studied algorithm have been developed: one is scalar and the other has been optimized through the use of AVX-256 instructions. The optimized version employs computation vectorization, processing eight pixels simultaneously using 256-bit registers, which theoretically allows up to an eightfold speedup. Computational experiments were conducted using images with resolutions of 1920x1080 and 2560x1440 pixels, across various kernel radius and standard deviation values. The results demonstrated that implementing SIMD instructions resulted in a speed enhancement ranging from 6.9 to 7.3 times when compared to the scalar approach. When the kernel radius increased, the acceleration remained consistently high, confirming the approach’s effectiveness for more complex computations. It was confirmed that execution time is primarily influenced by the kernel radius, while the standard deviation has a lesser effect, since the radius defines the filter’s area of influence. The speedup achieved in the experiments is close to the theoretical maximum, demonstrating the advantages of the optimized implementation. Future research prospects include combining SIMD optimization with multithreaded processing and studying the potential of more powerful instruction sets such as AVX-512.
Keywords: image processing, Gaussian smoothing, SIMD, AVX-256, parallel data processing.

Introduction. In today’s world of high-performance computing, efficient utilization of PC hardware capabilities is pivotal for optimizing data processing speeds. This implies not only a rational choice of computing platform, but also the optimization of software with regard to the processor architecture's particular characteristics such as vector instructions (SIMD – Single Instruction Multiple Data), multi-core processing, cache memory, and so forth. The application of such approaches enables a significant reduction in the execution time of complex computations, increases overall system performance, and ensures efficient scalability when processing large amounts of data [1]. Processing large datasets, particularly images, remains one of the most computationally intensive tasks. A typical example of such a task is the Gaussian smoothing algorithm, which is widely used for noise reduction and removal of details in digital images by performing a large number of similar arithmetic operations on

each image pixel [2]. In the context of growing data volumes and increasing software performance requirements, the optimization of such algorithms is becoming particularly relevant.

SIMD technology provides the necessary tools for parallel data processing at the processor instruction level. The core principle of SIMD is the execution of a single operation simultaneously on multiple data elements, which significantly enhances computational efficiency [3].

Related works. Image processing, particularly in artificial intelligence and computer vision systems, demands faster and more efficient data processing, making hardware acceleration with specialized equipment essential, as general-purpose CPUs face performance limitations when processing high-resolution data in real-time [4].

Unlike scalar computations, where each processor instruction processes a single data element, SIMD instructions operate on data vectors, enabling a significant increase in computational performance for algorithms with a high degree of data-level parallelism. Architecturally, SIMD is implemented by introducing specialized vector registers and corresponding instruction sets into processors. In modern CPUs, the width of SIMD registers has evolved from 64 bits in early implementations to 128, 256, and 512 bits in the latest architectures, allowing for the simultaneous processing of 4, 8, or 16 single-precision floating-point elements (32-bit floats), respectively [5, 6]. This architectural feature provides a theoretical speedup of calculations proportional to the number of elements that fit within a SIMD register. Consequently, SIMD is advisable to use in algorithms with iterative blocks containing uniform arithmetic operations, where the computation of each subsequent element is independent of the previous one.

A modified algorithm for solving the classical problem of multiplying ultra-large square data matrices using SIMD technology demonstrates a speedup in the range of 2.53–4.78x compared to traditional data processing methods and is independent of the amount of processed data [7]. In graph algorithms, the use of SIMD increases efficiency on the central processor. The evaluation results show that on an 8-core machine, enabling SIMD in a naïve multi-core implementation provides an additional speedup of 7.48x, averaged over ten benchmarks and three input datasets [8]. The application of custom SIMD-oriented optimizations improves the basic SIMD implementation by 1.67x and outperforms the scalar version by 12.46x.

SIMD instructions can enhance prediction performance through compression/recovery (CR) by up to 25% and reduce dynamic power consumption by up to 43% on real, unmodified applications using predictive execution [9]. CR can also execute unmodified legacy code with short vector instructions (AVX-2) on newer architectures with wider vectors (AVX-512), achieving up to a 56% increase in performance.

In image processing workflows, SIMD is suitable for hardware acceleration using a vector processor matrix to improve the performance of deblurring techniques for CT and MRI images affected by artifacts [10], for lookup tables (LUT) aimed at efficient image transformation on x86/64 processors by processing complex mathematical functions [11], and in other algorithms such as Gaussian smoothing [2].

Gaussian blur is a fundamental operation in image processing based on the convolution of an image with a Gaussian kernel. The basic principle of the algorithm involves replacing the value of each pixel with a weighted sum of the values of its neighboring pixels, where the weights are defined by the Gaussian kernel [12]. When implementing Gaussian blur in software, the computational complexity of the algorithm is $O(r^2 \times n^2)$ for an image of size $n \times n$ and a kernel of size $r \times r$. In the context of large images or real-time applications, this level of complexity can lead to unacceptable delays, making algorithm optimization essential.

A significant acceleration can be achieved by splitting the two-dimensional convolution into two consecutive one-dimensional operations [13]. This fundamentally

reduces the complexity to $O(r \times n^2)$. The splitting principle is based on the property of the Gaussian function, which allows the two-dimensional filter to be represented as the product of two one-dimensional filters. To further accelerate the Gaussian blur algorithm, parallel computing can be applied at various levels: for example, thread-level parallelism using OpenMP [2] and instruction-level vectorization using SIMD [2, 14].

Parallelizing the modified 1D convolution across processing cores increases performance by approximately 1.3x and reduces power consumption by 6.9% and 3.2% for 1D and 2D convolutions, respectively [2]. In [14], to improve the performance of one-dimensional convolution operations, both data-level and thread-level parallelism were employed using parallel programming models such as intraprocedural programming, automatic compiler vectorization, and open multiprocessing. The experimental results demonstrated that the performance of the obtained implementations significantly surpassed that of other approaches. The performance of the multithreaded versions of all implementations was greatly improved compared to single-core implementations, achieving a speedup of 52.33x over the optimal scalar version.

Research Objective. The objective of the present study is to efficiently utilize SIMD technology to accelerate image processing algorithms, with a focus on Gaussian smoothing as a case study. The work is focused on analyzing the performance of the scalar implementation of the algorithm and its optimized version using SIMD instructions, as well as demonstrating how parallel data processing can improve computational efficiency in tasks with a high level of computational complexity.

Main Part. Gaussian smoothing is implemented via the convolution operation of an image with a two-dimensional kernel, the values of which are determined by the Gaussian function [15]:

$$G(x,y)=\frac{1}{2\pi\sigma^2}e^{-\frac{x^2+y^2}{2\sigma^2}},$$

where (x, y) – are the coordinates of a pixel relative to the center of the kernel; σ – is the standard deviation of the Gaussian distribution, which defines the degree of blurring.

In the software implementation of the algorithm, the two-dimensional kernel is decomposed into two one-dimensional filters to optimize computational efficiency:

$$G(x,y)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{\frac{-x^2}{2\sigma^2}}\times\frac{1}{\sqrt{2\pi\sigma^2}}e^{\frac{-y^2}{2\sigma^2}}$$

Thus, the smoothing operation is represented as a sequential application of horizontal and vertical one-dimensional filters:

$$I'(x,y)=\sum_i\sum_j I(x-i,y-j)\times G(i,j),$$

where I – is the input image, I' – is the result of the smoothing process.

The C++ code developed within the framework of this study implements the Gaussian blur algorithm in two versions: scalar and optimized using SIMD technology based on the AVX-256 instruction set, which is part of the x86-64 processor architecture extensions. The code has been designed to process images represented as two-dimensional arrays of pixels. The implementation comprises the generation of a Gaussian kernel, the application of convolution in two directions (horizontal and vertical), and the comparison of the performance of both methods. The process begins with the creation of a Gaussian kernel, where the kernel size specifies the number of elements, and the standard deviation σ controls the width of the Gaussian curve, thereby determining the degree of image blurring. The kernel

is formed based according to the mathematical formula for the Gaussian distribution. Following the calculation of the kernel values, a process of normalization is then applied.

Image processing is carried out in two stages. The first stage involves horizontal convolution. For each pixel at coordinates (x, y), a weighted sum of neighboring pixel values in the horizontal row is calculated. The result is stored in an intermediate buffer of the float data type. The second stage – vertical convolution – is performed in a similar manner, but on the intermediate buffer: for each pixel at coordinates (x, y), a weighted sum of pixel values in the vertical column is computed. The results are stored in an output array of the float data type, which represents the final blurred image. Edge pixel processing (accesses beyond array boundaries) at both stages is managed using a mirroring method, implemented via the std::max and std::min functions applied to the corresponding indices.

The optimized version of the algorithm is implemented using AVX-256 instructions from the <immintrin.h> header. This version also performs processing in two stages but accelerates computation by vectorizing, processing data in blocks of eight pixels at a time. The primary data type used for vector operations is __m256, which represents a 256-bit register and contains eight values of the float data type [16]. During the horizontal convolution stage, image rows are processed. For each row, the outer loop iterates over pixels in steps of 8, matching the size of the __m256 vector. Within the loop, data is loaded from the image array into the register using the _mm256_loadu_ps instruction. The core convolution operation is executed using the _mm256_fmadd_ps (fused multiply-add) instruction, which performs element-wise multiplication of the first two vectors and adds the result to a third, returning a new __m256 vector [16, 17]. Once convolution over all kernel elements is complete, the result is stored in an intermediate buffer using _mm256_storeu_ps. If the image width is not divisible by eight, the remaining pixels are processed sequentially using the scalar method described earlier. Vertical convolution in the SIMD version is carried out similarly, with adjustments for accessing columnar data.

The execution time of the algorithms is measured using std::chrono::high_resolution_clock from the <chrono> library [18].

In order to verify the accuracy of the results obtained from both versions, a comparative analysis is conducted between them. Within a loop iterating over all pixels, the absolute difference between corresponding float values is computed. If the difference exceeds a threshold of 10^{-5}, a discrepancy in the results is recorded.

Computational experiments were conducted using the following test environment: CPU Intel Core i7-12700H, 14 cores, 20 threads; RAM 32 GB (2 Goodram DDR4: 16 GB, 3200 MHz); Microsoft Visual Studio C++ 2022 IDE; Microsoft Windows 10 OS, <immintrin.h> library, SIMD AVX 256 bit, x64.

Results and Discussion. The experiments were conducted on a range of images with resolutions of 1920x1080 and 2560 x1440 pixels. Each image underwent ten experimental runs with varying blur radii and standard deviations. This experimental setup enables the investigation of the impact of the blur radius and standard deviation on computation time.

The results obtained from the experiments conducted with various configurations and image resolutions (Table 1 and Table 2) confirm the theoretical advantages of using SIMD technology. For an image with a resolution of 1920x1080 pixels and a kernel radius of $r = 5$, the scalar implementation may take approximately 275 ms, whereas the optimized version utilizing AVX instructions reduces this time to 40 ms, achieving a speedup of nearly 7x. For higher resolutions such as 2560x1440, performance gains are also substantial: the scalar version executes in approximately 480 ms, while the SIMD version completes in about 70 ms, indicating consistent acceleration. Minor deviations from the theoretical maximum can be attributed to overhead associated with data vectorization, result de-vectorization, and processing of edge cases, which cannot be fully vectorized.

An increase in the kernel radius up to 10 leads to an increase in computational complexity; however, the relative acceleration achieved through SIMD remains substantial. For an image with a resolution of 1920x1080, the scalar processing time increases to 475 ms, while the SIMD-optimized version maintains a stable execution time of approximately 68 ms. This scalability highlights the effectiveness of SIMD optimization for more complex computations.

Table 1.

Experimental results for an image with a resolution of 1920x1080 pixels

№	Kernel radius *r*	Standard deviation *σ*	Computation time, ms		Acceleration
			No-AVX	AVX-256	
1	5	1	275	40	6.88
2		2	271	39	6.95
3		3	279	40	6.98
4		4	279	40	6.98
5		5	280	40	7.00
6	10	1	470	68	6.91
7		2	475	68	6.99
8		3	472	68	6.94
9		4	473	68	6.96
10		5	475	68	6.99

Table 2.

Experimental results for an image with a resolution of 2560x1440 pixels

№	Kernel radius *r*	Standard deviation *σ*	Computation time, ms		Acceleration
			No-AVX	AVX-256	
1	5	1	480	69	6.96
2		2	474	68	6.97
3		3	483	70	6.90
4		4	476	69	6.90
5		5	489	70	6.99
6	10	1	837	115	7.28
7		2	837	114	7.34
8		3	841	115	7.31
9		4	833	115	7.24
10		5	839	115	7.30

The obtained results demonstrate that the computation time is influenced by the kernel radius *r*, whereas increasing the standard deviation *σ* results in relatively stable execution time (Fig. 1).

Figures 2 and 3 present the outcomes of image processing using the Gaussian smoothing algorithm with various blurring parameters. As illustrated in Fig. 2, increasing the standard deviation *σ* while maintaining the same radius *r* yields a noticeable effect, but it is less significant compared to increasing the radius itself. In Fig. 3, more blurred images are produced due to the increased radius. It can thus be concluded that the radius defines the effective area of influence of the filter. It determines how many pixels surrounding each processed pixel are taken into account for the blurring operation. When the radius is small, even a large *σ* does not result in significant blurring, as pixels outside the radius are not included in the computation.

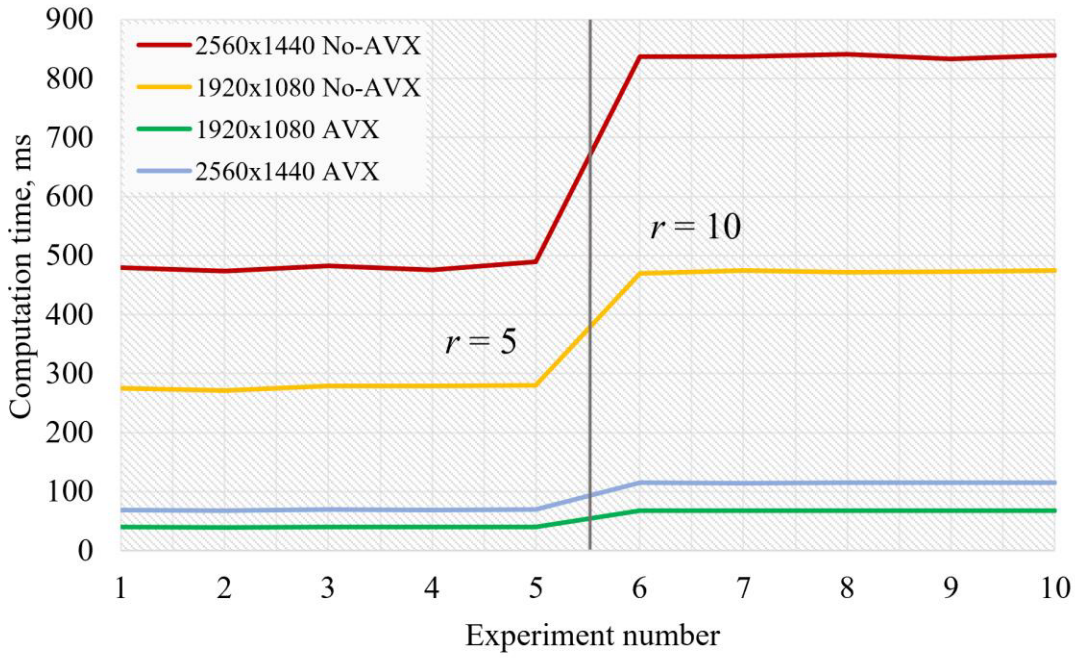


Fig. 1. Execution time results of computational algorithms for images of different resolutions

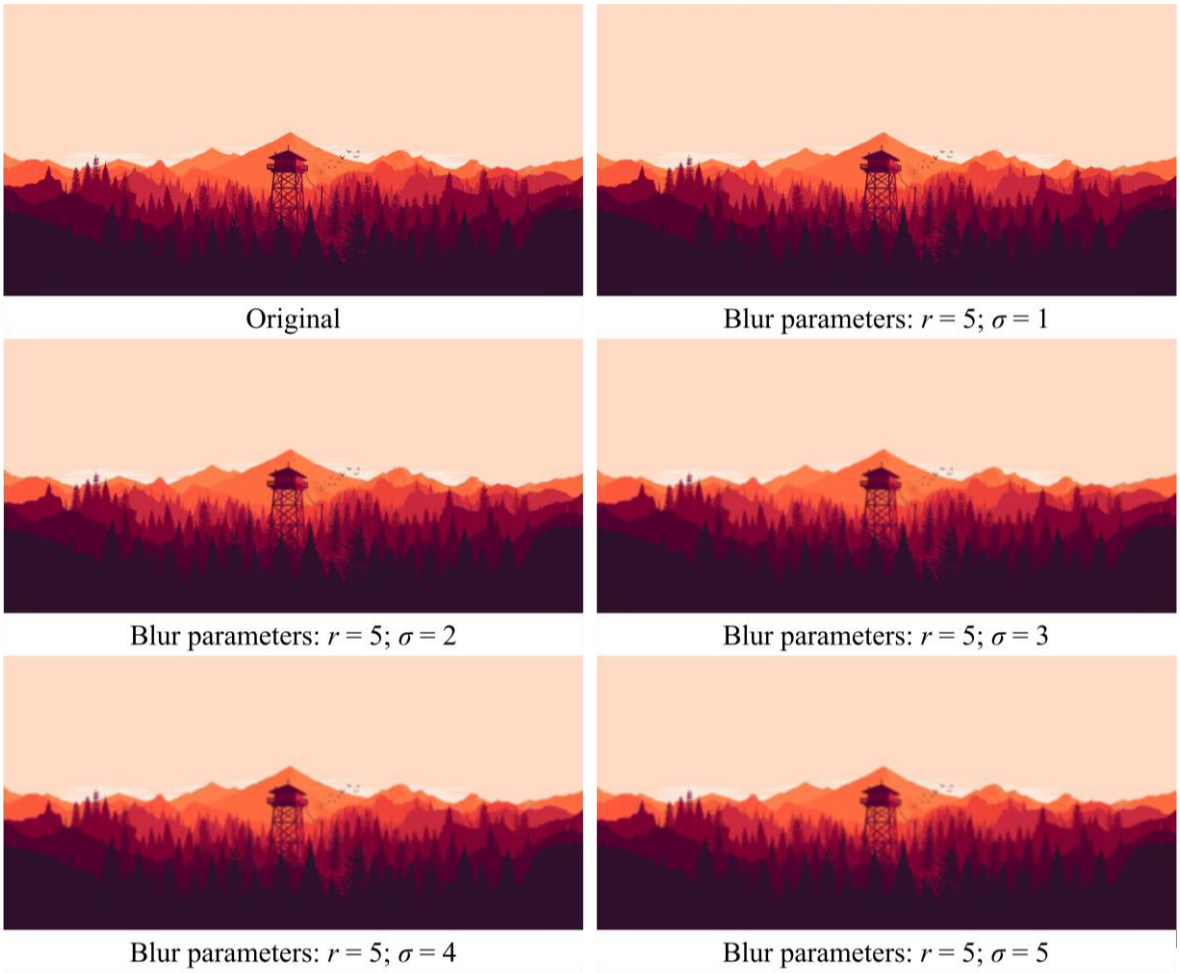


Fig. 2. Image processing results with kernel radius $r = 5$

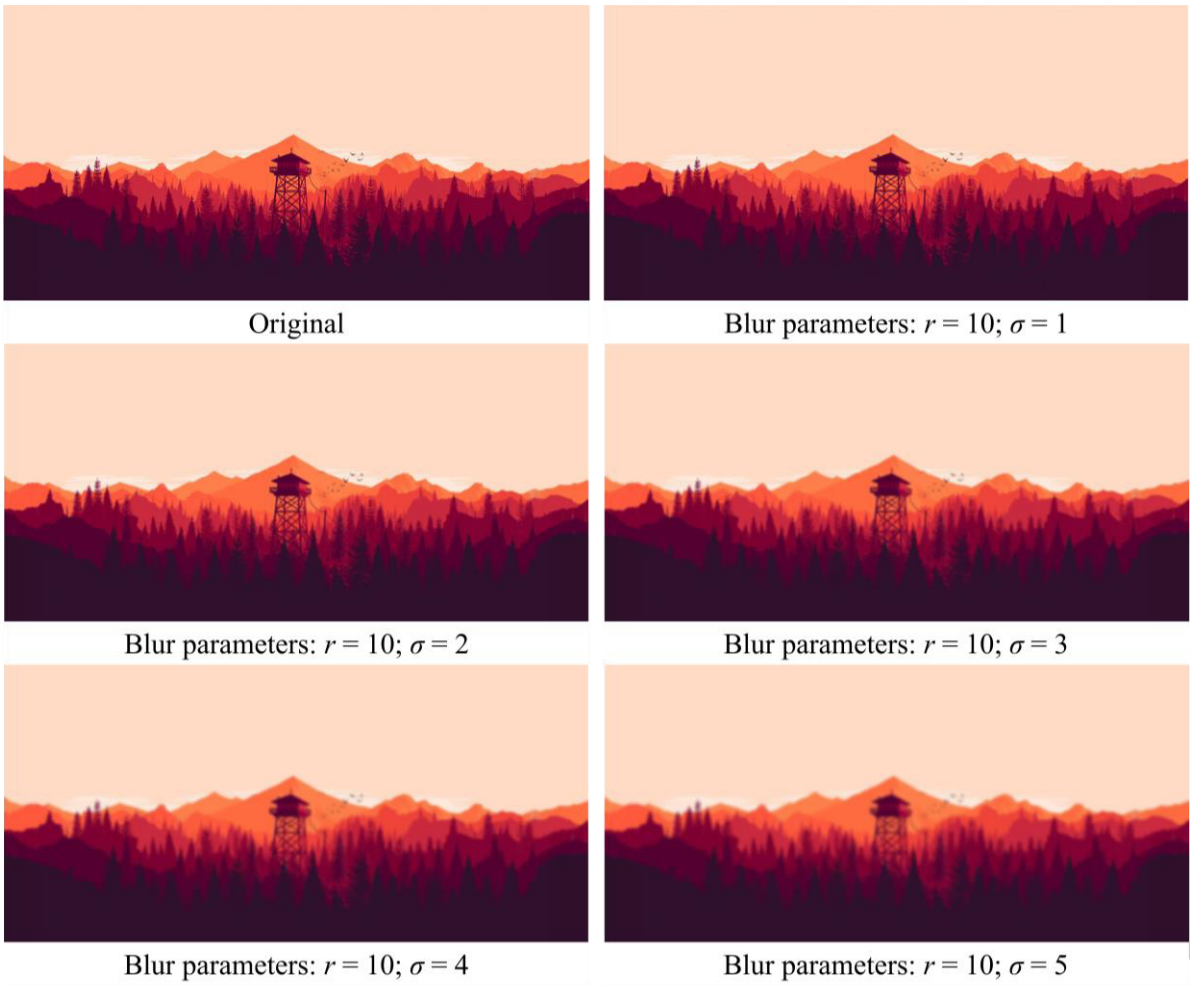


Fig. 3. Image processing results with kernel radius $r = 10$

Conclusions. The conducted research demonstrates the significant potential of utilising SIMD instructions to optimize image processing algorithms, particularly those involving Gaussian smoothing. The achieved speedup of 6.9–7.3x while maintaining identical output quality confirms the effectiveness of this approach for practical applications. Theoretically, the maximum increase in processing speed when using AVX-256 instructions for single-precision data type operations is 8x, since a single register can accommodate eight values of the float data type. The actual speedup obtained is close to the theoretical maximum, which indicates the effectiveness of the implementation. The slight deviation from the theoretical maximum can be attributed to overheads of data vectorization, result devectorization, and the processing of edge cases that cannot be fully vectorized.

Future research directions include combining SIMD optimization with multithreaded processing to achieve additional acceleration on multi-core processors, as well as exploring the potential of other instruction sets, such as AVX-512.

References

1. Masciari E., Napolitano E.V. Sustainability and High Performance Computing. *Lecture Notes in Computer Science*. 2024. P. 237–242. URL: https://doi.org/10.1007/978-3-031-78093-6_21
2. Zin N. Oo. The Improvement of 1D Gaussian Blur Filter using AVX and OpenMP. *2022 22nd Int. Conf. Control, Automat. Syst. (ICCAS)*, Nov. 27–Dec. 1 2022. Jeju, 2022. P. 1493–1496. URL: https://doi.org/10.23919/iccas55662.2022.10003739
3. Kusswurm D. SIMD Fundamentals. *Modern Parallel Programming with C++ and Assembly Language*. 2022. P. 1–16. URL: https://doi.org/10.1007/978-1-4842-7918-2_1

4. Vasile C.-E., Ulmămei A.-A., Bîră C. Image Processing Hardware Acceleration—A Review of Operations Involved and Current Hardware Approaches. 2024. Vol. 10, №12. P. 298. URL: https://doi.org/10.3390/jimaging10120298
5. Zhulkovskyi O., Zhulkovska I., Kurliak P., Sadovoi O., Ulianovska Y., Vokhmianin H. Using asynchronous programming to improve computer simulation performance in energy systems. *Energetika*. 2025. Vol. 71, №1. P. 23–33. URL: https://doi.org/10.6001/energetika.2025.71.1.2
6. Zhulkovskyi O., Zhulkovska I., Vokhmianin H., Firsov A., Tykhonenko I. Application of SIMD-instructions to increase the efficiency of numerical methods for solving SLAE. *Comput. Syst. Inf. Technol*. 2024. №4, P. 126–133. URL: https://doi.org/10.31891/csit-2024-4-15
7. Zhulkovskyi O.O., Zhulkovska I.I., Vokhmianin H.Y., Firsov O.D., Riabovolenko V.A. Research of progressive tools of parallel computations with the use of SIMD architecture. *Inform. math. methods simul.* 2023. Vol. 13, №3–4. P. 228–235. URL: https://doi.org/10.15276/imms.v13.no3-4.228
8. Zheng R., Pai S. Efficient Execution of Graph Algorithms on CPU with SIMD Extensions. *2021 IEEE/ACM Int. Symp. Code Gener. Optim. (CGO)*, Feb. 27–Mar. 3 2021. Seoul, 2021. P. 262–276. URL: https://doi.org/10.1109/cgo51591.2021.9370326
9. Barredo A., Cebrian J.M., Moreto M., Casas M., Valero M. Improving Predication Efficiency through Compaction/Restoration of SIMD Instructions. *2020 IEEE Int. Symp. High Perform. Comput. Archit. (HPCA)*, Feb. 22–26 2020. San Diego, 2020. P. 717–728. URL: https://doi.org/10.1109/hpca47549.2020.00064
10. Sharma P., Dubey A.K., Goyal A. Hardware Acceleration Using SIMD Based Vector Processor Array to Enhance Performance of Deblurring Methods for CT and MRI Images Having Motion Blur Artifacts. *2023 Int. Conf. Smart Syst. appl. Elect. Sci. (ICSSES)*, Jul. 7–8 2023. Tumakuru, 2023. P. 1–6. URL: https://doi.org/10.1109/icsses58299.2023.10199266
11. Kamei H., Honda S., Hayashi K., Maeda Y., Fukushima N. Lookup Register-Tables with Interpolation for Effective Image Transformation on x86/64 CPUs. *2024 IEEE Int. Conf. Vis. Commun. Image Process. (VCIP)*, Dec. 8–11 2024. Tokyo, 2024. P. 1–5. URL: https://doi.org/10.1109/vcip63160.2024.10849896
12. Tai L., Zhang L., Zhou X., Zhang S. Research on Image Restoration Processing Based on Gaussian Blur Algorithm. *2023 3rd Int. Signal Process., Commun. Eng. Manage. Conf. (ISPCEM)*, Nov. 25–27 2023. Montreal, 2023. P. 384–389. URL: https://doi.org/10.1109/ispcem60569.2023.00075
13. Kelefouras V., Keramidas G. Design and Implementation of 2D Convolution on x86/x64 Processors. *IEEE Trans. Parallel Distrib. Syst.* 2022. Vol. 33, №12. P. 3800–3815. URL: https://doi.org/10.1109/tpds.2022.3171471
14. Moradifar M., Shahbahrami A. Performance Improvement of Gaussian Filter using SIMD Technology. *2020 Int. Conf. Mach. Vis. Image Process. (MVIP)*, Feb. 18–20, 2020. IEEE, 2020. URL: https://doi.org/10.1109/mvip49855.2020.9116883
15. Nixon M.S., Aguado A.S. Basic image processing operations. *Feature Extraction & Image Processing for Computer Vision*. 2012. P. 83–136. URL: https://doi.org/10.1016/b978-0-12-396549-3.00003-3
16. Intel® Intrinsics Guide. URL: https://www.intel.com/content/www/us/en/docs/intrinsics-guide/index.html
17. Intel® Architecture Instruction Set Extensions Programming Reference. URL: https://www.intel.com/content/dam/develop/external/us/en/documents/319433-024-697869.pdf
18. Standard library <chrono>. URL: https://learn.microsoft.com/en-us/cpp/standard-library/chrono

ПРИСКОРЕННЯ ОБЧИСЛЮВАЛЬНИХ АЛГОРИТМІВ ОБРОБКИ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ SIMD

О.О. Жульковський, Г.Я. Вохмянін, І.І. Жульковська,
Ю.В. Ульяновська, Е.А. Рябоволенко

Дніпровський державний технічний університет
2, Дніпробудівська вул., м.Кам'янське, 51918, Україна
Університет митної справи та фінансів
2/4, Володимира Вернадського вул., м.Дніпро, 49000, Україна
Email: olalzh@ukr.net

Раціональний вибір обчислювальної платформи, оптимізація програмного забезпечення з урахуванням особливостей архітектури процесора дозволяє значно зменшити час виконання складних обчислень, підвищити продуктивність системи в цілому та забезпечити ефективну масштабованість при обробці великих обсягів даних. В роботі досліджується проблема прискорення обчислювальних алгоритмів обробки зображень, зокрема алгоритму Гауссового згладжування, із використанням технології паралелізму на рівні даних SIMD. Алгоритм Гауссового згладжування, який застосовується для зменшення шуму та видалення дрібних деталей із зображень, характеризується високою обчислювальною складністю через необхідність виконання численних арифметичних операцій над кожним пікселем. У зв'язку з цим оптимізація таких алгоритмів є актуальною задачею, а технологія SIMD відкриває можливості для паралельної обробки даних з використанням розширених інструкцій процесора, що дозволяє суттєво підвищити продуктивність обчислень. Метою дослідження є підвищення ефективності алгоритму Гауссового згладжування за рахунок SIMD-оптимізації обчислень. Розроблено два варіанти програмної реалізації досліджуваного алгоритму – скалярний та оптимізований з використанням інструкцій AVX-256. Оптимізована версія алгоритму застосовує векторизацію обчислень, обробляючи одночасно вісім пікселів у 256-бітних регістрах, що теоретично може забезпечити прискорення до восьми разів. Обчислювальні експерименти проводилися із зображеннями розмірами 1920x1080 та 2560x1440 пікселів із різними значеннями радіуса ядра та стандартного відхилення. Результати показали, що використання SIMD-інструкцій забезпечує прискорення в межах 6.9–7.3x порівняно зі скалярною реалізацією. При збільшенні радіуса ядра прискорення залишалося стабільно високим, що підтверджує ефективність підходу для більш складних обчислень. Підтверджено, що час виконання залежить переважно від радіуса ядра, тоді як зміна відхилення має менший вплив, оскільки радіус визначає зону дії фільтра. Отримане в результаті експериментів прискорення наближається до теоретичного максимуму, демонструючи переваги оптимізованої реалізації. Перспективи подальших досліджень передбачають поєднання SIMD-оптимізації з багатопоточною обробкою та вивчення можливостей використання більш продуктивних інструкцій типу AVX-512.

Ключові слова: обробка зображень, Гауссове згладжування, SIMD, AVX-256, паралельна обробка даних.

DOI 10.15276/imms.v15.no1.24
УДК 621.37

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 24-38

ЗАСТОСУВАННЯ ХАОСУ В АЛГОРИТМАХ ГЕНЕРАЦІЇ КЛЮЧІВ

О.В. Агаджанян, А.Р. Агаджанян, О.А. Сиропятов

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: o.v.ahadzhanian@op.edu.ua, 7985798@op.edu.ua, o.a.syropiatov@op.edu.ua

Сучасні вимоги до безпеки інформаційних систем акцентують увагу на новітніх методах генерації криптографічних ключів, одним із яких є використання властивостей хаотичних систем, що робить їх перспективними джерелами ентропії для криптографії. Мета дослідження: проаналізувати можливості застосування хаотичних динамічних систем, зокрема автогенераторів, для генерації криптографічних ключів у системах захисту інформації. Наукова та практична значущість роботи полягає в обґрунтуванні ефективності хаотичних генераторів для формування високоентропійних псевдовипадкових послідовностей і їх застосування в створенні захищених систем генерації ключів відповідно до сучасних вимог безпеки.Методологія дослідження включає теоретичний аналіз хаотичних динамічних систем, вивчення режимів автогенераторів на прикладі атрактора Лоренца, а також статистичний і ймовірнісний аналіз сигналів із оцінкою їх розподілів і кореляцій. Основні результати і висновки: визначено, що біфуркації є критичними точками переходу системи до хаотичного режиму, що породжує сигнали з високою ентропією; показано, що хаотичні генератори здатні працювати як генератори шуму та автогенератори, змінюючи характеристики розподілу вихідних сигналів; підтверджено, що вихідні послідовності є аперіодичними та можуть мати безперервний спектр, що є ключовою властивістю для криптографічної стійкості; наведено обґрунтування доцільності використання хаосу в алгоритмах формування шумових послідовностей для захисту інформації. Цінність дослідження – робота внесла вагомий внесок у розуміння ролі хаотичних систем у криптографії, зокрема у створенні нових алгоритмів генерації ключів із високим ступенем ентропії, що розширює спектр засобів забезпечення інформаційної безпеки. Практичне значення – отримані результати можуть бути використані при розробці апаратних і програмних генераторів криптографічних ключів на основі хаотичних систем, що підвищить захищеність інформаційних систем від несанкціонованого доступу та атак.

Ключові слова: хаос, генерація ключів, криптографія, автогенератор, ентропія, аттрактор Лоренца, псевдовипадкові послідовності

Вступ. Сучасні вимоги до безпеки інформаційних систем дедалі більше орієнтуються на нестандартні підходи до генерації криптографічних ключів. Одним із перспективних напрямів є використання властивостей хаотичних систем. Теорія хаосу — це розділ математики, що досліджує поведінку нелінійних динамічних систем, які за певних умов можуть демонструвати складну, на перший погляд випадкову, але детерміновану поведінку. Таке явище отримало назву динамічний (детермінований) хаос. Особливістю подібних систем є надзвичайна чутливість до початкових умов, що робить їх складнопередбачуваними та ідеальними для криптографічних застосувань.

Однією з технічних реалізацій хаотичних систем є генератори шуму, які створюють електричні сигнали у заданому частотному діапазоні. Вони вже мають застосування у пристроях захисту інформації від несанкціонованого доступу. Проте, як буде показано в подальшому, за певних умов генератор хаосу може виконувати роль автогенератора — пристрою з самозбудженням, здатного до стійкої генерації сигналів без зовнішнього збурення.

Автогенератори широко застосовуються в системах формування сигналів, і в контексті інформаційної безпеки вони можуть виступати як джерело

псевдовипадкових, але керованих послідовностей. Завдяки зворотному зв'язку, що забезпечує перевищення коефіцієнта підсилення над одиницею, такі системи можуть працювати в різних режимах — м’якому або жорсткому — в залежності від умов запуску та стійкості коливань. У результаті формується сигнал, властивості якого визначаються характеристиками самої системи і можуть бути використані для генерації криптографічних ключів з високим ступенем ентропії.

На сьогодні існує широкий спектр методів генерації криптографічних ключів, серед яких все більшої популярності набувають підходи, засновані на використанні хаотичних систем. Хаос у фізичних та електронних системах характеризується складною, але детермінованою динамікою, що є ідеальним джерелом високої ентропії для формування ключів. У науковій літературі описано численні реалізації таких генераторів — як апаратних, так і програмних. Наприклад, у роботі Rahman et al. (2022) [1] представлено метод генерації ключів на основі логістичного відображення для шифрування AES у системах IoT. У дослідженні Pellicer-Lostao & Lopez-Ruiz (2008) [2] показано, що двовимірні хаотичні карти здатні генерувати криптографічно стійкі псевдовипадкові біти. Вітчизняні дослідники, зокрема Дмітрієв О.С., Єфремов Є.В., Максимов Н.А. та Панас А.І., також розглядали використання автогенераторів зі специфічними схемами включення для формування хаотичних шумових коливань, придатних до застосування у системах захисту інформації.

Попри те, що класичні криптографічні стандарти, такі як NIST SP 800-90A [3], прямо не використовують хаос як джерело ентропії, сучасні дослідження демонструють, що хаотичні генератори можуть успішно відповідати вимогам до криптографічно стійких генераторів псевдовипадкових чисел (CSPRNG). Наприклад, Nguyen et al. (2021) [4] запропонували гіперхаотичну систему на основі п’яти змінних, яка демонструє високу швидкість генерації та проходить тести NIST SP 800-22, Diehard та TestU01. А в новітній роботі Song et al. (2025) [5] розроблено гібридну криптографічну систему "CryptoChaos", що поєднує кілька хаотичних карт із сучасними хеш-функціями (SHA-3) та алгоритмами постквантового шифрування (X25519). Такий підхід дозволяє створювати стійкі, адаптивні та незалежні системи захисту, що базуються на фізичних властивостях нелінійної динаміки.

Метою цієї статті є дослідження можливостей застосування хаотичних динамічних систем, реалізованих у вигляді автогенераторів, в алгоритмах генерації ключів для інформаційних систем захисту.

Основний розділ. Після детального вивчення підходів формування хаотичних коливань було віддано перевагу саме методам отримання хаосу за допомогою Атракторів. Такі схеми реалізують чисельне рішення диференційних рівнянь. Для побудови експерименту та отримання необхідних результатів нашу увагу привернув метод формування хаосу за Лоренцом [6].

Атрактор Лоренца в свою чергу описує, як стан нелінійної тривимірної динамічної системи змінюється з плином часу хаотичним чином. Атрактор був спочатку відкритий Едом Лоренцем, який вивів його зі спрощеної моделі конвекційних валів в земній атмосфері. Однак він також виникає в лазерах і динамо.

Дифференціальні рівняння (1), які визначають атрактор Лоренца [6, 7]:

$$\begin{aligned} dx / dt &= Sigma * (yx) \\ dy / dt &= (Rho-z) * x – y \\ dz / dt &= x * y - Beta * z, \end{aligned} \qquad (1)$$

де Sigma згадується як число Прандтля, Rho називають числом Релея, а бета - геометричним фактором. У Micro-Cap такі диференціальні рівняння можна моделювати за допомогою поведінкових моделей, доступних в розділі "Макро". Схема аттрактора Лоренца представлена нижче [8, 9].

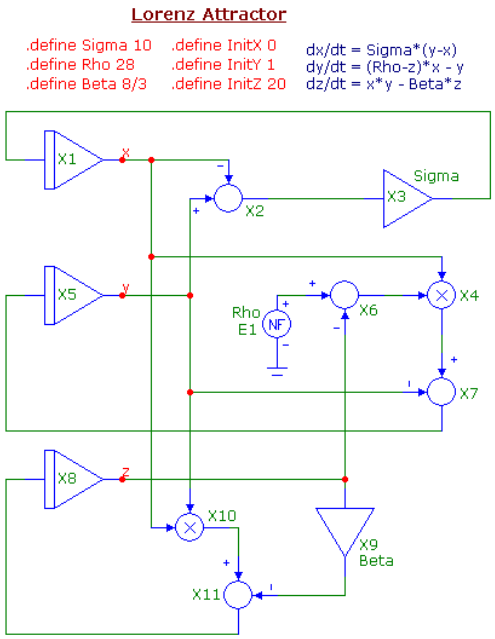


Рис. 1. – Аттрактор Лоренца в програмі Microcap

Вузли x, y і z обчислюють напруги, еквівалентні їх відповідним змінним в наведених вище рівняннях. Змінна x обчислюється за допомогою макросу Int, макросу Sub і макросу Amp. Допоміжний макрос (X2) забирає напругу в вузлі y на напругу в вузлі x. Потім різниця передається в макрос підсилювача (X3), параметр gain якого встановлений на Sigma. Вихідні дані макросу Amp потім вводяться в макрос Int (X1), який обчислює інтеграл для отримання x.

Змінна y обчислюється за допомогою макросу Int, двох макросів Sub, макросу Mul і джерела функції NFV. Джерело функції NFV (E1) видає напругу, еквівалентну Rho. Допоміжний макрос (X6) віднімає значення Rho на напругу в вузлі z. Потім різниця вводиться в макрос Mul (X4), де вона множиться на напругу в вузлі x. Потім цей продукт подається в інший допоміжний макрос (X7), де він віднімається з напруги в вузлі y. Потім ця різниця вводиться в макрос Int (X5), який обчислює інтеграл для отримання y.

Змінна z обчислюється за допомогою макросу Int макросу Mul, макросу Amp і макросу Sub. Напруги в вузлах x і y множаться за допомогою макросу Mul (X10). Напруга в вузлі z масштабується коефіцієнтом Beta за допомогою макросу Amp (X9). Ці два продукти вводяться в допоміжний макрос (X11). Потім різниця вводиться в макрос Int (X8), який обчислює інтеграл для отримання z.

Значення Sigma, Rho і Beta встановлюються за допомогою операторів define.

Наступні три оператори визначення також присутні на схемі:

define InitX 0, .define InitY 1 .define InitZ 20

Ці оператори визначення встановлюють початкові значення для змінних x, y і z. InitX, InitY і InitZ використовуються для визначення параметра VINIT для макросів X1, X5 і X8 Int відповідно. Параметр VINIT макросу Init встановлює початкову напругу на виході інтегратора. Аналогічно з іншими хаотичними системами атрактор Лоренца дуже чутливий до початкових умов, навіть невелика зміна призведе до іншого сюжету.

Загальні налаштування для відображення хаотичної поведінки з атрактором Лоренца - це встановити Sigma на 10, Rho на 28 і Beta на 8/3 [6]. З використанням цих значень виконується 200-секундний перехідний аналіз, який дає класичний графік "метелик", коли V (Z) будується в залежності від V (X), як показано на рис.2.

Біфуркація - це якісна зміна поведінки динамічної системи при нескінченно

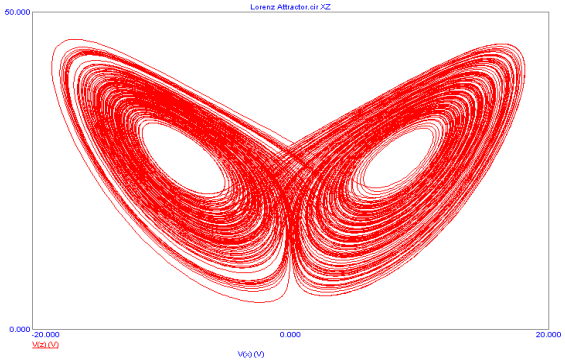


Рис. 2. – Бифуркації при Rho = 28

малій зміні її параметрів. Також для проведення дослідження для нас важливо таке поняття як «ентропія».

Ентропія зазвичай застосовується для опису рівноважних (оборотних) процесів.

У статистичній фізиці ентропія характеризує ймовірність здійснення будь-якого макроскопічного стану. Крім фізики, термін широко вживається в математиці: теорії інформації та математичної статистики. У цих областях знання ентропія визначається статистично і називається статистичною або інформаційною ентропією [6].

Розглянемо зміни в поведінці рішення системи Лоренца при різних значеннях параметра Rho. Rho < 1 – атрактором є початок координат, інших стійких точок немає.

1 < Rho < 13,927 – траєкторії спірально наближаються (це відповідає наявності загасаючих коливань) до двох точок.

Ці точки визначають стан стаціонарного режиму конвекції, коли в шарі формується структура з обертових валів рідини.

Rho ≈ 13,927 – якщо траєкторія виходить з початку координат, то, зробивши повний оборот навколо однієї зі стійких точок, вона повернеться назад в початкову точку -виникають дві гомоклінічні петлі. Поняття гомоклінічної траєкторії означає, що вона виходить і приходить в одне і те ж положення рівноваги.

Rho > 13,927 – залежно від напрямку траєкторії, приходить до однієї з двох стійких точок. Гомоклінічні петлі перероджуються в нестійкі граничні цикли, також виникає сімейство складно влаштованих траєкторій, що не є атрактором, а скоріше навпаки, що відштовхує від себе траєкторії. Іноді за аналогією ця структура називається «дивним репеллером».

Rho ≈ 24,06 – траєкторії тепер ведуть не до стійких точок, а асимптотично наближаються до нестійких граничних циклів – виникає власне аттрактор Лоренца. Однак обидві стійкі точки зберігаються до значень Rho ≈ 24,74.

Rho ≈ 28 – класичне значення параметра, розглянуте у статті Лоренца.

Всі три стани рівноваги нестійкі і траєкторії з їх околиць притягуються до хаотичного (локального) атрактору (який, таким чином, самозбуджуємо по відношенню до всіх станів рівноваги). Хаотичний атрактор має дробову ляпуновську розмірність, для якої аналітична оцінка зверху може бути отримана аналітично через форму ляпуновської розмірності глобального атрактора, а оцінка знизу може бути отримана аналітично.

При великих значеннях параметра Rho траєкторія зазнає серйозних змін. Шильников і Каплан показали, що для великих Rho система перетворюється на режим автоколивань, у якій, якщо зменшувати параметр, спостерігатиметься перехід до хаосу через послідовність подвоєння періоду коливань.

Нижче наведемо рисунки моделювання атрактора у програмі Microcap.

На початку будуть наведені біфуркації X, Y та Z, також графік сигналу, функція

розподілу та щільність ймовірності при Rho=28 та початкових умовах x=0, y=1, z=20 (рис 3).

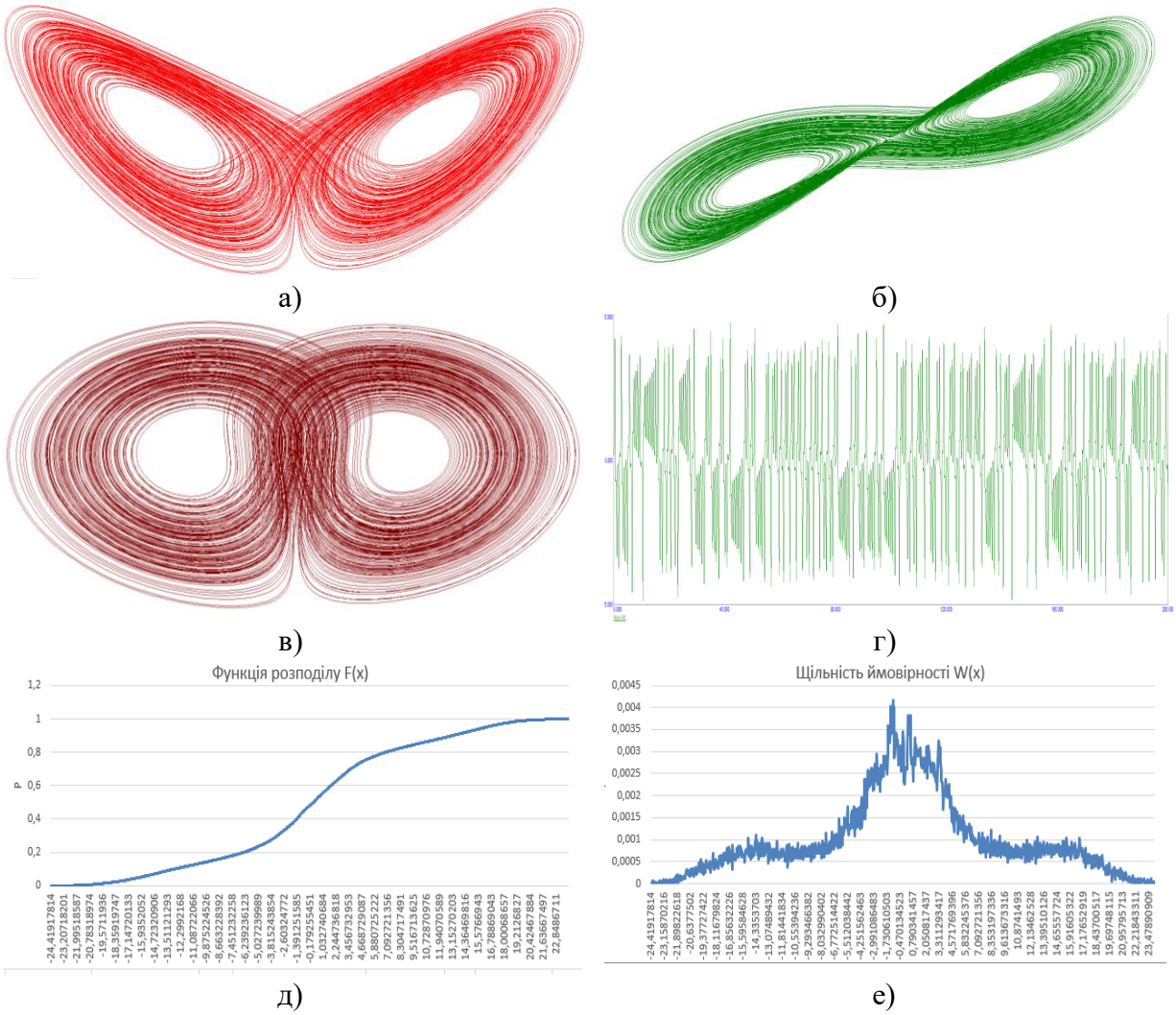


Рис. 3. – Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 28, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – XY; (в) – YZ; (г) – Сигнал; (д) - Функція розподілу; (е) - Щільність ймовірності

На рис. 3 (е) наведено розрахунок щільності ймовірності за наступними числовими характеристиками: сер. значення – a = 0.150363519; дисперсія – σ^2 = 81.53201942, медіана – m = 0.147919755. Отримання йомовірнісних характеристи віпадкової величини взято за допомгою відведення у. Зроблено усереднення за часом та обрано частотний метод визначення йомовірності за допомогою аналізу 40000 значень відггуку атрактору Лоренца.

В загальному вигляді систему рівнянь руху системи можливо викласти у вигляді (2) згідно [6]:

$$V_i(\vec{x}) = \frac{dx_i}{dt},\ i = 1, 2, \ldots, N. \qquad (2)$$

Заповнення фазового простору системи відбувається шляхом численного інтегрування системи рівнянь Лоренца, яка є несиметрична за часом (3):

$$-\sigma x - \sigma y = \frac{dx}{dt};\ rx - y - xz = \frac{dy}{dt};\ -bz + xy = \frac{dz}{dt}. \qquad (3)$$

Всі величини, які входять до рівняння 3 разом з часом (t) беруться у безрозмірному вигляді.

X, Y та Z – це змінні пропорційні відповідно швидкості конвективного руху. Sigma та Beta – це константи, відповідно 10 та 8/3. Параметр Rho може бути аналогічний (для генераторів іншого типу) параметру збудження. Фазову траєкторію використовують за алгоритмом подвійної апроксимації (4).

$$X_{i,\,n+1} = x_{in} + \frac{1}{2}[V_i(x_n, y_n, z_n) + V_i(x_{n+1}, y_{n+1}, z_{n+1})]\Delta t. \qquad (4)$$

Виявилося, що фазова траєкторія затягується в область (атрактор Лоренца), що представляє собою два «вихори», які мають своїми центрами дві різні нерухомі точки. Траєкторія потрапляє в околиці однієї з них, здійснює біля неї деяку кількість оборотів і потім, віддаляючись від неї, переміщається в околицю другої нерухомої точки, описує тепер уже у неї якусь кількість оборотів, віддаляється, потрапляє в околиці першої нерухомої точки тощо.

Це доводить, що такі фазові траєкторії системи нестійкі. Це проявляється в сильній залежності розрахункової траєкторії від початкових умов (від вибору початкової точки), так що неможливо передбачити заздалегідь, ні в околицю з яких нерухомих точок виявиться в перший раз затягнутою дана траєкторія, ні яке число оборотів вона зробить в кожній окремій серії. Як нестійкий і обмежений у фазовому просторі, рух даної системи виявляється стохастичним і має чітко виражену турбулентну структуру.

Надалі атрактор Лоренца піддався всебічному вивченню. Була досліджена його структура для різних значень параметра Rho.

Виявилося, що тут має місце своєрідний гістерезис: якщо ми збільшуємо Rho, то конвективний (регулярний) потік зривається в турбулентний (стохастичний) при Rho — 24,74, якщо ж, навпаки, зменшуємо Rho, то турбулентний рух переходить в конвективний при Rho = 24,06. У вузькій області значень 24,06 < Rho < 24,74 в системі Лоренца існують три атрактори, два з яких відповідають регулярному руху, а третій — стохастичному. Виявилося також, що перехід до стохастичного руху відбувається в ній через ряд біфуркацій.

У тому, що рівняння Лоренца несиметричні за часом, легко переконатися безпосередньо. Таким чином, цей динамічний хаос, що виникає в даній системі, є незворотнім.

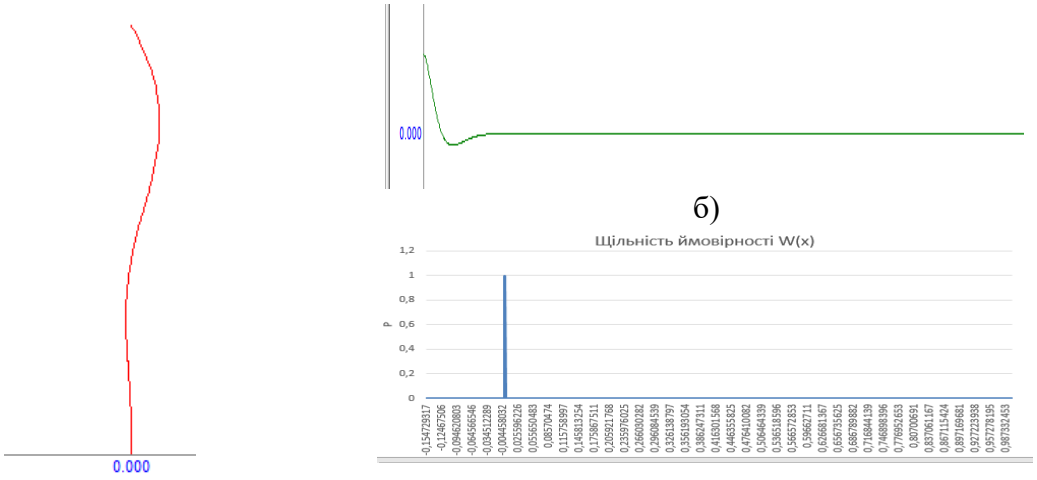
Це зумовлює особливу топологічну природу атрактора Лоренца, яка кардинально відрізняє його від стохастичних атракторів, що виникають в оборотних (реверсивних) динамічних системах. Аттрактор Лоренца є класичним прикладом детермінованого хаосу, де хаотична поведінка виникає з абсолютно детермінованих рівнянь руху без зовнішніх випадкових впливів. Його топологічні властивості характеризуються фрактальною структурою та складною геометрією, що забезпечує високу чутливість до початкових умов і складність прогнозування подальшого розвитку системи.

У противагу цьому, стохастичні атрактори формуються під впливом випадкових процесів і шумів у системах із зворотністю динаміки, що призводить до статистично описуваної поведінки.

Такий різний характер атракторів визначає їхнє застосування у моделюванні різноманітних фізичних, біологічних і технічних процесів, зокрема у сфері генерації псевдовипадкових послідовностей для криптографії.

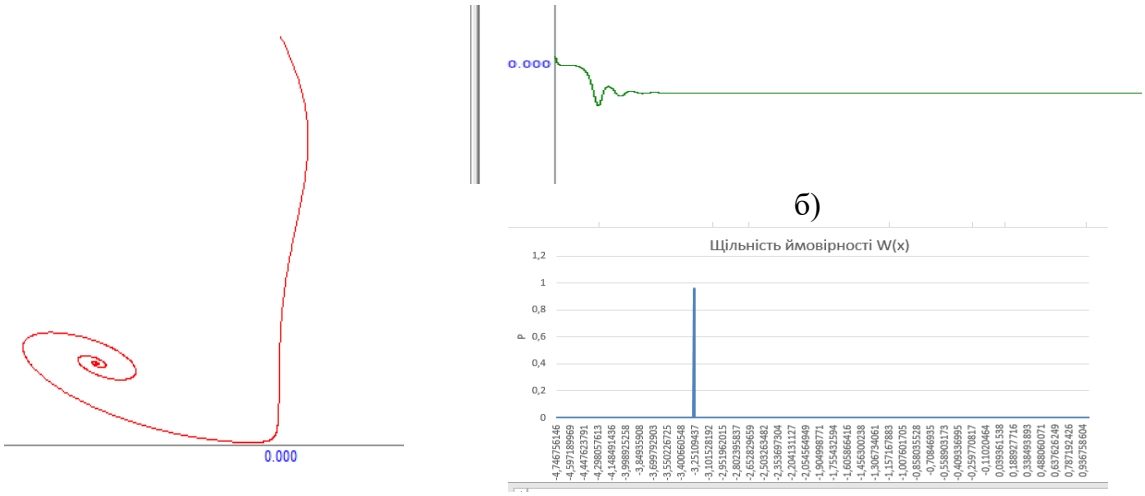
Далі наведені результати моделювання лише найважливіших параметрів дослідного алгоритму формування хаотичних послідовностей за схемою атрактора Лоренца. Показані біфуркації (XZ), вигляд хаотичного сигналу у часовому просторі. Визначені щільності розподілу ймовірності для аналізу саме у площині застосування алгоритму для формування ключів.

Варіації параметрів показані на рис. 4-9.



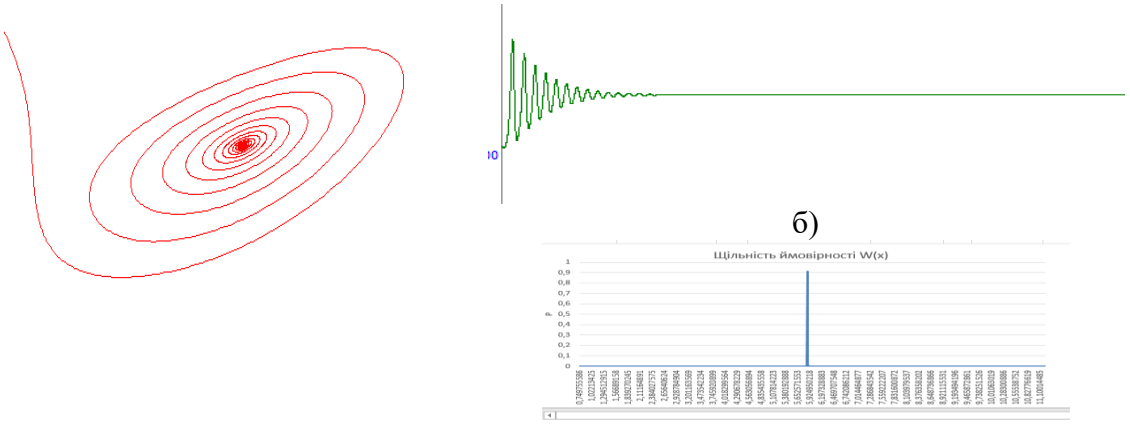
а) б) в)

Рис. 4. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 0.5, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – Сигнал; (в) - Щільність ймовірності. Параметри: a = 0.000337217; дисперсія – σ^2 = 0.000436894, медіана m = 0



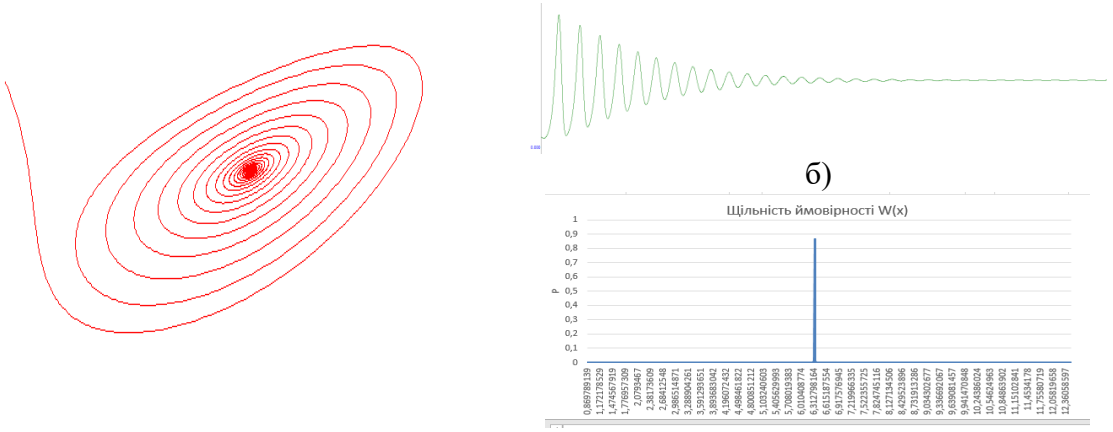
а) б) в)

Рис. 5. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 5, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – сигнал; (в) - щільність ймовірності. a = -3.230049362; дисперсія – σ^2 = 0.118095236, медіана m = -3.26598665



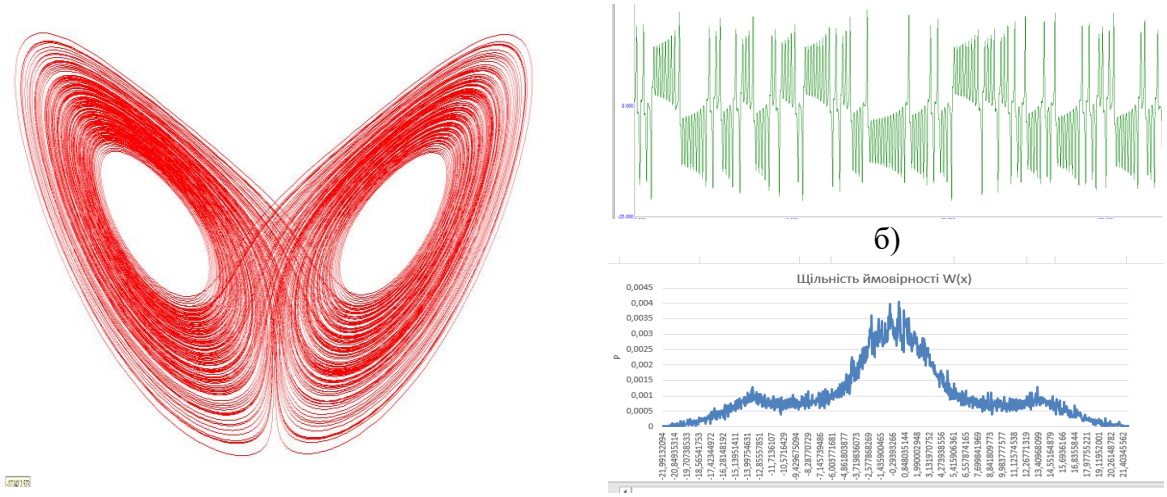
а) в)

Рис. 6. - Результати моделювання схеми Атрактора Лоренца з параметрами: Rho = 13.927, x = 0, y = 1, z = 20.a = 5.851226298; σ2 = 0.179453846, m = 5.871287205



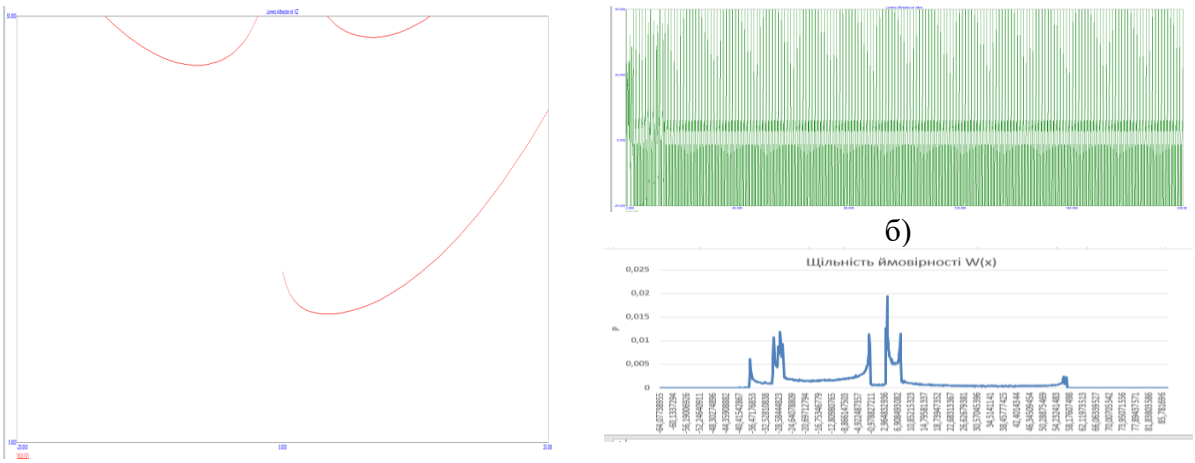
а) в)

Рис. 7. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 16, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – Сигнал; (в) - Щільність ймовірності.
Параметри: a = 6.300076775; дисперсія – σ2 = 0.271385236, медіана – m = 6.324556591



а) в)

Рис. 8. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 24.06, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – Сигнал; (в) - Щільність ймовірності.
Параметри: a = 0.156394423; дисперсія – σ2 = 65.72242363, медіана – m = –0.176483671



а) в)

Рис. 9. - Результати моделювання схеми Атрактора Лоренца з параметрами: Rho = 100, x = 0, y = 1, z = 20. a = -4.229658168; σ^2 = 504.443928, m = -3.800248801

Далі приведемо результати моделювання при стандартному Rho = 28, але різних початкових умовах. На рис. 10-18 наведені щільності розподілу ймовірності за різними критеріями. На рис. 19 визначено коваріаційну функцію для хаотичної послідовності.

Рис. 10. - Щільність ймовірності схеми атрактора з параметрами: Rho = 28, x = 10, y = 1, z = 20

Рис. 11. Щільність ймовірності схеми атрактора з параметрами: Rho = 28, x = 50, y = 1, z = 20

Рис. 12. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 100, y = 1, z = 20

Рис. 13. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 0, y = 10, z = 20

Рис. 14. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 0, y = 50, z = 20

Рис. 15. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 0, y = 100, z = 20

Рис. 16. - Щільність ймовірності схеми з параметрами: Rho = 28, x = 0, y = 1, z = 200

Рис. 17. - Щільність ймовірності схеми з параметрами: Rho = 28, x = 0, y = 1, z =

Рис. 18. - Щільність ймовірності схеми Атрактора з наступними параметрами: Rho = 28, x = 0, y = 1, z = 2000

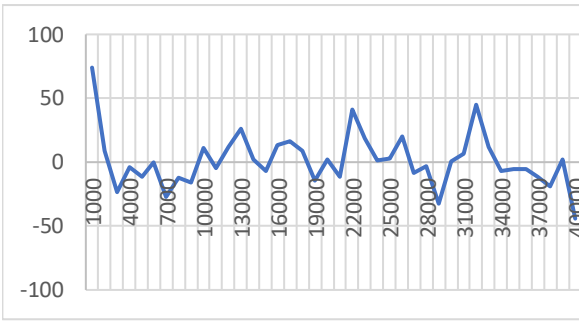


Рис. 19. - Коваріаційна функція реалізації сигналу з наступними параметрами: Rho = 28, x = 0, y = 1, z = 2000

До завершення визначень статистичних параметрів атрактора побудовано коваріаційну функцію вихідного сигналу на відведенні y (рис. 19) відповідно до [7]. Коваріаційна функція побудована у границі від 1 до 1000 значень, другий масив було взято зі збільшенням значення +1000. Таким чином у вихідні послідовності (y) було проаналізовано першу 1000 значень та порівняно з наступними 1000 значень масиву через 1000 значень. Отримано 40 значень функції коваріації.

Особлива топологічна природа атрактора Лоренца, зокрема його складна фрактальна структура, впливає на характер динаміки системи, що значно відрізняє його від стохастичних атракторів у оборотних системах. Ці властивості визначають специфіку переходів у системі від регулярного до хаотичного режиму, що знаходить своє відображення у змінах ймовірнісних характеристик випадкових процесів, які описують поведінку системи. Аналіз цих характеристик дозволяє глибше зрозуміти природу хаосу і вплив параметрів системи на формування статистичних властивостей генерованих сигналів.

Значення біфуркацій в теорії динамічного хаосу визначається тією обставиною, що саме з ними пов'язаний перехід системи від регулярного руху до стохастичного, при якому фазова траєкторія, змінюючи свою топологію, перестає бути гладкою лінією. Аналіз ймовірнісних характеристик випадкових процесів (дискретного випадкового сигналу) показав наступне: такі характеристики, як щільність розподілу ймовірності, змінюються залежно від режиму роботи атрактора. Характер функції щільності ймовірностей варіюється від нормального розподілу (коли спостерігаються нерівномірні зміни ймовірностей в області ±3σ (рис. 18) до розподілу Парето (рис. 4(e)), що характеризується концентрацією ймовірності у локалізованій області значень, а також до гамма-розподілу, який відзначається несиметричністю лівої та правої частин функції розподілу (рис. 3(e)). Відповідно до властивостей коваріаційної функції можна зробити висновок, що у вихідній послідовності навіть у малих вікнах існує невеликий статистичний взаємозв’язок.

Далі розглянемо порівняльний статистичний аналіз криптоалгоритмів, що дозволить оцінити практичні наслідки описаних теоретичних результатів. Результати статистичних випробувань алгоритмів DES, СКЗД, а також GAMMA 4, проведеного на ЕОМ, є перевірка на випадковість шифртексту і ключового потоку при різних варіантах формування ключової послідовності і вихідного тексту.

Узагальненою характеристикою випадковості будь-якої сукупності чисел, в тому числі і досліджуваних двійкових послідовностей, є ентропія:

$$H = \sum_{i=0}^{N-1} P_i * \log_2 P_i. \qquad (5)$$

Ентропія максимальна для рівноймовірних випадкових послідовностей, коли:

$$P_i = 1/N_1 = const, \qquad \mathrm{H}_{max} = \log_2 N^{-1} \text{ [біт]}. \tag{6}$$

Аналізу підлягає байтова структура шифртексту, тоді $N^{-1} = 2^8$.

$\mathrm{H}_{max} = 8$, якщо в експерименті ентропія H близька до H_{max}. Таким чином, дана характеристика свідчить про близькість експериментально одержуваних вибіркових розподілів ймовірності шифртексту і шифрограм до рівноймовірних розподілів для ключів всіх досліджених довжин і відкритих текстів будь-яких типів. У статистиці більше за інших використовують розподіл у вигляді χ^2

У нашому випадку приймаємо гіпотезу рівноймовірного розподілу досліджуваної послідовності, і тоді:

$$P_i = 1/N_1 = 1/2^8 \text{ [біт]} \tag{7}$$

При $\mathrm{E} > 30$ ($\mathrm{E} = N^{-1} - 1 = 255$ – розподіл степенів свободи) розподіл величини:

$$\chi_{\text{ср.}} = \sqrt{2\chi^2} - \sqrt{2E},$$
$$\chi^2 = \sum_{i=0}^{N^1-1} \frac{(v_i - N_1 * P_i)^2}{N_1 P_i}, \text{ при (7) має вигляд: } \chi^2 = \sum_{i=0}^{255} \frac{(v_i - N_1 2^{-8})^2}{N_1 2^{-8}} \tag{8}$$

близько до нормального з нульовим математичним очікуванням і одиничною дисперсією.

Для перевірки правдоподібності гіпотези про равновероятном розподілі досліджуваних послідовностей шифртексту і шифргамми проводяться наступні дії:

1. Обчислюється величина χ^2 для прийнятого в експерименті обсягу вибірки $N_1 = 2^{13} = 8192$ байту, то отримуємо:

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - 32)^2}{32} \tag{9}$$

2. Обчислюємо величину $\chi_{\text{ср.}}$

Оскільки розподіл величини $\chi_{\text{ср.}}$може вважатися практично нормальним (10) (число ступенів свободи E = 255) з нульовим математичним очікуванням і одиничною дисперсією, то відхилення $\chi_{\text{ср.}}$ від математичного очікування не більше ніж на три одиниці гарантує високу значимість гіпотези про рівномовірному розподілі.

$$\chi_{\text{ср.}} = \sqrt{2\chi^2} - \sqrt{510} = \sqrt{2\chi^2} - 22{,}583179 \tag{10}$$

Для дослідження двійкової послідовності зашифрованих даних (шифртексту) і двійкової послідовності шифргаммі (ключового потоку) складається, так звана, маркувальна таблиця, яка, незалежно від довжини тестових файлів, являє собою таблицю об'ємом 28 осередків. Досліджувана двійкова послідовність розбивається на 8-розрядні байти і кожен байт розглядається як одне з 256 чисел. Таким чином, непересічні восьмиграми досліджуваної двійкової послідовності представляються як трирозрядні десяткові числа. На перетині відповідного рядка і стовпця у маркувальній таблиці записано кількість випадків, у яких дане число зустрілося серед N чисел у досліджуваній послідовності.

На основі маркувальних таблиць отримують наступні статистичні характеристики:

- значення максимального елемента таблиці Max;
- значення мінімального елемента таблиці Min;
- відхилення $\chi_{\text{ср.}}$ від математичного очікування;
- квадрата відхилення χ^2;
- ентропії H;

$$\mathrm{H} = -\sum_{i=0}^{255} \left(\frac{v_i}{N}\right)_i * \log_2 \left(\frac{v_i}{N}\right),$$

- полюсності за формулою (10)

$$P = (2N_1 - N)/\sqrt{N}, \qquad (10)$$

де: N_1 – кількість одиниць у послідовності. Якщо кількість одиниць рівна кількості нулів у дослід жувальній послідовності, то P=0.

Результат та обговорення. Вочевидь, що статистичні характеристики шифртексту повинні залежати від статистичних характеристик відкритого тексту і його довжини, а також і від вихідного значення ключового регістра. При цьому, чим вище ентропія відкритого тексту, тим більш високе значення ентропії слід очікувати в шифртексту. Цей же результат, в загальному випадку, найбільш вірогідний при збільшенні довжини відкритого тексту. Структура змісту ключового регістра найчастіше призводить до збільшення ентропії шифртексту у випадках, коли кількість одиничних символів приблизно дорівнює числу нульових символів. Незалежно від конкретного криптоалгоритму найменше значення ентропії шифртексту слід очікувати в разі такої структури відкритого тексту, що складається, наприклад, тільки з нульових або тільки з одиничних двійкових символів. Аналогічний висновок щодо ентропії можна зробити і для такої структури секретного ключа, що складається, наприклад, тільки з нульових або тільки з одиничних двійкових символів. Очевидно, поєднання цих двох умов в одному експерименті ставить криптоалгоритм в найбільш складне становище, тому значення наведених вище статистичних характеристик слід досліджувати саме для таких поєднань відкритих текстів і ключових послідовностей.

Об'єктом дослідження в процесі випробувань кожного криптоалгоритму були, перш за все, статистичні характеристики шифртексту. Однак, для потокових адитивних шифрів, до яких відноситься криптоалгоритм GAMMA 4, не менший інтерес представляють статистичні характеристики шифргамми (або ключової послідовності), тому за програмою обчислювалися статистичні характеристики послідовності, що являє собою порозрядну логічну суму шифртексту і відкритого тексту. Подібні обчислення статистичних характеристик аналогічної послідовності проводилися і для обох стандартних криптоалгоритмів.

Час обробки (шифрування) кожного файлу фіксувався вбудованими електронними годинами ПЕОМ з точністю до однієї сотої частки секунди. При цьому в інтервалі часу шифрування процесор не мав додаткових завдань. В якості секретних ключів для статистичних випробувань криптоалгоритмів використовувалися двійкові послідовності довжини:

- 56 біт для криптоалгоритму DES;
- 60 біт для криптоалгоритма GAMMA 4;
- 256 біт для кріптоалгоритма по ГОСТ 28147-89, що складаються:
- з одних двійкових символів"0";
- з одних двійкових символів "1";
- з випадкової (або псевдовипадкової) послідовності двійкових символів "0" або "1";

Як випадкові (або псевдовипадкові) синхросилки для статистичних випробувань криптоалгоритмів використовувалися двійкові послідовності довжини. Такі синхросилки формувались алгоритмом атрактора Лоренца:

- 56 біт для криптоалгоритму DES;
- 60 біт для криптоалгоритма GAMMA 4;
- 256 біт для кріптоалгоритма по ГОСТ 28147-89, що складаються:
- з одних двійкових символів " 0 " з одиницею в молодшому розряді;
- з одних двійкових символів " 0 " з одиницею в старшому розряді.

В якості тестових використовувалися файли довжини 8192 байта:

файл null_8.pas, що складається з 65536 двійкових символів “0”;

файл edin_8.pas, що складається з 65536 двійкових символів “1”;

файл teks_8.pas, що складається з 65536 двійкових символів "0" і " 1 " звичайного текстового документа.

Таким чином, використані в процесі випробувань сукупності тестових вхідних файлів і секретних ключів займають весь діапазон можливих структур даних і ключів від одного граничного положення до іншого, включаючи найчисленніші проміжні варіанти, що дозволяє судити про діапазон представлення вхідних даних програмних моделей.

Результати статистичних випробувань трьох алгоритмів захисту інформації наведені на рис. 20.

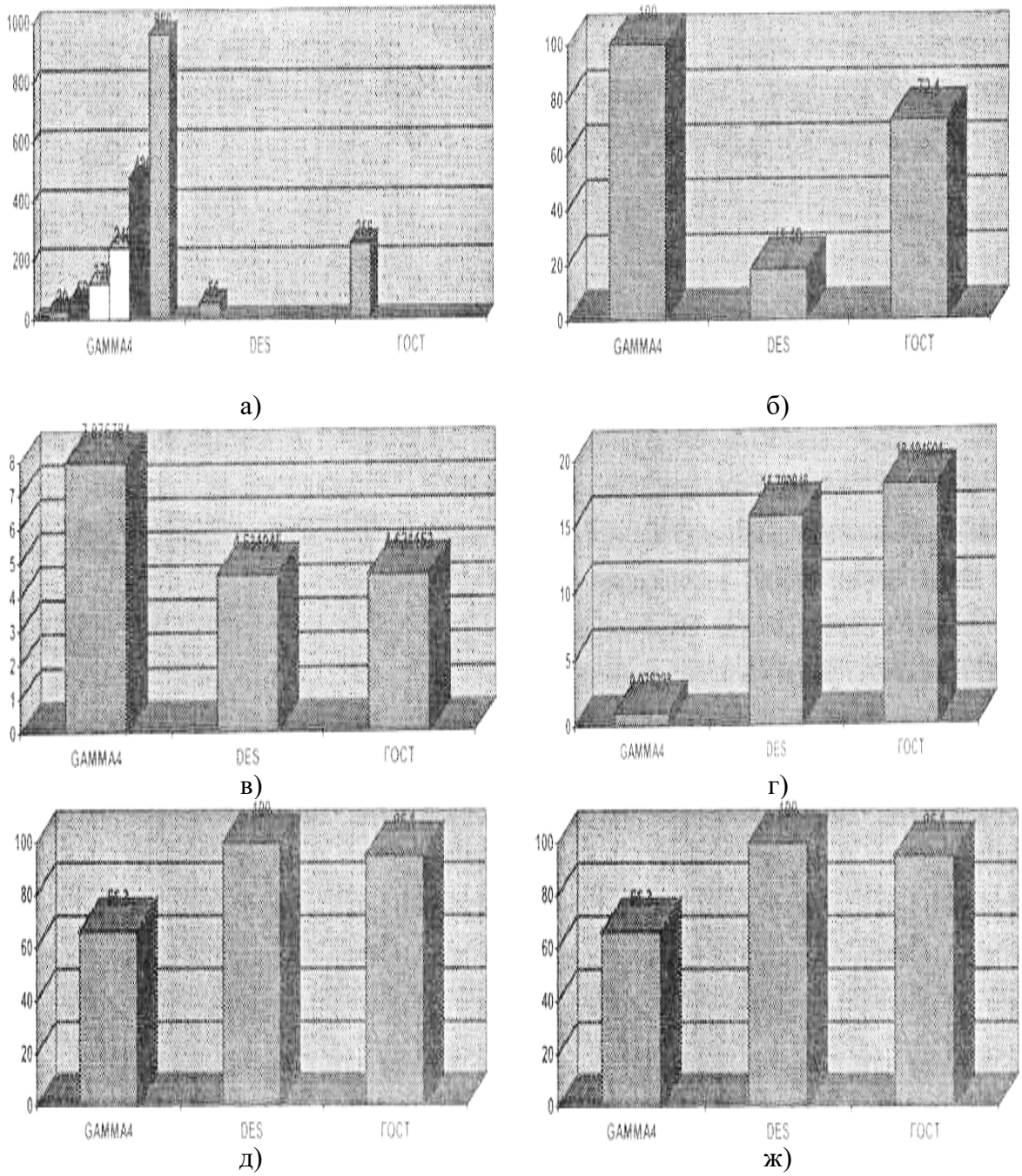


Рис. 20. - Результати статистичних випробувань, де: (а) – довжина ключа (практична стійкість), двійкових розрядів, (б) – швидкодія, %, (в) – ентропія шифртексту (ідеальне значення – 8.0), (г) – полюсність шифртексту (ідеальне значення – 0), (д)) - складність реалізації (відносний обсяг пам'яті для розміщення процедури шифрування), (ж) - середнє значення різниці елементів маркувальних таблиць (граничне значення = 0)

Отримані результати свідчать про досить високу ефективність алгоритму захисту GAMMA 4. Однак алгоритм GAMMA 4 в даний час не сертифікований і отже

може розглядатися лише як ефективний алгоритм цифрового маскування.

Основні висновки. Біфуркації у теорії динамічного хаосу відіграють ключову роль, оскільки саме вони визначають перехід системи від регулярного, детермінованого руху до хаотичного, стохастичного режиму. При цьому фазова траєкторія системи втрачає гладкість і змінює свою топологію, що є ознакою виникнення хаосу.

Аналіз коваріаційної функції показав, що навіть у малих часових вікнах вихідна послідовність має невеликий, але стійкий статистичний взаємозв'язок, що свідчить про певну структуру хаотичного сигналу.

Ймовірнісні характеристики випадкових процесів змінюються залежно від режиму роботи атрактора і можуть набувати вигляду різних функцій розподілу — від нормального до розподілу Парето та гамма-розподілу, що вказує на складність та різноманітність статистичних властивостей таких сигналів.

Підтверджено, що хаотична динаміка породжує аперіодичні послідовності з безперервним спектром, що є важливою властивістю для використання у системах захисту інформації.

Використання генераторів хаосу для формування шумових послідовностей у криптографічних алгоритмах дозволяє підвищити рівень скритності та стійкості систем, особливо в контексті активного зашумлення.

Атрактор Лоренца демонструє дві режимні поведінки — як генератор шуму та як автогенератор — при зміні параметра Rho, що змінює характер розподілу вихідних сигналів і робить його потенційно корисним у системах зв'язку, де шумова складова зазвичай оцінюється нормальним розподілом.

Хоча фрактальні розмірності атракторів є важливим параметром для кількісної оцінки складності систем, у цій роботі основна увага приділялась аналізу вихідних послідовностей, а не безпосередньому визначенню фрактальних розмірностей.

Всі досліджені атрактори є фрактальними множинами, що підтверджується графіками біфуркацій у фазовому просторі, а фрактальна самоподібність атрактора Лоренца базується на гіпотезі Пуанкаре, доведеній Григорієм Перельманом.

Список літератури

1. Rahman M., Hossain M., Hoque M. Chaos and Logistic Map Based Key Generation Technique for AES-driven IoT Security. *IEEE Access*. 2022. Vol. 10. P. 78150–78163. DOI: 10.1109/ACCESS.2022.3190076.
2. Pellicer-Lostao C., Lopez-Ruiz R. Pseudo-random bit generation based on 2D chaotic maps // *Computers & Mathematics with Applications*.– 2008. Vol. 59(10). P. 3258–3268. DOI: 10.1016/j.camwa.2009.08.036.
3. SP 800-90A Rev. 1. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* / National Institute of Standards and Technology (NIST). – Gaithersburg, MD, 2015. 76 p.
4. Nguyen V.H., Ha N.D., Nguyen T.T. Designing a Pseudo-Random Bit Generator with a Novel 5D Hyperchaotic System. *Applied Sciences*. – 2021. – Vol. 11(14). Article 6394. DOI: 10.3390/app11146394.
5. Song K., Li Y., Zhang H. A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications. *IEEE Trans. on Information Forensics and Security*. – 2025 (in press). Preprint: arXiv:2403.12345.
6. Дмитрієв А.С. *Генерація хаосу* / А.С. Дмитрієв. М.: Техносфера, 2012. 424 с.
7. Філіпський Ю.К. *Випадкові процеси в радіо колах: навч. посібник* . Ю.К. Філіпський. – Одеса: Наука і техніка, 2012. 176 с.
8. Опис програмного забезпечення MICRO–CAP [Електронний ресурс]. Режим доступу: http://www.spectrum-soft.com/index.shtm
9. Логвинов В.В., Фриск В.В. *Схемотехніка телекомунікаційних пристроїв, радіоприймальні пристрої систем мобільного та стаціонарного радіозв'язку, теорія електричних кіл*. М.: СОЛОН–ПРЕСС, 2011. 656 с.

APPLICATION OF CHAOS IN KEY GENERATION ALGORITHMS

O.V. Ahadzhanian, A.R. Ahadzhanian, O.A. Syropiatov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.v.ahadzhanian@op.edu.ua, 7985798@op.edu.ua, o.a.syropiatov@op.edu.ua

Modern requirements for the security of information systems focus on the latest methods of generating cryptographic keys, one of which is the use of the properties of chaotic systems, which makes them promising sources of entropy for cryptography. Research objective: To analyze the possibilities of using chaotic dynamic systems, in particular autogenerators, for generating cryptographic keys in information protection systems. The scientific and practical significance of the work lies in substantiating the effectiveness of chaotic generators for forming high-entropy pseudorandom sequences and their application in creating secure key generation systems in accordance with modern security requirements. The research methodology includes a theoretical analysis of chaotic dynamic systems, a study of the modes of autogenerators using the example of the Lorentz attractor, as well as statistical and probabilistic analysis of signals with an assessment of their distributions and correlations.Main results and conclusions: It was determined that bifurcations are critical points of the system's transition to a chaotic mode that generates signals with high entropy. It is shown that chaotic generators are able to work as noise generators and autogenerators, changing the characteristics of the distribution of output signals. It is confirmed that the output sequences are aperiodic and can have a continuous spectrum, which is a key property for cryptographic stability. The feasibility of using chaos in algorithms for generating noise sequences for information protection is justified.Value of the study: The work has made a significant contribution to understanding the role of chaotic systems in cryptography, in particular in creating new algorithms for generating keys with a high degree of entropy, which expands the range of information security tools. Practical significance: The results obtained can be used in the development of hardware and software cryptographic key generators based on chaotic systems, which will increase the security of information systems from unauthorized access and attacks.

Keywords: chaos, key generation, cryptography, autogenerator, entropy, Lorentz attractor, pseudorandom sequences

DOI 10.15276/imms.v15.no1.39
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp. 39-47

ТЕОРІЯ ГРАФІВ ЯК ОСНОВА МЕТОДІВ ВБУДОВУВАННЯ ІНФОРМАЦІЇ

І.І. Борисенко, І.С. Вінковська

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
Email: boris_enko63@ukr.net

У сучасному цифровому середовищі, де витоки даних і кібератаки стають все більш поширеними, задача створення надійних засобів захисту інформації є надзвичайно актуальною. У епоху цифрових технологій захист веб – сайтів, організація надійних способів передачі та зберігання даних, особливо конфіденційної інформації, стали важливими аспектами будь-якого бізнесу чи організації і активно розвиваються. Однак, із зростанням залежності від Інтернету ризик кіберзагроз також зріс експоненціально. В комплексних системах захисту інформації широке застосування знайшли стеганографічні методи, принцип роботи яких полягає в створенні скритих каналів зв'язку у вже існуючих потоках даних в інформаційно-телекомунікаційних системах. Задача вибору стеганографічного методу дозволяє вирішити деякі вимоги, що висуваються перед стеганосистемою при її побудові. Однією із найважливіших вимог є забезпечення стійкості стеганосистеми до атак стеганоаналізу. Статистичні методи стеганоаналізу намагаються виявити найменші зміни у статистичній поведінці файла, викликані стеганографічним перетворенням. Суть статистичних методів полягає в оцінюванні ймовірності існування стеганографічного приховування з невідомою стеганосистемою на основі критерію оцінки наближення досліджуваного контейнера до "природнього". Метою роботи є підвищення ефективності стеганосистеми шляхом модифікації методу приховування інформації, розробленого на основі теорії графів. Поставлена мета була досягнута шляхом вводу в зазначений метод блоку знаходження максимального паросполучення. Результатом роботи є розробка модифікованого методу приховування інформації, який можна застосовувати для побудови стеганографічних систем. Ефективність запропонованого методу досягається за рахунок збереження статистик першого порядку контейнера і має кращі показники ніж у метода - прототипа. Значущість результату полягає у підвищені загальної стійкості стеганосистеми до статистичних атак.

Ключові слова: стеганосистема, стеганографічний метод, стійкість стеганосистеми, статистичні методи стеганоаналізу, стеганографічне перетворення

Вступ. Одним з найбільш перспективних підходів до виявлення існування прихованого каналу передачі інформації є підхід, що представляє собою введення прихованої інформації в файл як порушення статистичних законів природних контейнерів. При такому підході аналізуються статистичні характеристики досліджуваного контейнера і встановлюється, чи схожі вони (характеристики) з характеристиками природних контейнерів (якщо так, то прихованої передачі інформації немає), або вони схожі з характеристиками контейнерів з вбудованою інформацією (якщо так, то виявляється факт існування прихованого каналу передачі даних). Цей клас стегоатак є ймовірносним, тобто вони не дають однозначної відповіді, а формують оцінки типу «ця досліджувана послідовність містить приховане повідомлення з ймовірністю 90%». Ймовірнісний характер статистичних методів стегоаналізу не є істотним недоліком, оскільки на практиці ці методи часто дають оцінки ймовірності існування стегоканала, що відрізняються від одиниці або нуля на нескінченно малі значення [1].

У класі статистичних методів стегоаналізу використовується безліч статистичних характеристик, таких як оцінка ентропії, коефіцієнти кореляції, залежності між елементами послідовностей, умовні розподіли, відмінність розподілів за

критерієм хі-квадрат, оцінка числа переходів значень молодших бітів у сусідніх елементах контейнера і багато інших [2,3].

Більшість статистичних атак, як правило, не потребують спеціальних технічних та програмних засобів і високої кваліфікації атакуючого і можуть проводитись без специфічного програмного або технічного забезпечення, без спеціальної підготовки та кваліфікації зловмисника.

Так, наприклад, найпростіші тести оцінюють кореляцію елементів контейнера, в які можуть бути вбудовані приховані повідомлення. Це робить такий і подібний вид атак надзвичайно простим і поширеним, і саме це диктує високу потребу у забезпеченні стійкості прихованого повідомлення до збурних дій викликаних вбудовуванням повідомлення в контейнер.

Програмні інструменти приховування інформації такі як Steganos, Outguess, Jsteg, Jphs, S-Tools та інші прості в використанні і здатні створити стеганографічний канал з великою пропускною здатністю. Ці інструменти, як правило, використовують метод найменшого значущого біта (LSB) та його модифікації, але стеганоконтейнери, які створені за допомогою LSB, успішно виявляються методами стеганоаналізу.

Цей факт призвів до появи цілого ряду робіт, присвячених методам вбудовування в молодший біт без суттєвого порушення закону розподілення бітів.

Наприклад, тривіальною модифікацією методу LSB-replacement є LSB-matching, який випадковим чином змінює піксельні значення на ± 1 так, що молодші біти пікселів відповідають бітам повідомлення, що вбудовується. Завдяки такій модифікації LSB-*matching* стеганоконтейнери набагато важче розпізнаються методами стеганоаналізу.

Вбудовування інформації в контейнер призводить до зміни його характеристик. Ці зміни використовуються методами стеганоаналізу для розпізнавання стеганоконтейнерів.

Чим менше збурень зазнає контейнер під час вбудовування інформації, тим важче стеганоаналітичним методам забезпечити низький рівень похибки при розпізнаванні.

В останній час активно ведуться роботи по створенню стеганографічних методів та алгоритмів, розробники яких намагаються забезпечити найменш можливий вплив на контейнер вбудованої інформації як за рахунок вибору елементів контейнера для вбудовування так і специфіки самого алгоритму [4-7].

Група методів, так звані методи мінімального стеганографічного збурення, значно підвищує стійкість стеганографічних систем.

Отже, якщо забезпечити обмін елементів контейнера, а не їх модифікацію, то тим самим будуть максимально збережені статистичні характеристики контейнера. Саме такий принцип положено в метод представлений в [8].

Постановка задачи. Метою роботи є підвищення ефективності стеганосистеми шляхом модифікації методу приховування інформації, розробленого на основі теорії графів запропонованого в [8].

Для досягнення мети вирішуються задачі.

1. Модифікувати алгоритм знаходження паросполучень, що є основою для модифікації методу [8].
2. Провести оцінку ефективності, зокрема порівняльну, модифікованого і базового методу.

Контейнер, який буде використовуватися для вбудовування інформації позначимо літерою С, а його елементи s_i, тоді $C = \{s_1, ..., s_i, ..., s_n\}$, де n – кількість елементів контейнера, $s_i \in S$ – множина значень.

Визначимо функцію $f:S\to\{0,...,p-1\}$, яка кожному s_i ставить у відповідність залишок від ділення s_i на p, позначимо цю операцію $s_i \oplus p$. Для вбудовування одного елемента повідомлення будемо використовувати не один елемент контейнера, а групу з c елементів так, як це запропоновано в [8]. Такий підхід дає більшу свободу вибору одного елемента з c для модифікації. Таким чином, після розбивки елементів контейнера на $k=\left\lfloor \frac{n}{c} \right\rfloor$ неперетинаючихся груп одержимо структуру $C'=\{c_1,...,c_i,...,c_k\}$, де $c_i=(s_{i1},...,s_{ic})$. Будь-яке $c_i^{'}=f(f(s_{i1})+...+f(s_{ic}))$ визначає деяке значення, яке вже вбудоване в контейнер.

Повідомлення, позначимо його $M=\{m_1,...,m_i,...,m_k\}$ кодуємо за тим же принципом, що й елементи контейнера, тобто $m_i\in\{0,...,p-1\}$. Наприклад, якщо $p=2$, то значеннями m_i є біти.

Вузол графа представляє собою структуру $v_i(X_i,Y_i)$, де $Y_i=(y_{i1},...,y_{ic})$ – i-та група цільових значень, а $X_i=(x_{i1},...,x_{ic})$ – позиції елементів контейнера, які складають Y_i. Вузли створюються тільки у випадку, коли $m_i\neq c_i'$. Використання парослучень побудованого графа дасть можливість зменшити кількість корегованих елементів контейнера і вбудовування інформації буде в більшій мірі відбуватися за рахунок їх обміну.

Як вже відмічалося, що вузли графа створюються тільки у випадку, коли $m_i\neq c_i$, але не зважаючи на це їх кількість є значною.

Так, наприклад, при вбудовуванні повідомлення розміром 1КВ в середньому маємо три тисячі вузлів і до десяти тисяч ребер, а при збільшенні розміру вкладень до 4КВ кількість вузлів відповідно збільшується в чотири рази, а кількість ребер сягає півтора мільйони. Тому автори [8] відмовилися від використання списків суміжності, а запропонували дві структури, які також є громіздкими.

В даній роботі пропонується контейнер розбити на блоки і для кожного блоку будувати граф, розмір якого дозволить використовувати його матрицю суміжності, яка однозначно представляє граф.

Основна частина. Важливим етапом роботи нового стеганографічного алгоритму є знаходження найбільшого парослучення в графі, що є самостійною комбінаторною задачею, яка відноситься до NP-повних і має експоненціальну часову складність. У цьому зв'язку розробляються різні евристики з поліноміальною часовою складністю, які в обмін на зниження часу роботи алгоритму не дають точного розв'язку, тому розробка нових алгоритмів залишається актуальним завданням.

Парослученням (або незалежною множиною ребер) графа G називають множину ребер у якій ніякі два ребра не суміжні.

Парослучення графа G називають максимальним, якщо воно не міститься в жодному парослученні з більшою кількістю ребер, і найбільшим, якщо кількість ребер у ньому найбільша серед усіх парослучень графа G [9].

В роботі пропонується алгоритм знаходження найбільшого парослучення, назвемо його z_blok, на базі матриці суміжності графа, двоїстого до даного.

Розглянемо вихідний граф (рис.1), та побудуємо до нього двоїстий (рис.2) за правилом: вузлами будуть ребра вихідного графа, які позначені номерами від одного до десяти, і два вузли суміжні, якщо ребра, які їм відповідають, також суміжні в вихідному графі, тобто інциндентні одному й тому ж вузлу.

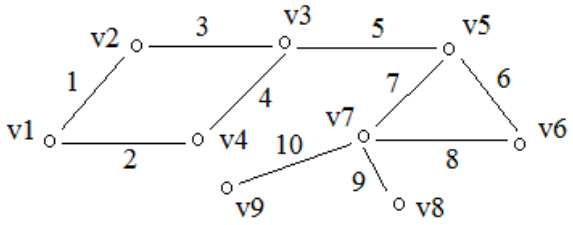


Рис.1. Вихідний граф

Найбільше паросполучення відповідає найбільшій незалежній множині вершин [9].

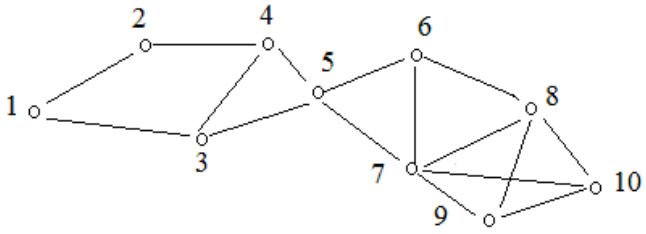


Рис.2. Граф, двоїстий до вихідного

Побудуємо матрицю суміжності A (рис.3) для двоїстого графа.

номер вузла	1	2	3	4	5	6	7	8	9	10
1	X	1	1							
2	1	X		1						
3	1		X	1	1					
4		1	1	X	1					
5			1	1	X	1	1			
6					1	X	1	1		
7					1	1	X	1	1	1
8						1	1	X	1	1
9							1	1	X	1
10							1	1	1	X

Рис.3. Матриця суміжності двоїстого графа

Аналіз матриці суміжності A показує, що якщо, наприклад, строки та стовпці з номерами 1, 4, 6 та 9 (вузли з такими номерами утворюють незалежну множину) переставити так, щоб вони стояли поряд, то на діагоналі матриці утворюється нульовий блок. Отже, матрицю суміжності треба перебудувати так, щоб вона мала блочно-діагональний вигляд. Нульові квадратні блоки будуть відповідати максимальним незалежним множинам вершин.

Алгоритм z_blok :

а) побудувати граф, двоїстий до вихідного з матрицею суміжності $A=(a_{ij})$ розміром $n\times n$;

б) аналізувати пари сусідніх стрічок $(i,i+1)$, i - непарне:

1) $\sum_{j=1}^{i-1} a_{ij} > \sum_{j=1}^{i-1} a_{i+1,j}$,

2) $\sum_{j=1}^{i-1} a_{ij} = \sum_{j=1}^{i-1} a_{i+1,j}$ і $\sum_{j=i+2}^{n} a_{ij} > \sum_{j=i+2}^{n} a_{i+1,j}$,

3) $\sum_{j=1}^{i-1} a_{ij} = \sum_{j=1}^{i-1} a_{i+1,j}$ і $\sum_{j=i+2}^{n} a_{ij} = \sum_{j=i+2}^{n} a_{i+1,j}$ але одиниця в стрічці i до головної діагоналі зустрілася раніше, ніж в стрічці $i+1$;

при виконанні будь-якої умови виконати перестановку стрічок i та $i+1$ та відповідних стовпців;

в) аналізувати пари сусідніх стрічок $(i, i+1)$, i - парне;

виконати перестановку стрічок i та $i+1$ та відповідних стовпців при виконанні однієї з умов представлених у пункті б).

Алгоритм закінчує свою роботу, якщо немає пар $(i, i+1)$, для яких виконуються умови 1) – 3). З побудованих блоків вибрати блок найбільшого розміру, номери стрічок (стовпців), що йому відповідають будуть складати найбільшу незалежну множину двоїстого графа і найбільше паросполучення вихідного.

П'ята ітерація для непарного i являється останньою ітерацією роботи алгоритму z_blok.

Алгоритмом виділено чотири нульові блоки: перший блок розміром 4x4 відповідає вузлам з номерами 1, 6, 9 та 4, другий блок розміром 3x3 відповідає вузлам 10, 2, 3, третій блок розміром 2x2 відповідає вузлам 8, 5, останній блок відповідає вузлу 7 (рис.4). Отже, найбільший блок є шуканим, таким чином, найбільша незалежна множина представлена вузлами 1, 6, 9 ,4 в двоїстому графі і ребра саме з такими номерами є найбільшим паросполученням у вихідному графі.

номер вузла	1	6	9	4	10	2	3	8	5	7
1	X					1	1			
6		X						1	1	1
9			X		1			1		1
4				X		1	1		1	
10			1		X			1		1
2	1			1		X				
3	1			1			X		1	
8		1	1		1			X		1
5		1		1			1		X	1
7		1	1		1			1	1	X

Рис. 4. Матриця суміжності A , i - непарне, п'ята ітерація

Алгоритм вбудовування повідомлення.

Процес вбудовування повідомлення представимо схемою (рис.5), взявши конкретні значення параметрів графової моделі c=3 та p=4 [8].

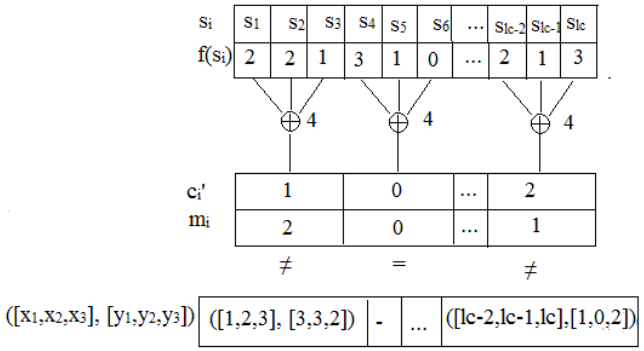


Рис.5. Схема вбудовування повідомлення

Перша стрічка містить елементи контейнера. Друга – визначені значення функцією f. Три (в загальному випадку c) елемента $f(s_i)$ модифікуються завдяки застосуванню операції додавання по модулю 4 (в загальному випадку по модулю p) щоб одержати значення c_i', які порівнюються з елементами повідомлення m_i. Якщо значення не співпали, як в першому та останньому випадку, то створюється вузол, як показано в останній стрічці. Цільові значення вузла [y_1,y_2,y_3] обчислюються додаванням різниці $m_i - c_i'$ до кожного значення $f(s_i)$. Заміна одного з $f(s_i)$ на його цільове значення приведе у відповідність c_i' та m_i.

Розглянемо як створюються ребра [8]. Вище було зазначено, що алгоритм вбудовування переслідує мету в більшій мірі елементи контейнера обмінювати, ніж модифікувати. Розглянемо вузли перший і останній схеми, представленої на рисунку 5. Цільове значення елемента s_1 дорівнює трьом при значенні $f(s_1) = 2$, а елемента s_{lc} дорівнює двом при $f(s_{lc}) = 3$. Якщо різниця їх значень $d = | s_1 - s_{lc} |$ дозволяє обміняти ці елементи місцями, тобто обмін не визве видимого спотворення контейнера, то створюється ребро. Легко помітити, що ребер між двома вузлами може бути декілька, наприклад, також можна створити ребро (s_3, s_{lc-2}) за умови виконання вимоги до різниці їх значень. Це дає більше ступенів свободи для вибору з цих ребер одного, виходячи, наприклад, з мінімальності значення d.

Стеганографічний алгоритм, назвемо його graf_matching, представимо наступними кроками.

Крок 1. Розбиваємо матрицю контейнера – зображення на блоки заданого розміру.

Крок 2. Для кожного блоку будуємо граф G_i, виконуючи дії представлені схемою, зображеною на рисунку 5.

Крок 3. Для побудованого графа G_i будуємо граф, двоїстий до даного G_{di}, який представляється матрицею суміжності.

Крок 4. Знаходимо незалежні множини вузлів на графі G_{di}, використовуючи алгоритм z_blok.

Крок 5. На графі G_i визначаємо найбільше паросполучення.

Крок 6. Для вузлів, які належать найбільшому паросполученню виконуємо обмін елементів контейнера.

Крок 7. Для вузлів, які не належать найбільшому паросполученню виконуємо модифікацію елементів контейнера.

Щоб декодувати повідомлення, вбудоване алгоритмом graf_matching треба розбити матрицю стеганоконтейнера на блоки того самого розміру, що і при вбудовуванні. Використовуючи ті самі значення для параметрів c і p, які використовувалися при вбудовуванні, обчислити $f(s_i)$ та c_i'. Значення c_i' є елементами повідомлення.

Оцінка ефективності модифікованого методу. Для оцінки ефективності модифікованого методу вбудовування повідомлення було проведено обчислювальний експеримент в ході якого була зроблена оцінка алгоритму знаходження паросполучень z_blok шляхом порівняння його з відомими алгоритмами karp-sipser та Куна (табл.1) та порівняльний аналіз модифікованого методу з методом [8] (табл.2).

Таблиця 1.

Визначення частки об'єму контейнера, що підлягає корегуванню P(%)

Контейнер	Алгоритм	Блок 1	P	Блок 2	P	Блок 3	P	Блок 4	P
Autumn.tif									
Кількість елементів		47 - 53		49-57		45-59		50-58	
Кількість паросплучень	karp-sipser	22 - 20	13-3	24-18	21-1	24-19	11-7	28-21	8-2
	куна	21 - 20	13-5	24-17	22-1	24-19	11-7	27-20	10-4
	z_blok	22 - 19	13-3	25-17	20-3	23-20	11-5	28-20	9-2
Canoe.tif									
Кількість елементів	karp-sipser	44-50		43-51		45-60		46-61	
Кількість паросп-чень	karp-sipser	18-19	12-3	18-19	12-2	19-20	12-1	20-21	12-1
	куна	17-19	13-3	18-19	12-2	19-20	10-1	21-22	11-2
	z_blok	18-20	13-3	19-20	11-1	20-21	9-1	22-23	9-1

Як видно з табл.1, z_blok не тільки не гірший за методи karp-sipser і Куна, але і показав кращі результати в деяких випадках. Так, наприклад, блок 2 і блок 4 для контейнера Autumn.tif і блоки 2,3,4 для контейнера **Canoe.tif** вказують на те, що алгоритм z_blok знаходить більше паросполучень і частка об'єму інформації для корегування менша, а отже робота z_blok більш якісна.

Таблиця 2.

Статистичні показники викривлення контейнера

Назва показника	Оригінал	Алгоритм [8]	Graf_matching
Средня абсолютна різниця $\mathrm{AD} = \frac{1}{XY}\sum_{x,y}\left\|C_{x,y} - S_{x,y}\right\|$	0	0,0823	0,0228
Нормована середня абсолютна різниця $\mathrm{NAD} = \frac{\sum_{x,y}\left\|C_{x,y} - S_{x,y}\right\|}{\sum_{x,y}\left\|C_{x,y}\right\|}$	0	3,7577e-04	1,8760e-04
Середньоквадратична помилка $\mathrm{MSE} = \frac{1}{XY}\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2$	0	0,0823	0,0228
Відношення «сигнал/шум» $\mathrm{SNR} = \frac{\sum_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2}$	∞	6,4724e+05	9,3503e+05
Максимальне відношення «сигнал/шум» $\mathrm{PSNR} = \mathrm{XY} \cdot \frac{\max_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2}$	∞	7,1958e+05	2,6918+06

В таблиці 2 наведені деякі статистичні показники, які свідчать про те, що в результаті застосування розробленого методу викривлень контейнера, при вбудовуванні повідомлення, відбувається менше, ніж коли застосовується метод прототип, а отже статистики контейнера зберігаються краще. Це відбувається за рахунок модифікації алгоритму знаходження парасполучень в результаті чого парасполучення знаходяться більш якісно і кількість пікселів, які треба модифікувати, зменшується.

Висновок. В роботі вирішено задачу підвищення ефективності стеганосистеми шляхом розробки модифікації методу вбудовування повідомлення, запропонованого в [8].

В ході модифікації запропоновано поліпшення знаходження максимального парасполучення, як основи алгоритму вбудовування повідомлень на основі теорії графів. Проведено експериментальні дослідження на реальних зображеннях, які використовувалися в якості контейнера та на різних повідомленнях, які кодувалися різноманітним чином. Експериментально доведена більша ефективність розробленого метода в порівнянні з [8]. При застосуванні розробленого методу краще зберігаються статистики першого порядку, а отже можна стверджувати, що статистичному стегааналізу виявити вкладення буде важче, ніж при застосуванні [8].

Результати роботи можуть бути використані для побудови нових стеганографічних систем, стійких до статистичних атак та для розв’язку задач, які зводяться до пошуку парасполучень у графі.

Список літератури

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография/ М.: Солон-Пресс, 2002. 272 с.
2. Швидченко И.В. Методы стеганоанализа для графических файлов. *Штучний інтелект.* 2010. №4. С. 696-705.
3. BÖhme *R.* Advanced statistical steganalysis. Berlin, Heidelberg: Springer-Verlag, 2010.
4. Filler T., Judas J., Fridrich J. Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. *Forensics and Security*. 2011. V. 6(1). P. 920–935.
5. Kodovský J., Fridrich J., Holub V. On Dangers of Overtraining Steganography to an Incomplete Cover Model. *Proc. ACM Multimedia & Security Workshop, Niagara Falls, New York*. 2011. P. 69-76.
6. Filler T., Fridrich J. Gibbs construction in Steganography. *Forensics and Security*. 2010. V.5(4). P. 705-720.
7. Fridrich J., Filler T. Practical methods for minimizing embedding impact in steganography. *Proceedings SPIE, Electronic Imaging, Steganography, and Watermarking of Multimedia Contents IX*. 2007. 6505. P. 2-3.
8. Hetzl S., Mutzel P. A graph-theoretic approach to steganography. *Proc. Communication and Multimedia security*. 2005. P.119-128.
9. Харари Ф. Теория графов, М.:Мир, 1993. С.203.

GRAPH THEORY AS THE BASIS OF METHODS FOR EMBEDDING INFORMATION

I.I. Borysenko, I.S. Vinkovska

National Odesa Polytechnic University
1, Shevchenko Ave, Odesa, 65044, Ukraine
Email: boris_enko63@ukr.net

In today's digital environment, where data leaks and cyberattacks are becoming more common, the task of creation reliable means of information protection is extremely urgent. In the digital age, the protection of websites, the organization of reliable ways to transfer and store data, especially confidential information, have become important aspects of any business or organization and are actively developing. However, with the increase in dependence on the Internet, the risk of cyber threats has also increased exponentially. In complex information security systems, steganographic methods are widely used, the principle of which is to create hidden communication channels in existing data flows in information and telecommunication systems. The problem of choosing a steganographic method allows you to solve some of the requirements put forward for the steganographic system when it is built. One of the most important requirements is to ensure the resistance of the stegosystem to stegoanalysis attacks. Statistical methods of steganoanalysis attempt to detect the slightest changes in the statistical behavior of a file caused by steganographic transformation. The essence of statistical methods is to assess the probability of the existence of the steganographic of hiding of an unknown stegano system based on the criterion for assessing the approh of the study container to the "natural" one. The purpose of the work is to increase the efficiency of the stegan system by modifying the method of hiding information developed on the basis of graph theory. The goal was achieved by entering the maximum steam combination block into the specified method. The result of the work is the development of a modified method of hiding information, which can be used to build steganographic systems. The effectiveness of the proposed method is achieved by preserving the first-order statistics of the container and has better performance than that of the prototype method. The significance of the result lies in increasing the overall resistance of the hip system to statistical attacks.

Keywords: steganosystem, steganographic method, steganosystem stability, statistical methods of steganoanalysis, steganographic transformation

DOI 10.15276/imms.v15.no1.48
УДК 004.946:681.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 48-57

РЕГРЕСІЙНА МОДЕЛЬ НАПРУГИ АКУМУЛЯТОРНОЇ БАТАРЕЇ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ЧАСОВИХ ТА ТЕМПЕРАТУРНИХ ДАНИХ

В.В. Жуковський[1], О.Б. Москаль[2], Н.А. Жуковська[3]

Національний університет водного господарства та природокористування
11, вул. Соборна, м. Рівне, 33028, Україна
Emails: v.v.zhukovskyy@nuwm.edu.ua[1], o.b.moskal@nuwm.edu.ua[2]
n.a.zhukovska@nuwm.edu.ua[3]

В умовах стрімкого розвитку технологій Інтернету речей (IoT) та їхнього широкого впровадження, забезпечення надійного і тривалого функціонування автономних пристроїв стає першочерговим завданням. Багато таких пристроїв живляться від акумуляторних батарей, часто у комбінації з сонячними панелями. Їх ефективність пристроїв суттєво залежить від зовнішніх факторів, таких як час доби і температура. Дана робота присвячена дослідженню залежності напруги акумуляторної батареї автономного IoT пристрою від цих двох ключових факторів. Метою наукового дослідження було створення математичної моделі, що встановлює аналітичну залежність між напругою акумуляторної батареї, часом доби (в годинах UTC) та температурою навколишнього середовища (°C). Наукова значущість роботи полягає у поглибленні розуміння впливу зовнішніх факторів на енергетичні характеристики автономних IoT пристроїв, що працюють на відновлюваних джерелах енергії. Практична цінність полягає у створенні інструменту для прогнозування стану батареї, що може бути використано для підвищення надійності та ефективності систем моніторингу на базі IoT.Для досягнення мети було використано метод покрокової регресії. На першому етапі, з використанням функції linfit у середовищі Mathcad, було побудовано степеневі функції, що апроксимують залежність напруги від часу доби для різних температурних діапазонів. На другому етапі, коефіцієнти цих степеневих функцій були апроксимовані поліноміальними функціями другого порядку, залежними від температури. Для побудови моделі було використано емпіричні дані, зібрані з реального IoT пристрою Tank Toad, що виконує моніторинг рівня води, а також дані про погодинні температури з веб-ресурсу open-meteo.com за період з 1 вересня 2024 року по 10 лютого 2025 року. Дані про погоду було відфільтровано, щоб включити лише нічний час доби та дні з низьким рівнем хмарності, мінімізуючи вплив підзарядки від сонячних панелей. Основним результатом роботи є узагальнена регресійна модель, що представлена у вигляді аналітичного виразу, який дозволяє обчислити напругу батареї як функцію часу та температури. Оцінка точності моделі показала відносну похибку 1.37% для контрольної точки, що свідчить про задовільну апроксимацію. Висновки дослідження підтверджують значущість часу доби та температури як факторів, що впливають на розряд акумуляторної батареї. Цінність проведеного дослідження полягає у розробці практичного інструменту для моделювання енергетичних характеристик автономних IoT пристроїв, що може сприяти створенню більш енергоефективних та надійних систем. Отримана регресійна модель може бути використана в системах моніторингу для прогнозування стану батареї, адаптивного керування частотою передачі даних, раннього виявлення аномалій та оптимізації роботи пристроїв.

Ключові слова: Інтернет речей (IoT), автономний пристрій, регресійна модель, апроксимація, степенева функція, поліноміальна функція, акумуляторна батарея.

Вступ. Впровадження технологій інтернету речей (IoT) у різноманітні галузі, включаючи моніторинг навколишнього середовища та управління ресурсами, вимагає забезпечення надійної та довготривалої роботи автономних пристроїв. Особливо актуальним є питання енергоефективності та прогнозування стану джерел живлення таких пристроїв, зокрема, акумуляторних батарей, що часто використовуються у поєднанні з відновлюваними джерелами енергії, такими як сонячні панелі.

Розглядається клас автономних IoT пристроїв Tank Toad, призначених для вимірювання рівня води у резервуарах [1; 2]. Живлення цих пристроїв забезпечується від акумуляторних батарей, що підзаряджаються сонячними панелями. Ефективність роботи сонячних панелей, а отже і процес заряду батареї, суттєво залежить від зовнішніх факторів, насамперед від інтенсивності сонячного випромінювання та температури навколишнього середовища. Зокрема, низька інтенсивність сонячного випромінювання (наприклад, у похмурі дні) та екстремальні температури можуть значно впливати на динаміку заряду/розряду акумуляторної батареї та, як наслідок, на працездатність пристрою. Відомо, що при досягненні напруги 12.6 В пристрій переходить у режим енергозбереження, а при зниженні напруги до 12.0 В – вимикається, що може призвести до перерв у зборі даних та функціонуванні системи моніторингу в цілому.

Враховуючи зазначені фактори, актуальною науково-практичною задачею є розробка моделі для прогнозування напруги акумуляторної батареї автономних IoT пристроїв на основі даних про час доби та температуру навколишнього середовища. Така модель дозволить не тільки краще зрозуміти вплив зовнішніх факторів на енергоспоживання та стан батареї, але й створити основу для розробки інтелектуальних систем моніторингу та управління енергоспоживанням пристроїв. Зокрема, точне прогнозування напруги батареї може бути використано для:

- оптимізації частоти передачі даних. Адаптивне регулювання частоти оновлення даних в залежності від прогнозованого рівня заряду батареї, особливо у періоди низької сонячної активності,
- раннього виявлення аномалій. Ідентифікація відхилень фактичної напруги від прогнозованих значень, що може сигналізувати про несправності в системі живлення або зміну умов експлуатації.
- прогнозування терміну служби батареї. Оцінка залишкового ресурсу акумуляторної батареї на основі динаміки її розряду та прогнозованих зовнішніх умов.

Метою даної роботи є побудова регресійної моделі, що встановлює залежність напруги акумуляторної батареї автономного IoT пристрою від часу доби та температури навколишнього середовища. Для досягнення поставленої мети планується використовувати набір емпіричних даних, отриманих від реальних пристроїв моніторингу рівня води та застосувати методи регресійного аналізу для ідентифікації та верифікації моделі. Отримані результати матимуть важливе значення для розробки енергоефективних та надійних систем IoT моніторингу, що працюють в автономному режимі з використанням відновлюваних джерел енергії.

Огляд наукових джерел. У наукових джерелах досліджується проблема прогнозування швидкості зниження ємності акумуляторних батарей на основі даних, отриманих під час заряджання. Автори [3] пропонують лінійну регресійну модель, навчання якої здійснюється на часових та електричних даних, що відповідають різним режимам роботи батареї (заряджання, розряджання, режим простою). Модель відзначається високою точністю та низькими обчислювальними витратами, що дозволяє використовувати її в режимі реального часу для прогнозування зниження ємності.

Інші науковці концентруються на розробці методу оцінки стану здоров’я (SoH) батарей, який враховує варіабельність швидкого заряджання за допомогою аналізу характерних ознак, отриманих з зарядних профілів [4]. Цікавими є роботи, де розглядаються температурно-орієнтовані стратегії оптимізації енергоспоживання в гібридних електротранспортних системах [5].

У підсумках, більшість досліджень зосереджена на оцінці стану здоров’я батарей (SoH) для забезпечення оптимальної роботи та безпеки батарей [6]. Проте наш підхід відрізняється тим, що ми прагнемо побудувати регресійну модель, орієнтовану на майбутнє інтелектуальне керування IoT-пристроями Tank Toad, яка, окрім

прогнозування зниження ємності, також дозволятиме своєчасно виявляти аномалії в роботі енергетичних систем.

Збір емпіричних даних. Для дослідження впливу температури на динаміку розряду акумуляторної батареї автономного IoT пристрою в умовах мінімізованого впливу сонячного випромінювання, було використано історичні дані погодинних температур на висоті 2 метри та загальної хмарності, отримані за допомогою API механізму з веб-ресурсу історичних погодних даних open-meteo.com для регіону де встановлений IoT пристрій (штат Вайомінг, США) [7]. Для стандартизації часових міток, час у метеорологічних даних було конвертовано до формату GMT0. Було відібрано виключно дані, що відповідають годинам з ясною та сонячною погодою, з метою зосередження на впливі температури після періоду максимального заряду батареї протягом дня. Для цього було критерій "сонячного дня", що визначався як день, що передує ночі, із загальною хмарністю ("Cloud cover Total") не вище 20% протягом світлового дня (з 08:00 до 18:00 MST). Даний параметр "Cloud cover Total" є доступний на веб-ресурсі open-meteo.com.

Одночасно, з внутрішньої бази даних системи моніторингу TankToad було отримано відповідні погодинні вимірювання напруги акумуляторної батареї пристрою Tank Toad AC-2 за період з 1 вересня 2024 року по 10 лютого 2025 року (табл.1).

Таблиця 1.

Емпіричні значення напруги акумуляторної батареї та відповідних температур навколишнього середовища

Година (UTC)	-21..-14(°C)	-14..-7 (°C)	-7..0(°C)	0..+7(°C)
0	13.42	13.44	13.58	13.74
1	13.11	13.16	13.19	13.31
2	13.06	13.12	13.14	13.35
3	13	13.08	13.11	13.29
4	12.98	13.04	13.07	13.15
5	12.96	13.02	13.04	13.14
6	12.94	13.02	13.01	13.12
7	12.92	13	12.99	13.01
8	12.91	12.99	12.96	12.99
9	12.9	12.98	12.93	12.98
10	12.88	12.96	12.92	12.96
11	12.86	12.96	12.9	12.92
12	12.85	12.97	12.89	12.89
13	12.84	12.96	12.88	12.88
14	12.83	12.96	12.86	12.86

Для аналізу було відібрано виключно дані за нічний час, що охоплює період від заходу до сходу сонця у Вайомінгу, з метою мінімізації впливу підзарядки від сонячних панелей. З метою узагальнення температурних значень та створення компактної матриці даних, діапазон температур було розділено на чотири інтервали: -21°C до -14°C, від -14°C до -7°C, від -7°C до 0°C, та від 0°C до +7°C. Для кожної години доби та кожного температурного інтервалу було обчислено середнє значення напруги акумуляторної батареї, що дозволило сформувати усереднену таблицю залежності напруги від години доби та температурного діапазону.

Таким чином, підготовлений набір усереднених даних, представлений у табличній формі, дозволяє дослідити залежність напруги акумуляторної батареї від узагальненої температури навколишнього середовища в умовах нічного режиму роботи пристрою, коли основним фактором розряду є час роботи пристрою та температурні умови.

Визначення математичної залежності поверхні. В рамках дослідження з метою визначення аналітичного виразу для опису складної поверхні, що представлена

дискретним набором даних, було застосовано метод регресійного аналізу [8; 9]. Першим етапом цього процесу є апроксимація даних першого стовпця таблиці 1 за допомогою степеневої функції. Цей підхід базується на припущенні про потенційну степеневу природу залежності досліджуваної величини від першого аргументу. Для полегшення математичних викладок зменшимо кількість годин в таблиці 1 до 8-ми. Нову отриману матрицю назвемо матрицею Q . Тобто матриця Q містить усереднені значення напруги акумуляторної батареї для кожної години доби в межах певних температурних діапазонів (бінів). Перший стовпець цієї матриці, який будемо апроксимувати, відповідає першому температурному біну, а саме діапазону від -21°C до -14°C.

Для апроксимації першого стовпця даних було обрано степеневу функцію наступного вигляду:

$$F_c(x) = a_1 \cdot x^{0.5} + b_1 \cdot x + c_1 \tag{1}$$

де $F_c(x)$ – апроксимуюча функція, що залежить від змінної x, яка в даному контексті представляє годину доби (UTC).

x – незалежна змінна, що відповідає годинам доби.

a_1, b_1, c_1 – коефіцієнти регресії, які необхідно визначити.

Для визначення оптимальних коефіцієнтів a_1, b_1 та c_1 було використано метод лінійної регресії за допомогою функції *linfit* у програмному середовищі Mathcad. Функція *linfit* мінімізує суму квадратів відхилень між значеннями напруги першого стовпця матриці Q та значеннями, передбаченими апроксимуючою функцією $F_c(x)$.

Синтаксис виклику функції *linfit* у середовищі Mathcad:

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} := \text{linfit}(X, Q^{\langle 0 \rangle}, F_c)$$

де X – вектор незалежних змінних, що відповідає вектору годин доби,

$Q^{\langle 0 \rangle}$ – вектор залежних змінних, що відповідає першому стовпцю матриці Q вхідних даних тобто усередненим значенням напруги акумуляторної батареї для температурного діапазону -21°C до -14°C. Символ $\langle 0 \rangle$ в Mathcad позначає вилучення нульового стовпця (першого стовпця з індексацією від нуля),

F_c – задана функція, що визначає форму апроксимуючої залежності.

В результаті застосування функції *linfit* до першого стовпця матриці Q були отримані наступні значення коефіцієнтів регресії:

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} -0.33525417 \\ 0.05702230 \\ 13.41265020 \end{pmatrix} \tag{2}$$

Таким чином, апроксимуюча степенева функція для першого стовпця матриці Q набуває вигляду (значення коефіцієнтів округлено до двох знаків після коми для зручності представлення):

$$f_{pwr}(x) = -0.335 \cdot x^{0.5} + 0.057 \cdot x + 13.413 \tag{3}$$

На рисунку 1 відображено емпіричні значення напруги акумуляторної батареї для температурного діапазону -21°C до -14°C (позначені як $Q^{\langle 0 \rangle}$) та відповідну апроксимуючу степеневу функцію $f_{pwr}(x)$. Візуальний аналіз підтверджує високу якість наближення, демонструючи близьку відповідність між теоретичною моделлю та експериментальними даними.

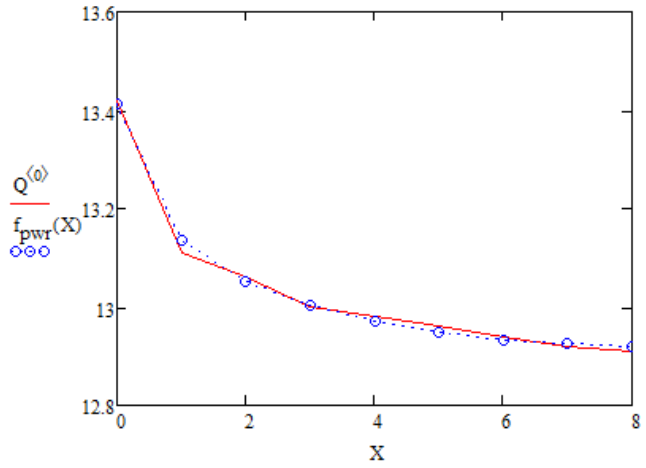


Рис. 1. Графічне представлення апроксимації першого стовпця матриці даних степеневою функцією.

Для кількісної оцінки ступеня кореляції між емпіричними та модельними значеннями було розраховано коефіцієнт кореляції Пірсона, значення якого склало corr $(Q^{\langle 0\rangle}, f_{pwr}(X)) = 0.99721$. Значення коефіцієнта кореляції, близьке до 1, свідчить про високий ступінь відповідності між апроксимуючою функцією та емпіричними даними, що можна кваліфікувати як ідеальне наближення.

Ітераційна апроксимація стовпців матриці даних та формування матриці коефіцієнтів регресії. Для розширення моделі апроксимації на всю досліджувану поверхню, наступним кроком є застосування процедури лінійної регресії до кожного стовпця матриці Q. Цей підхід дозволяє дослідити, як змінюються коефіцієнти степеневої функції при переході від одного температурного діапазону до іншого, тобто, при зміні другого аргументу залежності, представленого вектором Y^T.

З метою автоматизації процесу апроксимації кожного стовпця матриці Q степеневою функцією, було розроблено програмний алгоритм, реалізований у середовищі Mathcad. Алгоритм базується на ітераційному застосуванні функції *linfit* до кожного стовпця матриці даних.

Опис алгоритму ітераційної апроксимації.

1. Ініціалізація матриці коефіцієнтів. На початку роботи алгоритму створюється матриця R_h, призначена для зберігання коефіцієнтів регресії, отриманих для кожного стовпця матриці Q. Розмірність матриці R_h визначається як $3 \times n$, де 3 відповідає кількості коефіцієнтів степеневої функції (a_1, b_1, c_1), а n – кількості стовпців у матриці Q.

2. Циклічна обробка стовпців. Для обробки кожного стовпця матриці Q застосовується цикл *for* з індексом ітерації i, що змінюється від 0 до $n-1$, де n – кількість стовпців матриці Q. На кожній ітерації i обробляється i-й стовпець матриці Q, позначений як $Q^{\langle i\rangle}$.

3. Апроксимація поточного стовпця. На кожній ітерації циклу, для i-го стовпця матриці Q ($Q^{\langle i\rangle}$), виконується процедура лінійної регресії за допомогою функції *linfit*. Функція *linfit* використовує вектор незалежних змінних X (що відповідає вектору годин доби) та вектор залежних змінних $Q^{\langle i\rangle}$ (що представляє собою i-й стовпець матриці Q та відповідає усередненим значенням напруги для відповідного температурного діапазону), а також задану степеневу функцію F_c. Результатом роботи

функції *linfit* є вектор коефіцієнтів $\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix}$, що забезпечують оптимальну апроксимацію даних i-го стовпця матриці Q степеневою функцією $F_c(x)$.

4. Збереження коефіцієнтів у матриці. Отримані на кожній ітерації коефіцієнти a_1, b_1, c_1 зберігаються у відповідному стовпці матриці R_h. Зокрема, елементу $R_{0,i}$ присвоюється значення a_1, $R_{1,i}$ – значення b_1, та $R_{2,i}$ – значення c_1.

5. Завершення циклу. Після завершення ітерацій для всіх стовпців матриці Q, матриця R_h міститиме набір коефіцієнтів степеневої функції, отриманих для кожного температурного діапазону.

Матриця коефіцієнтів регресії R_h:

Таким чином, після в результаті виконання описаного алгоритму, було отримано матрицю коефіцієнтів регресії R_h, представлену наступному у вигляді:

$$R_h = \begin{pmatrix} -0.335 & -0.301 & -0.385 & -0.322 \\ 0.057 & 0.052 & 0.064 & 0.026 \\ 13.413 & 13.433 & 13.563 & 13.713 \end{pmatrix} \quad (4)$$

Кожен стовпець матриці R_h відповідає певному температурному діапазону (стовпцю матриці Q) та містить коефіцієнти a_1, b_1, c_1 степеневої функції, що найкраще апроксимує залежність напруги від часу доби в межах цього діапазону температур.

Апроксимація коефіцієнта a_1 поліноміальною функцією залежно від температури. На попередньому етапі, в результаті ітераційної апроксимації стовпців матриці даних, було отримано матрицю коефіцієнтів регресії (4). Для побудови узагальненої моделі, що описує залежність поверхні від двох змінних, необхідно встановити аналітичний вираз для коефіцієнтів регресії як функцій від другого аргументу, яким у нашому випадку виступає температура. На даному кроці зосередимося на апроксимації першого рядка матриці (4), що містить коефіцієнти a_1, поліноміальною функцією.

Для апроксимації залежності коефіцієнта a_1 від температури було обрано поліноміальну функцію другого порядку $f_a(x)$. Вибір поліноміальної функції зумовлений її гнучкістю та здатністю апроксимувати широкий спектр залежностей. Функція $f_a(x)$ має наступний вигляд:

$$f_a(x) = C_{a11} + C_{a12} \cdot x + C_{a13} \cdot x^2 \quad (5)$$

де $f_a(x)$ – апроксимуюча функція для коефіцієнта a_1, що залежить від змінної x, яка в даному контексті представляє середнє значення температури для відповідного температурного діапазону; x – незалежна змінна, що відповідає середнім значенням температури для кожного температурного біну, вектор яких позначено як Y_t; C_{a11}, C_{a12}, C_{a13} – коефіцієнти поліноміальної регресії, які необхідно визначити.

Для визначення коефіцієнтів C_{a11}, C_{a12}, C_{a13}, що забезпечують найкраще наближення поліноміальної функції $f0_{par}(x)$ до емпіричних значень коефіцієнта a_1, було застосовано функцію *linfit* у середовищі Mathcad. Синтаксис виклику функції *linfit* для апроксимації коефіцієнта a_1 є наступним:

$$\begin{pmatrix} C_{a11} \\ C_{a12} \\ C_{a13} \end{pmatrix} := \text{linfit}(Y_t, (R_h^T)^{\langle 0 \rangle}, F_d) \tag{6}$$

де Y_t – вектор незалежних змінних, що відповідає вектору середніх значень температури для кожного температурного біну, транспонований ($Y_t = Y^T$), $(R_h^T)^{\langle 0 \rangle}$ – вектор залежних змінних, що відповідає першому рядку транспонованої матриці R_h, тобто, вектору коефіцієнтів a_1, отриманих для кожного температурного біну, F_d – функція, що визначає вектор базисних функцій для поліноміальної регресії другого порядку: $F_d(x) = \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix}$.

Для графічної оцінки якості апроксимації коефіцієнта a_1 поліноміальною функцією $f_a(yt)$, побудовано рисунок, де представлено залежність емпіричних значень коефіцієнта a_1 (позначені як $(R_h^T)^{\langle 0 \rangle}$) та апроксимуючу функцію $f_a(yt)$. Візуальний аналіз графічного представлення дозволяє оцінити ступінь відповідності поліноміальної моделі до дискретних значень коефіцієнта a_1. Як видно з рисунка 2, апроксимуюча функція досить точно відтворює загальну тенденцію зміни коефіцієнта a_1 залежно від температури, хоча і не є ідеальною апроксимацією в кожній точці.

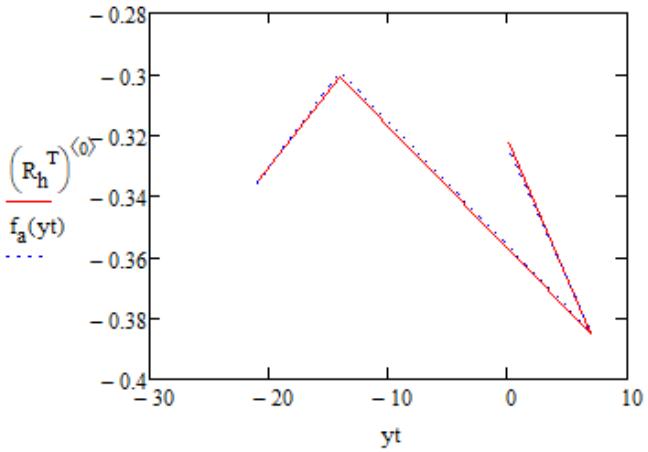


Рис. 2. Графічне представлення апроксимації коефіцієнта a_1 поліноміальною функцією

Аналогічним чином, на наступних етапах дослідження було здійснено апроксимацію коефіцієнтів b_1 та c_1 (другий та третій рядки матриці R_h) поліноміальними функціями другого порядку, які будуть позначені як $f_b(x)$ та $f_c(x)$ відповідно. Отримані поліноміальні вирази для коефіцієнтів a_1, b_1 та c_1 як функцій від температури використані для формування узагальненої математичної моделі поверхні залежності напруги акумуляторної батареї від часу доби та температури навколишнього середовища.

На основі отриманих коефіцієнтів поліноміальних апроксимацій, узагальнююча математична модель для опису досліджуваної поверхні залежності напруги акумуляторної батареї ($f_{surface}(X,Y)$) від часу доби (X) та температури (Y) представлена наступним рівнянням:

$$f_{surface}(X,Y) = (C_{a11} \cdot Y + C_{a12} \cdot Y^2 + C_{a13}) \cdot \sqrt{X} + \\ +(C_{b11} \cdot Y + C_{b12} \cdot Y^2 + C_{b13} \cdot) \cdot X \\ +(C_{c11} \cdot Y + C_{c12} \cdot Y^2 + C_{c13}) \quad (7)$$

де: X – час доби (UTC).

Y – температура навколишнього середовища (°C).

C_{a11}, C_{a12}, C_{a13}, C_{b11}, C_{b12}, C_{b13}, C_{c11}, C_{c12}, C_{c13} – числові значення коефіцієнтів поліноміальної регресії, отримані вище.

Підставляючи у рівняння (7) отримані числові значення коефіцієнтів поліноміальної регресії, модель поверхні набуває вигляду:

$$f_{surface}(X,Y) = (-0.00638 \cdot Y - 0.00033 \cdot Y^2 - 0.32353) \cdot \sqrt{X} + \\ +(0.00188 \cdot Y + 0.00015 \cdot Y^2 + 0.03774) \cdot X + \\ +(0.00014 \cdot Y - 0.00058 \cdot Y + 13.63141) \quad (8)$$

Для кількісної оцінки точності отриманої узагальнюючої моделі, було проведено розрахунок відносної похибки апроксимації для контрольної точки з координатами $(X = 3, Y = 7)$. Розраховане за моделлю значення напруги склало $f_{surface}(3,7) = 13.112$ В. Порівняння цього значення з емпіричним значенням напруги для аналогічних умов дозволило оцінити відносну похибку моделі, яка становить 1.37453%. Таке значення похибки свідчить про задовільну точність отриманої моделі та її придатність для опису досліджуваної залежності напруги акумуляторної батареї від часу доби та температури.

Для візуальної оцінки адекватності отриманої регресійної моделі, на рис. 3 представлено графік поверхні, що відображає залежність напруги акумуляторної батареї, передбачену моделлю, від часу доби та температури. На тому ж графіку накладено емпіричні значення для порівняння.

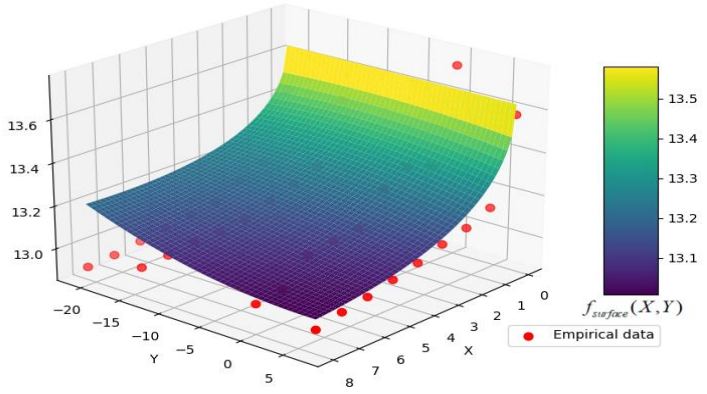


Рис. 3. Графік поверхні регресійної моделі у порівнянні з емпіричними вимірюваннями

Висновок. У даній роботі було успішно розроблено регресійну модель, що описує залежність напруги акумуляторної батареї автономного IoT пристрою від часу доби та температури навколишнього середовища. В рамках дослідження було зібрано масив емпіричних даних, що включав погодинні значення температури, отримані з веб-ресурсу open-meteo.com та відповідні вимірювання напруги акумуляторної батареї, зафіксовані від реального IoT пристрою протягом періоду з 1 вересня 2024 року по 10 лютого 2025 року. Для побудови регресійної моделі застосовано метод покрокового регресійного аналізу, що включав апроксимацію стовпців матриці даних степеневою функцією та подальшу поліноміальну апроксимацію коефіцієнтів регресії. Усі обчислення та аналіз даних було виконано у програмному середовищі Mathcad. Оцінка точності отриманої моделі продемонструвала задовільну відповідність емпіричним даним з відносною похибкою в контрольній точці на рівні 1.37%, що свідчить про

потенційну придатність розробленої моделі для практичних застосувань, зокрема, у задачах прогнозування стану акумуляторних батарей та оптимізації енергоспоживання автономних пристроїв інтернету речей. Отримані результати підкреслюють значущість часових та температурних факторів у динаміці розряду акумуляторних батарей та створюють основу для подальших досліджень у напрямку розробки інтелектуальних систем управління енергоспоживанням автономних IoT пристроїв, що працюють на відновлюваних джерелах енергії.

Список літератури

1. Zhukovskyy V., Printz D., Zhukovska N., Hubach M., Rajab H. IoT based Intelligent Information-Analytical System Architecture for Water Tank Monitoring. *International Conference on Information Technology (ICIT)*. 2021. P. 924–928.
2. Zhukovskyy V., Printz D., Zhukovska N. Human-Computer Interaction in IoT System for Water Tank Monitoring and Controlling. *IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*. 2023. P. 1–5.
3. Vedel P., Hubka L. Linear Regression Model of Li-Ion Battery Capacity Losing Rate Based on Equivalent Circuit Model Parameters and Operation Modes. *International Conference on Smart Systems and Technologies (SST)*. 2022. P. 243–248.
4. Acquarone M., Miretti F., Giuliacci T.A., Duque J., Misul D.A., Kollmeyer P. Regression based battery state of health estimation for multiple electric vehicle fast charging protocols. *Journal of Power Sources*. V. 624, 2024, P. 235601. DOI: 10.1016/j.jpowsour.2024.235601.
5. Acquarone M., Anselma P.G., Miretti F., Misul D. Battery temperature aware equivalent consumption minimization strategy for mild hybrid electric vehicle powertrains. *IEEE Vehicle Power and Propulsion Conference (VPPC)*. 2022, pp. 1–6.
6. Paul S., Ray S. Comparative Study of Different Regression Models for Estimating Lithium Ion Battery Pack Capacity. *IEEE 3rd Applied Signal Processing Conference (ASPCON)*. 2023. P. 161–165.
7. Free Open-Source Weather API Open-Meteo.com. URL: https://open-meteo.com/
8. Kuzlo M., Moshynskyi V., Zhukovska N., Zhukovskyy V. Deformations of soil masses under the action of human-induced factors. *IAPGOS*, V. 14. No. 1, 2024. P. 111–114, URL: doi: 10.35784/iapgos.5824.
9. Zhukovskyy V., Bachyshyna L., Zhukovska N., Mykhailova Y. Regression analysis of grain production transformation in western, central and steppe regions of Ukraine. *11th International Conference on Simulation and Modelling in the Food and Bio-Industry (FOODSIM)*. 2020. З. 197–200.

REGRESSION MODEL OF THE BATTERY VOLTAGE OF THE INTERNET OF THINGS DEVICES BASED ON TIME AND TEMPERATURE DATA

V.V. Zhukovskyy[1], O.B. Moskal[2], N.A. Zhukovska[3]

National University of Water and Environmental Engineering
11, Soborna St., Rivne, 33028, Ukraine
Emails: v.v.zhukovskyy@nuwm.edu.ua[1], o.b.moskal@nuwm.edu.ua[2],
n.a.zhukovska@nuwm.edu.ua[3]

With the rapid development of Internet of Things (IoT) technologies and their widespread adoption, ensuring the reliable and long-term operation of autonomous devices is becoming a top priority. Many such devices are powered by batteries, often in combination with solar panels. Their efficiency depends heavily on external factors such as time of day and temperature. This paper is devoted to the study of the dependence of the battery voltage of an autonomous IoT device on these two key factors. The purpose of the research was to create a mathematical model that establishes an analytical relationship between the battery voltage, time of day (in UTC hours), and ambient temperature (°C). The scientific significance of the work is to deepen the understanding of the impact of external factors on the energy characteristics of autonomous IoT devices running on renewable energy sources. The practical value lies in the creation of a tool for predicting the state of the battery, which can be used to improve the reliability and efficiency of IoT-based monitoring systems. To achieve this goal, a stepwise regression method was used. At the first stage, using the linfit function in Mathcad, power functions were constructed to approximate the voltage dependence on the time of day for different temperature ranges. At the second stage, the coefficients of these power functions were approximated by second-order polynomial functions depending on temperature. To build the model, we used empirical data collected from a real IoT device, Tank Toad, which monitors water levels, as well as hourly temperature data from the open-meteo.com website for the period from September 1, 2024, to February 10, 2025. The weather data was filtered to include only nighttime and low cloud days, minimizing the impact of solar panel recharging. The main result of the work is a generalized regression model presented in the form of an analytical expression that allows calculating the battery voltage as a function of time and temperature. The model accuracy assessment showed a relative error of 1.37% for the control point, which indicates a satisfactory approximation. The conclusions of the study confirm the importance of time of day and temperature as factors affecting battery discharge. The value of this study lies in the development of a practical tool for modeling the energy characteristics of autonomous IoT devices, which can contribute to the creation of more energy-efficient and reliable systems. The resulting regression model can be used in monitoring systems to predict the state of the battery, adaptively control the data rate, detect anomalies early, and optimize device performance.

Keywords: Internet of Things (IoT), autonomous device, regression model, approximation, power function, polynomial function, battery.

DOI 10.15276/imms.v15.no1.58
УДК 004.942

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp.58-70

МАТЕМАТИЧНА МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ НА ОСНОВІ МЕТОДУ FUZZY TOPSIS

О.Я. Ковальчук[1], Л.В. Бабала[1], Р.І. Іваницький[2]

[1]Західноукраїнський національний університет
11, Львівська вул., м. Тернопіль, 46009, Україна
[2]Тернопільський національний педагогічний університет імені Володимира Гнатюка
2, М. Кривоноса вул., м. Тернопіль, 46027, Україна
Emails: olhakov@gmail.com, ludaduma7@gmail.com, romikiv@ukr.net

У статті представлено модель прийняття рішень на основі методу нечіткого TOPSIS для оцінювання ефективності впровадження інтелектуальних технологій запобігання злочинності в комплексну інформаційну систему правоохоронних органів України. Здійснено класифікацію інтелектуальних технологій запобігання злочинності та виділено три основні категорії: інтегровані технології операційного контролю, технології відеоаналізу та технології датчиків IoT. Визначено ключові елементи інтелектуальних технологій, які включають системи відеоспостереження з аналізом відео, розпізнавання облич та номерних знаків, інтелектуальні датчики руху та тривоги, інтеграцію з системами екстреного реагування, аналітику даних для виявлення кримінальних патернів. Запропоновано сім критеріїв оцінювання: ефективність запобігання злочинності, відповідність політиці запобігання злочинності, конкурентоспроможність, розвиток сектора послуг, економічна життєздатність, застосовність у галузі та ефективність управління. Визначено сім альтернативних технологічних рішень та розроблено математичний апарат для реалізації нечіткого TOPSIS з використанням трикутних нечітких чисел. Побудовано трирівневу ієрархічну структуру моделі оцінювання, яка дозволяє здійснювати обґрунтований вибір технологічних рішень з урахуванням множини критеріїв та невизначеності експертних оцінок. Практична значущість роботи полягає у можливості використання розробленої моделі для оптимізації архітектури комплексної інформаційної системи правоохоронних органів шляхом аналізу продуктивності різних конфігурацій. Наукова новизна роботи полягає в розробці моделі прийняття рішень, яка, на відміну від існуючих підходів, враховує невизначеність експертних оцінок та дозволяє здійснювати багатокритеріальний аналіз альтернативних технологічних рішень. Запропоновано класифікацію інтелектуальних технологій запобігання злочинності та визначено їх ключові елементи, що створює теоретичне підґрунтя для подальших досліджень у цій сфері. Подальші дослідження можуть бути спрямовані на практичну апробацію розробленої моделі, вдосконалення системи критеріїв оцінювання та розширення множини альтернативних технологічних рішень.

Ключові слова: інтелектуальні технології, запобігання злочинності, fuzzy TOPSIS, прийняття рішень, штучний інтелект, IoT-пристрої, відеоаналітика.

Вступ. Традиційні підходи до боротьби зі злочинністю, які зосереджені переважно на реагуванні та управлінні після скоєння злочину, поступово втрачають свою ефективність [1]. Стрімкий розвиток інформаційних технологій (IT) та впровадження IoT-пристроїв у міську інфраструктуру, поряд із використанням інноваційних технологій правопорушниками для скоєння злочинів, вимагають більш збалансованого підходу до забезпечення суспільної безпеки [2]. Пріоритетними у боротьбі зі злочинністю стали превентивні заходи безпеки та використання передових технологій запобігання злочинності для прогнозування злочинів, реагування у реальному часі та управління після скоєння злочину, що суттєво підвищує рівень суспільної безпеки [3].

Однак, разом із впровадженням інноваційних рішень виникає необхідність у новому підході до оцінювання ефективності імплементації таких інновацій, особливо за умов сучасної технологічної війни. Традиційні методи оцінки не здатні повною мірою охопити багатовимірність та складність сучасних інтелектуальних систем прийняття рішень щодо прогнозування злочинності [4]. Одним із дієвих інструментів може стати модель на основі методу fuzzy TOPSIS, який забезпечує можливість враховувати невизначеність та багатокритеріальність при оцінюванні ефективності систем запобігання злочинності [5]. Такий підхід забезпечує більш точну та об'єктивну оцінку, що є критично важливим для прийняття обґрунтованих рішень щодо впровадження інтелектуальних систем у сфері запобігання злочинності.

Представлена стаття є продовженням серії робіт щодо проблем розробки інноваційної методології застосування сучасних ІТ для підвищення ефективності прийняття рішень щодо запобігання, прогнозування та розслідування кримінальних злочинів в Україні [5–11].

Огляд літератури. Питання впровадження інноваційних ІТ для підвищення ефективності боротьби зі злочинністю останнім часом були предметом наукових розвідок окремих авторів. В. Чой (W. Choi) та інші розробили модель прийняття рішень на основі техніки впорядкування переваг за подібністю до ідеального рішення для впровадження інтелектуальних послуг запобігання злочинності через екологічний дизайн у муніципальних центрах управління Сеулу, Південна Корея [3]. Дж. Янг (J. Yang) та співавтори представили нову методологію оцінювання факторів, що впливають на прийняття рішень вуличними злочинцями, використовуючи технологію відстеження погляду у віртуальному середовищі гри Grand Theft Auto 5 та запропонували новий спосіб збору кількісних даних для дослідження вуличних пограбувань [12]. Р. Мінарді (R. Minardi) та інші розробили модульну систему запобігання злочинності для якісного оцінювання кримінальних ризиків для італійського міста Сіракузи. Система включає онтологію кримінального ризику, модуль отримання контекстних даних з OpenStreetMap та інтерфейс геоінформаційної системи (ГІС) [13]. M-s. Park (М. Парк) та H. Lee (Х. Лі) проаналізували систему безпеки нових розумних міст шляхом проведення аналізу інтелектуальної служби попередження злочинності вільної економічної зони Інчхон у Південній Кореї [14]. M. P. Basilio (П. Базиліо) та V. Pereira (В. Перейра) досліджували методи багатокритеріального прийняття рішень для запобігання та контролю злочинності з урахуванням обмеженості ресурсів [15].

Однак розвідки з цієї тематики є фрагментарними та таргетовані на конкретні регіони, які мають суттєво різний рівень розвитку ІТ-інфраструктури, що ускладнює впровадження універсальних рішень та порівняння результатів досліджень. Більшість із них проводились для високотехнологічних міст розвинених країн світу. Для України комплексні дослідження з питань впровадження інтелектуальних систем прийняття рішень щодо запобігання злочинності на сьогодні не проводились.

Мета роботи. Метою даної роботи є представити інтелектуальну систему прийняття рішень щодо запобігання злочинності і запропонувати новий підхід до оцінювання ефективності впровадження таких інновацій для підвищення ефективності запобігання, прогнозування та розслідування кримінальних злочинів в Україні.

Для досягнення поставленої мети у роботі вирішуються такі завдання:

- класифікувати інтелектуальні технології запобігання злочинності;
- визначити елементи інтелектуальних технологій запобігання злочинності;
- представити модель прийняття рішень на основі техніки впорядкування переваг за подібністю до ідеального рішення TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) для впровадження цих технологій у комплексну інтелектуальну систему правоохоронних органів.

Інтелектуальні технології запобігання злочинності. Технологія запобігання злочинам – це технологія, яка надає інформаційну підтримку правоохоронним органам з попередження правопорушень. Вона стрімко розвивається з початком 4-ї промислової революції. Системи відеоспостереження, які є ключовою технологією запобігання правопорушенням і основним засобом розкриття злочинів, забезпечують моніторинг через інтегровані технологічні інструменти в поліцейських відділеннях та центрах протидії злочинності. Незважаючи на стрімке зростання кількості систем відеоспостереження, правоохоронні органи не мають ресурсних можливостей для постійного інтерактивного моніторингу безпекової ситуації. Це призводить до несвоєчасного реагування на злочин. Для подолання обмежень традиційного контролю технічно розвинені країни світу впроваджують системи запобігання злочинам на основі інтелектуальних технологій, таких як штучний інтелект (ШІ), Інтернет речей (IoT) та великі дані [3].

Базовими технологіями у системі інтелектуального запобігання злочинам є аналіз відеозаписів на основі ШІ, платформи для аналітики даних про правопорушення та зондування даних на основі IoT. Для аналізу відеозаписів переважно використовують технології розпізнавання поведінки правопорушників або відстеження підозрюваних у відеоматеріалах. Вони включають інтелектуальне відеоспостереження (наприклад, насильство), автоматичне відстеження підозрюваних, систему розпізнавання облич, ідентифікацію номерних знаків та геоінформаційні системи (ГІС) безпеки відеоспостереження [16–18]. Платформи для аналітики даних про правопорушення переважно використовують технології просторового та часового прогнозування злочинів, технології підтримки прийняття рішень щодо запобігання злочинності та технології інтеграції/підключення до пов’язаних систем. Вони включають платформи соціальної безпеки; системи прогнозування злочинів на основі закономірностей/тенденцій даних про злочинність, поліцейську діяльність у гарячих точках/картографування злочинності/географічне профілювання; інформацію про відео в режимі реального часу, пов’язану з патрульними автомобілями; технології підтримки прийняття рішень із запобігання злочинам на основі ГІС та інтегровані операційні системи розумного міста [19]. Для IoT зазвичай обирають такі технології, як датчики руху для запобігання вторгненню та датчики освітлення для запобігання нічним злочинам. Зокрема це датчики руху в об’єктах контролю доступу; датчики розпізнавання аномальних звуків; датчики відкриття/закриття вхідних дверей/вікон; технології регулювання освітлення на основі виявлення пішоходів; розумні вуличні ліхтарі на основі датчиків IoT та інтегроване поліцейське обладнання [20].

В Україні лише розпочинається впровадження інтелектуальних технологій для запобігання кримінальним правопорушенням. Платформа CrimeDataLab забезпечує аналіз офіційної статистики протидії злочинності. У її склад входить інтелектуальний асистент CrimeScale, призначений для аналізу кримінальної статисти [21]. В окремих містах впроваджується концепція «Безпечного міста» на основі комплексу інноваційних технологічних рішень. Зокрема платформа INNI забезпечує інтеграцію різних систем відеоспостереження з відповідними інфраструктурними та безпековими системами. Відеоаналітика INNI контролює безпеку на вулицях і дорогах міста, може ідентифікувати порушення правил дорожнього руху, керувати світлофорами та освітленням. Ця платформа забезпечує оперативне реагування правоохоронних органів на правопорушення та здатна ідентифікувати злочинців.

Інтелектуальні технології запобігання злочинності використовують сучасні технологічні рішення для зменшення рівня злочинності та підвищення безпеки у громадських місцях. Ці технології поєднують фізичні, соціальні та технологічні аспекти для створення середовища, яке запобігає злочинним діям.

До таких технологій належать:

– системи відеоспостереження з аналізом відео – використання ШІ для автоматичного виявлення підозрілих ситуацій або аномальної поведінки;
– розпізнавання облич та номерних знаків – для ідентифікації осіб та транспортних засобів у реальному часі;
– інтелектуальні датчики руху та тривоги – автоматичне виявлення руху у контрольованих зонах та миттєве сповіщення про загрози;
– інтеграція з системами екстреного реагування – поєднання з місцевими правоохоронними органами або службами порятунку для швидкого реагування на інциденти;
– аналітика даних для виявлення кримінальних патернів – використання великих даних для виявлення закономірностей у злочинних діях і попередження майбутніх правопорушень.

На рис. 1 представлено три категорії інтелектуальних технологій запобігання злочинності, які можуть стати основою для розробки комплексної інтелектуальної системи прийняття рішень щодо запобігання злочинності в Україні.

Рис. 1. Інтелектуальні технології запобігання злочинності

1. Інтегровані технології операційного контролю – це системи, що об'єднують моніторинг та управління для цілей запобігання злочинності:
– ГІС-аналіз інформації про громадську безпеку. Забезпечують підтримку прийняття рішень щодо встановлення нових камер відеоспостереження на основі аналізу місць злочинів. Система використовує геопросторові дані для визначення оптимальних локацій для встановлення камер спостереження на основі даних про кримінальну активність;

– аналіз та прогнозування злочинності на основі великих даних. Технологія використовує аналітику великих даних для реагування на різні типи злочинів та їх прогнозування. Система обробляє великі масиви даних для виявлення закономірностей та передбачення потенційних кримінальних інцидентів;
– інтелектуальна платформа управління забезпечує інтегрований контроль систем відеоспостереження, мобільних додатків та карт злочинності;
– дрон/робот-контроль забезпечує підтримку безпілотного патрулювання.

2. Технології відеоаналізу використовують ШІ для автоматичного розпізнавання підозрілої поведінки, відстеження осіб, ідентифікації номерних знаків та миттєвого сповіщення правоохоронців про потенційні загрози у режимі реального часу:
– системи відеоспостереження з удосконаленими функціями для аналізу відео за допомогою ШІ;
– автоматичне розпізнавання аномальної поведінки (наприклад, напад, скупчення людей) на основі аналізу шаблонів глибокого навчання.
– Виявлення вторгнень у контрольовані зони забезпечує сповіщення про порушників у контрольованих зонах через відеоаналіз;
– автоматичне відстеження об’єктів через системи відеоспостереження (наприклад, підозрюваних або зниклих осіб);
– розпізнавання облич для виявлення зниклих чи підозрюваних у злочинах осіб;
– розпізнавання номерних знаків – контроль за незаконним паркуванням, несплаченими податками та викраденими транспортними засобами.

3. Технології датчиків IoT:
– датчики виявлення руху – контроль доступу та виявлення руху у контрольованих зонах;
– датчики відкриття/закриття дверей – контроль доступу та виявлення відкриття/закриття дверей у контрольованих зонах;
– звукові датчики – виявлення криків та голосів, що кличуть на допомогу в екстрених ситуаціях;
– голосові попередження – автоматичні голосові сповіщення на основі сенсорних даних про аномальні ситуації (наприклад, пожежа);
– домашні датчики та дистанційне керування – виявлення вторгнень у житло та контроль дистанційного керування.

Оцінювання моделі прийняття рішень щодо запобігання злочинності. Ефективність різних технологічних компонентів інтелектуальної системи прийняття рішень щодо запобігання злочинності (алгоритмів обробки даних з камер відеоспостереження, датчиків IoT та інших джерел інформації) оцінюють ще на етапі проектування такої системи. Такий підхід може забезпечити вибір найбільш ефективних рішень для конкретних умов застосування та можливість оптимізації архітектури системи шляхом аналізу продуктивності різних конфігурацій.

У роботі запропоновано модель прийняття рішень на основі техніки впорядкування переваг за подібністю до ідеального рішення (TOPSIS) для впровадження інтелектуальних технологій у комплексну інформаційну систему правоохоронних органів України [7]. З цією метою визначено відповідні критерії. Для оцінки ефективності впровадження розглянутих вище інтелектуальних технологій запобігання злочинності у комплексну інформаційну систему правоохоронних органів визначено відповідні альтернативи, які відображають різні методи або підходи до вибору відповідних технологій. Аналіз та порівняння цих альтернатив може стати основою для оцінювання індивідуальних перевагах і недоліків з точки зору ефективності запобігання злочинності та забезпечення суспільної безпеки. Метою є створити комплексну рамку для оцінювання ефективності впровадження інтелектуальних технологій запобігання злочинності та прийняття обґрунтованих

рішень щодо дієвих практик використання інноваційних рішень для забезпечення громадської безпеки.

Критерії оцінювання елементів інтелектуальних технологій запобігання злочинності. У роботі представлено підхід до визначення критеріїв, заснований на ґрунтовному аналізі літератури та найкращих міжнародних практик. На основі консолідації знань з опублікованих досліджень запропоновано комплексний набір критеріїв, який відображає ключові аспекти ефективності впровадження інтелектуальних технологій у діяльність правоохоронних органів для попередження та розкриття кримінальних злочинів [18, 22].

1. Ефективність запобігання злочинності – оцінювання впливу на запобігання злочинності у результаті застосування технології: оцінка результативності технології щодо зменшення рівня злочинності у конкретних регіонах або громадах.

2. Відповідність політиці запобігання злочинності – оцінювання відповідності технології державним та територіальним політикам у сфері запобігання злочинності.

3. Конкурентоспроможність – оцінювання конкурентоспроможності технології на ринку з огляду на наявні послуги та технології, їхню ефективність і доцільність.

4. Розвиток сектора послуг – оцінювання технологічних тенденцій і потенціалу ринку в галузі послуг, що забезпечують безпеку, з урахуванням можливостей для зростання і розширення ринку.

5. Економічна життєздатність – оцінювання ефективності інвестицій, економічної життєздатності та потенціалу комерціалізації технології: аналіз вартості впровадження, витрат на підтримку та прибутковість у довгостроковій перспективі.

6. Застосовність у галузі – оцінювання застосовності технології у конкретній галузі з урахуванням управління ризиками (наприклад, захист персональних даних, адміністративні затримки, співпраця з службами екстреної допомоги тощо).

7. Ефективність управління – оцінювання ефективності управління та стійкості операцій і діяльності технології у довгостроковій перспективі, включно з аналізом екологічної, економічної та соціальної стійкості для забезпечення сталого розвитку.

Визначення альтернатив (вибір технологічних елементів запобігання злочинності). У роботі проведено аналіз сучасних інтелектуальних технологій, які можуть підвищити ефективність запобігання злочинності, покращити безпеку громадян і сприяти оперативному реагуванню правоохоронних органів, забезпечити ефективний контроль за криміногенною ситуацією, зменшити ризики злочинності та покращити координацію правоохоронних органів України.

1. Інтелектуальна система відеоспостереження на базі ШІ:
- використання високоякісних камер відеоспостереження з удосконаленими можливостями для аналізу злочинної діяльності;
- покращена чіткість зображення та підтримка нічного бачення для ефективного моніторингу.

2. Аналіз за допомогою ШІ для забезпечення громадської безпеки:
- виявлення порушень (незаконне паркування, викидання сміття, куріння у заборонених місцях тощо);
- ідентифікація підозрілої або девіантної поведінки (нетверезі особи, неповнолітні правопорушники тощо).

3. Аналіз ШІ для запобігання злочинності:
- автоматичне відстеження підозрюваних через систему відеоспостереження;
- розпізнавання обличчя для пошуку зниклих осіб та ідентифікації правопорушників;
- виявлення потенційних загроз (акти насильства або підозрілі дії) для попередження злочинів у реальному часі.

4. Автоматичне розпізнавання аномальної поведінки:
- постійний моніторинг відеопотоку з камер спостереження;

– виділення людей та їх дій у кадрі;
– поточної поведінки з базою нормальних шаблонів;
– виявлення відхилень та класифікація типу аномальної поведінки (скупчення людей, агресивні рухи тощо).
– генерування сповіщень для операторів системи безпеки.

5. Система моніторингу злочинності:
– інтерактивні карти злочинності для аналізу ризикованих зон;
– автоматизований аналіз відео з камер спостереження;
– інтеграція з екстреними службами для швидкого реагування.

6. Мобільний додаток для запобігання злочинності:
– підвищення безпеки людей, що повертаються додому вночі;
– функції екстреного сповіщення та виклику допомоги.

7. Роботизовані та дронові системи безпеки:
– автоматичне патрулювання в районах із підвищеним рівнем злочинності;
– відеоспостереження та передача даних у реальному часі до поліційних відділків та центрів управління;
– миттєве реагування на підозрілі ситуації та інтеграція зі службами безпеки.

Ієрархічна структура моделі оцінювання інтелектуальної системи прийняття рішень щодо запобігання злочинності. Для встановлення ієрархії серед ключових атрибутів спроектовано ієрархію між атрибутами, що стосуються прийняття рішень – критеріями та альтернативами. Першим рівнем запропонованої ієрархічної структури є вибір технологічних елементів запобігання злочинності. Другий рівень складають сім критеріїв оцінювання альтернатив. Третій рівень формують альтернативи – семи вибраних моделей для аналізу та запобігання злочинності (рис. 2).

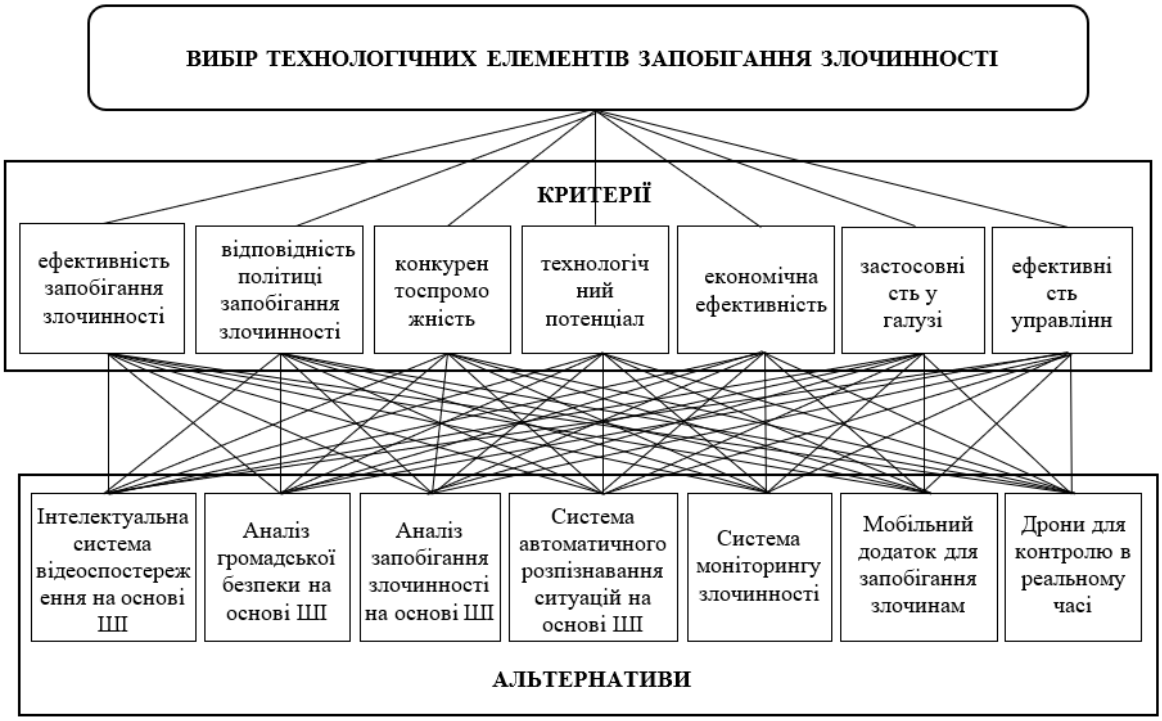


Рис. 2. Ієрархічна структура моделі оцінювання інтелектуальної системи прийняття рішень щодо запобігання злочинності

Математична модель прийняття рішень щодо впровадження інтелектуальних технологій запобігання злочинності. Це дослідження спрямоване на підтримку прийняття рішень щодо впровадження інтелектуальних систем для запобігання

злочинності у правоохоронних органах України. Відповідно, важливо вибрати методологію дослідження, підкріплену науковими доказами та логікою. У цьому контексті нечітке багатокритеріальне прийняття рішень (fuzzy MCDM – multi-criteria decision-making) широко використовується в академічній спільноті для надання об'єктивних пріоритетних альтернатив критеріям оцінки залежно від мети дослідження. TOPSIS може забезпечити раціональну логіку для прийняття рішень, оцінювання найкращих та найгірших альтернатив. Цей метод надає можливість вимірювати ефективність усіх альтернатив з багатокритеріальної перспективи [22]. Метод базується на знаходженні найкращого рішення шляхом визначення відстаней між різними альтернативами та ідеальними точками у багатовимірному просторі. Він дієвий у ситуаціях, де неможливо точно виміряти критерії або де існує значна невизначеність. Основна ідея методу полягає в тому, щоб знайти альтернативу, яка одночасно максимально наближену до позитивного ідеального розв'язку та максимально віддалену від негативного ідеального розв'язку. Це досягається через складний математичний апарат нечіткої логіки, який перетворює оцінки, представлені у лінгвістичній формі, на числові значення.

У роботі використано теорію нечітких множин [23] для вирішення проблеми невизначеності при прийнятті рішень на основі TOPSIS. Ця теорія вводить нечітку логіку та нечітку множину для подолання неточності та неоднозначності суб'єктивного судження в оцінці. Як передова методологія, нечіткий TOPSIS може математично виражати неоднозначні явища, включаючи нечітку кількісну інформацію, суб'єктивні та нечіткі судження, визначати раціональні альтернативи для прийняття рішень.

Для оцінювання інтелектуальних систем для запобігання злочинності на основі нечіткого TOPSIS спочатку було обирано та досліджено критерії оцінювання, а потім ваги отриманих критеріїв оцінки застосовуються для оцінки альтернатив. Для критеріїв оцінки використано 7-бальну шкалу Лікерта. Передбачається, що опитування буде проведено серед експертів, які володіють технічними знаннями. Шкала Лікерта – це біполярний метод шкалювання, який послідовно вимірює позитивні та негативні відповіді на запитання анкети. Для більш об'єктивної кількісної оцінки даних у роботі застосовано M – трикутне нечітке число (TFN – Triangular Fuzzy Number), наближене за допомогою лінійної функції належності. M використано для обчислення ваг. $M_1 = (l_1, m_1, u_1)$ – функція належності для нижньої, середньої та верхньої меж для одного чіткого значення (рис. 3).

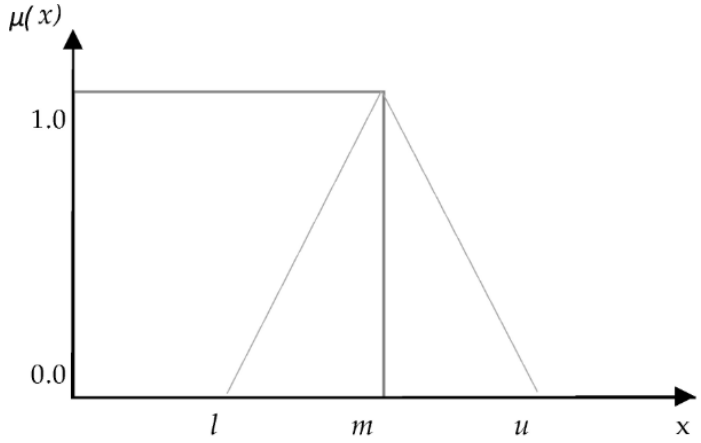


Рис. 3. Трикутне нечітке число

TFN представлене як трикутник із трьох точок (l, m, u). l = нижня межа, m = середня межа, u = верхня межа). Їх площа є величиною TFN. Для обчислення TFN у роботі використано нечітку шкалу, представлену у таблиці 1 [24].

Таблиця 1.

Нечітка шкала оцінювання критеріїв

Оцінка у лінгвістичній формі	**TFN**
Надзвичайно низька	(0 0 0,1)
Дуже низька	(0, 0,1 0,3)
Низька	(0,1 0,3 0,5)
Середня	(0,3 0,5 0,7)
Висока	(0,5 0,7 0,9)
Дуже висока	(0,7 0,9 1)
Надзвичайно висока	(0,9 1 1)

У роботі запропоновано використати рівняння (1)–(4) для визначення TFN $S_i = (l_i, m_i, u_i)$ для i-го атрибута. Для кінцевого розрахунку нормалізованого власного вектора мінімального значення для дефазифікації TFN S_i за критеріями оцінки [25, 26].

$$S_i = \sum_{j=1}^{m} M_{ij} \times \left[\sum_{i=1}^{n} \sum_{j=1}^{m} M_{ij} \right]^{-1} \tag{1}$$

$$\sum_{j=1}^{m} M_{ij} = \left(\sum_{j=1}^{m} l_{ij}, \sum_{j=1}^{m} m_{ij}, \sum_{j=1}^{m} u_{ij} \right) \tag{2}$$

$$\sum_{i=1}^{n} \sum_{j=1}^{m} M_{ij} = \left(\sum_{i=1}^{n} \sum_{j=1}^{m} l_{ij}, \sum_{i=1}^{n} \sum_{j=1}^{m} m_{ij}, \sum_{i=1}^{n} \sum_{j=1}^{m} u_{ij} \right). \tag{3}$$

$$\left[\sum_{i=1}^{n} \sum_{j=1}^{m} M_{ij} \right]^{-1} = \left[\frac{1}{\sum_{i=1}^{n} \sum_{j=1}^{m} l_{ij}}, \frac{1}{\sum_{i=1}^{n} \sum_{j=1}^{m} lm_{ij}}, \frac{1}{\sum_{i=1}^{n} \sum_{j=1}^{m} l_{ij}} \right]. \tag{4}$$

Рівняння (1) є сумою оцінок, визначених до фазифікації для кожного з елементів. Рівняння (2) є трикутною фазифікацією на основі значень l, m та u за нечіткою шкалою. Рівняння (3) є сумою критеріїв оцінки для кожного значення l, m та u. Рівняння (4) є кінцевим значенням TFN, яке є оберненим значенням до суми l, m та u.

У роботі запропоновано обчислювати фазифікацію альтернатив за критеріями за рівнянням (5), а нечітку вагу – за рівнянням (6) [27].

$$a_{ij} = \min_k (a_{ij}^k), b_{ij} = \frac{1}{k} \sum_{k=1}^{k} b_{ij}^k, c_{ij} = \max_k (c_{ij}^k) \tag{5}$$

$$w_{j1} = \min_k (w_{j1}^k), w_{j2} = \frac{1}{k} \sum_{k=1}^{k} \left(w_{j2} \right), w_{j3} = \max_k \sum_{k=1}^{k} \left(w_{j3} \right) \tag{6}$$

Далі обчислюються матриці рішень $\tilde{V} = \left(v_{lj} \right)$ та $v_{lj} = r_{lj} \times w_j$ за допомогою нормалізованої матриці рішень $\tilde{R} = \left[r_{lj} \right]$ (формули (7) та (8)). Ваги критеріїв оцінки (TFN) з розраховуються за формулою (4) [27].

$$(\tilde{r}_{lj}) = \left(\frac{a_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*} \frac{c_{ij}}{c_j^*} \right), c_j^* = \max_i \left(c_{ij} \right) \text{ (критерії вигоди)} \tag{7}$$

$$\tilde{r}_{lj} = \left(\frac{a_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*} \frac{c_{ij}}{c_j^*} \right), c_j^* = \max_i \left(c_{ij} \right) \text{(критерії вартості)} \tag{8}$$

Після цього обчислюються нечітке позитивне ідеальне рішення (FPIS) за формулою (9) та нечітке негативне ідеальне рішення (FNIS) за формулою (10).

$$A^* = \left(v_1^*, v_2^*, \ldots, v_n^*,\right), \tag{9}$$

де $(\tilde{v}_j^*) = \max_i (v_{ij3})$.

$$A^- = (\tilde{v}_1^-, \tilde{v}_2^-, ..., \tilde{v}_n^-,), \tag{10}$$

$\tilde{v}_j^- = \min_i (v_{ij1})$.

Для обчислення відстаней до FPIS та FNIS для кожної з альтернатив, у цьому дослідженні використано метод розрахунку відстані між двома TFN, запропонований у [24]. При $\tilde{x} = \left(a_1, b_1 c_1\right)$, $\tilde{y} = \left(a_2, b_2 c_2\right)$ відстань між двома TFN обчислюється за формулою (11). Остаточна відстань до FPIS та FNIS для кожної з альтернатив обчислюється за формулою (12).

$$d(\tilde{x}, \tilde{y}) = \sqrt{\frac{1}{3}\left[\left(a_1 - a_2\right)^2 + \left(b_1 - b_2\right)^2 + \left(c_1 - c_2\right)^2\right]}, \tag{11}$$

$$d_i^* = \sum_{j=1}^{n} d\left(\tilde{v}_{lj}, \tilde{v}_j^*\right), d_i^- = \sum_{j=1}^{n} d\left(\tilde{v}_{lj}, \tilde{v}_j^-\right). \tag{12}$$

Коефіцієнт близькості для кожної з альтернатив CC_i обчислюється за формулою (13).

$$CC_i = \frac{d_i^-}{d_i^- + d_j^*} \tag{13}$$

Після цього визначаються ранги альтернатив від найвищого CC_i до найнижчого.

Висновки. Дана робота присвячена розробці моделі прийняття рішень на основі методу нечіткого TOPSIS для оцінювання ефективності впровадження інтелектуальних технологій запобігання злочинності у комплексну інформаційну систему правоохоронних органів України. Здійснено класифікацію інтелектуальних технологій запобігання злочинності та виділено три основні категорії: інтегровані технології операційного контролю, технології відеоаналізу та технології датчиків IoT. Визначено ключові елементи інтелектуальних технологій запобігання злочинності, зокрема системи відеоспостереження з аналізом відео, розпізнавання облич та номерних знаків, інтелектуальні датчики руху та тривоги, інтеграція з системами екстреного реагування, аналітика даних для виявлення кримінальних патернів. Розроблено модель прийняття рішень на основі методу нечіткого TOPSIS для оцінювання ефективності впровадження інтелектуальних технологій в комплексну інформаційну систему правоохоронних органів. Запропоновано математичний апарат для реалізації нечіткого TOPSIS, що базується на використанні трикутних нечітких чисел та забезпечує можливість враховувати невизначеність при оцінюванні альтернатив за визначеними критеріями. Розроблена ієрархічна структура моделі оцінювання може бути використана для прийняття обґрунтованих рішень щодо впровадження інтелектуальних технологій запобігання злочинності в діяльність правоохоронних органів України.

Список літератури

1. Berezka K., Kovalchuk O., Banakh S., Zlyvko S., Hrechaniuk R. A Binary Logistic Regression Model for Support Decision Making in Criminal Justice. *Folia Oeconomica Stetinensia*. 2022. Vol. 22(1). P. 1–17. DOI: https://sciendo.com/article/10.2478/foli-2022-0001.
2. Cai Y., Li D., Wang Y. Intelligent crime prevention and control big data analysis system based on imaging and capsule network model. *Neural Process. Lett*. 2020. Vol. 53. P. 2485–2499.

3. Choi W., Na J., Lee S. Evaluating Intelligent CPTED Systems to Support Crime Prevention Decision-Making in Municipal Control Centers. *Applied* Sciences. 2024. Vol. 14(15):6581. DOI: https://doi.org/10.3390/app14156581.
4. Joshi C., Curtis-Ham S., D'Ath C., Searle D. Considerations for Developing Predictive Spatial Models of Crime and New Methods for Measuring Their Accuracy. *ISPRS International Journal of* Geo-Information. 2021. Vol. 10(9):597. DOI: https://doi.org/10.3390/ijgi10090597.
5. Guzman E., Andres B., Poler R. A Decision-Making Tool for Algorithm Selection Based on a Fuzzy TOPSIS Approach to Solve Replenishment, Production and Distribution Planning Problems. *Mathematics*. 2022. Vol. 10(9):1544. DOI: https://doi.org/10.3390/math10091544.
6. Kovalchuk O., Shevchuk R., Babala L., Kasianchuk M. Support vector machine to criminal recidivism prediction. *Intl Journal of Electronics and Telecommunication*. 2024. Vol. 70(3). P. 691–697. DOI: https://doi.org/10.24425/ijet.2024.149598.
7. Kovalchuk O., Kasianchuk M., Karpinski M., Shevchuk R. Decision-Making Supporting Models Concerning the Internal Security of the State. *International Journal of Electronics and Telecommunications*. 2023. Vol. 69. No. 2. P. 301–307. DOI: https://doi.org/10.24425/ijet.2023.144365.
8. Kovalchuk O., Karpinski M., Banakh S., Kasianchuk M., Shevchuk R., Zagorodna N. Prediction Machine Learning Models on Propensity Convicts to Criminal Recidivism, *Information*. 2023. Vol. 14(3). P. 161. DOI: https://doi.org/10.3390/info14030161.
9. Ковальчук О. Я. Метод головних компонент для моделювання ризиків кримінальної злочинності. Вісник Хмельницького національного університету. 2023. № 5. С. 154-158.
10. Kovalchuk O. Modeling the risks of the confession process of the accused of criminal offenses based on survival concept. Scientific Journal of TNTU. 2022. Vol. 108(4), pp. 27–37. DOI: https://doi.org/10.33108/visnyk_tntu2022.04.
11. Kovalchuk O. Correspondence analysis for detecting risk factors for criminal recidivism. *Scientific Journal of TNTU*. 2023. Vol. 111. No 3. P. 35–47. URL: https://visnyk.tntu.edu.ua/index.php?art=736.
12. Yang J., Kim D., Jung S. Using Eye-Tracking Technology to Measure Environmental Factors Affecting Street Robbery Decision-Making in Virtual Environments. *Sustainability*. 2020. Vol. 12(18):7419. DOI: https://doi.org/10.3390/su12187419.
13. Minardi R., Villani M.L., De Nicola A. Semantic Reasoning for Geolocalized Assessment of Crime Risk in Smart Cities. *Smart Cities*. 2023. Vol. 6(1):179–195. DOI: https://doi.org/10.3390/smartcities6010010.
14. Park M-s., Lee H. Smart City Crime Prevention Services: The Incheon Free Economic Zone Case. *Sustainability*. 2020. Vol. 12(14):5658. DOI: https://doi.org/10.3390/su12145658
15. Basilio M. P., Pereira V. Operational research applied in the field of public security: The ordering of policing strategies such as the ELECTRE IV. *J. Model. Manag*. 2020. Vol. 15. P. 1227–1276.
16. Khan P. Byun Y. Park, N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics*. 2020. Vol. 9:484.
17. You J. D. Study on construction safe smart city from crime. *Korean Assoc. Police Sci. Rev*. 2017. Vol. 19. P. 199–222.
18. Socha R., Kogut B. Urban video surveillance as a tool to improve security in public spaces. *Sustainability*. 2020. Vol. 12:6210.
19. Cai Y., Li D., Wang Y. Intelligent crime prevention and control big data analysis system based on imaging and capsule network model. *Neural Process. Lett*. 2020. Vol. 53. P. 2485–2499.

20. Park M., Lee H. Smart city crime prevention services: The Incheon free economic zone case. *Sustainability*. 2020. Vol. 12:5658.
21. Карчевський М. В. (2022). Протидія злочинності в Україні у форматі data science. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. № 2(98). С. 202−227. DOI: https://doi.org/10.33766/2524-0323.98.202-227.
22. Kim G., Park C.S., Yoon K.P. Identifying investment opportunities for advanced manufacturing systems with comparative integrated performance measurement. *Int. J. Prod. Econ*. 1997. № 50. С. 23−33.
23. Zadeh L. Fuzzy sets. *Inf. Control*. 1965. Vol. 8. P. 338−353.
24. Chen C. Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy Sets Syst*. 2000. Vol. 114. P. 1−9.
25. Choi W., Kim T., Na J., Youn J. Assessment of Dynamic Object Information Utilization Service in a Control Center for Each Urban Scale via Fuzzy AHP. *Systems*. 2023. Vol. 11:368.
26. Choi W., Jang B., Jung I., Sung H., Jang Y. Evaluation of Preferences for a Thermal-Camera-Based Abnormal Situation Detection Service via the Integrated Fuzzy AHP/TOPSIS Model. *Appl. Sci*. 2023. Vol. 13:11591.
27. Sorin N., Simona D., Ioan D. Fuzzy TOPSIS: A General View. *Procedia Comput. Sci*. 2016. Vol. 91. P. 823−831.

MATHEMATICAL DECISION-MAKING MODEL FOR IMPLEMENTING CRIME PREVENTION INTELLIGENT TECHNOLOGIES BASED ON FUZZY TOPSIS METHOD

O.Ya. Kovalchuk[1], L.V. Babala[1], R.I. Ivanytskyy[2]

[1]West Ukrainian National University
11, Lvivska Str., Ternopil, 46009, Ukraine
[2]Ternopil Volodymyr Hnatiuk National Pedagogical University
2 M. Kryvonosa. Str., 46009 Ternopil, Ukraine
Emails: olhakov@gmail.com, ludaduma7@gmail.com, romikiv@ukr.net

The article presents a decision-making model based on the fuzzy TOPSIS method for evaluating the effectiveness of implementing intelligent crime prevention technologies in the integrated information system of Ukrainian law enforcement agencies. Intelligence crime prevention technologies have been classified into three main categories: integrated operational control technologies, video analysis technologies, and IoT sensor technologies. Key elements of intelligent technologies have been identified, including video surveillance systems with video analysis, face and license plate recognition, intelligent motion sensors and alarms, integration with emergency response systems, and data analytics for criminal pattern detection. Seven evaluation criteria are proposed: crime prevention effectiveness, compliance with crime prevention policy, competitiveness, service sector development, economic viability, industry applicability, and management effectiveness. Six alternative technological solutions have been identified, and a mathematical apparatus has been developed for implementing fuzzy TOPSIS using triangular fuzzy numbers. A three-level hierarchical structure of the evaluation model has been constructed, enabling the justified selection of technological solutions considering multiple criteria and uncertainty in expert assessments. The practical significance of the work lies in the possibility of using the developed model to optimize the architecture of the integrated law enforcement information system by analyzing the performance of various configurations. The scientific novelty of the work lies in developing a decision-making model that, unlike existing approaches, accounts for uncertainty in expert assessments and enables multi-criteria analysis of alternative technological solutions. A classification of intelligent crime prevention technologies has been proposed, and their key elements have been identified, creating a theoretical foundation for further research in this field. Future research may focus on practical testing of the developed model, improving the evaluation criteria system, and expanding the set of alternative technological solutions.
Keywords: intelligent technologies, crime prevention, fuzzy TOPSIS, decision making, artificial intelligence, IoT devices, video analytics

DOI 10.15276/imms.v15.no1.71
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp. 71-82

ЗАХИЩЕНА СИСТЕМА ДЛЯ СТВОРЕННЯ ТА ПРОВЕДЕННЯ ОПИТУВАНЬ

В.Р. Капелюшний, Н.І. Кушніренко, О.В. Троянський

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: kushnirenko@op.edu.ua, o.v.troyanskiy@op.edu.ua

У сучасних умовах цифрової трансформації особливої уваги набуває забезпечення безпеки для проведення онлайн-опитувань. Актуальність проблеми обумовлена активним використанням веб-сервісів для організації навчального процесу та підвищеними вимогами до захисту персональних даних, запобігання академічному шахрайству та забезпеченню прозорості результатів. Метою даної роботи є розробка безпечного веб-застосунку для створення, проведення та контролю опитувань, який забезпечує захист персональних даних користувачів, підтримку академічної доброчесності та відповідає сучасним вимогам кібербезпеки. У роботі здійснено аналіз сучасних систем для тестування знань (Google Forms, Quizlet, SurveyMonkey, Typeform), виявлено їх переваги та недоліки в контексті безпеки, зокрема обмежену підтримку двофакторної автентифікації та слабкий захист даних у стані спокою. Запропоновано та реалізовано безпечну систему опитувань з підтримкою сучасних криптографічних протоколів. Для захисту даних використано симетричний алгоритм шифрування AES-256, що дозволяє гарантувати конфіденційність і цілісність збережених результатів. Розроблена система також підтримує двофакторну автентифікацію, перевірку геолокації, email підтвердження, шифрування HTTPS/TLS, автоматичне завершення сесії та механізм цифрових водяних знаків, який дозволяє ідентифікувати джерело витоку тестового контенту. Проведено практичну реалізацію системи розмежування прав доступу, створення ролей студентів та викладачів, впроваджено систему моніторингу входів і змін. Результати дослідження підтверджують доцільність створення власної системи як безкоштовної альтернативи популярним сервісам із недостатнім рівнем безпеки. Запропоноване рішення може впроваджуватись у закладах освіти для підвищення якості процесу тестування знань та забезпечення високого рівня безпеки даних користувачів.

Ключові слова: система опитувань, шифрування, кібербезпека, водяні знаки, RBAC, двофакторна автентифікація, геолокація, академічна доброчесність

Вступ. Сучасна освіта активно переходить до цифрових форматів, що зумовлює потребу у створенні безпечних систем для дистанційного навчання, тестування знань та проведення різноманітних опитувань. Згідно з інформацією Segura, у 2024 році в середньому відбувалося понад 2200 атак на веб-сервіси щодня, більшість з яких були спрямовані на системи обміну інформацією, включаючи платформи для навчання та проведення опитувань [1]. Згідно з звітом ENISA [2] та рекомендаціями OWASP [3], ключовими ризиками для веб-платформ є несанкціонований доступ до облікових записів, ін'єкційні атаки (SQL, XSS), використання застарілого програмного забезпечення та слабка політика управління сеансами.

Як зазначено в дослідженні [4], онлайн-системи навчання мають низку системних вразливостей, серед яких несанкціонований доступ до облікових записів, вразливість до атак на сесію та недостатній контроль за збереженням результатів тестування. У даній роботі запропоновано рекомендації щодо покращення інформації небезпеки в освітньому середовищі, а також розроблена власна система для створення та проведення опитувань, яка забезпечує високий рівень захисту даних, гнучке керування курсами та тестами, а також підтримку ключових механізмів забезпечення академічної доброчесності.

Системи тестування знань відіграють критично важливу роль в освітньому процесі. Вони дозволяють ефективно проводити оцінювання, перевіряти знання,

організовувати курси та отримувати зворотний зв'язок. Такі програмні рішення як: Google Forms, Quizlet, SurveyMonkey, Typeform пропонують широкі можливості для створення та проведення опитувань. Однак, вони мають деякі недоліки в контексті безпеки: відсутність двофакторної автентифікації у безкоштовних версіях, обмежений захист персональних даних, неможливість контролювати академічну доброчесність. У зв'язку з цим, розробка власного безпечного застосунку для тестування знань є актуальним завданням.

Серед найпоширеніших інструментів для створення онлайн-опитувань вирізняється Google Forms [5], що надає користувачам широкі можливості для налаштування анкет відповідно до їхніх потреб. Простота використання та можливість здійснювати інтеграції з іншими сервісами Google робить платформу зручною як для навчальних, так і для робочих цілей.

Ще однією популярною платформою є Quizlet [6], яка дозволяє не лише створювати тести, а й використовувати картки для інтерактивного навчання. Її функціонал орієнтований як на студентів і викладачів, так і на молодшу аудиторію. Основна перевага полягає в застосуванні методів активного навчання – не лише для контролю знань, а й для кращого запам'ятовування матеріалу.

Платформа SurveyMonkey [7] заснована у 1999 році є потужним засобом для створення, проведення і аналізу опитувань. На відміну від деяких аналогів, вона дозволяє працювати з готовими шаблонами, що значно спрощує процес розробки тестів та анкет.

Порівняно новою, але сучасною платформою є Typeform [8], запущена у 2012 році. Вона вирізняється візуально привабливим дизайном, широким набором інтерактивних елементів і діалогових підходів до побудови опитувань. Завдяки цьому користувачі більше залучаються до процесу, що підвищує рівень проходження опитувань до кінця.

Критично важливим аспектом використання онлайн-форм для тестування є захист отриманих даних. Особиста інформація, результати тестів чи конфіденційні відомості повинні зберігатися у безпеці, адже їх витік може призвести до репутаційних і фінансових втрат. Тому оцінка надійності обраної платформи є важливою для запобігання зовнішнім загрозам та несанкціонованому доступу.

Google Forms використовує протокол HTTPS та алгоритм AES-256 для шифрування переданих і збережених даних, а також інфраструктуру Google Key Management для керування ключами. Додатковий захист забезпечується двофакторною автентифікацією та можливістю контролю доступу до платформ. Платформа відповідає стандартам GDPR, CCPA та ISO 27001 [9].

Quzlet забезпечує базовий захист даних шляхом SSL та HTTPS, проте не надає детальну інформацію про шифрування даних при їх збереженні. Компанія співпрацює з рекламними партнерами, що може створювати ризики для конфіденційності. Двофакторна автентифікація передбачена лише у платній версії [10].

Сервіс SurveyMonkey підтримує HTTPS-з'єднання та шифрування за допомогою AES-256. Дата-центри платформи розташовані в США, Канаді та Ірландії. Двофакторна автентифікація доступна лише у платних тарифах. Деякі дані користувача можуть бути видалені повністю протягом 90 днів неактивності [11].

Typeform розгорнута в хмарному сервісі Amazon Web Services і також використовує шифрування AES-256 та захист HTTPS, а метадані форм підлягають шифруванню. Двофакторна автентифікація не є вбудованою функцією, але може бути активованою через Google або Microsoft. Сервіс відповідає вимогам GDPR, CCPA та SOC Type II [12].

Серед проаналізованих платформ Google Forms та SurveyMonkey забезпечують найвищий рівень безпеки завдяки сучасному шифруванню та підтримці двофакторної автентифікації. Quizlet та Typeform надають базовий, захист, проте не надають повної прозорості щодо збережених даних в стані спокою. При виборі платформи варто

враховувати не лише їх функціональність, а й рівень захисту персональної інформації, що особливо актуально у сфері освіти.

Усе це підкреслює актуальність розробки власного веб-застосунку для проведення опитувань, який би поєднував гнучкий функціонал з високим рівнем захисту, шифруванням даних, підтвердженням дії користувача, геолокаційним моніторингом і системою цифрових водяних знаків. Такий підхід дозволить підвищити довіру до результатів тестування, забезпечити прозорість навчального процесу та відповідність міжнародним стандартам.

Мета роботи. Метою роботи є підвищення безпеки процесу проведення опитувань в освітньому середовищі шляхом розробки захищеної веб-системи, яка реалізує сучасні механізми інформаційної безпеки та враховує потреби користувачів з різними ролями. Для досягнення поставленої мети було визначено такі основні задачі:

– розробити функціонал та інтерфейс безпечної веб-системи з урахуванням потреб різних ролей користувачів;

– реалізувати авторизацію через Google, двофакторну автентифікацію та підтвердження змін персональних даних через email-коди;

– реалізувати захист чутливої інформації на основі шифрування AES-256, підтвердження локації, завершення опитувань в разі покидання сторінки, автоматичне завершення сесії, захист від XSS-атак;

– реалізувати механізм формування водяного знака для виявлення джерела витоку завдань.

Основна частина. Для захисту конфіденційних даних, отриманих під час використання систем опитувань важливо використовувати надійні криптографічні алгоритми. Вибір відповідного методу шифрування залежить від обсягу даних, бажаної швидкості системи та вимог до безпеки. У сучасній практиці застосовується як симетричні, так і асиметричні підходи до шифрування, кожен із яких має свої переваги та обмеження.

Для шифрування даних в системі опитувань було обрано AES-256, який є одним з найпоширеніших симетричних криптографічних алгоритмів. AES відзначається високою криптостійкістю та офіційно затверджений як стандарт в США. Він працює з блоками по 128 біт та підтримує ключі довжиною 128, 192 або 256 біт. Найвищий рівень захисту забезпечує AES-256, який має 14 раундів перетворень та використовує унікальні раундові ключі, що генеруються з основного ключа [13].

AES-256 поєднує у собі кілька етапів обробки даних: підстановка байтів (SubBytes), перестановка рядків (ShiftRows), змішування стовпців (MixColumns) і накладання ключа (AddRoundKey). Кожен з них виконує важливу функцію для досягнення криптостійкості [14]. Серед переваг AES-256 можна виділити високу швидкість обробки даних, можливість оптимізації під апаратне забезпечення та підтримку різних режимів шифрування. Алгоритм стійкий до відомих атак, а повний перебір ключів (2^{256} варіантів) є абсолютно недосяжним навіть для суперкомп'ютерів. Саме тому AES-256 було обрано для шифрування даних у стані спокою – як надійний, продуктивний та загальновизнаний стандарт.

Від безпеки програмного забезпечення залежить захист зібраних даних, забезпечення їхньої цілісності та стійкість до зовнішніх атак. Система повинна відповідати сучасним стандартам кібербезпеки, включаючи можливі адаптації до нових загроз та постійного моніторингу подій. В запропонованій системі опитувань передбачено низку пов’язаних між собою заходів, які мінімізують потенційні ризики та гарантують стабільність роботи.

Важливим етапом забезпечення безпеки в системі опитувань є автентифікація – процедура перевірки особи користувача при вході в систему. Під час входу до системи користувач повинен ввести унікальний облікові дані: логін та пароль, які системи перевіряє на відповідність. У разі потреби може також виконуватися перевірка IP-адреси, сертифікату або додаткові верифікаційні дії. Якщо автентифікація завершилася успіхом,

наступним етапом є авторизація, тобто надання користувачу прав доступу до ресурсів. На рис. 1 показаний процес входу користувача в систему.

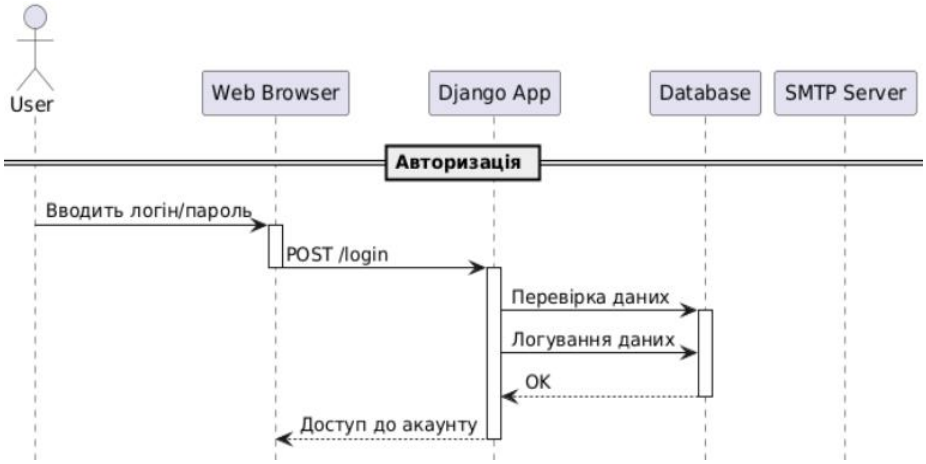


Рис. 1. Процес входу користувача в систему

Для підвищення рівня захисту впроваджено двофакторну автентифікацію (2FA), що надає додатковий рівень підтвердження особи – зазвичай це одноразові коди з SMS або email, телефонний дзвінок, резервний пароль чи спеціальний додаток [12]. Якщо не знайдено збігів щодо даного користувача, або він не зміг пройти до кінця процес автентифікації і підтвердити свою особу, йому буде відмовлено в доступі. Процес двофакторної автентифікації наведений на рис. 2.

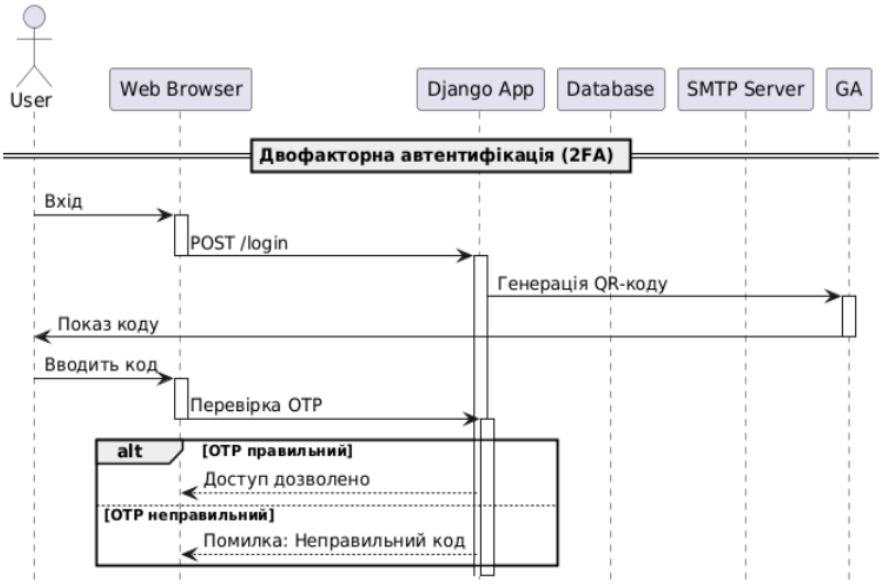


Рис 2. Процес двофакторної автентифікації користувача

Ще більш надійним методом автентифікації є використання біометричних даних – відбитків пальців або розпізнавання обличчя. Їх важко підробити, тому вони є потужним інструментом протидії шахрайству. Автентифікація слугує бар'єром для несанкціонованого доступу до системи та захищає персональні дані від сторонніх осіб.

Авторизація в запропонованій системі опитувань базується на моделі контролю доступу RBAC (Role Based Access Control) [15], яка дозволяє призначити доступ до функцій системи залежно від ролі користувача. Наприклад, студент може лише доєднатися до курсів та проходити опитування, викладач – створювати і редагувати тести та курси, керувати користувачами та системним налаштуванням.

Ще одним елементом безпеки є перевірка геолокації під час входу. Система фіксує поточну IP-адресу, визначає місто та країну, порівнює отримані значення з

попередніми збереженими даними. Якщо локація відрізняється, користувачеві надсилається одноразовий код на email. Доступ відкривається лише після успішного підтвердження. Процес перевірки локації користувача наведений на рис. 3.

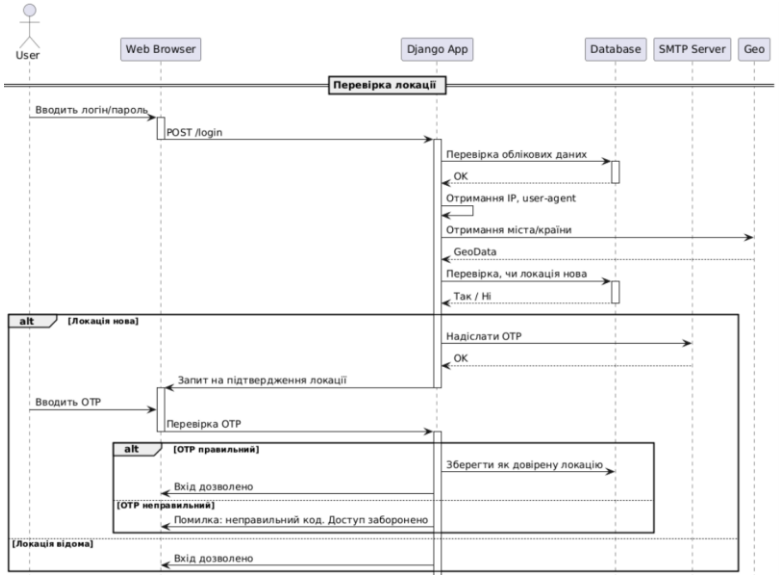


Рис 3. Процес перевірки локації користувача

Важливим аспектом забезпечення безпеки даних користувачів є політика створення надійних паролів. У системі встановлено мінімальну довжину пароля 12 символів, а також встановлені вимоги щодо використання великих та малих літер, цифр і спеціальних символів. Щоб уникнути зловживань або атак методом перебору, реалізовано блокування після декількох невдалих спроб входу. Після трьох помилок користувач мусить зачекати 60 секунд. Крім того, для безпеки сесій введено автоматичне завершення сесії після 12 годинної неактивності. При кожному запиті перевіряється час останньої активності, в разі перевищення ліміту, система автоматично завершує сесію користувача. З метою запобігання XSS-атакам, усі дані, які вводяться через форми, автоматично проходять санітизацію. Це гарантує, що шкідливі скрипти не потраплять у середовище виконання та не становитимуть загрозу для користувачів.

Щоб запобігти несанкціонованій зміні персональних даних, при спробі редагувати дані профілю, email або пароль, надсилається підтвердження на електронну пошту. Лише після введення коду, зміни зберігаються, у протилежному випадку вони скасовуються. На рис. 4 наведено механізм редагування профілю. Даний механізм застосовується для відновлення забутого пароля.

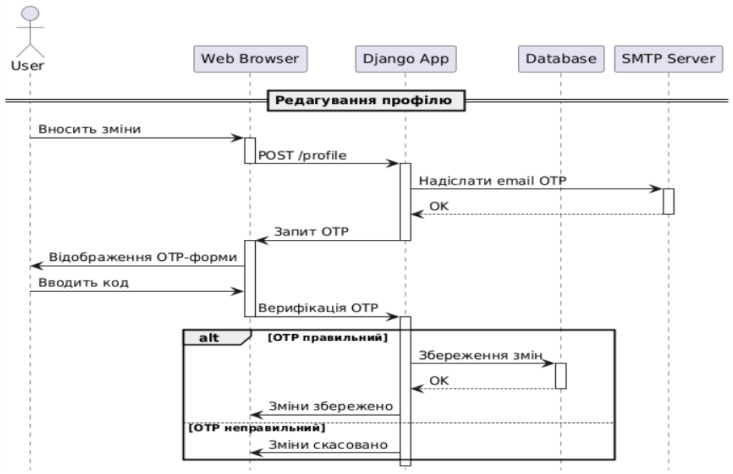


Рис. 4. Процес редагування профілю користувача

Для безпечної передачі інформації між клієнтом і сервером застосовується протокол HTTPS [16] у поєднанні з TLS. Під час встановлення з'єднання сторони узгоджують тимчасовий сесійний ключ, за допомогою якого шифрується трафік. Навіть у разі перехоплення потоку даних, без ключа інформація залишається недоступною для зловмисника. Враховуючи складність підбору ключа, злам такого з'єднання практично неможливий.

Забезпечення академічної доброчесності – ще один важливий аспект функціонування системи. Вона гарантує чесність, прозорість і довіру до результатів навчального процесу. Для запобігання несанкціонованого розповсюдження текстових матеріалів у системі реалізовано механізм додавання цифрових водяних знаків.

Водяний знак – унікальний ідентифікатор, який вбудовується у вміст тесту з метою захисту авторських прав і виявлення джерела витоку. У даній системі кожне запитання автоматично містить водяний знак, сформований на основі персональних даних користувача: його унікального ідентифікатора ID, прізвища, імені та дати народження.

Такий підхід дозволяє точно встановити, хто саме розповсюдив інформацію, якщо вона з'явилася у мережі, наприклад, на фото або знімку екрана. Генерований код вводиться у вигляді напівпрозорого сірого тексту над кожним запитанням, як це зображено на рис. 5.

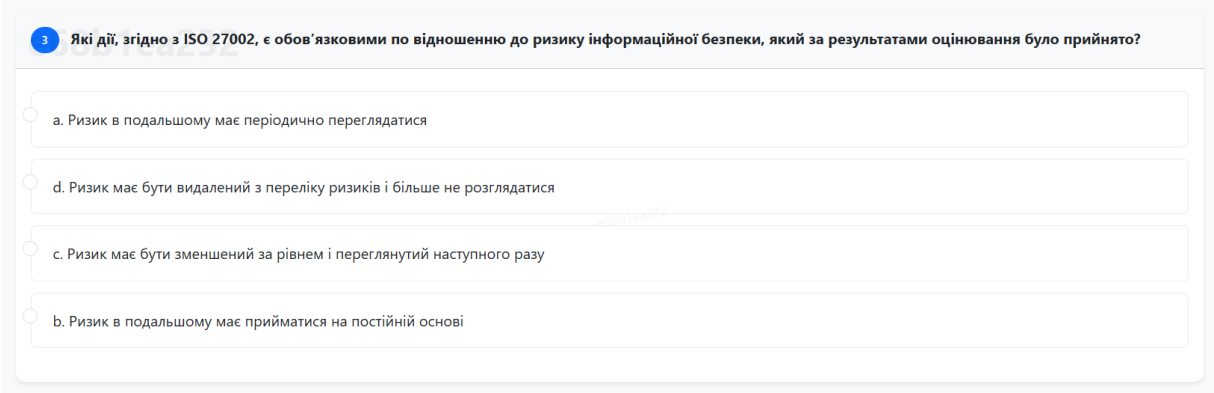


Рис. 5. Приклад розміщення водяного знаку на сайті

Для хешування використовується криптографічно стійка хеш-функція BLAKED2b [17], яка має властивість детермінованості, що дозволяє легко порівняти значення на зображенні з відповідним записом у базі даних, ідентифікувавши користувача, який порушив умови проходження опитування.

Інтерфейс системи розроблено відповідно до ролей користувачів – студентів та викладачів – з урахуванням типових сценаріїв взаємодії. Такий підхід забезпечує зручність, доступність та безпеку під час користування. Основу дизайну складають принципи мінімалізму й простоти, що дозволяє легко орієнтуватися навіть недосвідченим користувачам.

На головній сторінці розміщено назву системи, стислий опис її призначення та кнопку входу у верхній правій частині (рис. 6). Це забезпечує швидкий старт роботи з системою для обох категорій користувачів. Кнопка входу веде до стандартної форми авторизації. Дизайн головної сторінки побудований таким чином, щоб користувач відразу розумів основну мету ресурсу та легко орієнтувався.

Після авторизації з логіном і паролем, користувача перенаправляє на сторінку перевірки локації. Якщо виявлено нову IP-адресу, система запитує підтвердження через OTP-код, який надсилається на електронну пошту.

Це дозволяє запобігти спробам входу з невідомих пристроїв. Механізм реалізовано таким чином, щоб мінімізувати ризик несанкціонованого доступу. У разі відмови підтвердити нову локацію, доступ до акаунту блокується.

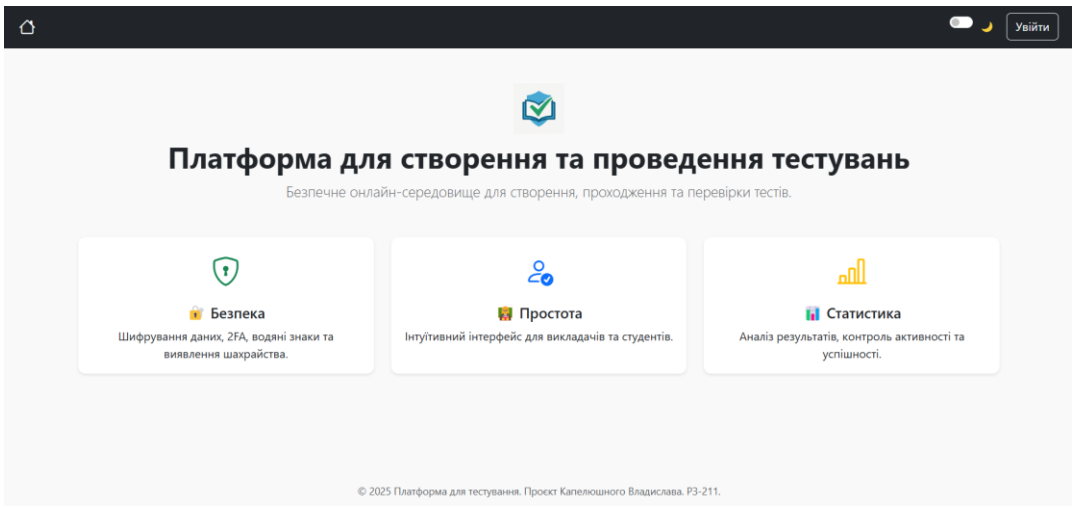


Рис. 6. Головна сторінка

При втраті пароля користувач може скористатися функцією «Забули пароль?». Після введення email-адреси, на пошту називається посилання для зміни пароля. Процес є простим та надійним, що забезпечує як зручність, так і захист акаунтів користувачів. Важливо що новий пароль повинен відповідати вимогам безпеки системи.

Кожен зареєстрований користувач має доступ до особистого профілю, де можна редагувати ім'я, прізвище, електронну пошту, номер телефону та аватар (рис. 7). Дана функціональність дозволяє підтримувати актуальність контактних даних. Усі зміни підтверджують кодом, який надходить на електронну пошту, що виключає можливість несанкціонованого редагування. Профіль має інтуїтивно зрозумілий інтерфейс редагування, що дозволяє легко оновлювати особисту інформацію.

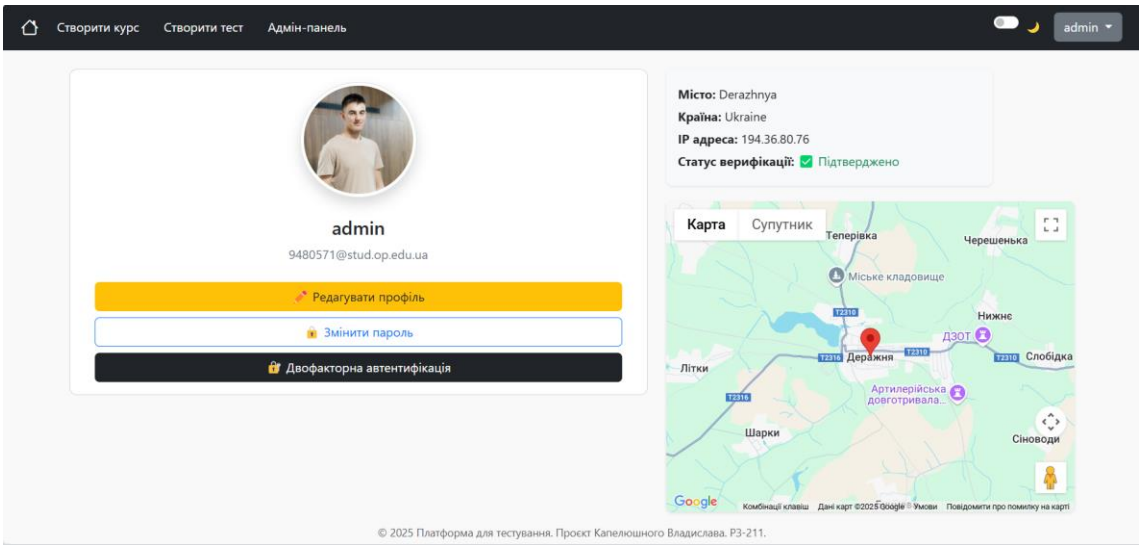


Рис. 7. Профіль користувача

Зміна пароля передбачає введення чинного пароля та нового – двічі, з додатковим підтвердженням через код з пошти, унеможливлюючи випадкову зміну пароля.

Для посилення безпеки реалізовано можливість активації двофакторної автентифікації через Google Authenticator. Процес налаштування 2FA передбачає сканування QR-коду або ведення секретного ключа вручну, після чого користувач

вводить шестизначний код із застосунка. Увімкнення цієї функції значно підвищує рівень захищеності облікового запису. Користувач також має змогу вимкнути двофакторну автентифікацію, підтвердивши цю дію через електронну пошту.

Для викладачів основним елементом взаємодії є панель адміністрування, яка надає доступ до керування курсами, тестами, користувачами та результатами. Панель має зручну навігацію та логічну структуру. Всі елементи згруповані за категоріями, що дозволяє швидко знаходити потрібні функції (рис. 8). Наприклад, викладач може перейти до списку наявних курсів, де зазначається назва, код доступу, кількість тестів і дата завершення. Кожен курс має набір кнопок для керування.

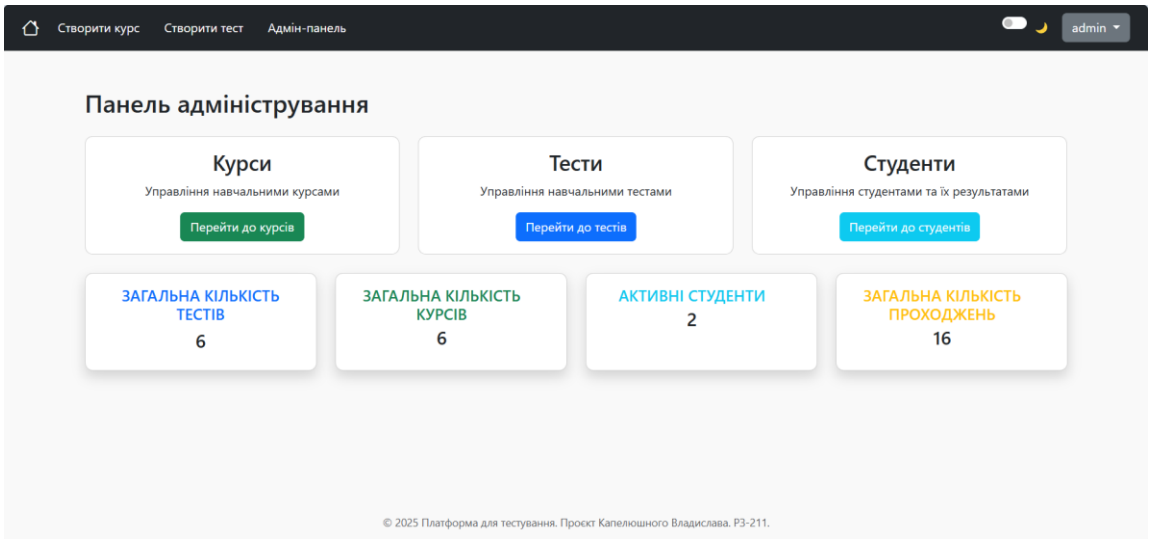


Рис. 8. Панель адміністрування

Кнопка «Створити курс» відкриває форму, в якій потрібно вказати назву, короткий опис і дату завершення. Код доступу до курсу генерується автоматично. Якщо дата завершення вказана – після неї тест буде недоступний. Курс може містити декілька тестів. Для перегляду результатів викладач може перейти до розділу статистики, де відображається ПІБ студента, отримані бали, дата проходження та кількість спроб. Інтерфейс також дозволяє виконувати пошук за курсом або студентом (рис. 9).

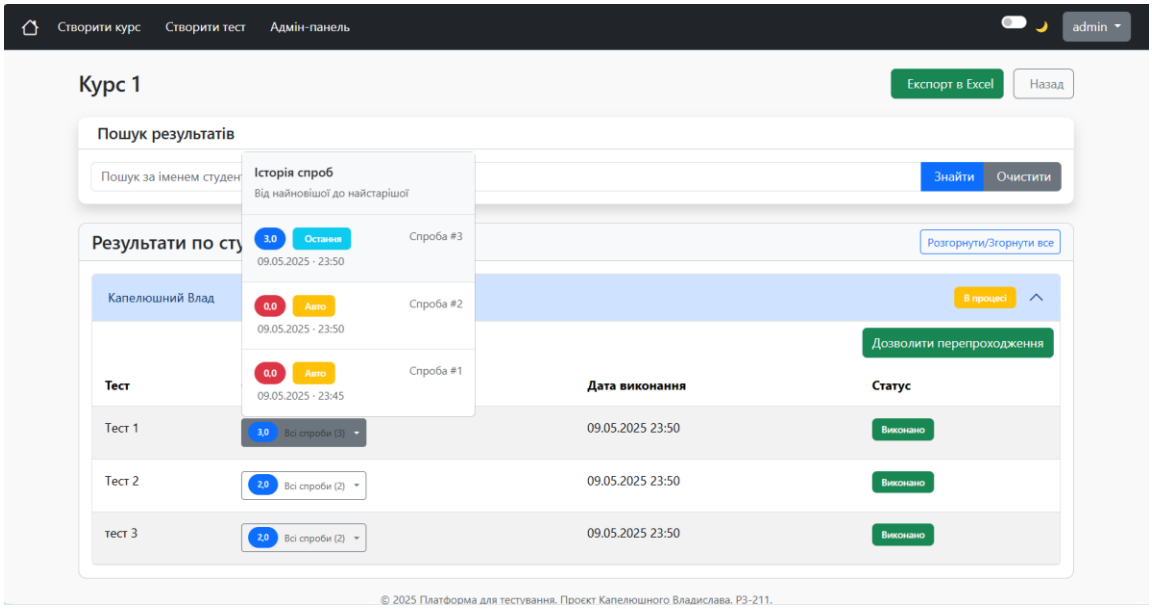


Рис. 9. Результати курсу

Відкривши вкладку «Перейти до тестів», викладач отримає доступ до списку всіх наявних в системі тестів, які можна редагувати та видаляти. При створенні нового тесту необхідно вказати назву, опис та пов'язаний курс. Після збереження, система автоматично перенаправляє користувача до інтерфейсу додавання запитань, що дозволяє безпосередньо після створення почати його наповнення контентом. Всі запитання можна редагувати, що забезпечує гнучкість при оновленні матеріалу (рис. 10).

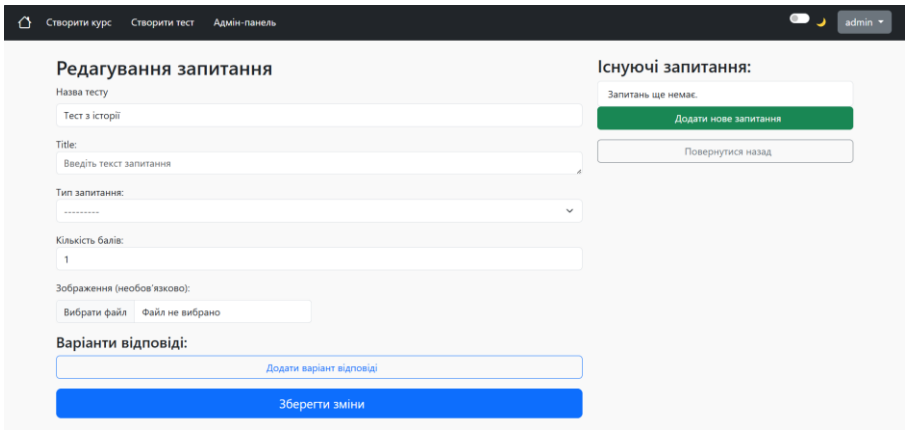


Рис. 10. Додавання запитань до тесту

Студенти після авторизації переходять до персональної панелі з вкладками: «Додати курс», «Додати тест», «Мої курси» та «Мої результати». Вони мають змогу додавати курс за кодом, який надає викладач. Якщо курс завершений або неактивний – система виведе відповідне повідомлення. Кожен студент може приєднатися до курсу лише один раз, після чого зберігає постійний доступ до всіх оновлень. У розділі мої курси студент бачить перелік приєднаних курсів та їх статус (рис. 11).

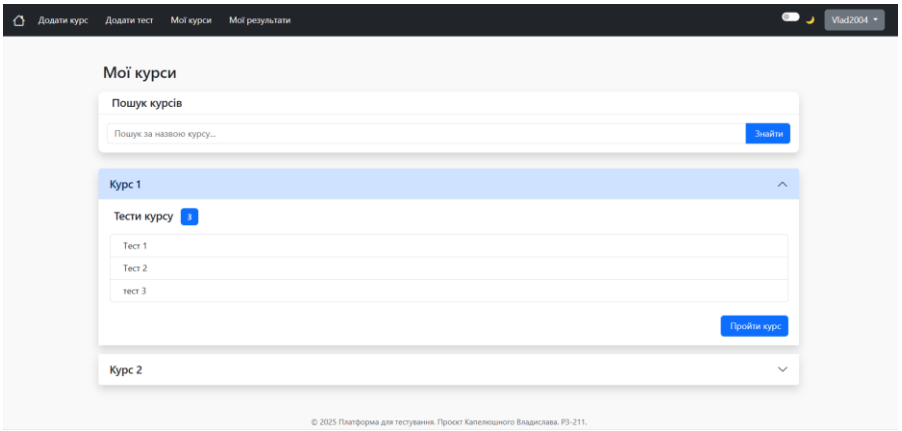


Рис. 11. Доступні для студента курси

Інтерфейс дозволяє швидко перейти до тестів, якщо вони активні. Під час проходження тесту студент бачить запитання з варіантів відповідей (рис. 12). Якщо запитання містить зображення – воно відображається праворуч. Студент може відповідати на питання у довільному порядку. Тест завершується вручну або автоматично – у випадку виходу користувача зі сторінки.

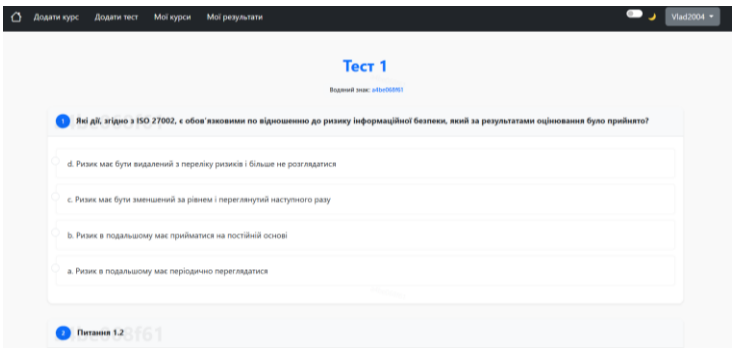


Рис. 12. Проходження тесту

Для реалізації системи було використано сучасні технології веб-програмування: Django, HTML, CSS, Bootstrap, PyCryptodome, що дозволило досягнути функціональної та візуальної відповідності потребам цільових користувачів. Інтерфейс системи адаптовано під ролі студентів та викладачів. Викладач може створювати курси, тести, редагувати запитання, контролювати кількість спроб проходження і переглядати результати. Студент може приєднуватися до курсів та тестів, проходити їх та переглядати свою статистику. Під час проходження тесту в кожному завдані відображаються водяні знаки, призначені для контролю академічної доброчесності та виявлення джерел витоку завдань. Реалізована система є комплексним безпечним рішенням для організації навчального процесу, враховуючи технічні вимоги та потреби користувачів залежно від їхніх ролей.

Висновки. У даній роботі було розглянуто ключові аспекти забезпечення безпеки системи опитувань, які є необхідною умовою для її ефективного та надійного функціонування. Визначено основні загрози пов'язані з використанням онлайн-систем, а також здійснено аналіз популярних сервісів з точки зору захисту персональних даних та відповідності сучасним вимогам кібербезпеки. Реалізована власна веб-система для створення та проведення опитувань, яка забезпечує широкий функціонал для тестування знань та надійний захист даних за допомогою сучасних механізмів інформаційної безпеки, а також має зручний і зрозумілий інтерфейс, адаптований під потреби викладачів та студентів. Описано реалізовані в системі механізми безпеки: шифрування даних в стані спокою, двофакторну автентифікацію, авторизацію на основі ролей, перевірку геолокації, політику складних паролів, автоматичне завершення сесій, захист від XSS-атак, підтвердження змін через електронну пошту, шифрування трафіку через HTTPS/TLC. Окрему увагу приділено академічній доброчесності. Запропоновано використання цифрових водяних знаків, для персоналізації кожного завдання та виявлення джерел витоку інформації. Такий підхід сприяє прозорості та контролю за розповсюдженням тестових матеріалів.

У сукупності реалізовані підходи дозволяють забезпечити високий рівень захисту системи опитувань, зберігаючи конфіденційність, цілісність та доступність даних, а також сприяють підтримуванню академічної етики в освітньому процесі. Розроблене програмне забезпечення може використовуватися як основа для впровадження в освітній процес навчальних закладів з метою безпечного й ефективного оцінювання знань. У перспективі можливе масштабування для розширення аналітики, підтримки мультимовності, додавання різних категорій завдань.

Список літератури

1. 32 Cybersecurity Stats You Can’t Ignore in 2025. https://segura.security/post/cybersecurity-stats-you-cant-ignore (дата звернення: 15.04.2025).
2. European Union Agency for Cybersecurity. Threat Landscape for Education Sector.https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

3. OWASP Foundation. Top 10 Security Risks for Web Applications. https://owasp.org/www-project-top-ten/
4. Zhang et al., Security Issues in Online Learning Platforms, IEEE Access. https://www.researchgate.net/publication/287717556_Security_Risks_and_Protection_in_Online_Learning_A_Survey
5. Google Форми: онлайн-редактор форм. https://workspace.google.com/products/forms/ (дата звернення: 02.05.2024).
6. Навчальні інструменти, картки та рішення з підручників. https://quizlet.com/ (дата звернення: 02.02.2025).
7. SurveyMonkey: The World's Most Popular Survey Platform. https://www.surveymonkey.com/?msockid=35a01cc759c3678138bb09d358d166a0 (дата звернення: 02.02.2025).
8. Google Forms. Безпека. https://www.google.com/intl/uk_ua/forms/about/#security (дата звернення: 05.02.2025).
9. Політика конфіденційності Quizlet. https://quizlet.com/privacy (дата звернення: 05.02.2025).
10. Two-factor authentication (2FA). https://help.surveymonkey.com/en/surveymonkey/account/two-factor-authentication/?utm_source=chatgpt.com#how-to-set-up-authenticator-app.
11. What happens to my data? – Help Center. https://help.typeform.com/hc/en-us/articles/360029581691 (дата звернення: 05.02.2025).
12. Aumasson J.-P. Serious Cryptography: A Practical Introduction to Modern Encryption. ed. by L. Chun. San Francisco, 2017. P. 59–75, 181-199.
13. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Global Edition / ed. by J. Tracy. Harlow, 2016. P. 177–179.
14. Що таке двофакторна автентифікація, і як вона працює. URL: https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracyuye (дата звернення: 20.02.2025).
15. Cruz J. P., Kaji Y., Yanai N. RBAC-SC: Role-based access control using smart contract. IEEE Access. 2018. P. 12240–12251.
16. Gourley D., Totty B., Sayer M., Aggarwal A., Reddy S. HTTP: The Definitive Guide. O'Reilly Media, Inc., 2002.
17. Aumasson J.-P., Meier W., Phan R. C.-W., Henzen L. The hash function BLAKE. Springer, 2014. URL: https://content.e-bookshelf.de/media/reading/L-3932227-bec7a2b730.pdf

В.Р. Капелюшний, Н.І. Кушніренко, О.В. Троянський

A SECURE SYSTEM FOR CREATING AND CONDUCTING SURVEYS

V.R. Kapelyushnyi, N.I. Kushnirenko, O.V. Troyanskiy

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: kushnirenko@op.edu.ua, o.v.troyanskiy@op.edu.ua

In the current conditions of digital transformation, security for online surveys is gaining special attention The relevance of this issue is driven by the widespread use of web services in the educational process, along with increased demands for the protection of personal data, the prevention of academic dishonesty, and the need to ensure transparency of results. The purpose of the work is to develop a secure web platform for creating, conducting and monitoring surveys that protects users' personal data, maintains academic integrity and meets modern cybersecurity requirements. The paper analyzes modern testing platforms (Google Forms, Quizlet, SurveyMonkey, Typeform), identifies their advantages and disadvantages in the context of security, in particular, limited support for two-factor authentication and weak data protection. A secure survey system with support for modern cryptographic protocols is proposed and implemented. The symmetric AES-256 encryption algorithm is used to protect the data, which guarantees the confidentiality and integrity of the stored results. The developed system also supports two-factor authentication, geolocation verification, email confirmation, HTTPS/TLC encryption, automatic session termination, and a digital watermarking mechanism that allows identifying the source of test content leakage. A practical implementation of an access control system has been carried out, including the creation of student and teacher roles and the introduction of a monitoring system for logins and changes. The results of the study confirm the feasibility of developing a custom platform as a free alternative to popular services with insufficient security levels. The proposed solution can be used in educational institutions to enhance the quality of knowledge assessment processes and ensure a high level of user data security.
Keywords: survey system, AES-256 encryption, cybersecurity, watermarks, RBAC, two-factor authentication, geolocation, academic integrity

DOI 10.15276/imms.v15.no1.83
УДК 004.04

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp.83-94

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ НА ОСНОВІ ШИФРОТЕКСТУ

А.С. Коляда, А.В. Павлишко, О.С. Лопаков, В.М. Тігарєв, В.В. Космачевський

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: a.s.koliada@op.edu.ua, pavlyshko.a.v@op.edu.ua, lopakov.o.s@op.edu.ua, tigarev.v.m@op.edu.ua, kosmachevsky.v.v@op.edu.ua

У сучасних умовах стрімкого розвитку технологій штучного інтелекту (ШІ) криптографія стикається з новими викликами, зокрема пов'язаними з можливістю використання алгоритмів машинного навчання для виявлення закономірностей у шифротекстах. З одного боку, ШІ використовується для підвищення ефективності захисту даних, а з іншого - створює загрози, пов'язані з автоматизованими атаками на криптографічні алгоритми. Метою цього дослідження є формування методики виявлення вразливостей у криптографічних алгоритмах шляхом аналізу шифротекстів за допомогою засобів машинного навчання. Для демонстрації ефективності підходу було обрано три шифри — AES-256 та ChaCha20 як сучасні криптографічні стандарти, і RC4 як приклад застарілого, криптоаналітично вразливого алгоритму. Наукова значущість роботи полягає у дослідженні нових векторів криптоаналізу з використанням Data Mining, а практична - в обґрунтуванні ризиків використання слабких алгоритмів. Роботу реалізовано у Google Colab з використанням згенерованих шифротекстів трьох алгоритмів. Дані оброблено як вектори байтів із нормалізацією, після чого навчені моделі Random Forest, XGBoost і глибинна нейронна мережа (MLP). Результати свідчать, що RC4 розпізнається з точністю 100%, що демонструє його повну вразливість до класифікаційних атак. AES і ChaCha20 показали вищу стійкість - їх шифротексти частково перекриваються у PCA-просторі, не мають яскраво виражених ознак та демонструють низьку важливість окремих байтів. Побудовано ROC-криві, теплові карти та проведено аналіз важливості ознак. Запропонована методика дозволяє оцінювати криптографічні реалізації з використанням засобів ШІ. Дослідження демонструє потенціал Data Mining у задачах криптоаналізу та може бути використане в безпековому аудиті, розробці криптографічних протоколів та в освітньому процесі.

Ключові слова: криптоаналіз, машинне навчання, класифікація, шифротекст, вразливість алгоритмів, інтелектуальний аналіз даних, шифрування, криптографічна стійкість.

Вступ. Стрімкий розвиток інформаційних технологій, особливо методів штучного інтелекту та інтелектуального аналізу даних (Data Mining), суттєво змінює сучасні підходи до інформаційної безпеки. У цьому контексті криптографія, яка залишається фундаментальним елементом захисту інформації, стикається з новими викликами та потенційними загрозами. Особливу увагу викликають можливості штучного інтелекту, які використовуються як для підсилення безпеки криптографічних систем, так і для створення нових типів атак. Актуальність теми обумовлена швидким впровадженням нейромереж, алгоритмів машинного навчання та глибинного навчання у різноманітні сфери безпеки інформації, включаючи криптоаналіз, виявлення слабких місць у алгоритмах шифрування та генерацію криптографічних ключів. Сучасні дослідження показують, що застосування алгоритмів штучного інтелекту здатне ефективно аналізувати великі об'єми криптографічних даних та виявляти в них приховані закономірності, що є потенційною загрозою для існуючих алгоритмів шифрування.

Незважаючи на значну кількість публікацій у сфері штучного інтелекту та криптографії, залишаються недостатньо дослідженими питання оцінювання стійкості сучасних криптографічних алгоритмів перед новими, AI-орієнтованими атаками. Ця робота має на меті заповнити прогалини у цій сфері, здійснивши огляд сучасних методів штучного інтелекту, що використовуються у криптоаналізі, а також експериментально оцінити вразливості популярних алгоритмів шифрування за допомогою алгоритмів машинного навчання.

У контексті практичного застосування криптографії, особливу роль відіграють не лише алгоритми, а й стандарти реалізації, описані в рекомендаціях NIST [1], зокрема щодо режимів блокового шифрування. Попри появу новітніх протоколів, у сучасних криптографічних системах досі можуть використовуватися реалізації, чутливі до некласичних векторів атак, зокрема - на основі аналізу шифротексту.

У статті буде розглянуто як теоретичні аспекти використання штучного інтелекту для аналізу стійкості криптографічних алгоритмів, так і практичні результати експериментів, які можна відтворити у доступному середовищі Google Colab. Це дозволить чітко сформулювати рекомендації щодо можливих заходів із посилення захисту криптографічних систем перед загрозами, які походять від сучасних методів аналізу даних і штучного інтелекту.

Огляд літератури. Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням обсягів конфіденційних даних, що зумовлює актуалізацію питань їх надійного захисту. Центральне місце серед інструментів забезпечення безпеки інформації займають криптографічні методи, ефективність яких суттєво залежить від стійкості до різноманітних видів атак [2].

Протягом останніх двох десятиліть значно зросла роль штучного інтелекту (ШІ) та інтелектуального аналізу даних (ІАД, Data Mining) в задачах інформаційної безпеки, зокрема у сфері криптографії. У дослідженнях [3; 4] зазначається, що використання алгоритмів машинного навчання (ML) надає нові можливості не лише для підвищення ефективності криптографічних механізмів, але й для здійснення більш витончених атак на них. Зокрема, однією із значущих тенденцій є застосування нейромережевих моделей для криптоаналізу класичних алгоритмів. Наприклад, у дослідженні Maghrebi та інших авторів [5] було продемонстровано можливості використання рекурентних нейронних мереж (RNN) для виявлення патернів та статистичних аномалій у потоках шифрованих даних, що суттєво полегшує атаки на основі обраного відкритого тексту (chosen plaintext attack).

Подібним чином, автори [6] запропонували методику застосування глибинного навчання (Deep Learning) з використанням згорткових нейромереж (CNN), яка дозволяє здійснювати класифікацію шифротекстів за криптографічним алгоритмом, незважаючи на відсутність доступу до секретного ключа. Цей підхід засвідчує реальну загрозу витоку інформації з боку нейромережевих криптоаналітичних інструментів.

Важливо відзначити також роботи у напрямку застосування методів Data Mining для виявлення атак на побічні канали (side-channel attacks). Дослідження Yu et al. [7] показало, що кластеризація та аналіз часових рядів дозволяють ефективно визначати характерні відмінності у часі виконання криптографічних алгоритмів, що вказує на вразливості цих алгоритмів до таких атак.

Окремої уваги заслуговує напрямок, пов'язаний із створенням генеративних моделей (GAN, VAE) для генерації та аналізу криптографічних ключів. Автори Huang та інші [8] продемонстрували, що GAN дозволяють генерувати псевдовипадкові ключі з високою ентропією, однак водночас їхній аналіз дозволяє знаходити приховані статистичні закономірності, що можуть бути використані зловмисниками. Також слід приділити увагу роботам, присвяченим аналізу можливостей штучного інтелекту в автоматизованому криптоаналізі та оцінці слабких реалізацій [9]. У цьому контексті доцільно враховувати не лише структуру алгоритмів, а й рівень їх реалізації в

обчислювальних середовищах, що стає все більш релевантним у зв'язку з активним використанням нейронних мереж у задачах виявлення вразливих ключів [10].

Водночас, у контексті швидкого розвитку квантових обчислень, окремі дослідження акцентують увагу на тому, що класичні алгоритми, включаючи AES і RSA, можуть втратити свою стійкість до новітніх атак. Це питання детально аналізується у праці [11], яка окреслює нові виклики та потенційні рішення для криптографії в постквантову епоху, зокрема із застосуванням підходів штучного інтелекту. Урахування викликів постквантової криптографії також є актуальним напрямом, що вимагає використання гібридних підходів. Зокрема, перспективними є постквантові алгоритми обміну ключами, такі як New Hope [12], однак їхня оцінка в контексті Data Mining-атак поки що обмежена.

Таким чином, попри значний масив публікацій, присвячених застосуванню штучного інтелекту в криптоаналізі, наразі бракує комплексного огляду, який би систематизував існуючі знання і містив практичне підтвердження у вигляді експериментального дослідження з використанням доступних інструментів, що і обумовлює вибір напрямку подальших досліджень.

Мета роботи. Метою даної статті є комплексний аналіз сучасних методів криптоаналізу, що базуються на застосуванні алгоритмів штучного інтелекту та інтелектуального аналізу даних, а також практичне оцінювання стійкості криптографічних алгоритмів різного покоління до подібних атак. Особлива увага приділяється порівнянню сучасних криптографічних стандартів (AES, ChaCha20) із застарілим, але історично важливим алгоритмом RC4, який відомий своєю вразливістю до статистичних атак.

Для досягнення поставленої мети визначено такі завдання:

- провести аналіз і систематизацію існуючих досліджень щодо використання алгоритмів машинного навчання та інтелектуального аналізу даних у криптоаналізі;
- розглянути особливості та потенційні можливості штучного інтелекту для атак на криптографічні алгоритми, зокрема атак, що ґрунтуються на ознаках шифротексту;
- виконати експериментальне дослідження з побудовою моделі машинного навчання, яка дасть змогу класифікувати шифротексти за типом використаного криптографічного алгоритму;
- здійснити оцінювання стійкості криптографічних алгоритмів AES, ChaCha20 та RC4 до атак, заснованих на методах штучного інтелекту, шляхом аналізу точності класифікаційних моделей;
- порівняти рівень розпізнаваності сучасних алгоритмів із алгоритмом RC4 як базовим прикладом статистично вразливої криптографії;
- надати рекомендації щодо підвищення стійкості криптографічних механізмів до атак з використанням інтелектуального аналізу.

Основний розділ. З метою досягнення поставленої мети було реалізовано експериментальне дослідження, що охоплює генерацію даних, підготовку ознак, побудову моделей машинного навчання та оцінювання їхньої здатності до класифікації шифротекстів. У цьому розділі наведено опис методики, вибору інструментів та інтерпретацію отриманих результатів.

Загальна методика дослідження. Для досягнення поставленої мети було сформульовано експериментальну методику, яка включає такі етапи:

- Генерація набору криптографічних даних.
- Попередня обробка та підготовка даних.
- Побудова моделей машинного навчання.
- Оцінювання ефективності моделей.
- Інтерпретація результатів.

Генерація та попередня обробка даних. На початковому етапі було згенеровано набір даних, у якому використовувались алгоритми AES-256, ChaCha20 та RC4. Для цього формувались відкриті тексти у вигляді псевдоангломовних фраз, згенерованих із частотним розподілом латинських літер та пробілів, що дозволяло відтворити природну структуру мови. Для кожного алгоритму було сформовано по 1000 прикладів, загальна кількість шифротекстів склала 3000. Кожне повідомлення мало довжину 128 байтів, що дозволяло аналізувати значення на рівні байтів після шифрування. RC4 використовував ключ довжиною 128 біт (16 байтів) та не відкидав перші байти, що спеціально моделювало вразливу реалізацію. Після шифрування дані було перетворено у числовий формат та нормалізовано в інтервалі [0; 1] за допомогою MinMaxScaler, щоб забезпечити сумісність із моделями ML (рис. 1).

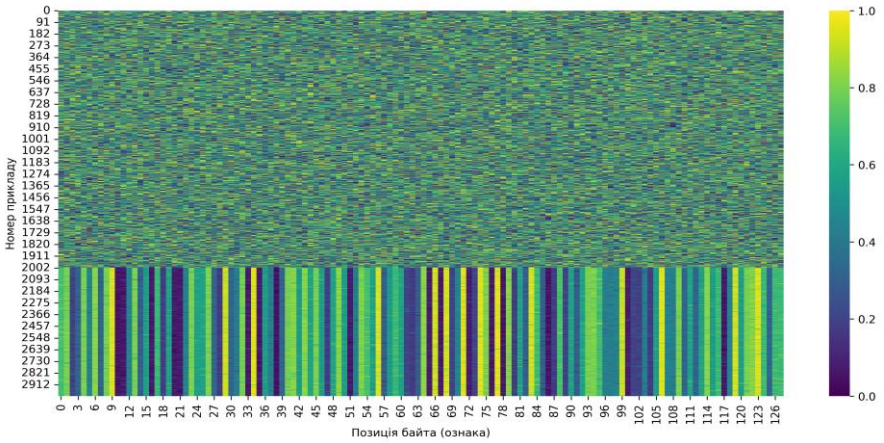


Рис. 1. Теплова карту нормалізованих шифротекстів, де спостерігаються характерні вертикальні структури для RC4, на відміну від випадкового фону AES і ChaCha20.

Побудова моделей машинного навчання. На другому етапі дослідження було здійснено побудову моделей машинного навчання для розв'язання задачі багатокласової класифікації шифротекстів за типом використаного алгоритму шифрування. З метою порівняльного аналізу ефективності було обрано три різні підходи, що репрезентують класичні, ансамблеві та нейромережеві моделі:

- Random Forest — ансамблевий метод, що ґрунтується на побудові великої кількості дерев рішень, кожне з яких тренується на випадковій підмножині даних. Кінцеве рішення приймається шляхом голосування. Цей метод є стійким до переобучення, добре працює з табличними структурованими даними й дозволяє інтерпретувати результати через механізм оцінювання важливості ознак.
- XGBoost (Extreme Gradient Boosting) — потужний ансамблевий алгоритм бустингу, що поєднує слабкі класифікатори у сильну модель. Завдяки оптимізованому обчисленню градієнтів, регуляризації та підтримці паралелізації, XGBoost демонструє високу точність на різноманітних наборах даних. Він особливо ефективний для розпізнавання прихованих закономірностей у великій кількості вхідних ознак, що актуально при аналізі шифротекстів.
- Глибинна нейронна мережа (Multi-Layer Perceptron, MLP) — повнозв'язна нейромережа, яка складається з кількох шарів перцептронів із нелінійною активацією. Використання глибинної структури дозволяє моделі апроксимувати складні багатовимірні функції розподілу, що особливо корисно при виявленні слабких статистичних відмінностей у криптографічно стійких шифротекстах.

Усі моделі були реалізовані у середовищі Google Colab з використанням бібліотек scikit-learn, xgboost для реалізації нейромережевої моделі [13]. Для кожної моделі було проведено крос-перевірку та підбір гіперпараметрів, зокрема: кількість дерев для

Random Forest, максимальна глибина та швидкість навчання для XGBoost, кількість нейронів, шарів і функцій активації для глибинної нейронної мережі.

Експериментальне дослідження. Після формування набору даних, усі шифротексти були випадковим чином поділені на тренувальну (70%) та тестову (30%) вибірки. На основі тренувального набору відбувалося навчання моделей машинного навчання, після чого їхня ефективність перевірялась на тестовому наборі. Для оцінювання якості класифікації було використано такі основні метрики:

- Accuracy (загальна точність класифікації) — відображає частку правильно класифікованих прикладів серед усіх. Ця метрика є загальною характеристикою якості, проте в умовах дисбалансу класів або багатокласової класифікації може бути недостатньо інформативною.
- Precision (точність для кожного класу) — визначає, яку частку з передбачених для певного класу об’єктів модель класифікувала правильно. Важлива, коли критичним є зменшення хибно позитивних спрацьовувань.
- Recall (повнота) — відображає, яку частку об’єктів певного класу модель змогла правильно ідентифікувати. Використовується для оцінки здатності моделі виявляти всі об’єкти цільового класу.
- F1-score — гармонійне середнє між Precision та Recall. Забезпечує збалансовану оцінку в тих випадках, коли важливо зберігати компроміс між виявленням об'єктів і уникненням хибних спрацювань.
- ROC-крива (Receiver Operating Characteristic) — це графік, що відображає співвідношення між True Positive Rate (повнотою) і False Positive Rate при зміні порогу класифікації. ROC-криві дозволяють візуально порівняти якість моделей у багатокласовому підході за схемою One-vs-Rest (OvR), де кожен клас по черзі вважається "позитивним", а решта — "негативними".
- AUC (Area Under the Curve) — числове значення, що визначає площу під ROC-кривою. Значення AUC $\in$ [0, 1], де 1.0 означає ідеальну класифікацію, а 0.5 — випадкове вгадування. У контексті багатокласової класифікації використовується середнє значення AUC для кожного класу.

Результати моделювання показали, що шифротексти, згенеровані алгоритмом RC4, були ідентифіковані з AUC = 1.00 у всіх протестованих моделях, що свідчить про повну відокремленість цього класу у просторі ознак. Інакше кажучи, моделі змогли безпомилково відокремити RC4 від інших алгоритмів, що є ознакою статистичної вразливості. Для алгоритмів AES та ChaCha20 значення AUC $\approx$ 0.73 вказує на високий ступінь подібності у їхній байтовій структурі та меншу розрізнюваність, що свідчить про вищу стійкість до класифікаційних атак на основі аналізу шифротексту.

Обґрунтування вибору алгоритмів і моделей. Алгоритми AES та ChaCha20 були обрані як приклади сучасних криптографічних стандартів, які активно використовуються в протоколах безпечної передачі даних, зокрема TLS 1.3. Алгоритм ChaCha20, запропонований Деніелом Бернштейном [14], став популярною альтернативою блочним шифрам завдяки високій швидкодії, потоковій природі та стійкості до атак на основі побічних каналів. RC4, у свою чергу, було включено до дослідження як приклад застарілого шифру, відомого своєю вразливістю до статистичних атак, зокрема при неправильній реалізації.

Для класифікації шифротекстів було обрано моделі машинного навчання, які довели свою ефективність у задачах багатокласової класифікації, аналізу структурованих даних і пошуку прихованих закономірностей. Random Forest забезпечує стабільну роботу навіть за наявності шуму та є інтерпретованим за рахунок оцінки важливості ознак. XGBoost демонструє високу точність і швидкість завдяки використанню градієнтного бустингу з оптимізацією втрат, що особливо важливо при обробці великих обсягів криптографічних даних. Глибинні нейронні мережі здатні моделювати складні нелінійні залежності між байтами шифротексту, що дає змогу

виявити приховані патерни навіть у високовипадкових послідовностях. Використання бібліотек машинного навчання реалізовано відповідно до сучасних рекомендацій щодо побудови моделей із застосуванням фреймворків scikit-learn як це описано в [15].

Методика оцінювання стійкості криптографічних алгоритмів. На основі точності класифікації запропоновано просту шкалу оцінювання стійкості алгоритму до атак на основі аналізу шифротексту:

Таблиця 1.

Рекомендації щодо рівнів стійкості алгоритмів

Точність класифікації (%)	**Рівень стійкості алгоритму**	**Рекомендації**
90-100	Низький (наявні серйозні закономірності)	Необхідний перегляд алгоритму
70-89	Помірний (потрібні додаткові перевірки)	Рекомендовані додаткові аналізи
50-69	Високий (мінімальні закономірності)	Алгоритм безпечний для більшості застосувань
<50	Дуже високий (закономірності не виявлено)	Алгоритм безпечний

За цією методикою:

- RC4 отримує оцінку "Низький рівень стійкості", оскільки моделі класифікували його з ідеальною точністю.
- AES та ChaCha20 мають високий або дуже високий рівень стійкості, оскільки класифікатор не зміг з надійністю розрізнити їх.

Результати та обговорення. У ході експериментального дослідження було проаналізовано ефективність моделей машинного навчання при класифікації шифротекстів, згенерованих за допомогою трьох криптографічних алгоритмів: AES-256, ChaCha20 та RC4. Оцінювання здійснювалось за низкою метрик, що дозволяє комплексно оцінити рівень стійкості кожного з алгоритмів до атак, заснованих на інтелектуальному аналізі даних.

Аналіз результатів класифікації шифротекстів. Результати класифікації шифротекстів наведено в таблиці 2. Усі три моделі машинного навчання — Random Forest, XGBoost та глибинна нейронна мережа — показали узгоджено високі результати при класифікації трьох типів шифротекстів (AES, ChaCha20, RC4), що свідчить про наявність розпізнаваних закономірностей у байтових структурах хоча б одного з класів.

Таблиця 2.

Зведені метрики класифікації шифротекстів за алгоритмами шифрування

Модель	**Accuracy**	**Precision (macro)**	**Recall (macro)**	**F1-score (macro)**	**ROC-AUC (ovr)**
Random Forest	0.6467	0.6467	0.6467	0.6466	0.8219
XGBoost	0.6711	0.6711	0.6711	0.6709	0.8365
Глибинна нейромережа	0.6633	0.6633	0.6633	0.6632	0.8321

Показники ROC-AUC перевищують 0.82 для всіх моделей, що вказує на високу чутливість моделей до відмінностей між принаймні одним із класів. Найвищу ефективність продемонструвала модель XGBoost, яка досягла точності класифікації 67.11% при AUC 0.8365, однак усі моделі показали узгоджену якість класифікації. Для уточнення, який саме клас найкраще класифікується, у таблиці 3 наведено детальний звіт моделі Random Forest. З нього видно, що саме шифротексти, згенеровані за допомогою RC4, були розпізнані з ідеальною точністю (Recall = 1.00, Precision = 1.00), тоді як класи AES і ChaCha20 частково перекривались, що знизило загальні макрооцінки.

Таблиця 3.

Деталізовані метрики класифікації за класами (модель Random Forest)

Клас	Precision	Recall	F1-score
AES	0.47	0.46	0.46
ChaCha20	0.47	0.48	0.48
RC4	1.00	1.00	1.00
Середнє (macro avg)	0.65	0.65	0.65
Зважене (weighted avg)	0.65	0.65	0.65

Як видно з результатів, моделі машинного навчання здатні виявляти приховані статистичні патерни в шифротекстах RC4, що дає змогу з високою точністю класифікувати його. Натомість AES та ChaCha20 демонструють вищу стійкість, оскільки їх шифротексти не мають чітко виражених відмінних ознак, що ускладнює класифікацію. Це підтверджує припущення про низьку криптостійкість RC4 до атак на основі ознак шифротексту, а також підкреслює важливість подібного аналізу при виборі алгоритмів для реальних криптографічних систем.

Візуалізація результатів експерименту. Для більш глибокого аналізу було побудовано ROC-криві для кожного з класів (рис. 2). Шифротексти RC4 були ідентифіковані з AUC = 1.00, що свідчить про повну відокремленість цього алгоритму у векторному просторі ознак. Водночас AES і ChaCha20 мали AUC ≈ 0.73, демонструючи схожі характеристики шифрування.

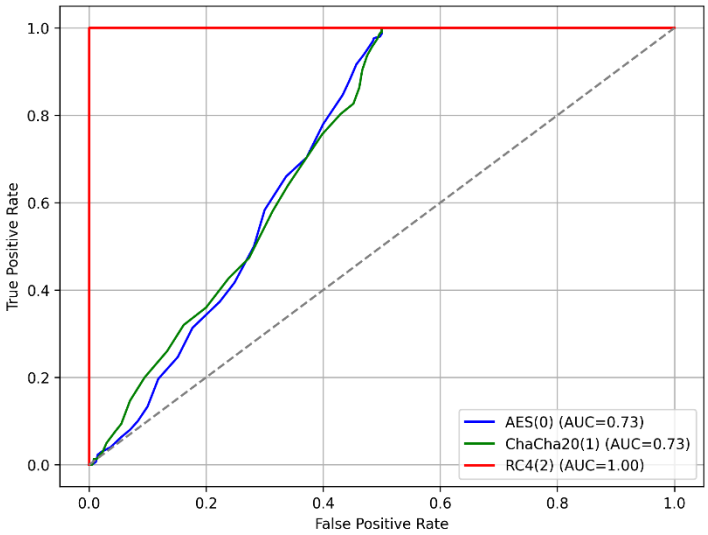


Рис. 2. ROC-криві класифікації шифротекстів (One-vs-Rest, Random Forest)

Також було виконано зниження розмірності ознак за допомогою методу головних компонент (Principal Component Analysis, PCA) — статистичного підходу, що

дозволяє спроєктувати багатовимірні дані в простір меншої кількості вимірів (наприклад, 2D), зберігаючи при цьому максимальну дисперсію. Це дає змогу візуалізувати структуру даних і виявити наявність кластерів або перекриттів між класами. Як видно на рис. 3, шифротексти, згенеровані за допомогою алгоритму RC4, формують щільний і добре ізольований кластер, що вказує на наявність стабільних повторюваних статистичних патернів. Натомість шифротексти, створені алгоритмами AES та ChaCha20, значною мірою перекриваються у PCA-просторі, що підтверджує відсутність яскраво виражених відмінностей у їхніх статистичних характеристиках — тобто вищу стійкість до класифікації на основі ознак шифротексту.

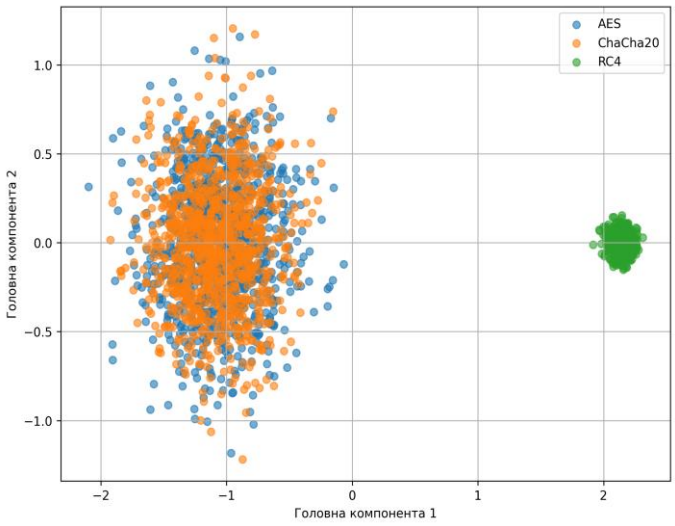


Рис 3. PCA-візуалізація простору шифротекстів

Для пояснення внутрішньої логіки моделей було проаналізовано важливість ознак (байтових позицій) у шифротекстах. Результати (рис. 4) показали, що класифікатор Random Forest використовував певні позиції з більшим впливом (наприклад, B74, B68, B34), що свідчить про залишкову структурність у RC4.

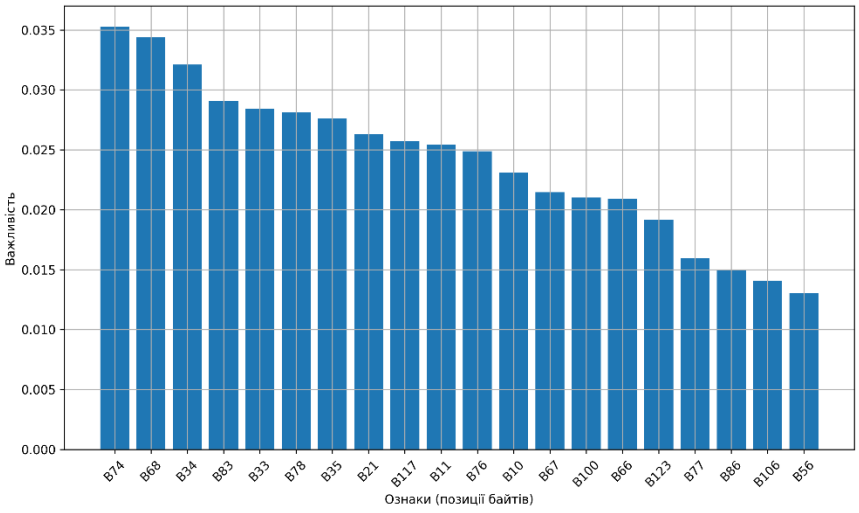


Рис 4. Важливість ознак у шифротекстах (Random Forest)

Крім загальних метрик класифікації, було побудовано матрицю помилок (confusion matrix), яка показує співвідношення реальних і передбачених класів (рис. 5). Вона ілюструє такі ключові моменти:

- Алгоритм RC4 розпізнається абсолютно точно: модель не зробила жодної помилки в класифікації шифротекстів цього алгоритму.
- Натомість, AES та ChaCha20 регулярно плутаються між собою, що підтверджує схожість їхніх статистичних ознак при обробці текстових повідомлень.
- Загальна точність моделі Random Forest склала 65%, однак усі помилки пов'язані лише з двома сучасними алгоритмами, а не з RC4.

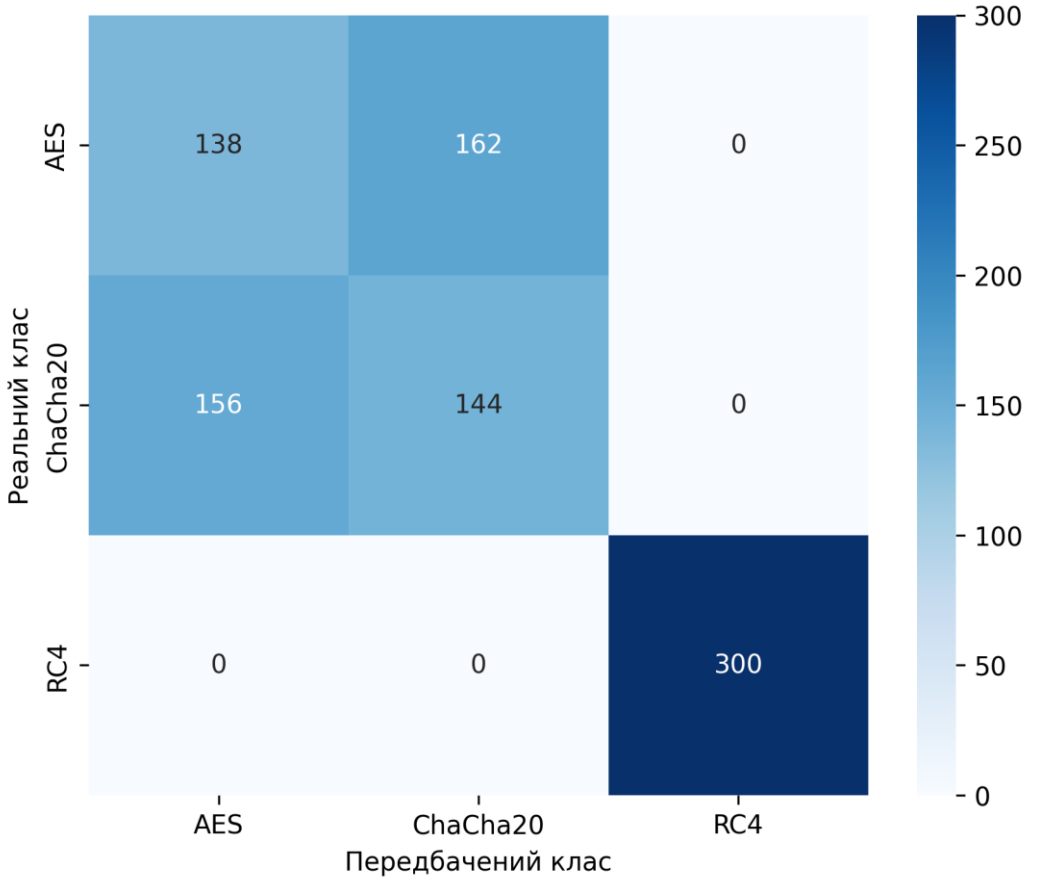


Рис 5. Матриця помилок класифікації шифротекстів (Random Forest, 3 класи)

Обговорення отриманих результатів. Аналіз отриманих результатів дозволяє зробити такі висновки щодо стійкості розглянутих алгоритмів:

- RC4 демонструє низький рівень стійкості, оскільки всі моделі змогли класифікувати його шифротексти з високою точністю. Це пов'язано з його відомими вразливостями, а також із тим, що шифротексти RC4 не забезпечують достатню ентропію на початку потоку.
- AES-256 і ChaCha20 виявились більш стійкими до класифікації, оскільки їхні шифротексти статистично невиразні. Особливо слід зазначити перевагу ChaCha20, який як потоковий шифр з довгою пермутацією забезпечує кращу випадковість навіть при шифруванні структурованих текстів.
- Значення ROC-AUC у діапазоні 0.73 для AES і ChaCha20 свідчить, що моделі все ж таки змогли у деяких випадках виявити незначні закономірності, що потребує подальшого дослідження.

Візуалізації (PCA, heatmap, ROC) підтверджують статистичну відокремленість RC4, вказуючи на те, що навіть базові моделі машинного навчання можуть використовуватись для ідентифікації слабких алгоритмів шифрування за одним лише шифротекстом. Таким чином, результати дослідження демонструють реальні можливості штучного інтелекту в задачах криптоаналізу, а також підкреслюють

необхідність виключення застарілих алгоритмів (RC4) з будь-яких сучасних криптографічних систем.

Висновки. За результатами проведеного дослідження, спрямованого на аналіз стійкості криптографічних алгоритмів до атак, що базуються на методах штучного інтелекту та інтелектуального аналізу даних, сформульовано такі висновки:

Аналіз наукової літератури підтвердив зростання ролі алгоритмів штучного інтелекту (ШІ) у сучасному криптоаналізі. З одного боку, ці методи можуть підсилювати захист інформації (наприклад, оптимізація генерації ключів), з іншого — становлять загрозу внаслідок можливості автоматизованого виявлення закономірностей у криптографічних даних.

Запропонована експериментальна методика, що базується на класифікації шифротекстів з використанням моделей Random Forest, XGBoost та глибинних нейронних мереж, дозволила ефективно виявити наявність або відсутність статистичних ознак у шифрованих даних, навіть без доступу до відкритого тексту.

Додавання до аналізу алгоритму RC4 дало змогу наочно продемонструвати ефективність підходу: моделі машинного навчання змогли класифікувати його шифротексти з точністю 100%, що вказує на істотну криптографічну вразливість даного алгоритму. Цей результат підкреслює необхідність повного виключення RC4 з практики сучасної інформаційної безпеки.

Сучасні алгоритми AES-256 та ChaCha20 показали високий рівень криптостійкості до атак на основі аналізу шифротекстів. Особливо слід відзначити ChaCha20, шифротексти якого виявились менш передбачуваними для моделей ML, що частково пов’язано з особливостями потокового шифрування та довготривалими пермутаціями в його структурі.

Візуалізаційні методи аналізу (PCA, теплові карти, важливість ознак) підтвердили відсутність чітких кластерів та інформаційно значущих байтів у шифротекстах AES і ChaCha20, на відміну від RC4, що лишає статистичні патерни. Це дозволяє використовувати такі підходи як ефективний інструмент виявлення вразливих реалізацій шифрів.

Практична реалізація в середовищі Google Colab засвідчила доступність і відтворюваність експериментів навіть на непрофесійних обчислювальних платформах, що підвищує прикладну цінність методу для освітніх, дослідницьких і тестувальних цілей.

Рекомендовано додатково оцінювати криптографічні алгоритми за допомогою інструментів штучного інтелекту та Data Mining. Класичні підходи криптоаналізу варто доповнювати автоматизованими методами аналізу статистики шифротекстів, що дозволить на ранньому етапі виявляти потенційні вразливості, зокрема в реалізаціях на рівні протоколів.

Напрями подальших досліджень передбачають:

розширення переліку досліджуваних шифрів, зокрема включення симетричних, асиметричних і постквантових алгоритмів;

тестування різних типів вхідних даних (наприклад, зображень, відео, IoT-трафіку);

аналіз чутливості моделей до модифікацій відкритого тексту, довжини повідомлення та ключів;

дослідження комбінованих атак, які поєднують Data Mining із побічними каналами (timing, EM, cache).

Список літератури

1. Dworkin M. *Recommendation for Block Cipher Modes of Operation: Methods and Techniques (NIST SP 800-38A)*. Gaithersburg : NIST, 2001. 66 p.
2. Stallings W. *Cryptography and Network Security: Principles and Practice*. 8th ed. Pearson Education, 2020. 832 p.

3. Alani M. M. Applications of machine learning in cryptography: a survey. *International Journal of Information Technology and Computer Science*. 2021. Vol. 13, № 2. P. 23–31.
4. Blum T. Neural Cryptography: The Next Frontier. *Cryptography Journal*. 2019. Vol. 32, № 1. P. 45–58.
5. Maghrebi H., Portmann C., Bohnert T. Reinforcement Learning for Cryptanalysis of Classical Ciphers. *IEEE Transactions on Information Forensics and Security*. 2021. Vol. 16. P. 3967–3979.
6. Chen W. AI-Based Key Generation for Enhanced Security. *Proceedings of the International Conference on Computer & Information Security (ICCIS)*. Tokyo, 2020. P. 112–119.
7. Yu Q., Liu J., Wang X. Side-channel attacks detection using machine learning methods. *Journal of Information Security and Applications*. 2022. Vol. 65. Art. no. 103123.
8. Huang Y., Lin J., Wang R. Deep Generative Adversarial Networks for Cryptographic Key Generation. *Journal of Cryptographic Engineering*. 2022. Vol. 12. P. 45–56.
9. Chouhan R., Jha R., Singh A. Cryptanalysis Using Artificial Intelligence Techniques: A Review. *Journal of Discrete Mathematical Sciences and Cryptography*. 2023. Vol. 26, № 1. P. 183–196.
10. Мельник А. О., Стрельбицький О. С. Застосування нейронних мереж для розпізнавання слабких криптографічних ключів. *Інформаційна безпека*. 2021. Т. 27, № 2. С. 141–150.
11. Коляда А. С., Павлишко А. В., Літвінов В. Ф. Криптографія після квантової ери: нові виклики та рішення для інформаційної безпеки. *Informatics and Mathematical Methods in Simulation*. 2024. Т. 14, № 3. С. 183–190.
12. Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-quantum key exchange - a new hope // *Proc. of the 25th USENIX Security Symposium*. 2016. P. 327–343.
13. Приклад коду для дослідження стійкості шифрів до атак машинного навчання. - Google Colab. – URL: https://colab.research.google.com/drive/107eYyp6E3JKI52WEj66lDAEZxDZKMhNj?usp=sharing.
14. Bernstein D. J. ChaCha, a variant of Salsa20. *Workshop Record of SASC*. Lausanne, Switzerland : EPFL, 2008. P. 1–7.
15. Géron A. *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. 3rd ed. O'Reilly Media, 2022. 858 p.

А.С. Коляда, А.В. Павлишко, О.С. Лопаков, В.М. Тігарєв, В.В. Космачевський

USING MACHINE LEARNING TO DETECT VULNERABILITIES IN CRYPTOGRAPHIC ALGORITHMS BASED ON CIPHERTEXT ANALYSIS

A.S. Koliada, A.V. Pavlyshko, O.S. Lopakov, V.M. Tigariev, V.V. Kosmachevskiy

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: a.s.koliada@op.edu.ua, pavlyshko.a.v@op.edu.ua, lopakov.o.s@op.edu.ua, tigarev.v.m@op.edu.ua, kosmachevsky.v.v@op.edu.ua

In the current era of rapid development in artificial intelligence (AI) technologies, cryptography faces new challenges, particularly those related to the potential use of machine learning algorithms to detect patterns in ciphertexts. On the one hand, AI is used to enhance data protection mechanisms; on the other hand, it introduces new threats associated with automated attacks on cryptographic algorithms. The aim of this study is to develop a methodology for identifying vulnerabilities in cryptographic algorithms by analyzing ciphertexts using machine learning techniques. To demonstrate the effectiveness of the approach, three ciphers were selected: AES-256 and ChaCha20 as modern cryptographic standards, and RC4 as a legacy cipher known for its cryptanalytic weaknesses. The scientific significance of this work lies in the exploration of new vectors for cryptanalysis based on data mining methods. Its practical value is in substantiating the risks of using weak encryption algorithms. The research was conducted using the Google Colab platform, where ciphertexts generated by the three algorithms were treated as normalized byte vectors. Models based on Random Forest, XGBoost, and a deep neural network (MLP) were then trained to classify the encrypted data. The results show that RC4 was classified with 100% accuracy, clearly demonstrating its vulnerability to classification-based attacks. In contrast, AES and ChaCha20 exhibited significantly greater resistance — their ciphertexts overlapped in PCA space, lacked strongly distinguishable features, and showed low per-byte feature importance. ROC curves were constructed, heatmaps visualized, and feature importance analyses conducted. The proposed methodology enables the assessment of cryptographic implementations using AI tools. The study highlights the potential of data mining in cryptanalysis tasks and can be applied to security auditing, cryptographic protocol development, and educational purposes.

Keywords: cryptanalysis, machine learning, ciphertext, classification, algorithm vulnerability, data mining, encryption, cryptographic robustness.

DOI 10.15276/imms.v15.no1.95
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 95-106

РОЗРОБКА ЗАСТОСУНКУ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ КІБЕРСТАЛКІНГУ

О.В. Кузан, Н.І. Кушніренко, В.О. Назаров, В.В. Подуфалов

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Email: kushnirenko@op.edu.ua

На сьогодні, кіберсталкінг показав себе як надзвичайно швидкозростаюче явище, яке спричинило зміну парадигм переслідування. Воно полягає у нав'язливому, систематичному втручанні в онлайн-життя жертви з метою психологічного тиску, маніпуляцій, залякування, тощо. Незважаючи на масштаб проблеми, ефективних засобів автоматизованого виявлення таких загроз українською мовою на сьогодні бракує. Метою даної роботи є підвищення безпеки користувачів у цифровому середовищі шляхом розробки застосунку для виявлення кіберсталкерської поведінки в електронних листах, з використанням машинного навчання. В рамках дослідження проведено аналіз явища кіберсталкінгу, а також сучасних підходів до його виявлення, який дозволив визначити напрямки розробки та основні завдання роботи. Розроблений застосунок базується на використанні алгоритму SVM для побудови моделей, навчання яких здійснюється на спеціально сформованому датасеті. Створено дві моделі: бінарну – для класифікації листів на «кіберсталкінг» і «не кіберсталкінг» та багатокласову – для поділу за типами: залякування, сексуальний харасмент і звичайний кіберсталкінг. Цей інструмент також надає можливість зберігати виявлені повідомлення кіберсталкера як докази, задля подальшого звернення жертв до кіберполіції. Тестування підходу показало його високу ефективність: загальна точність бінарної моделі склала 99%, багатокласова досягла 89%. Отримані результати засвідчують значний потенціал застосунку у виявлення кіберпереслідувань і таким чином підвищення рівня цифрової безпеки користувачів в онлайн-комунікаціях, тож запропонований застосунок для виявлення кіберсталкінгу може бути успішно впроваджений для особистого використання. Результати даної роботи можуть бути використані при подальших дослідженнях та розробках у сфері кібербезпеки та боротьби з кіберсталкінгом.

Ключові слова: кіберсталкінг, електронна пошта, машинне навчання, класифікація тексту, кібербезпека.

Вступ. В наш час цифрові технології стали невід'ємною складовою повсякденного життя суспільства. Їх стрімкий розвиток відкрив нові горизонти для комунікації та обміну інформацією в інтернеті. Однак, водночас із позитивними змінами, цифрова епоха принесла людству низку нових викликів, зокрема стрімке зростання кіберзлочинності, тобто злочинності саме в кіберпросторі. Традиційні злочини, пройшовши через технічну адаптацію, створили своїх кібернащадків, які незважаючи на деякі схожі риси, містять в собі важливі відмінності: мають власні механізми реалізації та інакший вплив, тому їх не можна розглядати виключно як продовження традиційних злочинів. Одним з таких кіберзлочинів, який наразі набирає обертів у своєму поширенні є кіберсталкінг. Сам термін походить від розуміння традиційного сталкінгу і відноситься до переслідування, яке відбувається в онлайн-середовищі. На сьогодні, не існує єдиного визначення чи чітких критеріїв кіберсталкерської поведінки, проте якщо проаналізувати які види поведінки найчастіше включаються в концептуалізацію та які конкретні критерії необхідні для того, щоб класифікувати модель поведінки як кіберсталкінг, то можна зробити певне узагальнення, що це форма нав'язливої поведінки, яка відбувається в кіберпросторі за допомогою цифрових технологій. Вона характеризується такими елементами як: небажаність поведінки, повторюваність, систематизованість, спосіб

здійснення – використання цифрових технологій; руйнівний вплив [1]. До найпоширеніших компонентів кіберсталкінгу вносять: пошук і збір інформації про жертву з метою переслідування, погроз і залякування онлайн; неодноразову небажану розсилку електронних листів та інших типів повідомлень; крадіжка особистих даних; підписка жертви на послуги; купівля товарів і послуг від імені жертви; видавання себе за жертву в Інтернеті; надсилання або розміщення приватних матеріалів, дезінформації; а також втягнення інших користувачів Інтернету в переслідування або погрози на адресу жертви [2, 3]. Тобто можна сказати, що кіберсталкерами задіяні майже всі куточки кіберпростору; і також, доречно зазначити, що ці елементи завжди трансформуватимуться в міру розвитку технологій.

Кіберсталкер – це особа, яка використовує технології та кіберпростір як засоби для залякування, погроз, переслідування та нагнітання страху за допомогою тактики переслідування. Кіберсталкери не утворюють єдиної, чітко визначеної групи, оскільки їхня поведінка та мотиви значною мірою залежать від особистісних характеристик конкретної особи. Кіберсталкер може бути знайомий жертві, або навпаки, дуже часто абсолютно незнайомі люди діють онлайн на умовах анонімності [2]. До сьогодні, найпопулярнішою типологією вважається розробка Л. Макфарлейн та П. Бочого, які провели ґрунтовне дослідження феномену, в результаті виділивши чотири основні типи кіберсталкерів – стриманий, інтимний, колективний, мстивий [4].

Особливу увагу приділяють саме інтимним кіберсталкерам. Хоча будь-хто може бути інтимним кіберсталкером, який, наприклад, надсилає жертві нав'язливі повідомлення з інтимним підтекстом, немає нікого, хто б краще підходив для цього злочину окрім попередніх партнерів. Оскільки попередні партнери часто мають у своєму розпорядженні особисту інформацію своїх колишніх, переслідування стає легким завданням. З цим питанням тісно переплітається інше: відповідно до досліджень, більшість кіберсталкерів є чоловіки, а жертви зазвичай – жінки. Важливим є також те, що кіберсталкінг відноситься до основних видів насильницької поведінки якій сприяють технології, тобто кібернасильства. Особливої поширеності він набув при скоєнні підвиду кібернасильства – кіберсексуального насильства [5, 6]. Жінки-переслідувані зазвичай гостріше відчувають негативні наслідки кіберпереслідувань, але їхні повідомлення про це часто ігноруються або сприймаються менш серйозно, ніж аналогічні випадки, про які повідомляють жертви-чоловіки, що сприяє продовженню кіберсталкерської поведінки, бо зловмисники відчувають безкарність у своїх діях [7].

Говорячи про наслідки, то їх усвідомлення відіграє головну роль у розробці дієвих заходів для протидії цьому явищу, підвищенні рівня обізнаності користувачів. І незважаючи на розбіжності в способах вимірювання злочину, були зроблені чіткі висновки щодо його негативного впливу. Прийнято вважати, що кіберсталкінг може змінюватися від небезпечних електронних повідомлень до потенційно смертельної зустрічі між кривдником і жертвою. І чим довше триває кіберпереслідування та чим інтенсивнішим воно стає, тим серйознішими є наслідки для жертви. Поведінка кіберзлочинця завдає шкоду фінансовій, кар'єрній, емоційній, психологічній, соціальній та фізичній сферам життя переслідуваного [1, 2]. Ці наслідки можуть не поширюватися на всіх жертв кіберсталкінга, проте коли вони виникають, то вносять хаос у життя жертви. Незважаючи на це, кіберпереслідування в суспільстві часто розглядається не як карне правопорушення, а просто аморальний вчинок. Це становить вагому проблему, тому що доведено, що кіберсталкінг – це перш за все кіберзлочин [7]. За даними досліджень, найпоширенішим серед переслідуваних є неформальне звернення за допомогою, а останнім йде звернення до правоохоронних органів. Багато хто з потерпілих вирішує не повідомляти про випадки кіберсталкінгу, побоюючись несерйозного ставлення. Навіть якщо справа заведена, потерпілі не рідко стикаються з проблемами протягом розслідування [8].

Є питання і поза відношення правової системи до кіберсталкінга як злочину. Притягнути злочинців до відповідальності досить складно з таких причин як: процедурні виклики, міжнародне та анонімне переслідування. Початковий етап розслідування кіберпереслідувань визначається жертвами як найбільш розчаровуючий. Кожен випадок кіберсталкінга має бути зафіксований, щоб встановити модель поведінки, яка відповідає пороговому значенню – необхідно довести щонайменше два інциденти. Тобто потерпілий повинен вести записи про свою власну взаємодію, що як доведено може травмувати жертв [9]. На даний момент в Україні кіберсталкінг не розглядається як окреме правопорушення. На практиці для захисту осіб, які зазнають переслідування, застосовуються інші норми законодавства. З останніх новин, 2 жовтня 2024 року на офіційному порталі Верховної Ради зареєстрували новий законопроєкт №12088, де пропонується внесення змін до чинного Закону «про запобігання та протидію домашньому насильству», які передбачають введення визначення терміну кіберпереслідування: «кіберпереслідування – вид злочинного переслідування, що передбачає постійне спостереження за постраждалою особою без її згоди чи законного дозволу за допомогою інформаційних та комунікаційних технологій, що може здійснюватися шляхом обробки персональних даних жертви, зокрема в результаті крадіжки особистих даних або шпигування за жертвою через її соціальні мережі або платформи обміну повідомленнями, електронну пошту та телефон, крадіжку паролів або злом її пристроїв для доступу до приватного простору за допомогою встановлення додатків геолокації, у тому числі шпигунського програмного забезпечення, або через викрадення її пристроїв» [10]. Проте у створеному законопроєкті наразі не запропоновано, до якого саме покарання притягуватимуть винних в кіберсталкінгу. До того ж, відсутні чітко визначені механізми для виявлення, фіксування, підтвердження кіберсталкінгу, збору доказів і захисту жертв.

Аналітичний огляд літератури дав зрозуміти, що, зважаючи на помірну ефективність тактик управління кіберсталкінгом, мечем для виявлення, захисту та запобігання цьому злочину мають стати саме технології [11]. Незважаючи на популярність так званих інтервенційних підходів, виявлення є життєво важливим у протистоянні проти кіберсталкерів. Воно необхідне для подальших дій, спрямованих на ізоляцію правопорушення, попередження жертви, блокування небажаної комунікації, а також для підтримки цифрового криміналістичного розслідування. Можна виділити такі методи, які наразі використовуються для виявлення кіберпереслідувань, як: статистичні; інтелектуальний аналіз даних; машинне навчання. Останній підхід відіграє головну роль у виявленні кіберсталкінгу. Машинне навчання активно використовується як самостійна методологія або як частина гібридного підходу для ідентифікації злочинної поведінки. Основна перевага цих алгоритмів – здатність швидко та точно аналізувати величезні масиви інформації, адаптуючись до нових викликів та змін. Методи машинного навчання поділяються на контрольовані, неконтрольовані, напівконтрольовані та навчання з підкріпленням. Кожен із них має свої особливості та застосовується залежно від специфіки завдання. Серед подібних робіт, можна виділити використання алгоритмів випадкового лісу та логістичної регресії для автоматичного виявлення повідомлень кіберзалякування, а також гібридні підходи, як наприклад використання методу кластеризації на основі правил і нечіткої логіки для виявлення мови ворожнечі, які досягли 94,5 % f1-міри [12]. В даній роботі буде використовуватися саме контрольоване навчання, яке передбачає використання маркованих даних, де кожен вхідний приклад має відповідний вихідний результат. Алгоритм навчається на основі залежностей між цими змінними, що дозволяє йому прогнозувати майбутні результати. Такий підхід широко застосовується для завдань регресії та потрібної нам класифікації. Результати досліджень показали, що числове представлення TF-IDF досягає найкращих показників при роботі з алгоритмами класифікації [13]. TF визначає, як часто слово зустрічається в тексті і IDF відповідає за важливість терміна. Фінальна вага терміна у тексті визначається

як добуток TF та IDF, тобто рідкісні слова, які часто зустрічаються в окремих текстах, отримують вищу вагу, ніж ті, що є загальновживаними. Алгоритм машинного навчання SVM із методом TF-IDF показує найкращі результати навчання, особливо в завданні класифікації саме текстових даних [14]. Метод опорних векторів працює за принципом пошуку оптимальної гіперплощини, яка розділяє дані на категорії, його мета – знайти межу розділу між ними так, щоб максимізувати відстань між найближчими точками категорій. Він добре працює з невеликими датасетами і нерівномірними розподілами, що є безумовною перевагою щодо інших алгоритмів машинного навчання [15].

Тож, враховуючи подану вище інформацію, а також визнаючи значний рівень популяризації української мови в міжособистісному спілкуванні серед українців будь-якого віку на даний час, і додавши до цього відсутність розробок технічного формату у виявленні кіберсталкінгу в українському кіберпросторі, актуальним буде рішення про створення застосунку, який би виявляв кібersталкерську поведінку на українській мові. Вибір технології для обміну цифровими повідомленнями пав на електронну пошту, яка поки залишається одним із найпопулярніших засобів комунікації, як для офіційного листування, так і для особистого спілкування. До тепер, вона тримає одну з лідуючих позицій для здійснення кіберсталкінга, що робить її важливим джерелом для аналізу загроз цього типу. До того ж, електронні листи можуть використовуватися як юридичні докази в справах про кібersталкінг, тому їх важливо виявляти та зберігати.

Мета і задачі дослідження. Метою цієї роботи є підвищення безпеки користувачів в онлайн-середовищі, шляхом розробки застосунку для автоматизованого виявлення ознак кібersталкерської поведінки з використанням машинного навчання.

Для досягнення поставленої мети були визначені наступні задачі:

- відбір навчальних даних для датасета;
- оцінка ефективності моделей на тренувальних даних;
- розробка застосунку для автоматизованого виявлення кіберсталкінгу;
- тестування застосунку.

Основна частина. В даній роботі використовується набір сучасних технологій, які надають можливість реалізувати ідею автоматизованого виявлення кіберсталкінгу на основі машинного навчання. Основою розробки стала мова програмування Python, яка відзначається великою кількістю спеціалізованих бібліотек для машинного навчання, таких як scikit-learn. Основні модулі застосунку включають в себе:

- автентифікацію та доступ до електронної пошти;
- попередню обробку тексту;
- класифікацію загроз за допомогою машинного навчання;
- оцінку ефективності класифікації;
- фільтрацію по відправнику;
- генерацію звітів та інтеграцію з користувацьким інтерфейсом.

Тобто, основна робота застосунку виглядатиме так: буде виконуватися підключення до електронної пошти користувача, отримання листів із поштових папок Inbox та Spam, відбір релевантних листів на основі часових обмежень (враховуються повідомлення за останні 30 днів). Для отримання електронних листів застосунок використоватиме Google Gmail API, а автентифікація та авторизація проходитиме через OAuth 2.0 – сучасний протокол, який надає обмежений доступ до ресурсів користувача. Текст листів пройде нормалізацію за допомогою функції, яка очищає його від зайвих символів, видаляючи URL-адреси, електронні пошти, числа та пунктуацію, видаляє символи іншої мови, тощо. Наступним йде перетворення тексту у векторний вигляд, тобто використання TfidfVectorizer з бібліотеки scikit-learn, яка перетворює текст у числовий формат, використовуючи метод TF-IDF. Отримана матриця ознак розділиться на навчальні та тестові вибірки у співвідношенні 80% на 20%. Окремо створюватимуться два набори: один для класифікації повідомлень як кібersталкінгових або ні, а інший – для визначення їхньої підкатегорії. Після підготовки даних ініціалізуватимуться дві

моделі SVM із лінійним ядром та збалансованими вагами класів. Задля покращення точності моделей застосовуватиметься GridSearchCV (Grid Search with Cross-Validation) – метод автоматизованого підбору оптимальних гіперпараметрів для моделей машинного навчання з 5-кратною крос-валідацією. Ця технологія використовується для пошуку оптимального значення параметра c в моделі SVM. Вона контролює баланс між правильною класифікацією навчальних даних і запобіганням перенавчанню. Одразу як завершиться навчання моделей, оцінюватиметься їх точність класифікації за допомогою певних метрик ефективності і ROC-кривих, результати фіксуватимуться у логах. Фільтрація по відправнику означає аналіз частоти повідомлень від окремих відправників. Якщо відправник надсилає понад 2 загрозливі листи, повідомлення вважається підозрілим, бо кіберсталкінг, як було визначено – це явище систематичне.

Для того, щоб розробити ефективну інтелектуальну систему, яка виконуватиме завдання класифікації текстових даних, спочатку необхідно зібрати датасет, на якому моделі і будуть навчатися. Якість даних безпосередньо впливає на точність, узагальнюваність та стійкість моделі, тому набір даних повинен відповідати певним вимогам, таким як репрезентативність та збалансованість. Зібраний набір даних на початку складався з 5559 повідомлень, що є достатньою вибіркою для початкового навчання, хоча збільшення розміру набору даних в подальшому суттєво покращило результати. Серед повідомлень є як кіберсталкерські, так і звичайні тексти. Дані були зібрані більшою частиною синтетично, тобто повідомлення формувалися на основі аналізу існуючих загроз та шаблонів поведінки кіберсталкерів, щоб максимально точно відобразити їхні реальні прояви; а також використовувались реальні повідомлення з датасетів англійською мовою, що включали тексти: кібербулінгу, хейтспічу, з сексуальним підтекстом, спам/неспам повідомлення, переведені на українську. Як було вказано, було проведено аугментацію даних, щоб збільшити набір навчальних даних. Аугментація – це методика штучного розширення обсягу даних шляхом їх модифікації для покращення узагальнювальної здатності моделей та зменшення ризику перенавчання. В цій роботі було використано два методи – переклад на іншу мову і назад, а також міксування слів у повідомленні для зміни порядку слів у реченні. Це дозволило збільшити різноманітність текстів, при цьому не змінюючи їхній зміст, і створити більш стійку підборку повідомлень. Отже, в результаті було створено файл у форматі Excel з 13466 повідомлень, який є набором даних для навчання двох моделей. Файл містить 3 мітки: Text, Label, Types, – де Text є текстом повідомлення, Label є класифікацією кіберсталкінг/не-кіберсталкінг і Types – це тип повідомлення. За розподілом повідомлень у датасеті: 7771 належать до категорії «Cyberstalking», а 5695 – до «No-Cyberstalking». Серед кіберсталкінгу, виділено три основні типи повідомлень: «Сексуальний харасмент» (2221), «Залякування» (2885) і «Звичайний» (2665). На рисунку 1 можна побачити як виглядає файл, який являє собою датасет для навчання моделей в застосунку.

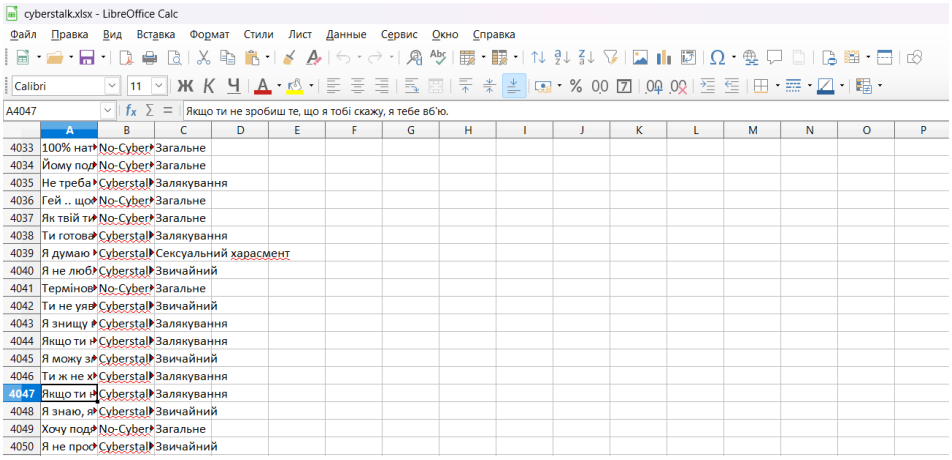


Рис.1. Зібраний набір даних

Об’єктивна оцінка якості побудованих моделей базуватиметься на низці загальновживаних у машинному навчанні метрик та підходів. Матриця помилок є одним із найважливіших інструментів. Вона представляє собою таблицю, яка відображає співвідношення між передбаченими та фактичними значеннями класів. Елементи цієї матриці включають кількість правильно класифікованих позитивних і негативних прикладів, а також кількість помилкових позитивних і негативних передбачень. На основі цієї матриці помилок розраховуються вже стандартні метрики ефективності моделі. Ті з них, які використовуватимуться, вказані нижче [17].

Влучність показує наскільки модель влучна у передбаченні позитивного класу:

$$\Pr ecision = \frac{TP}{TP + FP},$$

Повнота демонструє, яку частку з усіх реальних позитивних прикладів модель змогла правильно виявити:

$$\mathrm{Re} call = \frac{TP}{TP + FN},$$

F1-міра – гармонійне середнє між влучністю та повнотою, і використовується як зведений показник ефективності класифікації:

$$F - score = 2 * \frac{\Pr ecision * \mathrm{Re} call}{\Pr ecision + \mathrm{Re} call},$$

Загальна точність є загальним показником правильності роботи моделі:

$$Acurracy = \frac{TP + TN}{TP + TN + FP + FN}.$$

Додатково, будуть використовуватись середні значення показників (macro avg, weighted avg), задля врахування особливостей різного розподілу класів у тестовій вибірці. Macro avg – середнє арифметичне для всіх класів. Weighted avg – усереднене з урахуванням кількості прикладів кожного класу.

Тож, за допомогою описаних вище методів, проведемо оцінювання ефективності моделей із запропонованого підходу виявлення кіберсталкерської поведінки. Для основної бінарної моделі, яка виявляє чи є в повідомленні ознаки кібersталкінгу, клас 0 буде означати кібersталкінг, а клас 1 – не кібersталкінг. Що стосується багатокласової моделі визначення типів кібersталкінгу, то тут: клас 0 буде означати залякування, 1 – звичайний кібersталкінг, 2 – сексуальний харасмент. Першим етапом проходитиме оцінка бінарної моделі. Як видно з таблиці 2, модель допустила лише 22 помилки FN та 17 випадків FP.

Таблиця 2

Матриця помилок бінарної моделі

№	Клас	Прогноз 0	Прогноз 1
1	0	1523	22
2	1	17	1131

Таблиця 3 вказує, що модель має майже симетричні показники влучності та повноти, що є ознакою її стабільності. Значення F1-міри перебуває на рівні 0.98 – 0.99, а загальна точність становить 0.99. Високі значення macro avg та weighted avg говорять про відсутність критичного дисбалансу в розпізнаванні обох класів.

Таблиця 3

Оцінки ефективності бінарної моделі

№	Метрика	Клас 0	Клас 1	№	Метрика	Клас 0
1	Precision	0.99	0.98	5	Accuracy	0.99
2	Recall	0.99	0.99	6	Macro avg	0.99
3	F1-score	0.99	0.98	7	Weighted avg	0.99
4	Support	1545	1148			

В свою чергу, аналіз матриці помилок багатокласової моделі, таблиця 4, демонструє, що найбільша кількість правильних класифікацій спостерігається в класі «Залякування». Більшість помилок зосереджена між класами 0 і 2, та 1 і 2, це вказує на наявність перехресних ознак у змісті повідомлень. В таблиці 5 ми бачимо, що всі три класи мають показники precision і recall в діапазоні 0.88 – 0.91, тобто достатньо рівномірна якість класифікації, загальна точність моделі становить 0.89. Значення macro avg і weighted avg підтверджують, що модель справляється з усіма класами порівняно однаково добре, незважаючи на можливий дисбаланс у навчальній вибірці.

Таблиця 4

Матриця помилок багатокласової моделі

№	Клас	Прогноз 0	Прогноз 1	Прогноз 2
1	0	502	43	17
2	1	38	472	26
3	2	16	24	417

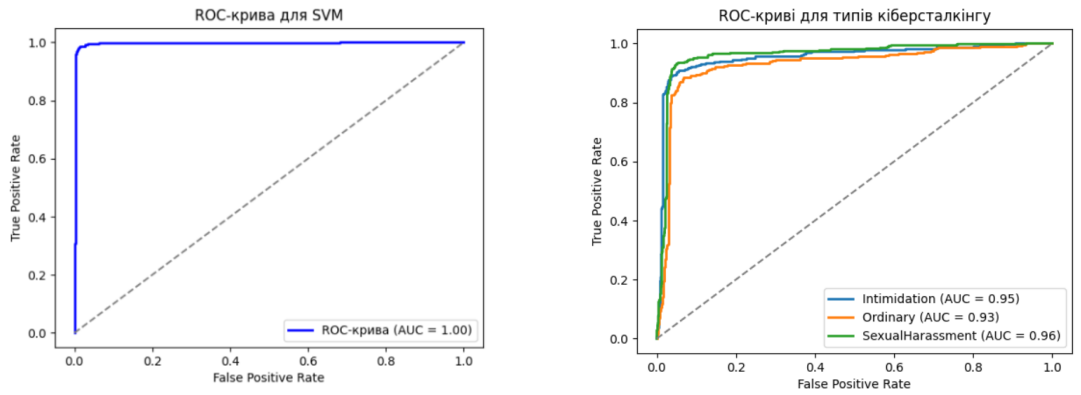
Таблиця 5

Оцінки ефективності багатокласової моделі

№	Метрика	Клас 0	Клас 1	Клас 2
1	Precision	0.90	0.88	0.91
2	Recall	0.89	0.88	0.91
3	F1-score	0.90	0.88	0.91
4	Support	562	536	457
5	Accuracy	0.89		
6	Macro avg	0.90		
7	Weighted avg	0.89		

Для візуалізації оцінки ефективності, побудуємо ROC-криві, які відображатимуть співвідношення між чутливістю та часткою хибно позитивних спрацювань моделей. Оптимальним є класифікатор, що наближається до верхнього лівого кута ROC-графіка. На обох графіках, криві мають AUC – площу під кривою – метрикою, яка кількісно виміряє здатність відокремлювати класи. Значення AUC наближається до одиниці для ідеального класифікатора.

Як можна побачити, на рисунку 2, в двох результатах, крива значно вище діагоналі випадкового вгадування, для бінарної моделі AUC = 1.00. Для багатокласової моделі AUC також зберігається на високому рівні: від 0.93 до 0.96, вказуючи таким чином на ефективність моделі навіть у складних сценаріях класифікації.



а) *б*)

Рис.2. Графіки ROC-кривих зі значеннями AUC:
а – бінарна модель; *б* – багатокласова модель

Для проведення тестування самого застосунку, на електронну пошту було спеціально надіслано 13 повідомлень, які містять в собі ознаки кіберсталкінгу, з яких 3 потрапили у спам і 10 у вхідні листи; 3 відправника надіслало більше 2 повідомлень, і в результаті вийшло 10 листів з кіберсталкінгом. Після запуску веб-застосунку у браузері відкривається перше представлення (рис. 3).

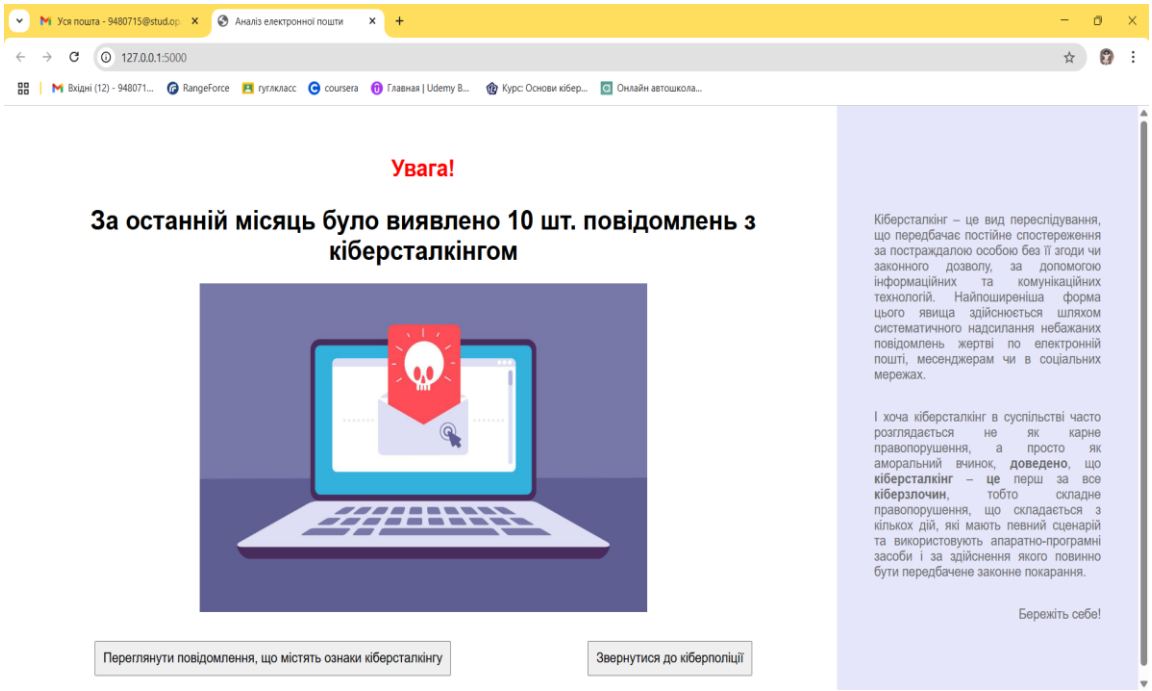


Рис.3. Головна сторінка веб-застосунку

Як можна побачити, програма виявила всі листи, які відповідають заданим фільтрам. З правого боку сторінки знаходиться невелика довідка для користувача, де визначається поняття кіберсталкінг і повідомляється користувачу, що він є карним кібезлочином.

Натискаємо кнопку перегляду повідомлень з кіберсталкінгом і таким чином переходимо до другого представлення (рис. 4).

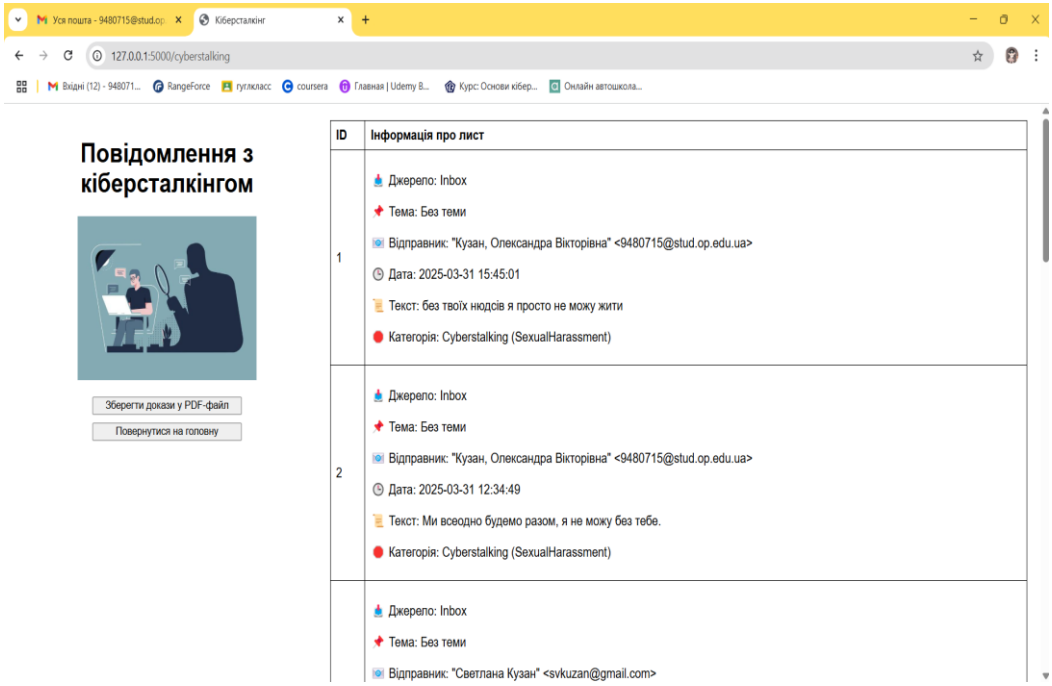
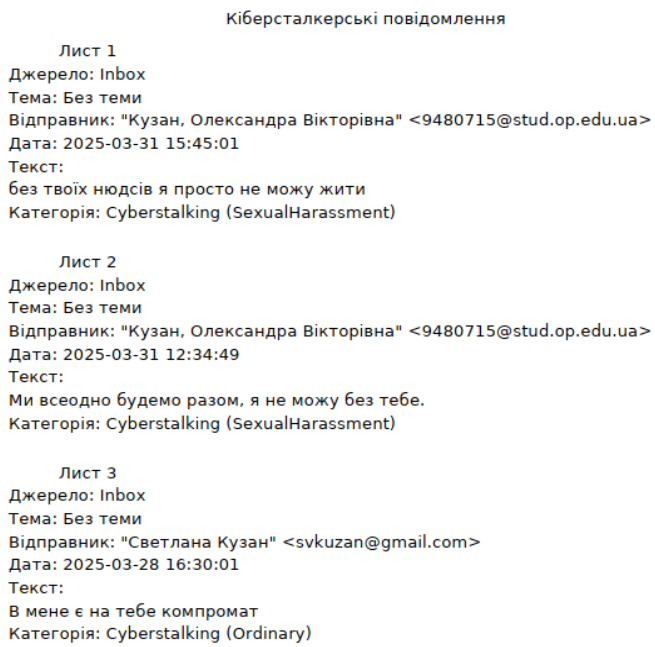


Рис.4. Друга сторінка веб-застосунку

Користувачу надаються відомості з виявлених листів, додається визначення типу кіберсталкерського повідомлення. Застосунок визначив типи повідомлень коректно, підібравши найбільш доречний варіант для кожного повідомлення. Сторінка містить в собі кнопку збереження доказів, натиснувши на яку, завантажується файл з інформацією, яку користувач бачить на екрані (рис. 5).



Кіберсталкерські повідомлення

Лист 1
Джерело: Inbox
Тема: Без теми
Відправник: "Кузан, Олександра Вікторівна" <9480715@stud.op.edu.ua>
Дата: 2025-03-31 15:45:01
Текст:
без твоїх нюдсів я просто не можу жити
Категорія: Cyberstalking (SexualHarassment)

Лист 2
Джерело: Inbox
Тема: Без теми
Відправник: "Кузан, Олександра Вікторівна" <9480715@stud.op.edu.ua>
Дата: 2025-03-31 12:34:49
Текст:
Ми всеодно будемо разом, я не можу без тебе.
Категорія: Cyberstalking (SexualHarassment)

Лист 3
Джерело: Inbox
Тема: Без теми
Відправник: "Светлана Кузан" <svkuzan@gmail.com>
Дата: 2025-03-28 16:30:01
Текст:
В мене є на тебе компромат
Категорія: Cyberstalking (Ordinary)

Рис.5. Завантажений пдф-файл

Повернувшись на першу сторінку, натискаємо на другу кнопку – звернення до кіберполіції, де користувачу надаються посилання для звернення по допомогу (рис. 6).

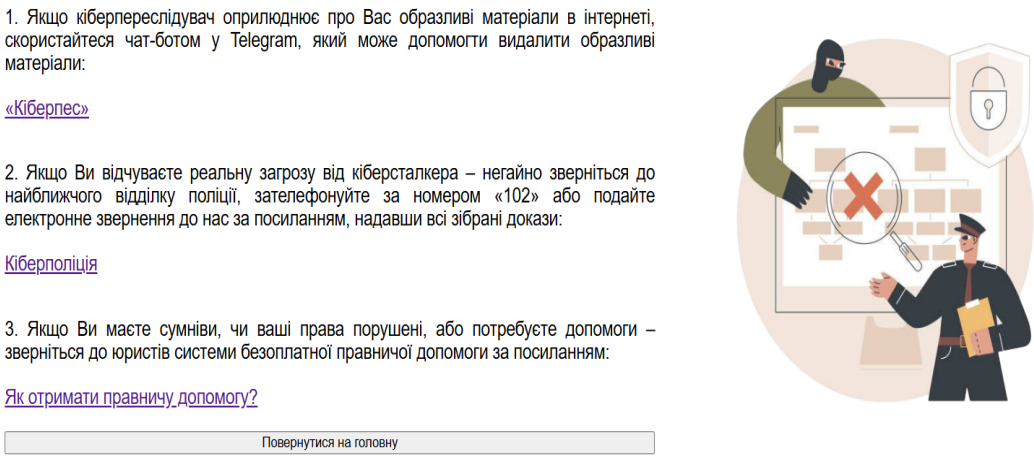


Рис.6. Третя сторінка веб-застосунку

Висновки. В даній роботі було проведено аналіз явища кіберсталкінгу, розглянуто його характеристики та небезпечні прояви, а також існуючі підходи до його виявлення і, на основі цього було розроблено застосунок, який дозволяє виявляти потенційні ознаки кіберсталкінгу в повідомленнях електронної пошти. В результаті роботи застосунку, користувач отримує автоматизований аналіз своєї електронної пошти на наявність кіберсталкінгових повідомлень та можливість вчасно вжити заходів для покарання зловмисника, без важких наслідків для себе. Ефективність застосунку забезпечує висока точність класифікації повідомлень за допомогою перевірених алгоритмів ML, які гарно показали себе у виявленні загроз: бінарна модель досягла загальної точності 99%, багатокласова модель має оцінку точності в 89% і впевнено розрізняє основні види кіберпереслідувань. Система працює з даними саме українською мовою, що є новим та актуальним для українського суспільства, може оновлюватися та навчатися на нових даних, а за допомогою веб-інтерфейсу користувач отримує чітке уявлення про виявлені загрози кіберсталкінгу. Отже, це дослідження має важливе теоретичне та практичне значення. Розроблений підхід чи сам застосунок може бути використаний для покращення безпеки користувачів в їх онлайн-комунікаціях.

Список літератури

1. Sheridan L. What is Cyberstalking? A Review of Measurements. *Journal of Interpersonal Violence.* 2021. URL: https://www.researchgate.net/publication/348467830_What_is_Cyberstalking_A_Review_of_Measurements.
2. Ahmed N. Cyberstalking: A content analysis of gender-based offenses committed online. 2019.
3. Goyal S., Kaur A. Impact of Cyberstalking on Women and Children: An Analysis. *International Journal of Research Publication and Reviews*. 2024. URL: https://www.researchgate.net/publication/385494443_Impact_of_Cyberstalking_on_Women_and_Children_An_Analysis.
4. Mcfarlane L., Bocij P. An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday.* 2003. URL: https://firstmonday.org/ojs/index.php/fm/article/view/1076.
5. Holyst B. Cyberstalking as a form of cyberharassment. *Ius novum.* 2015. URL: https://www.lazarski.pl/fileadmin/user_upload/dokumenty/czasopisma/ius-novum/2015/Ius_Novum_2_15_holyst.pdf.
6. Charan J. L. Cyber Stalkers and Cyber Bullies: Protecting Women in the Digital Age. *Cyber Crime & Cyber Securities in India*. 2023. URL: https://www.researchgate.net/publication/375120797_Cyber_Stalkers_and_Cyber_Bullies_Protecting_Women_in_the_Digital_Age.
7. Miftha A. The Social, Legal, and Technical Perspectives of Cyberstalking in India. 2024. URL: https://uobrep.openrepository.com/handle/10547/626190.

8. Kaur P., Dhir A., Tandon A., Alzeiby E. A. A systematic literature review on cyberstalking. An analysis of achievements and future promises. *Technological Forecasting & Social Change.* 2021. URL: https://www.researchgate.net/publication/347381968_A_systematic_literature_review_on_cyberstalking_An_analysis_of_past_achievements_and_future_promises.
9. O'shea B., Asquith N. L., Prichard J. Mapping Cyber-Enabled Crime: Understanding Police Investigations and Prosecutions of Cyberstalking. *International Journal for Crime, Justice and Social Democracy.* 2022. URL: https://www.crimejusticejournal.com/article/view/2096.
10. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг). Номер, дата реєстрації: 12088 від 02.10.2024. Верховна рада України. 2024. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/44972.
11. Tokunaga R. S., Aune K. S. Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking. *Journal of Interpersonal Violence.* 2015. URL: https://www.researchgate.net/publication/278793403_Cyber-Defense_A_Taxonomy_of_Tactics_for_Managing_Cyberstalking.
12. Gautam A. K., Bansal A. Automatic Cyberstalking Detection on Twitter in Real-Time using Hybrid Approach. *International Journal of Modern Education and Computer Science*. 2023. URL: https://www.mecs-press.org/ijmecs/ijmecs-v15-n1/IJMECS-V15-N1-5.pdf.
13. Gautam A. K., Bansal A. A Review on Cyberstalking Detection Using Machine Learning Techniques: Current Trends and Future Direction. *International Journal of Engineering Trends and Technology*. 2022. URL: https://ijettjournal.org/archive/ijett-v70i3p211.
14. Wen Z., Taketoshi Y., Xijin T. TFIDF, LSI and Multi-word in Information Retrieval and Text Categorization. *IEEE.* 2008. URL: http://meta-synthesis.amss.cas.cn/Publication/MSKS_Publications/Conference_papers/Paperlists/201410/P020141013596946632792.pdf.
15. Gautam A. K., Bansal A. Performance analysis of supervised machine learning techniques for cyberstalking detection in social media. *Journal of Theoretical and Applied Information Technology.* 2022. URL: https://scholar.google.fr/citations?view_op=view_citation&hl=ja&user=g0KKFIsAAAAJ&citation_for_view=g0KKFIsAAAAJ:QIV2ME_5wuYC.
16. Dakhaz M. A., Adnan M. A. Machine Learning Applications based on SVM Classification: A Review. *Qubahan Academic Journal.* URL: https://journal.qubahan.com/index.php/qaj/article/view/50/36.
17. Geeksforgeeks. Confusion Matrix in Machine Learning. URL: https://www.geeksforgeeks.org/confusion-matrix-machine-learning/.

О.В. Кузан, Н.І. Кушніренко, В.О. Назаров, В.В. Подуфалов

DEVELOPMENT OF AN APPLICATION FOR AUTOMATED DETECTION OF CYBERSTALKING

O.V. Kuzan, N.I. Kushnirenko, V.O. Nazarov, V.V. Podufalov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: kushnirenko@op.edu.ua

Today, cyberstalking has shown itself to be an extremely fast-growing phenomenon that has caused a paradigm shift in persecution. It consists of intrusive, systematic interference in the victim's online life for the purpose of psychological pressure, manipulation, intimidation, etc. Despite the scale of the problem, there are currently no effective means of automated detection of such threats in Ukrainian. The aim of this paper is to improve user safety in the digital environment by developing an application for detecting cyberstalker behavior in emails using machine learning. The study analyzed the phenomenon of cyberstalking, as well as modern approaches to its detection, which allowed us to determine the directions of development and the main tasks of the work. The developed application is based on the use of the SVM algorithm to build models, which are trained on a specially formed dataset. Two models have been created: a binary model for classifying emails into “cyberstalking” and “non-cyberstalking” and a multi-class model for dividing them by type: intimidation, sexual harassment, and ordinary cyberstalking. The tool also provides the ability to store detected cyberstalker messages as evidence for victims to report to the cyber police. Testing of the approach has shown its high efficiency: accuracy of the binary model was 99%, and the multi-class model reached 89%. The obtained results show the significant potential of the application in detecting cyberstalking and thus increasing the level of digital security of users in online communications, so the proposed application for detecting cyberstalking can be successfully implemented for personal use. The results of this work can be used in further research and development in the field of cybersecurity and cyberstalking.

Keywords: cyberstalking, email, machine learning, text classification, cybersecurity.

DOI 10.15276/imms.v15.no1.107
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 107-114

ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІЗУ РИЗИКІВ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ЕВАКУАЦІЇ КОРАБЛЯ

М.М. Масьонкова

Херсонська державна морська академія
20, Ушакова пр., м.Херсон, 73000, Україна
Email: masyonkova@gmail.com

У статті представлено інтелектуальну систему аналізу ризиків для надання комплексної підтримки у прийнятті рішень судноводієм під час надзвичайних ситуацій на всіх етапах евакуаційного процесу. Система складається з трьох взаємопов'язаних моделей, що базуються на байєсівських мережах: модель оцінювання ситуації для визначення необхідності оголошення загальної тривоги та ініціювання процесу евакуації, модель оцінювання збору для постійного контролю ефективності переміщення людей до збірних пунктів та виявлення проблемних зон судна, та модель оцінювання підготовки до залишення судна для прийняття обґрунтованого рішення про остаточну евакуацію. Кожна модель забезпечує динамічне обчислення показника ризику в режимі реального часу, комплексно враховуючи технічний стан судна, поточні та прогнозовані погодні умови, доступність засобів системи пошуку та рятування, близькість інших суден для надання допомоги, відстань від берега та рівень готовності пасажирів і екіпажу. Інтеграція спеціальних вузлів корисності та рішення дозволяє системі надавати конкретні обґрунтовані рекомендації командному складу щодо оптимальних дій у кожній конкретній ситуації. Розроблена інтелектуальна система може суттєво підвищити ефективність рятувальних операцій та значно зменшити людські втрати в критичних ситуаціях на морі, забезпечуючи структовану науково обґрунтовану підтримку у прийнятті життєво важливих рішень.

Ключові слова: інтелектуальна система, аналіз ризиків, байєсівські мережі, підтримка прийняття рішень, модель судноводія.

Вступ. Загострення геополітичної ситуації та військова агресія росії проти України кардинально змінили безпекову картину світу, створивши нові виклики для морського транспорту. Ескалація конфлікту на морі, включаючи атаки на цивільні судна у Чорному морі та блокування торговельних маршрутів, зростання кількості кібератак на морські судна, актуалізує питання безпеки пасажирів та екіпажу морських суден як ніколи раніше [1, 2]. У таких умовах надзвичайно важливим стає забезпечення ефективних процесів евакуації, які можуть врятувати сотні людських життів.

Процес залишення судна є надзвичайно складною та ризикованою операцією, що вимагає від осіб, відповідальних за безпеку всіх присутніх на борту, прийняття критично важливих рішень в умовах обмеженого часу. Кожен етап евакуаційного процесу по мірі розвитку надзвичайної ситуації характеризується специфічними труднощами та проблемами, які необхідно ефективно вирішувати для успішного завершення евакуації, передусім у контексті управління часом та організації переміщення людей [3]. Цей багатоетапний процес характеризується високим ступенем ризику та потребує значних часових ресурсів, що вимагає постійного та ефективного контролю з боку членів екіпажу.

В умовах сучасних безпекових викликів розробка інтелектуальних систем підтримки прийняття рішень для евакуації на морському та річковому траспорті набуває особливої актуальності, оскільки може суттєво підвищити ефективність рятувальних операцій та зменшити людські втрати в критичних ситуаціях.

Огляд літератури. Окремі наукові дослідження останніх років зосереджені на розробці та вдосконаленні методів і технологій евакуації морських суден. Ю. Лю та співавтори [4]

розробили стратегію евакуації, яка враховує пропускну здатність маршрутів та рівень ризику для керівництва евакуйованими особами у випадку пожежі. С. Чень та ін. розробили модель динамічної вагової оцінки для наукового та обґрунтованого визначення ризиків безпеки судноплавства, яка об'єднує суб'єктивні та об'єктивні фактори впливу через удосконалений метод аналізу ієрархій та дозволяє подолати недоліки статичного оцінювання завдяки безперервному навчанню на зразках навігаційного середовища та аварій. [5]. Л Лю та ін. запропонували удосконалену систему мурашиних колоній для вирішення завдань планування евакуаційних маршрутів натовпу на круїзних суднах [6]. Ю. Юе та ін. представили загальну модель та методологічну основу для моделювання повного циклу евакуації з круїзного лайнера [7]. З. Лю та співавтори запропонували інноваційний механізм евакуації, який інтегрує просторові характеристики судна з особливостями поведінки людей. Їхньою метою було створення моделі евакуаційного потенціалу морського судна та розробка системи підтримки прийняття рішень в екстрених ситуаціях для організації евакуації як членів екіпажу, так і пасажирів [8]. В. Чжан та ін. створили систему індексів навігаційного ризику для безпілотних суден в складних умовах плавання, використовуючи метод аналізу ієрархій та нечітку комплексну оцінку для визначення ваги факторів ризику та розробки моделі оцінювання, яка враховує особливості безпілотного судна, його сприйняття навколишнього середовища та можливості комунікації. [9]. Х. Чжан та ін. розробили динамічну модель для кількісного визначення каскадного ефекту пожежі в машинному відділенні морського судна [10]. Незважаючи на значні досягнення у цій сфері, залишається потреба у подальшому дослідженні інтелектуальних систем оцінки ризиків, які могли б забезпечити більш ефективну підтримку прийняття рішень в реальному часі під час евакуацій на морському та річковому транспорті.

Мета роботи. Метою даної роботи є розробка інтелектуальної системи аналізу ризиків для надання підтримки у прийнятті рішень судноводієм під час надзвичайних ситуацій на всіх етапах евакуаційного процесу.

Для досягнення поставленої мети у роботі вирішуються такі **завдання**:

- розробити інтелектуальну систему аналізу ризиків для надання інформаційної підтримки судноводію у прийнятті рішень під час надзвичайних ситуацій на кожному етапі процесу евакуації;
- визначити систему взаємопов'язаних моделей, що базуються на байєсівських мережах: модель оцінювання ситуації, модель оцінювання збору та модель оцінювання підготовки до залишення судна;

Інтелектуальна система аналізу ризиків. Інтелектуальна система аналізу ризиків спрямована на покращення розуміння ситуації судноводієм у складних обставинах евакуації та надання допомоги у прийнятті рішень протягом всього циклу управління надзвичайною подією. Для реалізації цього завдання система виконує постійне оцінювання ризиків, що дозволяє в реальному часі визначати рівень небезпеки, пов'язаної з операціями до початку та протягом евакуації. Інтелектуальна система аналізу ризиків включає три окремі моделі, що відповідають ключовим етапам евакуації: аналіз ситуації, організація збору людей та підготовка до залишення судна. Кожна модель забезпечує динамічне обчислення показника ризику за градуйованою шкалою. Інформація про характер ризиків передається командному складу миттєво для забезпечення обґрунтованого прийняття рішень.

Метою інтелектуальної системи аналізу ризиків є підвищення ситуаційної обізнаності судноводія в несприятливих умовах, що превалюють протягом евакуаційного процесу, а також забезпечення підтримки прийняття рішень щодо управління життєвим циклом інциденту/аварії. Для досягнення цієї мети інтелектуальна система аналізу ризиків здійснює динамічне оцінювання ризиків з метою кількісного визначення в режимі реального часу ризику, пов'язаного з діяльністю до та під час процесу евакуації. Запропонована інтелектуальна система складається з трьох різних

моделей, які охоплюють основні фази евакуації (оцінювання кризової ситуації, збір та підготовка до залишення судна). Кожна модель передбачає динамічний розрахунок індексу ризику за порядковою шкалою. Характеристика ризику надається в режимі реального часу судноводію для ефективної підтримки прийняття рішень, заснованих на ризику.

Модель оцінювання ситуації. Модель оцінювання ситуації активується після виникнення інциденту/аварії через згенерований сигнал. Її основною метою є підтримка рішення судноводія щодо того, чи потрібно оголосити загальну тривогу для ініціювання процесу евакуації. Оцінка базується на стані безпеки судна та рівні впливу небезпечних факторів на пасажирів.

Модель оцінювання збору. Модель оцінювання збору активується після оголошення загальної тривоги та спрямована на кількісне визначення ефективності процесу збору з точки зору затримок і того, чи знаходяться пасажири під загрозою під час переміщення до збірних пунктів. Основна функція полягає в допомозі членам екіпажу у визначенні тих зон судна, де можуть знадобитися запобіжні та/або коригувальні дії протягом процесу збору. Результатом є рівень ризику затримки, який розраховується для зон судна, розподілених за основними вертикальними зонами та конкретною палубою судна.

Модель оцінювання підготовки до залишення судна. Модель оцінювання підготовки до залишення судна також активується після оголошення загальної тривоги. Вона спрямована на надання розуміння того, чи більше судно не є безпечним для людей на борту, та підтримує рішення капітана про віддання наказу покинути судно. Оцінка враховує стан судна (який активний з моменту виявлення інциденту), уразливість людей після залишення судна та готовність до покидання. Результат оцінки надає рекомендацію судноводію та капітану.

Застосування інтелектуальної системи аналізу ризиків. Використання інтелектуальної системи аналізу ризиків відбувається у два основних етапи (рис. 1).

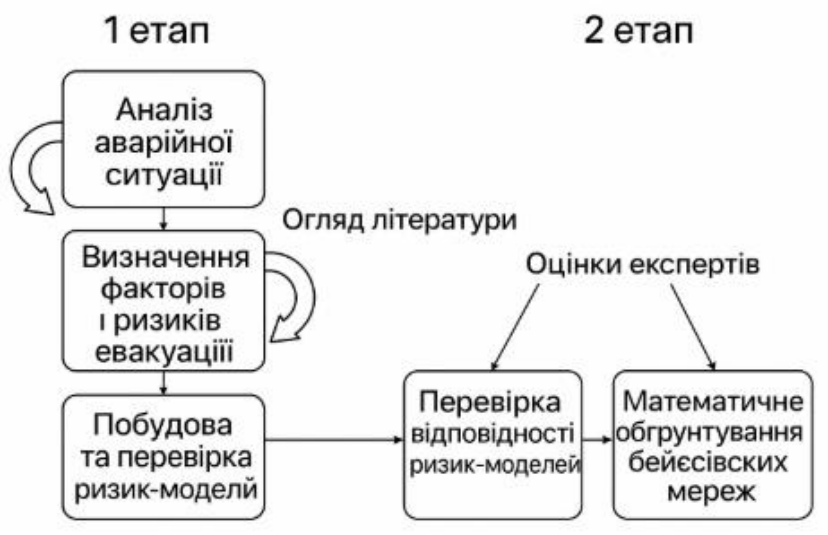


Рис. 1. Етапи застосування інтелектуальної системи аналізу ризиків

Усі три компоненти інтелектуальної системи аналізу ризиків базуються на байєсівських мережах. Це орієнтовані ациклічні графічні структури, де випадкові величини та вузли пов’язані напрямленими з’єднаннями, що демонструють статистичні та випадкові взаємозв’язки між елементами [11].

Створення ризик-моделей інтелектуальної системи аналізу ризиків передбачає наступні кроки:

І етап:

– ідентифікація факторів та показників, які впливають на рівень ризику при евакуації морських суден (на основі дослідження аварійних випадків, аналізу наукових публікацій та експертних оцінок);
– побудова ризик-моделей, включаючи структурування зв'язків між виявленими ризиковими факторами з урахуванням думки експертів та математичне обґрунтування байєсівських мереж;
– перевірка створених ризик-моделей.

II етап:

– перегляд та коригування моделей на основі коментарів експертів;
– валідація моделей.

Модель оцінювання ситуації. Модель призначена для формування висновку щодо тяжкості післяаварійної ситуації, яка залежить від можливості локалізації інциденту, безпосереднього впливу небезпечних умов на пасажирів та здатності судна забезпечити безпечні умови для пасажирів і екіпажу.

У моделі враховано наступні фактори ризику [12]:

– плавучість, остійність та водонепроникність;
– структурна цілісність;
– протипожежна безпека;
– стан критичних систем для керованості та навігації судна;
– стан критичних систем зв'язку (внутрішнього та зовнішнього).

Модель оцінювання збору. Спрямована на оцінювання ефективності процесу збору з точки зору часу та за аспектами, описаними нижче. Модель враховує наступні фактори ризику [3]:

– стан допоміжних систем;
– евакуаційні можливості;
– доступність засобів для евакуації;
– потік пасажирів у зоні.

Основними факторами ризику, що впливають на терміновість залишення судна, є: стан судна, який залежить від локалізації інциденту, стану корпусу судна (включаючи плавучість, остійність, водонепроникність та структурну цілісність) і стану навігаційних систем (тобто здатності судна до керування); рівень готовності людей і засобів масової евакуації (суден) до залишення судна.

Байєсівська мережа моделі оцінювання підготовки до залишення судна. При розробці структури моделі байєсівської мережі основою стала ідентифікація факторів ризику, що впливають на терміновість залишення судна, (рис. 2).

Побудована байєсівська мережа для оцінювання збору включає такі вузли системи пошуку та рятування :

– **Близькість інших суден для порятунку** визначає можливість надання допомоги іншими суднами щодо рятування пасажирів, які покинули судно з рятувальними човнами. Близькість інших суден залежить від щільності судноплавства в даному районі та від того, чи знаходяться поблизу судна, здатні реагувати на сигнали лиха, як частина вимог Міжнародної конвенції про пошук і рятування на морі (Конвенція SAR). Висока щільність означає, що пасажири матимуть високі шанси на рятування, в той час як низька щільність зменшує шанси на врятування та збільшує ризик екологічних небезпек після залишення судна.
– **Доступність засобів пошуку та порятунку** визначає час, який потрібен засобам системи пошуку та порятунку для прибуття на місце аварії, що залежить від відстані до найближчого рятувального центру і поточних погодних та морських умов.

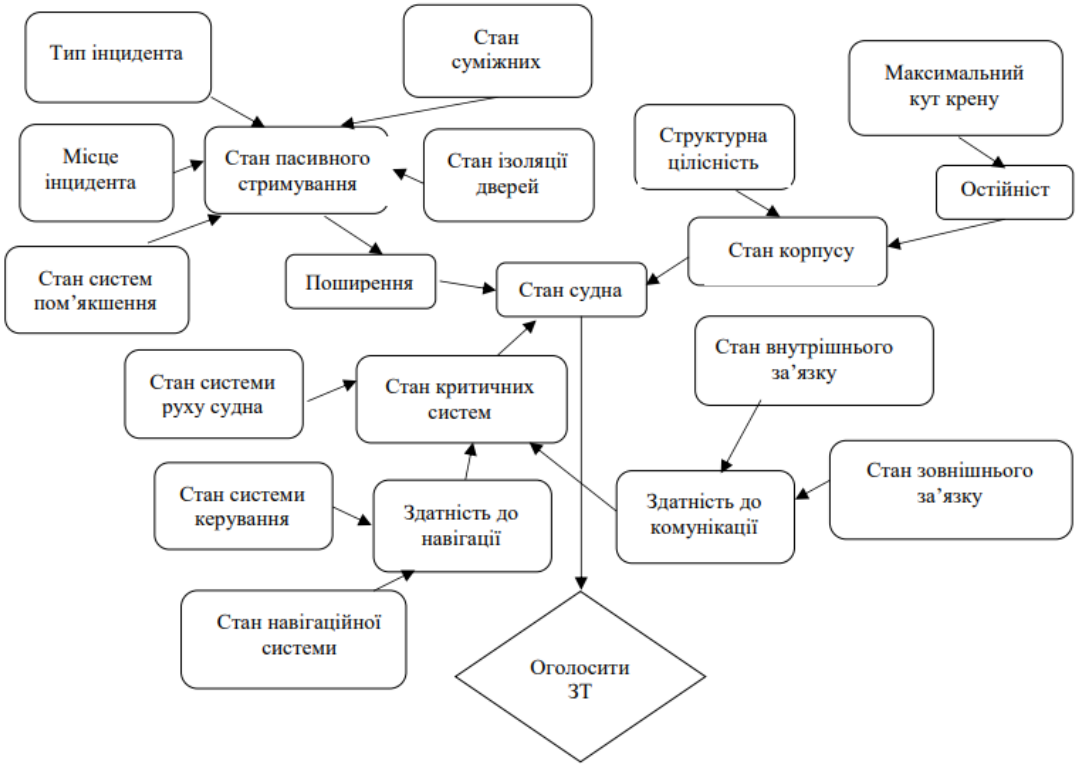


Рис. 2. Байєсівська мережа моделі оцінювання ситуації аналізу ризиків

- **Стан зовнішніх засобів** вказує, чи очікується надання допомоги після залишення судна або літакові засоби покинули судно. Це залежить від мобілізації системи пошуку та порятунку та відстані. Зовнішні засоби рятування очікуються, коли власті системи пошуку та порятунку повідомлені і знаходяться на шляху, а найближчі судна закриті до місця аварії у морі для надання допомоги.
- **Відстань від берега** вказує, чи можуть пасажири після залишення судна дістатися до берега безпечно протягом розумного часу. Якщо це трапляється поблизу берега, пасажири мають вищу ймовірність врятування навіть у найгіршому сценарії (наприклад, рятувальні човни).
- **Очікувані погодні умови.** Інформація про поточні погодні умови береться у формі 3-годинного прогнозу. Справедливі, помірні та суворі характеристики засновані на силі вітру та висоті хвиль. Суворі погодні умови збільшують час рятування більше ніж в 7 разів (суворо). Суворі погодні умови збільшують ймовірність 30-хвилинного навантаження людських збитків. Екстремальні температури (дуже холодні) також впливають на вразливість пасажирів.
- **Вразливість після залишення судна.** Стан вибору має потенційні несприятливі наслідки для безпеки пасажирів після впливу навколишньої небезпеки. Це залежить від того, як швидко їх можна доставити до безпеки вдома або на борт іншого судна чи на берег або на переважаючі погодні умови. Низькі рівні вразливості пов'язані з мінімальним впливом, або зі справедливими чи помірними погодними умовами (незалежно від часу до SAR) або зі швидкою системою пошуку та порятунку (незалежно від переважаючих умов).
- **Доступність засобів (суден) масової евакуації.** Вказує, чи судна масової евакуації пошкоджені, недоступні або загрожують підходу для нової посадки та залишення судна. Вони можуть бути доступними, якщо вони не зазнали пошкоджень до такої міри, що їх можливість плавання та водонепроникність порушені, і якщо вони безпечно доступні для нової посадки пасажирів.

- **Максимальний кут крену** вказує, чи система спуску суден масової евакуації здатна працювати як призначено, враховуючи кут крену судна. MEV можуть працювати в межах максимального кута крену і пошкодження, які система може зазнати від аварії. Судна масової евакуації будуть здатні до спуску лише якщо вони не зазнали якихось серйозних пошкоджень або їх системи спуску або їх конструкції, і якщо максимальний кут крену судна відповідає LSA коду [13].
- **Статус запуску суден масової евакуації** вказує кількість пасажирів, які прибули на збірні станції як відсоток від загальної кількості пасажирів на борту. Всі очікувані пасажири повинні прибути на збірні станції, щоб мати можливість організувати судно. Пасажири повинні бути готові до посадки на MEV перш ніж почати посадку на суднах масової евакуації. Конкретні відсотки можуть розглядатися як параметр, що можна налаштувати відповідно до специфічних властивостей судна
- **PAX (Пакс) на станціях збору** вказує кількість пасажирів, які прибули на збірні станції як відсоток від загальної кількості пасажирів на борту. Всі очікувані пасажири повинні прибути на збірні станції, щоб мати можливість організувати судно.
- **Готовність залишення судна.** Це оцінка ситуації перед покиданням судна з урахуванням впливу на безпеку пасажирів, якщо вони (1) залишаються на борту на своїх призначених збірних станціях, або (2) сідають на судна масової евакуації, евакуюються з судна та чекають на засоби системи пошуку та порятунку. Оцінка залежить від цілісності судна та операційного стану його підсистем з урахуванням інциденту та ступеня, до якого він був локалізований, потенційного впливу на безпеку людей з урахуванням наказу про залишення судна та готовності до покидання. Альтернативи рішення для судноводія/капітана, які підтримуються цією оцінкою, полягають у тому, щоб затримати та додатково оцінити ситуацію або негайно віддати наказ про залишення судна.

Аналогічно до моделі оцінки ситуації, в модель байєсівської мережі були включені вузол корисності та вузол рішення для оцінки того, чи потрібно віддавати наказ про залишення судна, базуючись на його «корисності» відповідно до станів кінцевого вузла шансів «Терміновість залишення судна».

Конкретно, кінцевий вузол шансів з'єднується з вузлом корисності. "Корисність" кожної альтернативи рішення оцінюється за якісною шкалою від 1 до 3 як "нагорода". Наприклад, видання наказу про залишення судна, коли терміновість залишення судна низька, розглядається як небажаний результат, який штрафується через вузол корисності, оскільки це може непотрібно піддати пасажирів екологічним небезпекам після залишення судна. Це також було підтверджено відгуками, отриманими під час експертних інтерв'ю. З іншого боку, видання наказу про залишення судна при помірній та/або високій терміновості залишення судна є бажаним результатом, який нагороджується через вузол корисності, оскільки це сприяло б захисту здоров'я та безпеки людей на борту. Оцінка кожної альтернативи рішення (тобто залишити, залишитися та перевірити) виходить як сума добутку корисностей з ймовірностями кожного стану кінцевого вузла шансів. Альтернатива з найвищим результатом є рекомендованим рішенням.

Висновки. У роботі запропоновано інтелектуальну систему аналізу ризиків для підтримки прийняття рішень судноводієм під час надзвичайних ситуацій на морських суднах. Система спрямована на покращення безпеки евакуаційних процесів та зменшення людських втрат у критичних ситуаціях, що особливо актуально в умовах сучасних геополітичних викликів та загострення безпекової ситуації на морі.

Розроблено комплексну систему, що складається з трьох взаємопов'язаних моделей, які охоплюють ключові етапи евакуаційного процесу: оцінювання ситуації, організацію збору людей та підготовку до залишення судна. Всі компоненти системи базуються на байєсівських мережах, що забезпечує ефективне моделювання невизначеності та складних взаємозв'язків між факторами ризику в умовах обмеженої інформації. Система забезпечує постійний моніторинг та оцінювання ризиків у режимі реального часу, що дозволяє своєчасно реагувати на зміни ситуації та приймати обґрунтовані рішення. Ідентифіковано та систематизовано широкий спектр факторів ризику, включаючи технічний стан судна, погодні умови, доступність рятувальних засобів, близькість інших суден та готовність пасажирів до евакуації.

Інтеграція вузлів корисності та рішення дозволяє системі надавати конкретні рекомендації щодо необхідності оголошення загальної тривоги або віддання наказу про залишення судна. Запропонована інтелектуальна система аналізу ризиків може суттєво підвищити ефективність управління надзвичайними ситуаціями на морських суднах. Система забезпечує судноводіям інформаційну підтримку у прийнятті критично важливих рішень, що може призвести до значного зменшення часу реагування та покращення результатів евакуаційних операцій.

Наступним етапом досліджень буде валідація розроблених моделей на основі реальних даних про морські аварії, інтеграцію системи з існуючими судновими системами безпеки та розширення функціональності для врахування специфічних типів суден та характеру надзвичайних ситуацій.

Список літератури

1. Cong L., Zhang H., Wang P., Chu C., Wang J. Impact of the Russia–Ukraine Conflict on Global Marine Network Based on Massive Vessel Trajectories. *Remote Sensing*. 2024. 16(8):1329.
2. Kovalchuk O., Shynkaryk M., Masonkova M., Banakh S. Cybercecurity: Technology vs Safety. *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany. 2020. P. 765−768.
3. Koimtzoglou, A., Themelis, N., Ventikos, N.P., Louzis, K., Koimtzoglou, M., Giannakis, K., Panagiotidis, P., Moustogiannis, S., Ramiro, M., Peña, J., et al. Assessing the Risk during Mustering in Large Passenger Vessels: A Digital Tool for Real Time Decision Support. *In Sustainable Development and Innovations in Marine Technologies*. *CRC Press: Boca Rato. FL, USA.* 2022. P. 269−276.
4. Liu, Y., Zhang, H., Zhan, Y., Deng, K., Dong, L. Evacuation Strategy Considering Path Capacity and Risk Level for Cruise Ship. *J. Mar. Sci. Eng*. 2022. Vol. 10. P. 398.
5. Chen S., Wu L., Xie C., Zhou L., Wang R., Liu Z., Zhu Q., Zhu L. Risk Evaluation of Navigation Environment Based on Dynamic Weight Model and Its Application. *Journal of Marine Science and Engineering*. 2022. Vol. 10(6):770.
6. Liu L, Zhang H, Xie J, Zhao Q. Dynamic Evacuation Planning on Cruise Ships Based on an Improved Ant Colony System (IACS). *J. Mar. Sci. Eng*. 2021. Vol. 9. P. 220.
7. Yue, Y., Gai,W.M., Deng, Y.F. Influence factors on the passenger evacuation capacity of cruise ships: Model-ling and simulation of full-scale evacuation incorporating information dissemination. *Process Saf. Environ. Protection*. 2022. Vol. 157. P. 466−483.
8. Liu, Z., Li, Y., Zhang, Z., Yu,W. A New Evacuation Accessibility Analysis Approach Based on Spatial Information. *Reliab. Eng. Syst. Saf.* 2022. Vol. 222 P. 108395.
9. Zhang W, Liu Z, Ma X. Research on Navigation Risk Assessment of Unmanned Ship Under Complex Navigation Conditions. *Journal of Marine Science and Engineering*. 2024. Vol. 12(11):1947.
10. Zhang, H., Li, C., Zhao, N., Chen, B.-Q., Ren, H., Kang, J. Fire Risk Assessment in Engine Rooms Considering the Fire-Induced Domino Effects. *J. Mar. Sci. Eng.* 2022. Vol. 10. P. 1685.

11. Huang, Y., van Gelder, P.H.A.J.M. Time-Varying Risk Measurement for Ship Collision Prevention. *Risk Anal.* 2020. Vol. 40. P. 24–42.
12. Ventikos, N.P., Themelis, N., Louzis, K., Koimtzoglou, A., Michelis, A., Koimtzoglou, M., Ragab, A. Evaluating Risk During Evacuation of Large Passenger Ships: A Smart Risk Assessment Platform for Decision Support. *In Trends in Maritime Technology and Engineering*. *CRC Press: London. UK.* 2022. Vol. 2. P. 283–294.
13. Hänninen, M. Bayesian Networks for Maritime Traffic Accident Prevention: Benefits and Challenges. *Accid. Anal. Prev*. 2014. Vol. 73. P. 305–312.

SMART RISK ANALYSIS SYSTEM FOR DECISION SUPPORT DURING SHIP EVACUATION

M.M. Masonkova

Kherson State Maritime Academy
20, Ushakov ave., Kherson, 73000, Ukraine
Email: masyonkova@gmail.com

The escalation of the geopolitical situation and Russia's military aggression against Ukraine have fundamentally changed the world's security landscape, creating new challenges for maritime transport. The escalation of conflict at sea, including attacks on civilian vessels in the Black Sea and the blockade of trade routes, makes the issue of passenger and crew safety on ships more urgent than ever before. The process of abandoning ship is an extremely complex and risky operation that requires those responsible for safety to make critically important decisions under conditions of limited time and high uncertainty. The article presents an intelligent risk analysis system for providing comprehensive decision support to navigators during emergency situations at all stages of the evacuation process. The system consists of three interconnected models based on Bayesian networks: a situation assessment model for determining the need to declare general alarm and initiate the evacuation process, a muster assessment model for continuous monitoring of the effectiveness of people's movement to assembly stations and identifying problematic areas of the ship, and an abandon ship preparation assessment model for making informed decisions about final evacuation. Each model provides dynamic real-time risk indicator calculations, comprehensively considering the ship's technical condition, current and predicted weather conditions, availability of search and rescue system resources, proximity of other vessels for assistance, distance from shore, and the readiness level of passengers and crew. The integration of special utility and decision nodes allows the system to provide specific justified recommendations to the command staff regarding optimal actions in each particular situation. The developed intelligent system can significantly improve the efficiency of rescue operations and substantially reduce human losses in critical situations at sea, providing structured, scientifically-based support for making vital decisions.

Keywords: smart system, risk analysis, Bayesian networks, decision support, navigator model.

DOI 10.15276/imms.v15.no1.115
УДК: 004.8:004.056

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 115-125

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Б.В. Приступа [1,2], Н.В. Герасимюк [2], Я.В. Рожковський[2]

[1]Військовий медичний клінічний центр Південного регіону
2, Пироговська вул., Одеса, 65044, Україна
[2]Одеський національний медичний університет
2, Валіховський провулок, Одеса, 65082, Україна
Email: bogdan.prystupa@onmedu.edu.ua

Сучасний розвиток цифрових технологій, таких як Інтернет речей, штучний інтелект та хмарні обчислення, сприяє зростанню обсягів даних, які потребують ефективного захисту. Штучний інтелект є перспективним напрямком у сфері кібербезпеки, оскільки дозволяє автоматизувати аналіз великих обсягів даних, ідентифікувати аномалії в трафіку та швидко реагувати на загрози. Основні результати дослідження включають визначення основних алгоритмів машинного навчання, що застосовуються у сфері кібербезпеки, серед яких підтримуючі векторні машини, дерева рішень, нейронні мережі, а також підходи, що базуються на підкріплювальному навчанні. Доведено, що використання глибокого навчання дозволяє досягати точності виявлення загроз до 96 відсотків, що перевищує традиційні методи аналізу кіберзагроз. Розглянуто проблеми, пов'язані з впровадженням штучного інтелекту у сфері кібербезпеки, зокрема вразливість моделей до атак на навчання, що можуть змінювати поведінку алгоритмів та обходити системи захисту. Оцінено регуляторні виклики та необхідність створення нормативних актів для контролю технологій автономних штучних інтелектуальних систем, що працюють поза контролем офіційних IT-структур організацій. Цінність дослідження полягає у розробці комплексного підходу до використання штучного інтелекту у сфері кібербезпеки, що дозволить підвищити рівень захисту інформаційних систем та мінімізувати ризики кібератак. Отримані результати сприятимуть розширенню наукових підходів у галузі інтелектуальних систем безпеки та розробці ефективних алгоритмів виявлення загроз у реальному часі. Практичне значення проведеного дослідження полягає у можливості застосування отриманих результатів для вдосконалення систем виявлення вторгнень, антивірусного програмного забезпечення, а також впровадження автоматизованих рішень для захисту критичних інфраструктур від кібератак.

Ключові слова: штучний інтелект, машинне навчання, кібербезпека виявлення загроз, аналіз аномалій, глибоке навчання.

Вступ. Стрімкий розвиток інтелектуальних технологій, Інтернету речей (IoT) та комп'ютерних пристроїв призвів до створення величезних обсягів даних, які потребують належного рівня захисту [1]. Хоча ці інновації значно спростили повсякденне життя та оптимізували бізнес-процеси, вони водночас спричинили нові виклики у сфері кібербезпеки, підвищивши ризик кібератак та витоку конфіденційної інформації [2].

Згідно зі звітом Cybersecurity Ventures (2023), кібервитрати у світі прогнозовано досягнуть 8 трильйонів доларів США у 2023 році, що робить кіберзлочинність третьою за величиною економікою після США та Китаю. Очікується, що глобальні витрати на кіберзлочинність зростатимуть на 15% щорічно протягом наступних трьох років, досягаючи 10,5 трильйонів доларів США щорічно до 2025 року [3]

Найпоширенішими типами атак залишаються фішинг, шкідливе програмне забезпечення, атаки на відмову в обслуговуванні (DoS), експлойти нульового дня та методи соціальної інженерії [4, 5].

Такі загрози несуть серйозні ризики для приватних осіб, підприємств і великих організацій, підриваючи їхню інформаційну безпеку та стабільність [6]. Останніми роками кібербезпека зазнає значних змін як у технологічних, так і в робочих аспектах

комп’ютерних систем [6]. Штучний інтелект є рушійною силою цих змін, оскільки машинне навчання (ML) та глибоке навчання (DL) є фундаментальними компонентами ШІ, які відіграють вирішальну роль у розкритті інформації з даних [7].

Штучний інтелект дозволяє аналізувати величезні обсяги даних, виявляти загрози в реальному часі та автоматизувати процеси захисту інформаційних систем. Це робить його невід'ємною частиною сучасних систем кібербезпеки. Проте, зростання кількості автономних інструментів ШІ створює новий феномен — Shadow AI. Це поняття означає використання несанкціонованих або нерегульованих систем штучного інтелекту, які працюють поза контролем офіційних IT-структур організацій. Shadow AI може сприяти підвищенню продуктивності, проте також створює значні ризики для безпеки даних та конфіденційності [8].

Таким чином, сучасні виклики у сфері кібербезпеки вимагають інтеграції передових рішень на основі штучного інтелекту, що дозволяють не лише виявляти загрози, а й забезпечувати адаптивний захист у реальному часі.

Мета дослідження. Метою цієї роботи є аналіз сучасних підходів до використання штучного інтелекту в кібербезпеці, виявлення ключових методів та технологій, що застосовуються для захисту інформаційних систем, а також оцінка їхньої ефективності. Зокрема, увага приділяється методам машинного навчання, аналізу поведінки, виявленню аномалій та системам автоматизованої відповіді на інциденти.

Для досягнення поставленої мети було використано методи системного аналізу, огляд наукової літератури, а також аналіз сучасних технологій штучного інтелекту, що застосовуються в кібербезпеці. Штучний інтелект у кібербезпеці відіграє ключову роль у забезпеченні захисту інформаційних систем. Його застосування дозволяє значно підвищити рівень виявлення загроз, скоротити час реагування на інциденти та знизити ризики фінансових втрат [9]. Системи на основі машинного навчання здатні аналізувати величезні обсяги даних, виявляючи потенційно небезпечну активність ще на етапі її зародження.

Інструменти та методи штучного інтелекту в кібербезпеці. За словами Камачо (2024), найпоширеніші методи AI, що використовуються в кібербезпеці, включають машинне навчання (Machine Learning) і глибоке навчання (Deep Learning) [10]. ML — це підгалузь штучного інтелекту, яка зосереджена на розробці алгоритмів і статистичних моделей, які дозволяють комп’ютерам вчитися та робити прогнози або рішення на основі [11]. Існує три основні типи ML, а саме: контрольоване навчання, неконтрольоване навчання та навчання з підкріпленням.

Глибоке навчання (DL) представляє собою напрям машинного навчання (ML), що використовує багатошарові штучні нейронні мережі (ANN) для виявлення складних взаємозв'язків та закономірностей у даних. Навчання відбувається на основі нейронної архітектури з кількох рівнів, яка включає вхідний шар, один або більше прихованих шарів та вихідний шар [11].

Застосування штучного інтелекту у сфері кібербезпеки значно підвищує ефективність виявлення загроз та реагування на інциденти. Завдяки алгоритмам машинного навчання можна аналізувати великі обсяги даних, розпізнавати аномалії та автоматизувати процеси захисту інформаційних систем. Різні методи ШІ використовуються для моніторингу мережевого трафіку, виявлення вторгнень, класифікації загроз та розпізнавання фішингових атак. Розглянемо основні інструменти та методи, що застосовуються для посилення безпеки в цифровому середовищі.

Системи виявлення вторгнень. У системах виявлення вторгнень (Intrusion detection systems англ) широко застосовуються різні алгоритми машинного навчання для класифікації мережевого трафіку. Наприклад, SVM і KNN використовуються для ідентифікації трафіку як нормального або шкідливого. SVM знаходить оптимальну гіперплощину для розділення класів даних, тоді як KNN класифікує об'єкти на основі найближчих сусідів [12, 13]. Наївний Байєс діє як ймовірнісний класифікатор, що

передбачає незалежність ознак і визначає ймовірність належності пакета до категорії «нормальний» або «шкідливий» [14, 15]. Дерева рішень (DT), своєю чергою, моделюють процес прийняття рішень шляхом рекурсивного поділу простору ознак [16, 17]. Для неконтрольованого навчання застосовується K-Means, що групує трафік у кластери, допомагаючи ідентифікувати аномалії та нові загрози [18, 19]. Штучні нейронні мережі (ANN) здатні навчатися як у контрольованому, так і в неконтрольованому режимах, ідентифікуючи складні шаблони вторгнень шляхом налаштування ваг та зв'язків між нейронами [20]. AdaBoost, у свою чергу, підвищує точність класифікації, зосереджуючись на складних для класифікації прикладах [21].

Мережеві системи виявлення вторгнень. У Мережеві системи виявлення вторгнень (Network intrusion detection system англ) алгоритми типу документа використовуються для класифікації трафіку за допомогою правил, сформованих на основі історичних даних [22, 23]. Random Forest (RF) підвищує точність шляхом об’єднання прогнозів кількох дерев рішень [**Ошибка! Закладка не определена.**]. Серед моделей глибокого навчання для NIDS виділяються Convolutional Neural Networks (CNN). Вони аналізують корисне навантаження пакетів, вивчаючи ієрархічні представлення функцій, що дозволяє виявляти складні шаблони атак [24, 25].

Розпізнавання зображень та CAPTCHA. Для розпізнавання зображень і CAPTCHA часто застосовуються підтримуючі векторні машини (Support Vector Machines SVM англ) та згорткові нейронні мережі (convolutional neural networks, CNNs англ). SVM визначає оптимальну гіперплощину для розділення класів зображень [26], а CNN використовує згорткові шари для вилучення характеристик зображень, забезпечуючи високу точність розпізнавання [27, 28]. Також використовується SVD (Single Value Decomposition англ), що дозволяє стискати та реконструювати зображення, забезпечуючи ефективне розпізнавання CAPTCHA [29, 30].

Виявлення фішингу та зловмисного програмного забезпечення. Для виявлення фішингу та шкідливого програмного забезпечення широко застосовуються штучні нейронні мережі та згорткові нейронні мережі. Наприклад, штучні нейронні мережі досягли точності 89,95% при класифікації фішингових електронних листів, а мережі глибоких переконань – 96,32% [31]. SVM та CNN використовуються для аналізу URL-адрес, заголовків електронних листів або мережевого трафіку, дозволяючи класифікувати об'єкти як легітимні або фішингові [32]. Q-Learning, у свою чергу, демонструє високу точність у виявленні шкідливого контенту завдяки адаптивному навчанню [33].

Класифікація трафіку та виявлення аномалій. У класифікації мережевого трафіку активно використовується K-Means, який кластеризує трафік на основі подібності [34]. Для детальної класифікації програм або протоколів ефективно застосовується CNN, що забезпечує високу точність та швидкість [35]. Для виявлення DoS-атак широко використовуються SVM та KNN. SVM класифікує трафік за характеристиками, такими як розмір пакета та тип протоколу [36], тоді як KNN швидко ідентифікує відхилення без попереднього навчання [37]. Дерева рішень (DT) розділяють простір ознак, допомагаючи виявляти аномалії, тоді як Principal Component Analysis (PCA) використовується для зменшення розмірності даних, спрощуючи виявлення відхилень [**Ошибка! Закладка не определена.**].

Юридичні та регуляторні виклики у протидії Shadow AI. Швидкий розвиток штучного інтелекту значно випереджає створення комплексних правових і регуляторних механізмів, що ускладнює контроль над несанкціонованими застосуваннями ШІ, відомими як Shadow AI. Хоча такі нормативні акти, як Загальний регламент захисту даних ЄС (GDPR), Закон про портативність та відповідальність медичного страхування США (HIPAA) та Закон про права студентів і конфіденційність освіти (FERPA), встановлюють основи управління ШІ, вони не враховують специфіку Shadow AI [38] Ці закони зосереджені на захисті даних, справедливості алгоритмів та прозорості, проте не

охоплюють системи, що працюють поза офіційним контролем, створюючи регуляторний вакуум.

Основні правові проблеми. Одна з головних юридичних проблем полягає у виявленні та запобіганні несанкціонованим впровадженням ШІ. Існуючі нормативні акти регулюють лише схвалені системи, залишаючи поза увагою програми, розгорнуті без дозволу [39, 40]. Це особливо критично в таких галузях, як охорона здоров'я, фінанси та освіта, де Shadow AI може призвести до витоків даних, алгоритмічних упереджень та неетичних рішень. Наприклад, нещодавній випадок із китайським стартапом DeepSeek, коли італійський орган із захисту даних Garante обмежив діяльність компанії через недотримання вимог щодо конфіденційності, яскраво ілюструє регуляторні прогалини [41].

Проблеми відповідальності. Ще однією важливою проблемою є юридична відповідальність за помилки, спричинені системами ШІ. Традиційні правові рамки не враховують автономність рішень, що ускладнює визначення відповідальної сторони у разі заподіяння шкоди [42, 43]. Наприклад, у сфері охорони здоров'я помилкові діагнози, зроблені несанкціонованими інструментами ШІ, викликають питання щодо відповідальності лікарів та розробників. Аналогічно, у фінансовій сфері використання ШІ для прийняття кредитних рішень може призвести до дискримінації позичальників, як це сталося у справі SafeRent Solutions, коли алгоритм несправедливо відмовляв заявникам із соціально вразливих груп [44].

Регуляторні прогалини та потенційні рішення. Недосконалість нормативної бази дозволяє Shadow AI працювати без належного контролю. Наприклад, GDPR забезпечує захист даних, проте не регулює специфічні аспекти прозорості та підзвітності алгоритмів [45, 46]. Як наслідок, компанії, які не впроваджують механізми управління ШІ, наражають себе на серйозні правові ризики [47]. Для вирішення цих проблем необхідне створення адаптивних регуляторних механізмів, що враховують специфіку Shadow AI. Наприклад, Акт про штучний інтелект ЄС передбачає класифікацію ШІ-систем за рівнем ризику та встановлення суворіших вимог до високоризикових застосувань [48]. Крім того, важливо впроваджувати регулярні аудити, проводити оцінку етичності алгоритмів та створювати спеціалізовані органи контролю, які зможуть своєчасно виявляти та блокувати несанкціоновані програми [49]. Таким чином, подолання юридичних та регуляторних викликів, пов'язаних із Shadow AI, вимагає комплексного підходу, що поєднує оновлення правових норм, технологічний нагляд та посилення відповідальності за впровадження і використання ШІ у критичних галузях.

Майбутні напрямки досліджень у сфері кібербезпеки. З огляду на зростаючі загрози у сфері кібербезпеки, майбутні дослідження мають зосереджуватися на інтеграції передових технологій, таких як квантові обчислення, штучний інтелект та блокчейн. Вони дозволять підвищити стійкість систем до сучасних кібератак, забезпечивши надійний захист критичної інфраструктури. Нижче наведено ключові напрями, які заслуговують на подальше вивчення.

Квантове машинне навчання (QML) та захист від квантових загроз. Інтеграція квантового машинного навчання (QML) у системи кібербезпеки може значно підвищити ефективність виявлення загроз завдяки швидшій обробці даних та адаптивним алгоритмам [50]. Зокрема, QML сприятиме швидкому виявленню вразливостей та створенню динамічних стратегій захисту. Подальші дослідження мають зосередитися на розробці квантово-стійких мереж та криптографії, таких як квантовий розподіл ключів (QKD), що забезпечує захист від атак на основі квантових обчислень [51].

Пояснюваний штучний інтелект (XAI). Удосконалення XAI дозволить підвищити прозорість алгоритмів кібербезпеки, мінімізуючи помилкові спрацьовування. Подальші дослідження мають зосередитися на балансі між конфіденційністю та інтерпретованістю моделей, що забезпечить кращу ідентифікацію загроз [52].

Нейросимволічний штучний інтелект. Поєднання розпізнавання образів нейронними мережами з символічним мисленням дозволить створити більш точні системи виявлення загроз у реальному часі [53]. Це значно підвищить стійкість до сучасних атак, включаючи змагальні методи, що стають дедалі складнішими.

Виявлення зловмисного ПЗ та глибоке навчання. З огляду на швидкий розвиток шкідливих програм дослідження мають зосередитися на адаптації інструментів штучного інтелекту для виявлення нових видів загроз. Особливо перспективними є моделі глибокого навчання, здатні аналізувати трафік без традиційного ручного вилучення функцій [54].

Безпека кіберфізичних систем (CPS). Глибоке навчання також відіграє ключову роль у захисті кіберфізичних систем, зокрема через федеративне навчання, яке дозволяє працювати з обмеженими наборами даних. Методології, такі як Deep Reinforcement Learning (DRL), вже демонструють ефективність у протидії атакам, таким як FGSM та BIM [55]

Протидія глибоким фейкам. Зростання кількості глибоких фейків вимагає розробки комплексних заходів протидії. Поєднання методів передачі навчання, розширення даних та пояснюваного ШІ дозволить підвищити точність виявлення фальшивого контенту [56].

Інтеграція блокчейну та ШІ для безпеки IoT. Поєднання прогнозної аналітики ШІ з технологією блокчейну дозволить створити децентралізовані системи безпеки для Інтернету речей (IoT). Це підвищить стійкість мереж до атак та забезпечить конфіденційність даних [57].

Підвищення конфіденційності у федеративному навчанні. Використання диференціальної конфіденційності (DP) у федеративному навчанні дозволить знизити ризики витоку даних під час навчання розподілених моделей. Це стане ключовим напрямом для захисту конфіденційності у великих системах [58].

Кібербезпека метавсесвіту. Оскільки Metaverse активно розвивається, дослідження мають зосереджуватися на захисті від вразливостей у віртуальних середовищах, що працюють на основі VR та AR. Це включає розробку контрзаходів, здатних забезпечити безпечну інтеракцію користувачів у віртуальних екосистемах [**Ошибка! Закладка не определена.**].

Спеціалізований ШІ для різних секторів. Адаптація інструментів ШІ для специфічних галузей, таких як охорона здоров'я, фінанси та енергетика, дозволить створити більш надійні системи безпеки. Це забезпечить відповідність нормативним актам та підвищить стійкість критичної інфраструктури до складних атак [**Ошибка! Закладка не определена.**9]. Розвиток цих напрямів досліджень сприятиме створенню більш стійких та адаптивних систем кібербезпеки, здатних ефективно реагувати на сучасні загрози. Подальше впровадження інноваційних технологій дозволить не лише захистити критичні інфраструктури, але й забезпечити безпеку в епоху цифрової трансформації. Такий підхід дозволяє підвищити точність виявлення вторгнень, одночасно зменшуючи кількість хибно-позитивних спрацювань. Застосування алгоритмів машинного навчання та глибокого навчання у системах IDS є ключовим напрямом для забезпечення кібербезпеки в сучасних інформаційних системах. Проте впровадження ШІ у кібербезпеку супроводжується певними викликами. Зокрема, ефективність моделей значною мірою залежить від якості навчальних даних. Якщо алгоритм навчається на неповних або викривлених даних, це може призвести до неправильних рішень, таких як блокування легітимних користувачів або пропуск реальних загроз. Крім того, ШІ-системи можуть стати мішенню для атак на навчання (adversarial attacks). Adversarial attacks є одним із найбільших викликів для ШІ-моделей у кібербезпеці. Зловмисники можуть вносити мінімальні зміни до вхідних даних, щоб ввести модель в оману. Наприклад, невеликі модифікації пікселів у зображенні можуть призвести до того, що модель класифікує його як безпечне, хоча насправді воно є загрозою [59]. Такі атаки

підкреслюють необхідність розробки стійких моделей, здатних виявляти спотворення даних та адаптуватися до них. Крім того, ефективність моделей значною мірою залежить від якості навчальних даних. Якщо алгоритм навчається на неповних або викривлених даних, це може призвести до неправильних рішень, таких як блокування легітимних користувачів або пропуск реальних загроз. Ще одним викликом є необхідність значних обчислювальних ресурсів для обробки великих обсягів даних. Це може стати серйозним бар'єром для малих і середніх підприємств, які не завжди мають доступ до таких ресурсів [60].

Висновки. Використання штучного інтелекту в кібербезпеці значно підвищує ефективність виявлення загроз, прискорює реагування на інциденти та дозволяє запобігати потенційним атакам. Завдяки технологіям машинного навчання, аналізу поведінки, виявлення аномалій і автоматизованим системам реагування сучасні системи безпеки стали більш стійкими до складних кібератак. Основною перевагою ШІ є його здатність до самонавчання та адаптації, що дозволяє ідентифікувати не лише відомі загрози, а й нові, завдяки постійному аналізу актуальних даних. Це забезпечує проактивний захист і дає змогу запобігати атакам на ранніх стадіях. Таким чином, штучний інтелект відкриває нові можливості для захисту інформаційних систем, забезпечуючи більш високий рівень безпеки та адаптивності до сучасних загроз. Подальший розвиток цієї технології дозволить ще ефективніше протидіяти кібератакам, підвищуючи захист даних у цифровому світі.

Список літератури

1. Sarker I.H., Kayes A.S.M., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*. 2020. V.7, №1. P. 1–29. URL: https://doi.org/10.1186/s40537-020-00318-5
2. Künzler F. Real cyber value at risk: An approach to estimate economic impacts of cyberattacks on businesses. *Master thesis, University of Zurich*. 2023. 127 p. URL: https://doi.org/10.5167/uzh-255756
3. Cybersecurity Ventures. Cybercrime To Cost The World 8 Trillion Annually In 2023. URL: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
4. McIntosh T., Jang-Jaccard J., Watters P., Susnjak T. The inadequacy of entropy-based ransomware detection. *Neural Information Processing*: 26th International Conference, ICONIP 2019. Sydney, Australia: Springer, Cham, 2019. P. 181–189. URL: https://doi.org/10.1007/978-3-030-36802-9-20
5. Sun N., Zhang J., Rimba P., Gao S., Zhang L.Y., Xiang Y. Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys & Tutorials*. 2018. V.21, №2. P. 1744–1772. URL: https://doi.org/10.1109/COMST.2018.2885561
6. Cremer F., Sheehan B., Fortmann M., Kia A., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance-Issues and Practice*. 2022. V.47, №3. P. 698–736. URL: https://doi.org/10.1057/s41288-022-00266-6
7. Sarker I.H. Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. *Annals of Data Science*. 2023. V.10, №6. P. 1473–1498. URL: https://doi.org/10.1007/s40745-022-00444-2.
8. Sharon M. What Is Shadow AI And What Can IT Do About It? *Forbes*. 2023. URL: https://www.forbes.com/sites/delltechnologies/2023/10/31/what-is-shadow-ai-and-what-can-it-do-about-it/
9. Ofusori L., Bokaba T., Mhlongo S. Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. *Applied Artificial Intelligence*. 2024. V.38, №1. URL: https://doi.org/10.1080/08839514.2024.2439609

10. Camacho N. The role of AI in cybersecurity: Addressing threats in the digital age. *Journal of Artificial Intelligence General Science (JAIGS).* 2024. V.3, №1. P. 143–154. URL: https://doi.org/10.60087/jaigs.v3i1.75
11. Ladosz P., Weng L., Kim M., Oh H. Exploration in deep reinforcement learning: A survey. *Information Fusion*. 2022. T.85. P. 1–22. URL: https://doi.org/10.1016/j.inffus.2022.03.003
12. Sultana J., Jilani A.K. Classifying cyberattacks amid COVID-19 using support vector machine. *Security Incidents & Response Against Cyber Attacks: Proceedings of the International Conference*. Cham: Springer, 2021. P. 161–175. URL: https://doi.org/10.1007/978-3-030-69174-5_8
13. Veena K., Meena K., Teekaraman Y., Kuppusamy R., Radhakrishnan A., Jain D.K. C SVM classification and KNN techniques for cybercrime detection. *Wireless Communications and Mobile Computing*. 2022. P. 1-9. URL: https://doi.org/10.1155/2022/3640017.
14. Yilmaz A.B., Taspinar Y.S., Koklu M. Classification of malicious android applications using naive Bayes and support vector machine algorithms. *International Journal of Intelligent Systems and Applications in Engineering*. 2022. V.10, №2. P. 269–274.
15. Rekha G., Malik S., Tyagi A.K., Nair M.M. Intrusion detection in cyber security: Role of machine learning and data mining in cyber security. *Advances in Science Technology and Engineering Systems Journal*. 2020. V.5, №3. P. 72–81. URL: https://doi.org/10.25046/aj050310
16. Achuthan K., Smith R., Patel S. Advances in Artificial Intelligence for Cybersecurity: Emerging Trends and Challenges. *Frontiers in Data Science*. 2024. V.10, №2. P. 123–135. URL: https://doi.org/10.3389/fdata.2024.1497535.
17. Kumari A., Mehta A.K. A hybrid intrusion detection system based on decision tree and support vector machine. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, 2020. P. 396–400. IEEE. URL: https://doi.org/10.1109/ICCCA49541.2020.9250753
18. Saheed Y.K., Arowolo M.O., Tosho A.U. An efficient hybridization of K-means and genetic algorithm based on support vector machine for cyber intrusion detection system. *International Journal on Electrical Engineering and Informatics.* 2022. V.14, №2. P. 426–442. URL: https://doi.org/10.15676/ijeei.2022.14.2.11
19. Bohara B., Bhuyan J., Wu F., Ding J. A survey on the use of data clustering for intrusion detection system in cybersecurity. *International Journal of Network Security & Its Applications*. 2020. V.12, №1. P. 1. URL: https://doi.org/10.5121/ijnsa.2020.12101
20. Saranya T., Sridevi S., Deisy C., Chung T.D., Khan M.K.A. Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science.* 2020. V.171. P. 1251–1260. URL: https://doi.org/10.1016/j.procs.2020.04.133
21. Divakar S., Priyadarshini R., Kumar Barik R., Sinha Roy D. An intelligent intrusion detection scheme powered by boosting algorithm. *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India. 2021. P. 205–209. URL: https://doi.org/10.1109/Confluence51648.2021.9377076
22. Guezzaz A., Benkirane S., Azrour M., Khurram S. A reliable network intrusion detection approach using decision tree with enhanced data quality. *Security and Communication Networks*. 2021. V.2021, №8. P. 1230593. URL: https://doi.org/10.1155/2021/1230593
23. Ferdiana R. A systematic literature review of intrusion detection system for network security: Research trends, datasets and methods. *2020 4th International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, Indonesia. 2020. P. 1–6. IEEE. URL: https://doi.org/10.1109/ICICoS51170.2020.9299068
24. Kim J., Kim H., Shim M., Choi E. CNN-based network intrusion detection against denial-of-service attacks. *Electronics*. 2020. V.9, №6. P. 916. URL: https://doi.org/10.3390/electronics9060916.

25. Mohammadpour L., Ling T.C., Liew C.S., Aryanfar A. A survey of CNN-based network intrusion detection. *Applied Sciences*. 2022. V.12, №16. P. 8162. URL: https://doi.org/10.3390/app12168162.
26. Dinh N.T., Hoang V.T. Recent advances of CAPTCHA security analysis: A short literature review. *Procedia Computer Science*. 2023. V.218. P. 2550–2562. URL: https://doi.org/10.1016/j.procs.2023.01.229.
27. Challagundla B., Gogireddy Y.R., Peddavenkatagari C.R. Efficient CAPTCHA image recognition using convolutional neural networks and long short-term memory networks. *International Journal of Scientific Research in Engineering and Management (IJSREM)*. 2024. V.8, №3. P. 1–5. URL: https://doi.org/10.55041/IJSREM29450.
28. Wang Z., Shi P., Uddin M.I. CAPTCHA recognition method based on CNN with focal loss. *Complexity*. 2021. V.2021, №1. P. 1–10. URL: https://doi.org/10.1155/2021/6641329
29. Ranjan V., Patidar K., Kushwaha R. An efficient image cryptography mechanism based on the hybridization of standard encryption algorithms. *ACCENTS Transactions on Information Security*. 2020. V.5, №20. P. 42–47. URL: https://doi.org/10.19101/TIS.2020.517004
30. Kaur S., Jindal A. Singular value decomposition (SVD) based image tamper detection scheme. *2020 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India. 2020. P. 695–699. IEEE. URL: https://doi.org/10.1109/ICICT48043.2020.9112432.
31. Hassan N.H., Fakharudin A.S. Web phishing classification model using artificial neural network and deep learning neural network. *International Journal of Advanced Computer Science & Applications*. 2023. V.14, №7. P. 535–542. URL: https://doi.org/10.14569/ijacsa.2023.0140759
32. Anupam S., Kumar Kar A. Phishing website detection using support vector machines and nature-inspired optimization algorithms. *Telecommunication Systems*. 2021. V.76, №1. P. 17–32. URL: https://doi.org/10.1007/s11235-020-00739-w
33. Kamal H., Gautam S., Mehrotra D., Sharif M.S. Reinforcement learning model for detecting phishing websites. *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation*. Cham: Springer, 2024. P. 309–326. URL: https://doi.org/10.1007/978-3-031-52272-7_13
34. Liao N., Li X. Traffic anomaly detection model using k-means and active learning method. *International Journal of Fuzzy Systems*. 2022. V.24, №5. P. 2264–2282. URL: https://doi.org/10.1007/s40815-022-01269-0
35. Salman O., Elhajj I.H., Kayssi A., Chehab A. Data representation for CNN based internet traffic classification: A comparative study. *Multimedia Tools & Applications*. 2021. V.80, №11. P. 16951–16977. URL: https://doi.org/10.1007/s11042-020-09459-4.
36. Abuali K., Nissirat L., Al-Samawi A. Advancing network security with AI: SVM-Based deep learning for intrusion detection. *Sensors (Switzerland)*. 2023. V.23, №21. P. 8959. URL: https://doi.org/10.3390/s23218959.
37. Alharbi Y., Alferaidi A., Yadav K., Dhiman G., Kautish S., Xia J. Denial-of-service attack detection over IPv6 network based on KNN algorithm. *Wireless Communications and Mobile Computing*. 2021. V.2021, №1. P. 1–6. URL: https://doi.org/10.1155/2021/8000869.
38. Muggah R., Margolis M. Why we need global rules to crack down on cybercrime. *World Economic Forum*. 2 січня 2023. URL: https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/?utm_source=chatgpt.com
39. Walter Y. Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*. 2024. V.4, №1. URL: https://doi.org/10.1007/s44163-024-00109-4

40. John-Otumu A.M., Ikerionwu C., Olaniyi O.O., Dokun O., Eze U.F., Nwokonkwo O.C. Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, Omu-Aran, Nigeria. 2024. P. 1–5. URL: https://doi.org/10.1109/seb4sdg60871.2024.10630186
41. Italy's privacy watchdog blocks Chinese AI app DeepSeek on data protection. *Reuters.* 30 січня 2025. URL: https://www.reuters.com/technology/artificial-intelligence/italys-privacy-watchdog-blocks-chinese-ai-app-deepseek-2025-01-30/?utm_source=chatgpt.com
42. Akpuokwe C.U., Adeniyi A.O., Bakare S.S. Legal challenges of artificial intelligence and robotics: A comprehensive review. *Computer Science & IT Research Journal*. 2024. V.5, №3. P. 544–561. URL: https://doi.org/10.51594/csitrj.v5i3.860
43. Joseph S.A. Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*. 2024. V.26, №9. P. 169–189. URL: https://doi.org/10.9734/jerr/2024/v26i91271
44. Basu S. AI tenant tool Safe Rent settles $2.3M housing bias lawsuit. *Read Write*. 2024. URL: https://readwrite.com/ai-tenant-algorithmscreening-tool-saferent-settles-2mhousing-bias-lawsuit/
45. Huang K., Yeoh J., Wright S., Wang H. Build Your Security Program for GenAI. *Future of Business and Finance*. 2024. P. 99–132. URL: https://doi.org/10.1007/978-3-031-54252-7_4
46. Salako A.O., Fabuyi J.A., Aideyan N.T., Selesi-Aina O., Dapo-Oyewole D.L., Olaniyi O.O. Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *Asian Journal of Research in Computer Science*. 2024. V.17, №12. P. 66–88. URL: https://doi.org/10.9734/ajrcos/2024/v17i12530
47. Olabanji S.O., Marquis Y.A., Adigwe C.S., Abidemi A.S., Oladoyinbo T.O., Olaniyi O.O. AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*. 2024. V.17, №3. P. 57–74. URL: https://doi.org/10.9734/ajrcos/2024/v17i3424
48. Balakrishnan A. Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector. *SSRN*. 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4842699
49. Adigwe C.S., Olaniyi O.O., Olabanji S.O., Okunleye O.J., Mayeke N.R., Ajayi S.A. Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*. 2024. V.24, №4. P. 126–146. URL: https://doi.org/10.9734/ajeba/2024/v24i41269
50. Rajawat A.S., Goyal S.B., Bedi P., Jan T., Whaiduzzaman M., Prasad M. Quantum machine learning for security assessment in the internet of medical things (IoMT). *Future Internet*. 2023. V.15. P. 271. URL: https://doi.org/10.3390/fi15080271
51. West M.T., Erfani S.M., Leckie C., Sevior M., Hollenberg L.C., Usman M. Benchmarking adversarially robust quantum machine learning at scale. *Physical Review Research*. 2023. V.5. P. 023186. URL: https://doi.org/10.1103/PhysRevResearch.5.023186
52. Baldassarre M.T., et al. Quantum Artificial Intelligence for Cyber Security Education in Software Engineering. *IS-EUD Workshops*. 2023. URL https://ceur-ws.org/Vol-3408/short-s3-04.pdf
53. Rjoub G., Bentahar J., Wahab O.A., Mizouni R., Song A., Cohen R., et al. A survey on explainable artificial intelligence for cybersecurity. *IEEE Transactions on Network and Service Management*. 2023. V.20. P. 5115–5140. URL: https://doi.org/10.1109/TNSM.2023.3282740

54. Qu J., Ma X., Li J., Luo X., Xue L., Zhang J., et al. An {Input-Agnostic} hierarchical deep learning framework for traffic fingerprinting. *32nd USENIX Security Symposium (USENIX Security 23)*. 2023. P. 589–606. URL https://www.usenix.org/conference/usenixsecurity23/presentation/qu
55. Zhang S., Bai G., Li H., Liu P., Zhang M., Li S. Multisource knowledge reasoning for data-driven IoT security. *Sensors.* 2021. V.21. P. 7579. URL: https://doi.org/10.3390/s21227579
56. Chow Y.W., Susilo W., Li Y., Li N., Nguyen C. Visualization and cybersecurity in the metaverse: a survey. *Journal of Imaging*. 2022. V.9. P. 11. URL: https://doi.org/10.3390/jimaging9010011
57. Alharbi S., Attiah A., Alghazzawi D. Integrating blockchain with artificial intelligence to secure IoT networks: future trends. *Sustainability.* 2022. V.14. P. 16002. URL: https://doi.org/10.3390/su142316002
58. Liu H., Li N., Kou H., Meng S., Li Q. FDRP: federated deep relationship prediction with sequential information. *Wireless Networks*. 2024. V.30. P. 6851–6873. URL: https://doi.org/10.1007/s11276-023-03530-2
59. Achuthan K., Smith R., Patel S. Advances in Artificial Intelligence for Cybersecurity: Emerging Trends and Challenges. *Frontiers in Data Science*. 2024. V.10, №2. P. 123–135. URL: https://doi.org/10.3389/fdata.2024.1497535
60. Vyas R., Purohit S. Machine Learning Techniques for Cyber Threat Detection. *Journal of Cybersecurity and Privacy.* 2024. V.5, №1. P. 45–62. URL: https://doi.org/10.1016/j.jcp.2024.012345

APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

B.V. Prystupa[1,2], N.V. Herasymiuk[2] , Ya.V. Rozhkovsky[2]

[1]Southern Region Military Medical Clinical Center
2, Pirogovska St., Odesa, 65044, Ukraine
[2]Odesa National Medical University
2, Valikhovsky Lane, Odesa, 65082, Ukraine
Email: bogdan.prystupa@onmedu.edu.ua

The modern development of digital technologies, such as the Internet of Things, artificial intelligence, and cloud computing, contributes to the growth of data volumes that require effective protection. Despite the advantages of digitalization, the use of intelligent systems is accompanied by increasing risks of data breaches, DoS attacks, phishing attacks, and zero-day exploits. Artificial intelligence is a promising field in cybersecurity, as it enables the automation of large-scale data analysis, anomaly detection in traffic, and rapid response to threats. The aim of this study is to analyze the application of artificial intelligence technologies to enhance cybersecurity, assess the effectiveness of machine learning and deep learning algorithms in threat detection, and examine the prospects and potential risks associated with the use of artificial intelligence in the protection of information systems. The scientific and practical significance of the study lies in justifying the necessity of using artificial intelligence in cybersecurity and evaluating its effectiveness in real-time cyberattack detection. The application of machine learning technologies helps reduce false positive alerts in intrusion detection systems and enhances incident response speed without human intervention. The research methodology includes a systematic analysis of modern artificial intelligence technologies used in cybersecurity, a review of scientific literature, and an analysis of deep learning algorithms such as neural networks, clustering methods, anomaly detection algorithms, and automated incident response techniques. The study identifies the main machine learning algorithms applied in cybersecurity, including support vector machines, decision trees, neural networks, and reinforcement learning-based approaches. It has been proven that deep learning allows achieving threat detection accuracy of up to 96%, surpassing traditional cyber threat analysis methods. The study examines issues related to the implementation of artificial intelligence in cybersecurity, particularly the vulnerability of models to adversarial attacks that can alter algorithm behavior and bypass security systems. Regulatory challenges and the necessity of creating legal frameworks for controlling autonomous artificial intelligence systems operating beyond the oversight of official IT structures in organizations are also evaluated. The value of this research lies in the development of a comprehensive approach to the use of artificial intelligence in cybersecurity, which will improve the protection of information systems and minimize cyberattack risks. The obtained results will contribute to the expansion of scientific approaches in the field of intelligent security systems and the development of effective real-time threat detection algorithms. The practical significance of this study is the possibility of applying the obtained results to enhance intrusion detection systems, antivirus software, and the implementation of automated solutions for protecting critical infrastructures from cyberattacks.

Keywords: artificial intelligence, machine learning, cybersecurity, threat detection, anomaly analysis, deep learning.

DOI 10.15276/imms.v15.no1.126
УДК 004.89:004.77

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp. 126-136

ШТУЧНИЙ ІНТЕЛЕКТ У СУЧАСНІЙ ВЕБРОЗРОБЦІ ТА ВЕБДИЗАЙНІ: БАГАТОРІВНЕВА КЛАСИФІКАЦІЯ ТА СИСТЕМАТИЗАЦІЯ

Ю.Г. Лобода, О.Г. Трофименко, С.Ю. Манаков , В.І. Гура

Національний університет «Одеська юридична академія»
23, Фонтанська дорога, м. Одеса, 65009, Україна
Emails: loboda@onua.ua, trofymenko@onua.edu.ua

Дослідження присвячене комплексному аналізу впливу технологій штучного інтелекту (ШІ) на процеси сучасної веброзробки та вебдизайну. Актуальність теми зумовлена стрімким розвитком технологій ШІ та необхідністю їх системної інтеграції у професійні процеси розробки програмного забезпечення. Мета дослідження полягає у формуванні багаторівневої класифікації інструментів ШІ за ступенем автономності та когнітивної взаємодії, систематизації екосистеми інструментів ШІ відповідно до етапів життєвого циклу розробки програмного забезпечення. Методологія дослідження базується на системному підході, який включає аналіз сучасної наукової літератури, функціональної класифікації інструментів ШІ та порівняльному аналізі реальних кейсів використання ШІ у веброзробці. Наукова новизна полягає у створенні комплексної систематизації інструментів ШІ для веброзробки, що враховує когнітивні аспекти взаємодії. Основні результати поєднують створення трирівневої класифікації інструментів ШІ (асистенти, генератори, автономні системи) та розробку концептуальної моделі екосистеми рішень ШІ за етапами життєвого циклу веброзробки. Розроблена концептуальна модель візуалізує характер інтеграції ШІ, підтверджуючи, що його вплив не обмежується етапом написання коду. Інструменти ШІ оптимізують кожен етап життєвого циклу веброзробки: від аналізу вимог (Notion AI) та прототипування (Uizard.io) до автоматизованого розгортання (GitLab AI) та проактивного моніторингу (Datadog AI). Особливе значення мають наскрізні процеси (SEO, a11y, A/B-тестування), які демонструють найвищий рівень зрілості інтеграції, оскільки вони функціонують неперервно та комплексно покращують продукт. Поєднання класифікації та моделі екосистеми дозволяє зробити висновок, що ефективне впровадження ШІ вимагає не точкових рішень, а побудови цілісної стратегії, яка враховує рівень автономності інструментів на кожному етапі розробки. Практична значущість результатів полягає у можливості використання запропонованої класифікації для обґрунтованого вибору інструментів, оптимізації процесів розробки, підвищення продуктивності команд та формування стратегічних рішень щодо впровадження технологій ШІ в ІТ-проєкти. Результати можуть бути використані як у професійній діяльності ІТ-компаній, так і в наукових дослідженнях у сфері інженерії програмного забезпечення.

Ключові слова: штучний інтелект, веброзробка, вебдизайн, життєвий цикл розробки, когнітивна взаємодія, автоматизація.

Вступ. Сучасний етап розвитку вебтехнологій характеризується стрімкою інтеграцією технологій штучного інтелекту (ШІ) в усі процеси створення та функціонування вебресурсів. Зростання складності програмних продуктів та підвищені вимоги до швидкості їх розробки стимулюють пошук нових методологій та інструментів [1]. Веброзробка та вебдизайн, як одні з найбільш динамічних сегментів ІТ-галузі, зазнають суттєвих змін і переходять від традиційних практик до гнучких, автоматизованих процесів на основі інтелектуальних систем.

У Концепції розвитку штучного інтелекту в Україні наголошено, що «використання технологій штучного інтелекту сприятиме зменшенню обсягу витрат, підвищенню ефективності виробництва, якості товарів і послуг» [2]. Штучний інтелект розширює можливості розробників та дизайнерів, проте відсутність цілісного розуміння його ролі на кожному етапі життєвого циклу розробки вебзастосунків створює невизначеність для бізнесу при ухваленні стратегічних рішень.

Попри значну кількість доступних на ринку інструментів ШІ, їхнє впровадження у робочі процеси часто має фрагментарний характер. Ключовою проблемою залишається відсутність уніфікованих підходів до кількісного оцінювання впливу використання рішень на основі ШІ на економічну ефективність та на продуктивність процесів веброзробки. Такий дефіцит ускладнює формування стратегічного бачення щодо повноцінної інтеграції інтелектуальних технологій у життєвий цикл створення вебзастосунків, навіть за умов наявності відповідних технічних інструментів.

Аналіз досліджень та публікацій показує активне зростання інтересу до застосування ШІ у веброзробці та вебдизайні. Основні напрями досліджень охоплюють різноманітні аспекти впровадження ШІ, зокрема автоматизацію процесів веброзробки, персоналізацію користувацького досвіду, оптимізацію продуктивності та зниження порогу входу для новачків, а також оцінювання ефективності використання інтелектуальних інструментів у цифрових продуктах.

Згідно з дослідженнями ШІ активно впроваджується у процеси розробки, тестування та обслуговування вебзастосунків, сприяючи автоматизації рутинних завдань і підвищенню продуктивності [1, 3, 4]. Генерація коду, автоматичне виявлення помилок, адаптивний дизайн і машинне тестування забезпечують зниження вартості розробки та покращення якості кінцевого програмного продукту. Дослідження [5, 6] відзначають, що використання ШІ у веброзробці сприяє зменшенню часу завантаження сторінок, ефективному розподілу навантаження та адаптації інтерфейсів до потреб користувачів.

Важливим напрямом є персоналізація контенту та взаємодії з користувачем. У роботах [1, 7, 8] підкреслено роль ШІ персоналізації досвіду користувача, зокрема через системи рекомендацій, аналіз поведінки користувачів та створення адаптивних інтерфейсів. Дослідники роблять висновки, що це не лише підвищує залученість, а й позитивно впливає на UX-показники. У роботах [3, 9, 10] зазначено, що завдяки штучному інтелекту та low-code платформам навіть користувачі без глибокої технічної підготовки можуть створювати складні вебзастосунки, використовуючи drag-and-drop інтерфейси та типові шаблони. Такий підхід сприяє демократизації розробки, розширює можливості малого бізнесу й стартапів, а також стимулює інноваційну активність.

Окрема група досліджень [9, 11-14] присвячена застосуванню генеративних моделей, алгоритмів машинного зору та інтелектуальних систем для побудови візуальних елементів та стилістичної адаптації вебінтерфейсів. Автори робіт [11, 16] акцентують на етичних викликах, пов’язаних із конфіденційністю, прозорістю алгоритмів і впливом автоматизації на креативну складову дизайну.

Особливу увагу приділено оцінюванню впливу ШІ на ефективність проєктної діяльності у веброзробці та вебдизайні. У роботах [1, 4, 5, 15-18] наведено результати емпіричних досліджень і метрик, які демонструють покращення продуктивності, зменшення кількості помилок, прискорення термінів виконання проєктів та позитивний вплив на користувацький досвід. Використання метрик Usability Goals Achievement Metric та Index of Integration дозволило кількісно оцінити рівень інтеграції ШІ в проєкт і його кореляцію з якістю кінцевого продукту [17]. Такі результати підтверджують практичну цінність впровадження ШІ у веброзробку.

Проведений аналіз засвідчує наявність ґрунтовної дослідницької бази щодо застосування технологій ШІ у веброзробці та вебдизайні. Водночас, попри стрімкий розвиток інструментів ШІ, спостерігається відсутність уніфікованих методичних підходів до їхньої системної інтеграції на всіх етапах життєвого циклу вебпроєктів. Недостатньо опрацьованими залишаються питання класифікації інструментів за ступенем автономності та когнітивної взаємодії, а також методи кількісної оцінки ефективності їх впровадження.

Метою даної роботи є формування багаторівневої класифікації інструментів штучного інтелекту за ступенем автономності та когнітивної взаємодії у сфері веброзробки та

вебдизайну, а також систематизація відповідної екосистеми за етапами життєвого циклу розробки.

Для досягнення поставленої мети визначено такі завдання:

– проаналізувати сучасні наукові публікації та дослідження для виявлення ключових напрямів, тенденцій та проблем у застосуванні ШІ у веброзробці та вебдизайні;

– розробити класифікацію інструментів ШІ, яка базується на рівні їхньої когнітивної взаємодії з користувачем та ступені автономності у виконанні завдань;

– систематизувати екосистему інструментів ШІ шляхом їх співвіднесення з основними етапами життєвого циклу розробки програмного забезпечення;

– створити комплексну концептуальну модель, яка візуально ілюструє інтеграцію інструментів ШІ у послідовні та наскрізні процеси веброзробки.

1. Класифікація інструментів ШІ за рівнем когнітивної взаємодії.

Сучасна екосистема веброзробки переживає період кардинальних трансформацій, зумовлених стрімким впровадженням технологій ШІ. Для системного розуміння цих змін та їхнього впливу на професійну діяльність веброзробників доцільно структурувати різноманітні інструменти ШІ за чіткими критеріями, що дозволить оцінити як поточний стан галузі, так і перспективи її розвитку.

Запропонована класифікація структурує інструменти ШІ на основі глибини їхньої інтеграції у творчі та технічні процеси. Вона виділяє три послідовні рівні, які відображають еволюцію ролі ШІ: від допоміжної функції, яка автоматизує рутинні операції, до повноцінного автономного агента, здатного напрацьовувати стратегічні рішення. Такий поділ дозволяє системно оцінити ступінь заміщення людської праці та потенціал для трансформації робочих процесів.

Перший рівень. Інструменти-асистенти (Assisted AI)

Інструменти-асистенти є найпоширенішою та найбільш інтегрованою у сучасні робочі процеси категорією рішень ШІ у веброзробці. Такі системи функціонують як високотехнологічні «помічники», які автоматизують рутинні мікрозавдання та надають контекстні підказки, при цьому залишають всі стратегічні рішення за людиною. Характерною особливістю цього рівня є потреба постійного контролю та керування з боку фахівця, оскільки інструменти доповнюють людські можливості і не замінюють при цьому креативне мислення та професійну інтуїцію.

У сфері розробки прикладом таких рішень є GitHub Copilot (https://github.com/copilot), який аналізує контекст написаного коду та пропонує наступний логічний рядок або блок коду, базуючись на патернах, вивчених з мільйонів репозиторіїв. Подібним чином працює Tabnine (https://www.tabnine.com), який забезпечує розумне автодоповнення коду та враховує стиль програмування конкретного проєкту. Amazon Q Developer (https://aws.amazon.com/q/developer) є інтелектуальним помічником, який не лише автоматизує створення та пояснення програмного коду, а й виконує проактивний аналіз безпеки, виявляє потенційні вразливості ще на етапі написання.

У дизайнерській сфері інструменти-асистенти представлені різноманітними плагінами для Figma, які автоматично перевіряють контрастність кольорів відповідно до стандартів доступності, інструментами автоматичного вирівнювання об’єктів, що економлять час на технічних операціях, та генераторами кольорових палітр, які створюють гармонійні комбінації на основі завантаженого зображення або заданих параметрів.

Другий рівень. Інструменти-генератори (Generative AI)

Цей рівень когнітивної взаємодії представляють інструменти-генератори, які здатні створювати цілісні артефакти на основі високорівневих текстових запитів користувача. Таки системи демонструють якісно вищий рівень автономності, оскільки можуть генерувати дизайн-макети, модулі коду, контент та інші складні об’єкти,

виходячи з абстрактного опису потреб. Однак результат їхньої роботи зазвичай потребує подальшої верифікації, доробки та адаптації людиною, що робить їх потужними інструментами для прискорення процесу створення початкових версій проєктів.

У розробці яскравим представником цієї категорії є v0.dev (https://v0.dev) від Vercel, здатний генерувати повноцінні React-компоненти за текстовим описом функціональності та зовнішнього вигляду. GitHub Copilot Chat розширює можливості базового Copilot, дозволяючи створювати функції, класи та навіть архітектурні рішення через діалоговий інтерфейс. Cursor AI (https://cursor.com/) пропонує генерацію комплексних архітектурних рішень та рефакторинг наявного коду з урахуванням кращих практик.

Дизайнерські інструменти-генератори представлені такими рішеннями, як Galileo AI (https://galileo.ai), який створює повноцінні UI-макети за текстовим описом бажаного інтерфейсу, враховуючи сучасні тренди та принципи UX. Uizard (https://uizard.io) спеціалізується на перетворенні рукописних ескізів та wireframes на цифрові прототипи з інтерактивними елементами. Midjourney (https://www.midjourney.com), хоча і не є спеціалізованим вебдизайн-інструментом, активно використовується для генерації унікальних графічних елементів, ілюстрацій та візуальних концепцій. Relume AI (https://www.relume.io) автоматизує початкові етапи проектування, створюючи карти сайтів та базові wireframes на основі опису бізнес-цілей та цільової аудиторії.

Третій рівень 3. Автономні системи (Autonomous AI)

Найвищий рівень когнітивної взаємодії представляють автономні системи, здатні самостійно керувати цілісними процесами з мінімальним втручанням людини. Такі системи характеризуються здатністю напрацьовувати складні рішення на основі заданих KPI та бізнес-цілей, адаптуватися до змінних умов та навіть самонавчатися на основі набутого досвіду. У контексті веброзробки такі системи поки переважно є експериментальними, однак уже демонструють вражаючий потенціал для кардинальної зміни галузі.

Прикладом автономних систем є :

– комплексні рішення для A/B тестування (табл.1), які не лише генерують альтернативні варіанти дизайну на основі аналізу поведінки користувачів, а й самостійно проводять тестування, аналізують статистичну значущість результатів та автоматично впроваджують найкращий варіант без втручання людини;

– системи динамічної персоналізації UI в реальному часі адаптують інтерфейс під конкретного користувача на основі його поведінкових патернів, демографічних даних та контексту взаємодії. Прикладом такої системи є Dynamic Yield (https://www.dynamicyield.com);

– автоматизовані системи SEO-оптимізації із самостійним внесенням змін здатні аналізувати позиції сайту в пошукових системах, виявляти можливості для покращення та самостійно вносити необхідні зміни в контент, метатеги та структуру сайту, відстежуючи при цьому ефективність внесених змін та коригуючи стратегію відповідно до отриманих результатів. Прикладом є Alli AI (https://www.alliai.com).

Таблиця 1.

Приклади автономних систем ШІ

Система	**Цільове призначення**	**Ключові функції**	**Особливості реалізації**
Agentic AI (agentic.ai)	Автономне UI-тестування	Генерація, виконання і адаптація сценаріїв у реальному часі	Працює як агент, який ухвалює самостійні рішення на основі середовища

Система	Цільове призначення	Ключові функції	Особливості реалізації
RoostGPT (Roost.ai)	AI-генерація варіантів для A/B експериментів	Створення UI-варіантів, інтеграція у пайплайни	Підтримка CI/CD; фокус на генеративному підході
testRigor (testrigor.com)	Тестування застосунків мовними інструкціями	Генерація тестів природною мовою, самовідновлення	Орієнтована на нетехнічних користувачів; A/B через інструкції
BlinqIO (blinq.io)	SaaS для багатоваріантного тестування	Генерація варіантів, поведінковий аналіз	Механізм самонавчання на основі попередніх результатів

Розроблена трирівнева класифікація демонструє чітку траєкторію розвитку інструментів ШІ у веброзробці: від асистентів, які доповнюють можливості фахівця, через генератори, які прискорюють створення артефактів, до автономних систем, що перебирають на себе управління комплексними процесами. Такий перехід від інструментальної підтримки до стратегічного партнерства визначає майбутній ландшафт цифрової індустрії та роль людини в ньому.

2. Систематизація екосистеми інструментів ШІ за етапами життєвого циклу веброзробки.

На основі аналізу сучасних джерел та практичного досвіду розроблено комплексну концептуальну модель екосистеми інструментів ШІ (рис. 1), яка охоплює всі етапи життєвого циклу веброзробки та демонструє системну інтеграцію штучного інтелекту у професійні процеси. Дана систематизація враховує як традиційні послідовні етапи SDLC, так і наскрізні процеси, які проходять через весь життєвий цикл продукту.

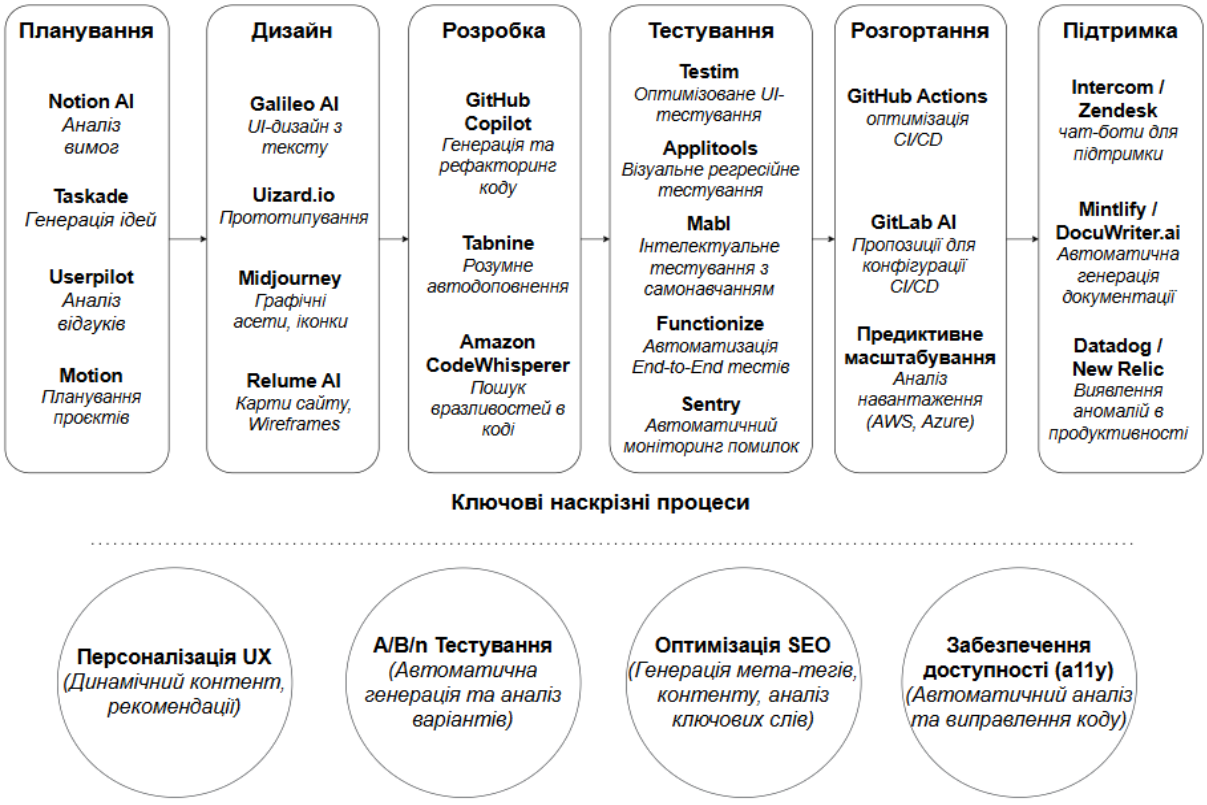


Рис. 1. Концептуальна модель екосистеми інструментів ШІ за етапами життєвого циклу веброзробки

1. Етап планування. Формування концепції та стратегії

Початковий етап життєвого циклу веброзробки стосується аналізу вимог, дослідження ринку, формування концепції продукту та створення технічного завдання. Сучасні інструменти ШІ значно оптимізують ці процеси, автоматизують збір і оброблення даних, структурування ідей та генерацію документації.

Notion AI (https://www.notion.com) трансформує підходи до технічного документування, аналізує неструктуровані описи проєктів, виявляє логічні суперечності у вимогах, генерує узгоджені специфікації та формує пропозиції щодо їх вдосконалення, дозволяє швидко перейти від ідеї до структурованого технічного завдання.

Taskade (https://www.taskade.com) використовує можливості генеративного ШІ для мозкових штурмів та структурування ідей, автоматично формує ієрархію понять і виявляє логічні зв'язки між пропозиціями, спрощує формування початкової концепції продукту та покращує спільну роботу команди.

Userpilot (https://userpilot.com) спеціалізується на поведінковій аналітиці, використовує алгоритми машинного навчання для виявлення прихованих патернів взаємодії користувачів та дозволяє прогнозувати їхні потреби. Такі дані критично важливі на ранніх етапах UX-дизайну, оскільки забезпечують орієнтацію на реальні очікування цільової аудиторії.

Motion (https://usemotion.com) забезпечує інтелектуальне планування проєктів. Система аналізує дедлайни, пріоритети, складність завдань і рівень завантаження членів команди. На основі цих параметрів Motion формує динамічні графіки роботи, автоматизує розподіл задач і підвищує командну продуктивність.

2. Етап дизайну. Створення візуальної концепції та UX

Дизайнерський етап традиційно вважався найбільш креативним та найменш придатним до автоматизації. Проте сучасні інструменти ШІ демонструють значний потенціал для трансформації цього процесу.

Galileo AI пропонує новий підхід до UI-дизайну, дозволяє генерувати повноцінні інтерфейси на основі текстових описів функціональності. Система автоматично враховує принципи юзабіліті, доступності та актуальні дизайн-тренди, аналізує велику кількість наявних рішень для створення оптимальних макетів під конкретні завдання.

Uizard.io (https://uizard.io) спеціалізується на трансформації ескізів і wireframes у цифрові прототипи. За допомогою алгоритмів комп'ютерного зору платформа розпізнає рукописні елементи та перетворює їх на інтерактивні компоненти, що значно прискорює розробку первинних інтерфейсів.

Midjourney, хоча й не є спеціалізованим вебдизайн-інструментом, широко використовується для створення унікальних графічних елементів, ілюстрацій і концептуального візуального оформлення, дозволяє дизайнерам ефективно досліджувати альтернативні стилістичні рішення на етапі формування візуальної стратегії проєкту.

Relume AI (https://www.relume.io) автоматизує створення інформаційної архітектури. Система генерує карти сайтів та базові wireframes на основі аналізу бізнес-цілей та аналізу цільової аудиторії.

3. Етап розробки. Програмування та технічна реалізація

Етап безпосередньої розробки програмного коду зазнав найбільших трансформацій завдяки впровадженню інструментів ШІ.

GitHub Copilot не лише генерує код на основі коментарів та контексту, а й здатен до рефакторингу наявного коду, оптимізації алгоритмів та автоматичного виправлення помилок. Система навчена на мільйонах публічних репозиторіїв та розуміє контекст проєкту, пропонує рішення, які відповідають архітектурі та стилю кодування конкретного застосунку.

Tabnine забезпечує розумне автодоповнення коду, що враховує не лише синтаксис мови програмування, а й специфіку проєкту, стиль команди та найкращі практики.

Amazon CodeWhisperer додає критично важливий компонент безпеки, автоматично аналізує код на наявність потенційних вразливостей та пропонує безпечні альтернативи.

Cursor AI реалізує концепцію повністю орієнтованого середовища розробки, в якому ШІ є активним учасником програмування, здатним підтримувати контекстний діалог із розробником і виконувати складні завдання, зокрема рефакторинг, документування та оптимізацію коду.

4. Етап тестування. Забезпечення якості та стабільності

Тестування традиційно вважається одним із найбільш трудомістких і критично важливих етапів життєвого циклу розробки програмного забезпечення [19]. Проте впровадження інструментів ШІ суттєво змінює цю сферу, автоматизує рутинні процеси та підвищує адаптивність тестових сценаріїв до змін у застосунку [20].

Testim (https://www.testim.io) застосовує алгоритми машинного навчання для створення стійких до змін тестів користувацького інтерфейсу. Завдяки цьому значно знижується потреба в ручному оновленні тестів при кожному редизайні інтерфейсу.

Applitools (https://applitools.com) трансформує візуальне тестування за допомогою механізмів ШІ, виявляє візуальні регресії і розбіжності. Інструмент автоматично порівнює знімки екранів, забезпечуючи кросбраузерну сумісність і виявлення навіть мінімальних відхилень у відображенні контенту.

Mabl (https://www.mabl.com/) реалізує підхід до інтелектуального функціонального тестування. Система автономно досліджує вебзастосунок, формує гіпотези щодо потенційних помилок та створює відповідні сценарії без потреби ручного програмування.

Functionize (https://www.functionize.com) надає можливість описувати тестові сценарії природною мовою, що значно знижує поріг входу для нетехнічних спеціалістів. На основі цих описів система автоматично генерує програмний код для тестування.

Sentry (https://sentry.io) забезпечує постійний моніторинг помилок у продуктивному середовищі, використовуючи ШІ для автоматичної класифікації, пріоритизації та виявлення першопричин проблем.

5. Етап розгортання. Автоматизація впровадження

Етап розгортання забезпечує перехід програмного продукту зі стадії розробки у продуктивне середовище, а також координацію дій між різними інфраструктурними компонентами. Використання інструментів ШІ на цьому етапі значно підвищує стабільність, швидкість та ефективність процесу.

GitHub Actions використовує елементи ШІ для оптимізації CI/CD-пайплайнів. Система аналізує зміни у кодовій базі та автоматично формує відповідні сценарії розгортання, знижуючи ймовірність помилок конфігурації та скорочуючи час доставки оновлень.

GitLab AI доповнює традиційні можливості CI/CD розширеним інтелектуальним управлінням конфігураціями, виявляє потенційні конфлікти та забезпечує їх автоматичне вирішення до моменту розгортання, мінімізує ризики збоїв у продакшн-середовищі.

AWS Auto Scaling із вбудованими механізмами ШІ забезпечує предиктивне масштабування. Система аналізує історичні патерни навантаження, трафік та інші показники й автоматично адаптує розподіл обчислювальних ресурсів. Такий підхід дозволяє підтримувати продуктивність застосунків на стабільному рівні при оптимальному використанні інфраструктури.

6. Етап підтримки. Моніторинг та еволюція продукту

Післявпровадженська підтримка вебзастосунків поступово еволюціонує від реактивного усунення помилок до проактивного управління життєвим циклом продукту, прогнозування збоїв і постійного вдосконалення функціональності.

Intercom (https://www.intercom.com/) та Zendesk (https://www.zendesk.com) інтегрують інтелектуальні чат-боти для автоматизованої підтримки користувачів.

Системи здатні вирішувати складні технічні запити, навчатися на основі діалогів із клієнтами та адаптувати відповіді до специфіки запиту, що підвищує якість обслуговування без залучення операторів.

Mintlify (https://www.mintlify.com/) та DocuWriter.ai (https://www.docuwriter.ai/) автоматизують процес створення та оновлення технічної документації. Інструменти аналізують зміни у кодовій базі та автоматично генерують або оновлюють опис API, інструкції для користувачів і супровідні технічні документи, що суттєво скорочує витрати часу та знижує ризик застарілої документації.

Datadog AI (https://www.datadoghq.com/) та New Relic (https://newrelic.com/) реалізують концепцію інтелектуального моніторингу, використовуючи алгоритми машинного навчання для виявлення аномалій у поведінці вебзастосунків. Системи прогнозують потенційні проблеми ще до їх появи, здійснюють аналіз причин збоїв, автоматично пропонують або застосовують коригування конфігурацій та масштабування інфраструктури відповідно до навантаження.

7. Наскрізні процеси. Інтеграція ШІ через весь життєвий цикл

Окрім інструментів, орієнтованих на окремі етапи життєвого циклу веброзробки, сучасна екосистема ШІ має низку наскрізних процесів, які функціонують неперервно від початкового аналізу вимог до підтримки продукту після впровадження.

Персоналізація користувацького досвіду (UX) реалізується як динамічна система, яка адаптує контент, структуру інтерфейсу та механізми навігації під кожного користувача в режимі реального часу. Системи аналізують поведінкові патерни, демографічні характеристики, контекст сесії та історію взаємодії для формування максимально релевантного досвіду.

A/B/n-тестування трансформувалося в автономні платформи експериментування ШІ, здатні генерувати гіпотези, автоматично створювати кілька варіантів інтерфейсу або контенту, оцінювати статистичну значущість отриманих результатів та впроваджувати оптимальні рішення без участі людини.

Оптимізація для пошукових систем (SEO) зазнала значних змін завдяки ШІ. Сучасні інструменти автоматично генерують метатеги, аналізують ключові слова та структуру контенту, прогнозують ефективність змін й адаптують вміст до специфіки алгоритмів ранжування пошукових систем.

Забезпечення доступності (a11y) вебресурсів також автоматизується. Рішення ШІ сканують код та візуальний інтерфейс, виявляють невідповідності стандартам WCAG (Web Content Accessibility Guidelines), пропонують або виконують автоматичне виправлення порушень, а також генерують альтернативні описи для графічних елементів і відео, що сприяє інклюзивності цифрових сервісів.

Загалом проведений аналіз демонструє, що інтеграція ШІ у веброзробку виходить за межі автоматизації окремих завдань і формує цілісну, взаємопов’язану екосистему. Інструменти ШІ не лише оптимізують усі послідовні етапи життєвого циклу програмного забезпечення, від планування до підтримки, а й забезпечують реалізацію наскрізних процесів, таких як персоналізація, SEO та автоматичне A/B-тестування, які функціонують неперервно. Таким підходом окреслюється фундаментальний перехід від фрагментованого виконання завдань до створення адаптивних, самонавчальних цифрових систем, в яких ШІ відіграє роль невід’ємного компонента розробницького процесу.

Результати та обговорення. У ході дослідження отримано два ключові результати: розроблено трирівневу класифікацію інструментів ШІ за рівнем когнітивної взаємодії та створено концептуальну модель екосистеми цих інструментів у розрізі життєвого циклу веброзробки. Запропонована класифікація на інструменти-асистенти, інструменти-генератори та автономні системи дозволяє структурувати ринок технологій ШІ та оцінити ступінь їхнього впливу на робочі процеси. Інструменти-асистенти (Tabnine, Amazon Q Developer) є базовим рівнем інтеграції, що підвищує індивідуальну

продуктивність, але зберігає повний контроль за розробником. Їх впровадження не вимагає суттєвої зміни методології роботи. Інструменти-генератори (v0.dev, Galileo AI) знаменують якісний перехід, де ШІ стає творчим партнером, здатним створювати повноцінні артефакти (код, дизайн-макети), змінює роль фахівця з «творця» на «редактора» та «верифікатора», що вимагає нових навичок для ефективної взаємодії й формулювання запитів. Автономні системи (Agentic AI, Dynamic Yield) є вищим рівнем, який делегує ШІ ухвалення рішень на основі бізнес-цілей, трансформує підходи до тестування, оптимізації та персоналізації, перетворюючи їх на самокеровані процеси. Запропонована класифікація надає компаніям чіткий фреймворк для стратегічного планування: від простих інвестицій в асистентів для підвищення ефективності до довгострокових вкладень в автономні системи для досягнення конкурентної переваги.

Розроблена концептуальна модель візуалізує характер інтеграції ШІ, підтверджуючи, що його вплив не обмежується етапом написання коду. Інструменти ШІ оптимізують кожен етап життєвого циклу веброзробки: від аналізу вимог (Notion AI) та прототипування (Uizard.io) до автоматизованого розгортання (GitLab AI) та проактивного моніторингу (Datadog AI). Особливе значення мають наскрізні процеси (SEO, a11y, A/B-тестування), які демонструють найвищий рівень зрілості інтеграції, оскільки вони функціонують неперервно та комплексно покращують продукт.

Поєднання класифікації та моделі екосистеми дозволяє зробити висновок, що ефективне впровадження ШІ вимагає не точкових рішень, а побудови цілісної стратегії, яка враховує рівень автономності інструментів на кожному етапі розробки.

Висновки. У статті проведено комплексний аналіз інтеграції ШІ-технологій у сучасну веброзробку та вебдизайн. Запропонована класифікація поділяє інструменти на три рівні за ступенем когнітивної взаємодії та автономності: асистенти, генератори та автономні системи. Така структура дає змогу оцінювати зрілість технологій та планувати їх впровадження. Створена концептуальна модель екосистеми інструментів ШІ наочно демонструє інтеграцію ШІ в усі етапи життєвого циклу веброзробки планування, дизайну, розробки, тестування, розгортання та підтримки, а також у наскрізні процеси, підтверджує перехід від локальної автоматизації до побудови комплексних інтелектуальних систем. Запропоновані класифікація та модель екосистеми слугуватимуть методичною основою для IT-компаній при ухваленні стратегічних рішень щодо впровадження ШІ, оптимізації робочих процесів та обґрунтування інвестицій у технології. Перспективи подальших досліджень лежать у площині розробки стандартизованої методики кількісної оцінки економічної ефективності від впровадження ШІ-інструментів, а також у дослідженні етичних аспектів використання автономних систем у творчих та інженерних процесах.

Список літератури

1. Upadhyaya N. Artificial Intelligence in Web Development: Enhancing Automation, Personalization, and Decision-Making. *International Journal of Advanced Research in Science, Communication and Technology*. 2024. Vol. 4(1). DOI: https://doi.org/10.48175/ijarsct-19367.
2. Концепція розвитку штучного інтелекту в Україні: розпорядження КМУ від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p
3. Vangavolu S. The Future of AI-Powered Web Development and Low-Code Platforms. *International Journal of Innovative Research in Science, Engineering and Technology.* 2025. Vol. 14. Issue 1. DOI : https://doi.org/10.15680/ijirset.2025.1401111.
4. Sonali S. J., Sonali S. G. The Impact of AI on Web Development. *International Journal of Scientific Research in Modern Science and Technology*. 2024. Vol. 3(8). P. 7-12. DOI: https://doi.org/10.59828/ijsrmst.v3i8.240
5. Ayyagiri A., Goel P., Renuka A. Leveraging AI and Machine Learning for Performance Optimization in Web Applications. *Darpan International Research Analysis*. 2024. Vol. 12(2). P. 199-218. DOI: https://doi.org/10.36676/dira.v12.i2.85

6. Cherukuri B. Enhancing Web Application Performance with AI - Driven Optimization Techniques. *International Journal of Science and Research (IJSR).* 2021. Vol. 100, no. 2. P. 1779-1788. DOI: https://doi.org/10.21275/sr21021103246.
7. Kosuru V. (2024). Integration of Artificial Intelligence with Web Development. *International Journal of Innovative Science and Research Technology (IJISRT)*. 2024. Vol. 9. Issue 8. P. 208-210. DOI: https://doi.org/10.38124/ijisrt/ijisrt24aug061
8. Manikantam S., Akhil P., Reddy K., Reddy G., Hariharan S., Kekreja V. Enhanced automated web scraping tool with proliferation of AI techniques. *2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET)*, Nagpur, India, 2024. P. 1-5. DOI: https://doi.org/10.1109/ICICET59348.2024.10616333.
9. Zhang K., Kumar V., Zhang M. Interactive Web: Leveraging AI-Driven Code Generation to Simplify Web Development Algorithms for Novice Programmers. *Artificial Intelligence and Big Data Trends.* 2025. DOI: https://doi.org/10.5121/csit.2024.150107.
10. Meshri A. Design to Code. *International Journal of Scientific Research in Engineering and Management (IJSREM).* 2025. Vol. 9. Issue 4. P. 1-4. DOI: https://doi.org/10.55041/ijsrem44881.
11. Yauheni M. How Artificial Intelligence will change Web Design: opportunities and challenges. *International Journal of Latest Engineering and Management Research (IJLEMR).* 2023. Vol. 8. Issue 6. P. 51-54. DOI: https://doi.org/10.56581/ijlemr.8.6.51-54.
12. Wang P. The Influence of Artificial Intelligence on Visual Elements of Web Page Design under Machine Vision. *Computational Intelligence and Neuroscience*. 2022. DOI: https://doi.org/10.1155/2022/4328400
13. Iqbal H. Sarker. AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. *SN Computer Science. SCI.* Vol. 3, Issue158, 2022. DOI: https://doi.org/10.1007/s42979-022-01043-x
14. Supolia M. AI-Driven Personalization and Recommendations for Web Design *Resources*. *International Journal of Scientific Research in Engineering and Management (IJSREM)*. Vol. 09, Issue 04, 2025. DOI: https://doi.org/10.55041/ijsrem44812
15. Kozhakhmetova A., Mamyrbayev A., Zhidebekkyzy A. Assessing the impact of artificial intelligence on project efficiency enhancement. *Knowledge and Performance Management*. 2024. Vol. 8. Issue 2. P. 109-126. DOI: http://dx.doi.org/10.21511/kpm.08(2).2024.09
16. Cherukuri B. Enhancing Web Application Performance with AI - Driven Optimization Techniques. *International Journal of Science and Research (IJSR)*. 2021. Vol. 10. Issue 2. P. 1779-1788. https://www.ijsr.net/getabstract.php?paperid=SR21021103246. DOI: https://doi.org/10.21275/sr21021103246.
17. Anitha C., Gupta N., Chintala B., Pilli D., Kesavan E., Ali M. Impact of Artificial Intelligence on Software Development Processes. *Journal of Information Systems Engineering and Management*. 2025. Vol. 10, No. 25. P. 431-437. DOI: https://doi.org/10.52783/jisem.v10i25s.4039.
18. Kapoor E. The Impact of Artificial Intelligence on Modern Website Design. *International Journal for Multidisciplinary Research*. 2024. Vol. 6. Issue 3. DOI: https://doi.org/10.36948/ijfmr.2024.v06i03.23234.
19. Трофименко О.Г., Дика А.І., Лобода Ю.Г. Аналіз уразливостей та проблем безпеки вебзастосунків. *Системні технології*. 2023. № 3(146). С. 25-37. DOI: https://doi.org/10.34185/1562-9945-3-146-2023-03.
20. Трофименко О.Г., Дика А.І., Лобода Ю.Г. Аналіз інструментів тестування вебзастосунків. *Кібербезпека: освіта, наука, техніка.* 2023. № 4(20). С. 62-71. DOI: https://doi.org/10.28925/2663-4023.2023.20.6271.

Ю.Г. Лобода, О.Г. Трофименко, С.Ю. Манаков , В.І. Гура

ARTIFICIAL INTELLIGENCE IN MODERN WEB DEVELOPMENT AND WEB DESIGN: MULTILEVEL CLASSIFICATION AND SYSTEMATIZATION

Yu.G. Loboda, O.G. Trofymenko, S.Yu. Manakov, V.I. Hura

National University “Odesa Law Academy”
23, Fontans'ka doroga st., Odesa, 65009, Ukraine
Emails: loboda@onua.ua, trofymenko@onua.edu.ua

The research is devoted to a comprehensive analysis of the impact of artificial intelligence (AI) technologies on the processes of modern web development and web design. The relevance of the topic is driven by the rapid development of AI technologies and the need for their systematic integration into professional software development processes. The purpose of the research is to develop a multi-level classification of AI tools based on their degree of autonomy and cognitive interaction, as well as to systematize the ecosystem of AI tools according to the stages of the software development life cycle. The research methodology is grounded in a systematic approach, which includes an analysis of current scientific literature, a functional classification of AI tools, and a comparative analysis of real-world cases of AI usage in web development. The scientific novelty of the research lies in creating a comprehensive systematization of AI tools for web development, considering the cognitive aspects of interaction. The main results of the research include the creation of a three-level classification of AI tools (assistants, generators, and autonomous systems), as well as the development of a conceptual model of the AI solutions ecosystem, structured according to the stages of the web development life cycle. This developed conceptual model visualizes the nature of AI integration, confirming that its impact extends beyond the stage of code writing. AI tools optimize each stage of the web development life cycle: from requirements analysis (Notion AI) and prototyping (Uizard.io) to automated deployment (GitLab AI) and proactive monitoring (Datadog AI). End-to-end processes (SEO, accessibility, A/B testing) are of particular importance, as they demonstrate the highest level of maturity of integration, functioning continuously and improving the product in a comprehensive manner. The combination of classification and ecosystem models allows for the conclusion that the effective implementation of AI requires not just point solutions, but the development of a holistic strategy that considers the level of autonomy of tools at each stage of development. The practical significance of the results lies in the ability to use the proposed classification for informed decision-making when selecting tools, optimizing development processes, improving team productivity, and forming strategic decisions for the introduction of AI technologies in IT projects. These results can be applied both in the professional activities of IT companies and in scientific research in the field of software engineering.
Keywords: artificial intelligence, web development, web design, development life cycle, cognitive interaction, automation.

DOI 10.15276/imms.v15.no1.137
УДК 004.04

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp. 137-149

МЕТОДОЛОГІЯ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ БАГАТОРІВНЕВОЇ МОДЕЛІ КІБЕРЗАХИСТУ ЗГІДНО З ВИМОГАМИ ЗАКОНОДАВСТВА УКРАЇНИ

В.В. Яцків, С.В. Івасьєв, А.Я. Давлетова, Л.М. Тимошенко

Західноукраїнський національний університет
11, Львівська вул., м. Тернопіль, 46020, Україна
Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: jazkiv@ukr.net, stepan.ivasiev@gmail.com, a7davletova@gmail.com, l.m.timoshenko@op.edu.ua

Робота присвячена практичним аспектам впровадження системи управління інформаційною безпекою (СУІБ) у державних установах відповідно до вимог Закону України №4336-IX. В межах дослідження проведено комплексний аналіз законодавчих вимог до організації та функціонування СУІБ, зокрема щодо побудови, впровадження, моніторингу і постійного удосконалення заходів кібербезпеки. Визначено п'ятирівневу структуру системи кіберзахисту, яка включає політичний, організаційний, технічний, оперативний та контрольний рівні, кожен із яких виконує свої функції у забезпеченні цілісності, конфіденційності та доступності інформації. Розроблено алгоритм організації та поетапного впровадження СУІБ на основі міжнародного стандарту ISO/IEC 27001, який адаптовано до особливостей українського законодавчого поля та практичних вимог державного сектору. З метою підвищення ефективності реалізації системи створено таблицю відповідності між положеннями Закону України №4336-IX та вимогами ISO/IEC 27001, що дозволяє перетворити нормативні вимоги у конкретні елементи СУІБ. В роботі представлено детальний план-графік впровадження СУІБ із чітким визначенням етапів, відповідальних виконавців, контрольних точок та очікуваних результатів, що забезпечує прозорість і керованість процесу. Окрему увагу приділено практичним рекомендаціям щодо технічних і організаційних заходів, спрямованих на підвищення рівня кіберзахисту інформаційних ресурсів. Запропоновані рішення сприяють не лише виконанню вимог чинного законодавства, але й формуванню системного підходу до управління кіберризиками, що є критично важливим в умовах сучасних викликів інформаційної безпеки. Результати дослідження можуть бути використані для оптимізації процесів забезпечення інформаційної безпеки, підвищення кіберстійкості та захисту критичної інформаційної інфраструктури.

Ключові слова: кіберзахист, інформаційна безпека, система управління інформаційною безпекою, ISO/IEC 27001, Закон України №4336-IX, критична інформаційна інфраструктура, державні інформаційні ресурси.

Вступ. В умовах загострення кіберзагроз та активізації інформаційної війни питання захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури набули особливої актуальності. Прийняття Закону України №4336-IX "Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури" [1] стало важливим кроком у формуванні комплексної системи національної кібербезпеки.

Закон визначає основні рівні системи кіберзахисту, які повинні функціонувати як єдиний взаємопов'язаний механізм. Особливого значення набувають вимоги щодо резервного копіювання, шифрування даних, заборони розміщення інформаційних систем на території держави-агресора, а також створення національної системи реагування на кіберінциденти.

Практична реалізація положень цього закону потребує розробки конкретних

методичних підходів та алгоритмів впровадження системи управління інформаційною безпекою (СУІБ) на основі міжнародних стандартів, зокрема ISO/IEC 27001 [2], адаптованих до українських реалій та законодавчих вимог.

Аналіз досліджень і публікацій. Питання впровадження СУІБ в державному секторі на основі міжнародних стандартів, зокрема ISO/IEC 27001 [2], активно досліджуються у вітчизняній та зарубіжній науковій літературі. Особливої актуальності ці дослідження набувають в умовах розбудови кіберзахисту державних установ в Україні відповідно до Закону №4336-IX [2].

Комплексне дослідження правових та організаційних ІБ державних органів України представлено у роботі [3], де проаналізовано подібності та відмінності українського та європейського законодавства у сфері інформаційної безпеки. Проаналізовано вплив процесів інформатизації на ефективність державного управління та виявлено нові загрози, що виникають у результаті активного використання інформаційної сфери. Розглянуто необхідність удосконалення доктринальних підходів до національної безпеки в інформаційній сфері, особливо в частині правового регулювання та уніфікації українського законодавства з європейськими стандартами.

В роботі [4] досліджено управління ІБ в контексті євроінтеграційних процесів. Проаналізовано стадії розвитку українського законодавства в інформаційній сфері. Виявлено, що підвищення ефективності адміністративно-правового забезпечення ІБ можливе через комплекс правових заходів, до яких належать чітке законодавче відображення балансу публічних і приватних інтересів в інформаційній сфері; послідовне застосування механізмів захисту прав людини для врегулювання інформаційних конфліктів; підвищення правової свідомості та компетентності державних службовців, представників усіх гілок влади та населення.

В роботі [5] досліджено практичні аспекти реалізації СУІБ на основі міжнародного стандарту ISO/IEC 27001 в організаціях різних типів. Виявлено, що рівень прийняття стандарту значно відрізняється між між IT-галуззю та іншими сферами діяльності. В результаті моделювання структурних рівнянь проаналізовано фактори низької прийнятності стандарту поза IT-сферою. Розроблено рекомендації для законодавців, органів стандартизації та сертифікації з метою стимулювання ширшого впровадження стандарту, де підкреслено важливість адаптації ISO/IEC 27001 до особливостей конкретної галузі.

Дослідження [6] акцентує увагу на методах оцінки ефективності реалізованих заходів ІБ в державному управлінні, зокрема на важливості внутрішнього аудиту та ризик-менеджменту. Авторами проаналізовано основні поняття та умови впровадження СУІБ на базі нормативних джерел. Визначено ряд ключових проблем, таких як відсутність організації СУІБ, застаріла документація, недостатній аналіз ризиків та обмежене застосування заходів захисту. Запропоновано впровадження регламентів ЄС, зокрема GDPR та директиви NIS, що сприяє підвищенню рівня захисту інформації та зменшенню порушень.

В роботі [7] досліджено сучасні виклики, що виникають у контексті гібридної війни, зокрема на прикладі конфлікту в Україні. Особливу увагу приділено ролі сучасних інформаційних та комунікаційних технологій, які використовуються для кібератак, дезінформації та оперативної координації військових дій. Проведено аналіз впливу цих технологій на міжнародну безпеку, зокрема підвищення ризиків для сусідніх країн, зокрема Польщі, у зв’язку з її геополітичним розташуванням. Авторами визначено специфіку захисту державних інформаційних систем в умовах гібридної агресії, яка включає як технічні, так і інформаційно-психологічні компоненти.

В роботі [8] досліджено роль політичної дипломатії в протидії інформаційним загрозам. Підкреслено роль цих заходів у забезпеченні інформаційної безпеки України та захисті демократичних цінностей.

В роботі [9] проаналізовано сучасні підходи та технології у сфері кібербезпеки,

зокрема застосування шифрування, криптографії та хмарних технологій у публічному секторі для ефективного захисту інформації. Дослідження зосереджене на стратегіях підвищення рівня безпеки та захисту критичної інфраструктури державних установ. Висвітлено необхідність адаптації до швидкозмінного цифрового середовища шляхом впровадження сучасних технологічних рішень і посилення міжнародної співпраці. Визначено важливість інтеграції міжнародних стандартів і практик для створення глобального цифрового простору.

В роботі [10] досліджено ефективність протидії України російській кіберагресії з початку повномасштабного вторгнення у лютому 2022 року. Визначено кроки для розвитку кіберзахисту і координації міжнародної допомоги, а також оцінено можливості їх застосування у майбутніх кризових ситуаціях. Результати дослідження містять рекомендації щодо пріоритетів у формуванні політики та практики у сфері кібербезпеки, зокрема у контексті посилення співпраці між державним і приватним секторами.

В роботі [11] запропоновано методологію оцінювання ризиків гібридних загроз, що поєднує логіко-лінгвістичний підхід із теорією нечітких множин. Цей підхід дозволяє враховувати багатовимірність та невизначеність сучасних кіберзагроз, що є особливо актуальним для державних установ, які стикаються з комплексними атаками, що поєднують технічні та інформаційно-психологічні елементи. Методологія включає дев'ять етапів, починаючи з ідентифікації загроз та експертної оцінки, і завершуючи визначенням рівня ризику та його інтерпретацією. Використання нечіткої логіки дозволяє інтегрувати експертні судження та моделювання ризиків, що сприяє більш точному розподілу ресурсів та підвищенню ефективності управління ризиками.

В роботі [12] досліджено методи порівняльної оцінки ризиків кіберзагроз, використовуючи середні значення та теорію нечітких множин. Такий підхід дозволяє враховувати як кількісні, так і якісні аспекти загроз, що є критично важливим для державних установ при формуванні стратегій кіберзахисту. Запропонована методика сприяє більш обґрунтованому прийняттю рішень щодо пріоритезації заходів безпеки та оптимізації ресурсів, що відповідає вимогам Закону України №4336-IX щодо впровадження ефективних СУІБ.

У дослідженні [13] представлено комплексний огляд організаційної та координаційної структури кіберзахисту держави, зокрема проаналізовано функціональні ролі ключових інституцій - Національного координаційного центру кібербезпеки (НКЦК) при РНБО України та Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ). Особливу увагу приділено процесу розробки й впровадження нової законодавчої бази у сфері кібербезпеки, включаючи нормативне регулювання розподілу повноважень, реагування на кіберінциденти, управління критичною інформаційною інфраструктурою та побудову стратегії кіберстійкості.

Проведений аналіз джерел показав, що сучасна наукова література відображає багатовимірність проблематики впровадження СУІБ у державних установах, охоплюючи як нормативно-правові аспекти, так і технічні, організаційні, а також питання міжнародної співпраці. Більшість досліджень підтверджують доцільність використання моделі ISO/IEC 27001 як основи для реалізації вимог Закону України №4336-IX, підкреслюючи необхідність інтегрованого підходу до кіберзахисту.

Мета роботи полягає у розробці практичних рекомендацій та методичних засад для впровадження СУІБ державних установ та об'єктів критичної інформаційної інфраструктури (КІІ) відповідно до законодавства у сфері інформаційної безпеки (ІБ).

Аналіз структури системи кіберзахисту. Закон України №4336-IX від 27 березня 2025 року, який набрав чинності 20 квітня 2025 року, [1] спрямований на посилення моніторингу та управління інформаційної безпеки (ІБ) в державному секторі та на об'єктах критичної інформаційної інфраструктури (КІІ). Згідно з текстом Закону визначено державну політику та основні складові системи кіберзахисту. Передбачено

створення та функціонування національної системи реагування на кіберінциденти, кібератаки та кіберзагрози, яка включає CERT-UA, а також галузеві та регіональні команди реагування, що формуються органами державної влади та місцевого самоврядування [14]. Визначено роль Державної служби спеціального зв'язку та захисту інформації України у забезпеченні формування та реалізації державної політики з кіберзахисту, здійсненні. стандартизації у сферах криптографічного та технічного захисту інформації, кіберзахисту та протидії технічним розвідкам, а також забезпеченні створення та функціонування національної системи реагування.

Закон передбачає створення резервних копій державних інформаційних ресурсів та їх зберігання відповідно до встановлених вимог. Визначено порядок авторизації з безпеки систем, об'єктів КІІ, що включає оцінку відповідності вимогам законодавства та стандартам у сфері захисту інформації. Встановлено вимоги до технічного захисту інформації, включаючи використання засобів технічного та криптографічного захисту інформації, які мають позитивний експертний висновок або документ про відповідність стандарту ІБ. Визначено обов’язки операторів критичної інфраструктури щодо дотримання вимог у сфері кіберзахисту, повідомлення про кіберінциденти, кібератаки, кіберзагрози та виконання інших зобов'язань щодо захисту інформації та кіберзахисту відповідно до законодавства. Закон передбачає проведення експертних досліджень засобів криптографічного захисту інформації та криптографічних алгоритмів з метою перевірки їх на відповідність вимогам нормативно-правових актів, оцінки ступеня захищеності інформації або науково-технічного рівня..

На основі аналізу положень Закону України № 4336-IX, можна визначити п’ять основних рівнів організації системи кіберзахисту, які є взаємопов’язаними і взаємозалежними. На рисунку 1 наведено схему рівнів кіберзахисту, побудовану на основі законодавчих вимог. Така структуризація ґрунтується на аналізі функцій суб’єктів забезпечення кіберзахисту, вимог до технічного та криптографічного захисту інформації, а також процедур реагування на кіберінциденти, передбачених законодавством.

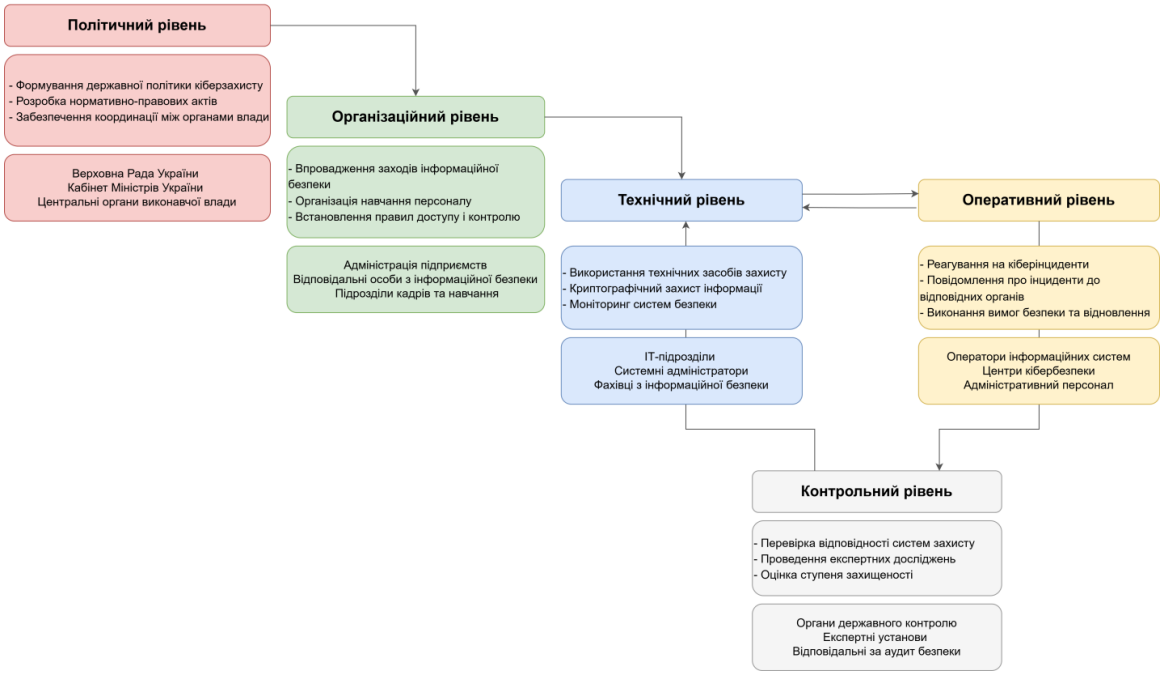


Рис. 1. Схема рівнів організації системи кіберзахисту

Кожен із наведених рівнів має власну сферу відповідальності, проте вони тісно взаємодіють між собою для забезпечення цілісної, ефективної системи захисту

державних інформаційних ресурсів і об’єктів КІІ.

Політичний рівень формує нормативну та стратегічну основу, на яку спираються інші рівні. Визначає загальну політику в галузі кіберзахисту, спрямовує діяльність організаційного, технічного, оперативного та контрольного рівнів.

Організаційний рівень реалізує політичні рішення через координацію заходів на технічному та оперативному рівнях. Відповідає за розробку та впровадження організаційних процедур, а також за підготовку систем до перевірок і аудитів, що здійснюються на контрольному рівні.

Технічний рівень забезпечує впровадження визначених політичними стандартами та організаційними планами конкретних технічних рішень та засобів захисту. Підтримує оперативний рівень, надаючи необхідні технічні інструменти реагування та є об’єктом оцінки на контрольному рівні.

Оперативний рівень використовує технічні інструменти для реагування на інциденти згідно з організаційними процедурами. Забезпечує безперервність функціонування системи та надає зворотний зв'язок для контрольного та політичного рівня.

Контрольний рівень здійснює аудит усіх попередніх рівнів та формує аналітичні висновки для зворотного зв'язку. Основним завданням є перевірка дотримання політик і стандартів, аудит організаційних процедур, оцінка технічних рішень та аналіз ефективності реагування на інциденти. Результати аналізу формують основу для коригування стратегії на політичному рівні.

Проаналізована структура системи кіберзахисту в контексті національного законодавства визначає загальнодержавні принципи та вимоги, які повинні бути імплементовані на рівні окремих суб'єктів господарювання (організацій) та операторів (об'єктів) критичної інфраструктури.

Алгоритм організації та впровадження СУІБ. Алгоритм організації СУІБ згідно із Законом №4336-IX включає наступні етапи:

1. Ініціація проекту та аналіз вимог:

- призначення відповідальної особи (CISO) або створення підрозділу ІБ;
- аналізу нормативно-правових вимог: Закон №4336-IX, Закон «Про інформацію», Закон «Про захист інформації в інформаційно-телекомунікаційних системах», НД ТЗІ та ін.;
- визначення об’єктів захисту, зокрема інформаційних систем, ресурсів, сервісів, сховищ, резервних копій, тощо.

2. Формування політик:

- розробка політик ІБ, резервного копіювання, реагування на інциденти, криптографічного захисту, зберігання копій;
- визначення порядку класифікації інформації.

3. Оцінка ризиків:

- визначення об'єкти критичної інфраструктури;
- проведення оцінку ризиків щодо конфіденційності, цілісності, доступності;
- категоризація систем (з високим, середнім, низьким ризиком).

4. Впровадження заходів:

- налаштування автоматичного резервного копіювання, шифрування за держстандартами (ДСТУ, AES тощо);
- зберігання копій у безпечних локаціях (в т.ч. за кордоном при потребі);
- впровадження систем управління подіями та інцидентами інформаційної безпеки SIEM (наприклад, Splunk, Wazuh);
- забезпечення контролю доступу, зокрема заборона доступу до ІТ-систем з територій РФ або окупованих регіонів.
- інтеграція з CERT-UA або створення власного SOC.

5. Реагування на інциденти та аудит:

- впровадження процедури виявлення та реагування на інциденти;
- проведення регулярних внутрішніх аудитів та тестування систем (наприклад, пентестинг);
- забезпечити навчання персоналу з питань ІБ;
- повідомлення про кіберінциденти до компетентних органів.

6. Актуалізація системи:

- проходження сертифікації КСЗІ (за потреби):
- підготовка звітів до компетентних органів ДССЗЗІ / НКЦК / профільного міністерства;
- регулярне оновлення політик або після критичних змін.

Для реалізаціїи вимог Закону України №4336-IX у вигляді СУІБ для державного органу або об'єкта КІІ, доцільно орієнтуватися на міжнародний стандарт ISO/IEC 27001, адаптований до українського законодавства. В таблиці 1 наведено відповідності положень Закону України №4336-IX та вимог ISO/IEC 27001, що демонструють, які заходи СУІБ відповідають нормам закону і як їх можна реалізувати.

Таблиця 1.

Відповідності Закону №4336-іх та ISO/IEC 27001

Положення Закону №4336-IX	Вимога ISO/IEC 27001	Механізм реалізації у СУІБ
Захист інформації в ІТС (CIA)	A.5.1, A.13.1	Політика ІБ, оцінка ризиків, контроль доступу, шифрування, аудит
Заборона розміщення даних на території ворога	A.11.1.1, A.13.2.1	Географічне обмеження хостингів, угоди з ЦОД, перевірка розміщення резервних копій
Резервне копіювання та зберігання копій	A.12.3.1, A.12.3.2	Розклад резервного копіювання, тестування відновлення, шифрування копій
Шифрування резервних копій	A.10.1.1, A.10.1.2	Використання криптографічних модулів, контроль ключів
Моніторинг та реагування на кіберінциденти	A.16.1.1 - A.16.1.7	SIEM-система, журнали подій, план реагування на інциденти, тестування готовності
Обмін інформацією про кіберінциденти	A.13.2.1, A.6.1.3	Взаємодія з CERT-UA, міжвідомчі протоколи, стандартизована звітність
Визначення об'єктів критичної інформаційної інфраструктури КІІ	A.6.1.2, A.8.1.1	Інвентаризація активів, класифікація, оцінка впливу, ризик-аналіз
Навчання персоналу	A.7.2.2	Регулярні навчання, внутрішні тренінги, курси з кіберзахисту
Контроль доступу до ІТС	A.9.1 - A.9.4	Аутентифікація, розмежування прав доступу, реєстрація дій користувачів
Координація з державними органами	A.6.1.4, A.6.2.1	Регламент взаємодії, звітність, технічне узгодження з регуляторами
Аудит та перевірка відповідності вимогам безпеки	A.18.2.1 - A.18.2.3	Внутрішній аудит, аналіз інцидентів, перевірка заходів контролю

Наведена таблиця дозволяє трансформувати законодавчі вимоги у конкретні елементи СУІБ на основі міжнародного стандарту. Для практичної реалізації цих вимог необхідно розробити алгоритм організації та впровадження СУІБ на рівні окремих об'єктів.

Представлена на рисунку 2 схема процесу впровадження СУІБ ілюструє взаємозв'язки між ключовими компонентами та етапами процесу. Така структура відображає класичний цикл PDCA, що відповідає принципам міжнародних стандартів

та забезпечує системний підхід до управління ІБ через постійне планування, впровадження, контроль та вдосконалення заходів захисту.

Схема відображає повний життєвий цикл СУІБ, що складається з основних рівнів управління:

Рівень управління розпочинається з керівництва, яке ініціює процес та затверджує політику ІБ - основоположний документ, що визначає стратегічні напрями забезпечення інформаційної безпеки організації.

Операційний рівень включає розробку процедур та стандартів, які деталізують політику ІБ та переходять у відділ ІБ - структурний підрозділ, відповідальний за впровадження заходів безпеки. Цей рівень також охоплює навчання персоналу, що забезпечує розуміння та дотримання вимог ІБ усіма співробітниками.

Технічний рівень представлений засобами захисту (технічні та програмні рішення), інфраструктурою (апаратно-програмний комплекс) та моніторингом і журналюванням (системи виявлення та реєстрації подій безпеки).

Рівень управління інцидентами та контролю включає моніторинг інцидентів (постійне відстеження подій безпеки), реагування на інциденти (процедури усунення загроз) та відновлення (заходи з повернення до нормального функціонування).

Рівень аудиту та оцінки завершує цикл аудитом ІБ (перевірка ефективності СУІБ), оцінкою ефективності (аналіз досягнення цілей безпеки) та звітуванням (документування результатів та рекомендацій).

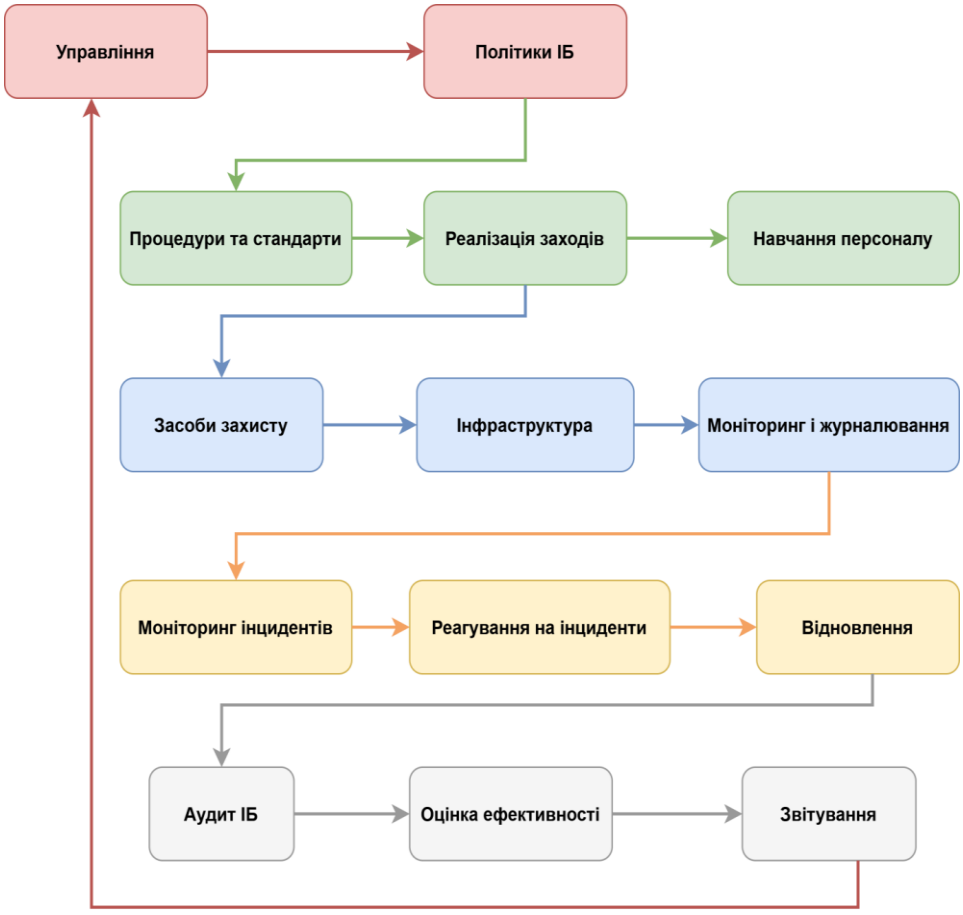


Рис. 2. Схема процесу впровадження СУІБ

Ключовою особливістю схеми є зворотний зв'язок, що з'єднує етап звітування з керівництвом, забезпечуючи безперервне вдосконалення СУІБ на основі отриманих результатів аудиту та оцінки ефективності.

Кожен із визначених п’яти рівнів організації національної системи кіберзахисту

корелює з етапами створення та впровадження СУІБ окремого об'єкта. Вимоги політичного рівня формалізуються через аналіз нормативно-правових актів та розробку внутрішніх політик ІБ. Організаційний рівень реалізується шляхом створення відповідних структур та процедур в організації. Технічний рівень - у впровадженні конкретних засобів захисту та моніторингу. Функції оперативного рівня забезпечуються за допомогою систем реагування на інциденти та звітування. Контрольний рівень реалізується шляхом внутрішнього аудиту та оцінки ефективності.

Трансформація державних вимог у процеси управління ІБ демонструє перехід від теоретичних положень законодавства до практичних заходів їх впровадження.

Розробка план-графіка впровадження СУІБ. Для забезпечення ефективного впровадження СУІБ та досягнення поставлених цілей ІБ необхідно здійснити детальне планування всіх етапів процесу з чітким визначенням часових рамок, відповідальних осіб та контрольних точок. План-графік впровадження СУІБ є ключовим інструментом управління проектом, який дозволяє трансформувати теоретичний алгоритм у практичний інструмент та послідовність конкретних дій.

Розробка та використання план-графіка забезпечує системний підхід до впровадження СУІБ через визначення тривалості кожного етапу, оптимальний розподіл ресурсів та координацію роботи між різними підрозділами. Це дозволяє уникнути хаотичного виконання завдань, мінімізувати ризики пропуску критично важливих заходів та забезпечити своєчасне досягнення проміжних результатів. Крім того, він служить основою для контролю та моніторингу процесу впровадження, надаючи можливість відстежувати прогрес виконання робіт, своєчасно виявляти відхилення від запланованих термінів та приймати корегувальні рішення. Документування планових та фактичних показників виконання також є важливим елементом звітності перед регуляторними органами та демонстрації відповідності нормативним вимогам у сфері кіберзахисту.

На основі даних таблиці 1 реалізовано план-графік впровадження СУІБ згідно із Законом України №4336-IX та ISO/IEC 27001 (таблиця 2).

Таблиця 2.

План-графік впровадження СУІБ

Етап	**Тривалість**	**Основні дії**	**Відповідальні**	**Результат**
Ініціація проєкту та аналіз вимог	4 тижні (1 місяць)	Призначення відповідальних, аналіз нормативної бази, визначення об'єктів захисту	Органи управління, відділ ІБ, юридичний відділ	Проєктний план
Формування політик ІБ	6 тижнів (1,5 місяці)	Створення політик резервного копіювання, управління доступом, реагування на інциденти	CISO, відділ ІБ, юридичний відділ	Пакет затверджених політик ІБ; Регламенти та процедури; Розподіл ролей та відповідальності
Оцінка ризиків та критичності	4 тижні (1 місяць)	Ідентифікація активів, виявлення загроз та вразливостей, оцінка ризиків	Відділ ІБ, IT- відділ, CISO, бізнес-підрозділи, зовнішні експерти	Реєстр активів; Звіт про оцінку ризиків; План управління ризиками
Впровадження технічних заходів	8 тижнів (2 місяці)	Налаштування систем шифрування, резервного копіювання, моніторингу та	Відділ ІБ, IT-відділ, системні адміністратори	Функціональні технічні засоби; Документація конфігурацій

Етап	Тривалість	Основні дії	Відповідальні	Результат
		SIEM		
Навчання персоналу	4 тижні (1 місяць)	Проведення тренінгів, роз'яснення політик, тестування знань персоналу	CISO, HR-департамент, тренери	Протоколи навчання; Сертифіковані користувачі
Реагування на інциденти	6 тижнів (1,5 місяці)	Створення CERT, налаштування систем сповіщення, тестування процедур реагування та відновлення	CERT-команда, відділ ІБ, ІТ- відділ	Функціонуюча система реагування; Процедури виявлення інцидентів
Аудит та оцінка ефективності	4 тижні (1 місяць)	Проведення внутрішнього аудиту, тестування на проникнення, оцінка відповідності стандартам	Зовнішні аудитори, відділ ІБ	Акт внутрішнього аудиту; Рекомендації з удосконалення
Сертифікація та звітність	2 тижні (0,5 місяця)	Оформлення звітів, узгодження, сертифікаційний аудит, планування подальшого розвитку СУІБ	CISO, відділ ІБ, керівництво, сертифікаційний орган	Сертифікат відповідності; Звіти регуляторам; Функціонуюча СУІБ

Представлений в таблиці 2 приклад план-графіка може бути адаптований відповідно до специфіки конкретного об'єкта, масштабу інформаційної системи та наявних ресурсів.

На рисунку 3 наведено графічне представлення плану впровадження СУІБ, що має поетапну структуру. Діаграма відображає послідовність, чіткі часові рамки та залежності між окремими етапами, що допомагає ідентифікувати завдання, затримка яких може вплинути на загальні терміни впровадження, та сконцентрувати увагу на найбільш важливих аспектах реалізації СУІБ. Такий підхід дозволяє ефективно планувати ресурси та оптимізувати загальну тривалість реалізації проекту.

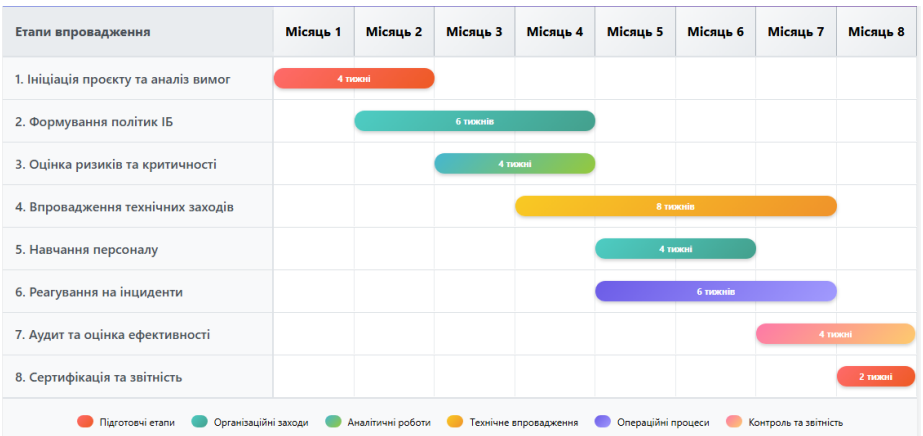


Рис. 3. Графічне представлення етапів впровадження СУІБ

Особливістю представленої діаграми є демонстрація того, що деякі етапи

можуть розпочинатися до повного завершення попередніх, зокрема технічне впровадження може частково перекриватися з розробкою процедур, а навчання персоналу може проводитися паралельно з налаштуванням технічних засобів. Такий підхід дозволяє скоротити загальний час впровадження та забезпечити більш ефективне використання ресурсів.

Практичні рекомендації щодо реалізації системи управління інформаційною безпекою. Результати дослідження дозволяють визначити пріоритетні напрями практичного впровадження СУІБ, що охоплюють як технічні, так і організаційні аспекти забезпечення кіберзахисту відповідно до вимог законодавства.

Проведення формальної категоризації інформаційних систем за рівнем критичності та розробка детальних карт ІТ-систем і ресурсів, а також узгодження з НКЦК забезпечують чітке визначення пріоритетів захисту та ефективний розподіл ресурсів. Впровадження процедур реагування на кіберінциденти, які охоплюють розробку процесів реагування на різні типи інцидентів, а також підключення до CERT-UA та встановленням цільових показників RTO - часу відновлення, RPO - допустимого рівня втрати даних, забезпечує оперативне відновлення функціонування інформаційних систем у разі інцидентів.

Використання сучасних технічних засобів кіберзахисту, серед яких SIEM-системи, рішень для захисту кінцевих точок та систем управління вразливостями - забезпечує проактивний захист і безперервний моніторинг загроз. Налагодження взаємодії з державними органами, що включає своєчасне надсилання звітів про кіберінциденти, виконання вимог нормативних актів, а також координацію з НКЦК, ДССЗЗІ та СБУ, підвищує рівень кібербезпеки на національному рівні.

Реалізація зазначених напрямів у рамках СУІБ дозволить організаціям відповідати вимогам національного законодавства, ефективно управляти кіберризиками та забезпечувати надійний захист критично важливої інформаційної інфраструктури.

Висновки. В роботі проаналізовано встановлену Законом України №4336-IX комплексну систему вимог до кіберзахисту державних інформаційних ресурсів. Виявлено ключові взаємозв'язки між її елементами визначено пять рівнів організації системи кіберзахисту та управління ІБ, що дозволяє забезпечити цілісне функціонування СУІБ.

Практична реалізація законодавчих вимог можлива шляхом адаптації положень міжнародних стандартів до українського правового поля. Побудована таблиця відповідності між положеннями Закону №4336-IX та вимогами стандарту ISO/IEC 27001 забезпечує інтеграцію міжнародних практик з національним регуляторним середовищем.

Запропоновано алгоритм розробки та впровадження СУІБ, який враховує законодавчі вимоги та створює методичну основу для її реалізації в державних установах.

Розроблено план-графік реалізації СУІБ із визначенням відповідальних осіб і контрольних точок дає змогу організовано управляти процесом реалізації вимог Закону України №4336-IX.

Сформульовано практичні кроки технічного й організаційного характеру, які спрямовані на підвищення ефективності функціонування СУІБ і забезпечення її відповідності вимогам державної політики у сфері кіберзахисту.

Список літератури

1. Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» ЗУ № 4336-IX, від 27.03.2025 URL: https://zakon.rada.gov.ua/laws/main/4336-20?utm_source=chatgpt.com#Text
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements URL:

https://www.iso.org/standard/27001
3. Klietsova N., Ahmadov V., Bieliakov K., Klochko A., Kravtsova T. Legal Issues of Information Security of Public Authorities in Ukraine and the European Union: Experience and Realities. *AD Alta: Journal of Interdisciplinary Research*. 2021. 11(2), 12-17. URL: https://www.magnanimitas.cz/ADALTA/110221/PDF/110221.pdf
4. Fedorenko V., Lytvyn N., Luchenko D. Legal Aspects of Information Security Management in the Conditions of Ukraine's European Integration. *Journal of Security and Sustainability Issues*. 2020. 10(2), 477-489. DOI: https://doi.org/10.9770/jssi.2020.10.2(9).
5. Mirtsch M., Blind K., Koch C., Dudek G. Information Security Management in ICT and Non-ICT Sector Companies: A Preventive Innovation Perspective. *Computers & Security.* 2021. 109. 102383. DOI: https://doi.org/10.1016/j.cose.2021.102383.
6. Szczepaniuk E.K., Szczepaniuk H., Rokicki T., Klepacki B. Information Security Assessment in Public Administration. *Computers & Security*. 2019. 90. 101709. DOI: https://doi.org/10.1016/j.cose.2019.101709.
7. Wróblewski W., Wiśniewski M. Cybersecurity in the context of Hybrid Warfare in Ukraine: Analysis of its impact on the public sector and society in Poland. *Central European Journal of Security Studies.* 2024. 1. 48-60. DOI: https://doi.org/10.15804/CEJSS.2023105.
8. Taranenko A. Ensuring information security: Countering Russian disinformation in Ukrainian speeches at the United Nations, *Social Sciences & Humanities Open*. 2024. Volume 10, 100987. DOI: https://doi.org/10.1016/j.ssaho.2024.100987.
9. Chumak O., Holovkin S, Piroh O., Pushkar T, Diegtiar O. Information protection and cyber security in the public and financial sectors. *Edelweiss Applied Science and Technology*. 2024. 8(5), 1164–1174. DOI: https://doi.org/10.55214/25768484.v8i5.1819
10. Axon L., Saunders J., Esteve-Gonzalez P., Carver J., Dutton W., Goldsmith M., Creese S. Private-public initiatives for cybersecurity: the case of Ukraine. *Journal of Cyber Policy.* 2025. 9. 1-24. DOI: https://doi.org/10.1080/23738871.2025.2451256.
11. Zybin S., Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S. Method for the Risk Assessing of Hybrid Threats in Cyber Security Based on Fuzzy Set Theory. URL: http://dx.doi.org/10.2139/ssrn.5143937
12. Korystin O.E., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O.O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory *International Journal of Computer Network and Information Security(IJCNIS)*. 2024. Vol.16, No.1, pp.24-34. DOI: https://doi.org/10.5815/ijcnis.2024.01.02
13. Davydiuk A., Potii O. New Report on National Cybersecurity Governance: Ukraine URL: https://ccdcoe.org/news/2024/new-report-on-national-cybersecurity-governance-ukraine/?utm_source=chatgpt.com
14. 14.Президент України підписав закон про кіберзахист державних інформаційних ресурсів. URL: https://duikt.edu.ua/ua/news-1-569-14204-prezident-ukraini-pidpisav-zakon-pro-kiberzahist-derzhavnih-informaciynih-resursiv_kafedra-cistem-tehnichnogo-zahistu-informacii

METHODOLOGY FOR IMPLEMENTING AN INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON A MULTILEVEL CYBERSECURITY MODEL IN ACCORDANCE WITH THE REQUIREMENTS OF UKRAINIAN LEGISLATION

V.V. Yatskiv, S.V. Ivasiev, A.Ya. Davletova, L.M. Tymoshenko

West Ukrainian National University
11, Lvivska Str. Ternopil, 46009, Ukraine
National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: jazkiv@ukr.net, stepan.ivasiev@gmail.com, a7davletova@gmail.com, l.m.timoshenko@op.edu.ua

The paper is devoted to the practical aspects of implementing an Information Security Management System (ISMS) in public institutions in accordance with the requirements of the Law of Ukraine No. 4336-IX. The study presents a comprehensive analysis of legislative requirements related to the organization and functioning of ISMS, particularly regarding the development, implementation, monitoring, and continuous improvement of cybersecurity measures. A five-level structure of the cybersecurity system has been defined, encompassing political, organizational, technical, operational, and control levels, each of which performs specific functions to ensure the integrity, confidentiality, and availability of information. An algorithm for organizing and gradually implementing the ISMS based on the ISO/IEC 27001 international standard has been developed, adapted to the specifics of Ukrainian legislation and the practical needs of the public sector. To enhance the effectiveness of the system's implementation, a mapping table was created between the provisions of the Law of Ukraine No. 4336-IX and the requirements of ISO/IEC 27001, enabling the transformation of regulatory provisions into specific ISMS elements. The study presents a detailed implementation roadmap with clearly defined stages, responsible actors, control points, and expected results, which ensures transparency and manageability of the process. Special attention is given to practical recommendations regarding technical and organizational measures aimed at strengthening the cybersecurity of information assets. The proposed solutions not only support compliance with current legislation but also contribute to the development of a systematic approach to cyber risk management, which is critically important in the face of modern information security challenges. The research results can be used to optimize information security processes, enhance cyber resilience, and protect critical information infrastructure.

Keywords: cybersecurity, information security, information security management system, ISO/IEC 27001, Law of Ukraine No. 4336-IX, critical information infrastructure, state information resources.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 15, номер 1, 2025. Одеса – 150 с., іл.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 15, No. 1, 2025. Odesa – 150 p.

Засновник: Національний університет «Одеська політехніка»

Зареєстровано Міністерством юстиції України 04.04.2011р.
Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Національного університету «Одеська політехніка», (протокол №9 від 25.03.2025р.)

Адреса редакції: Національний університет «Одеська політехніка»,

1, Шевченка проспект, Одеса 65044 Україна

Web: www.immm.op.edu.ua (immm.opu.ua)

Email: immm.ukraine@gmail.com