МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 16, № 1

Volume 16, No. 1

Одеса – 2026
Odesa – 2026

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.v16.no1.6
UDC 004.942

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 6-15

MODELING OF CRITICAL PHENOMENA IN PLEBANSKI-DEMIANSKI ISLAND SYSTEMS TAKING INTO ACCOUNT ROTATION AND ACCELERATION

H.V. Shapovalov[1], A.I. Kazakov[1], Yu. Muntyan[2], V. Oleynyk[3]

[1]National Odessa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[2]Odesa National Maritime Academy
8, Didrikhsona St., Odesa, 65052,Ukraine
[3]Odesa National University
2, Zmienko St., Odesa, 65026, Ukraine
Email: shapovalov@op.edu.ua[1]

Mathematical modeling of critical phenomena in systems described by island models is relevant. This is due to the fact that island models can be used to predict unstable states of elementary particles, which expands the possibilities of predicting processes in modern nuclear power engineering. Modeling of the vacuum-matter phase transition on the analysis of critical phenomena in island systems can be performed. The main provisions of the theory of catastrophes of Thom and phase transitions of Landau were used to predict the possibility of occurrence of critical phenomena in island systems. Calculations of phase states were made using the differential-topological approach. The results of the calculations indicate the possibility of fulfilling the conditions of phase transitions of the second kind, when two different phases of the system can coexist simultaneously. The system becomes unstable and can pass from one stable phase to another even with small fluctuations under such conditions. To calculate the phase states of island systems, the Plebanski-Demianski island model was studied taking into account rotation and acceleration.
Keywords: coexistence of phases, critical phenomena, phase spaces, island systems, matrix determinant.

Introduction. The prediction of the stability of island systems is directly related to the modeling of the stability of elementary particles [1 – 3], however, the problems of violation of the stability of phase states of such systems have not been sufficiently studied [4 – 7]. There are no studies that examine the conditions for the emergence of coexisting phases. However, the process of formation of critical spaces and spaces of coexistence of phases of different orders is possible in island systems under certain conditions [8 – 12]. Such states of the system can lead to a violation of stability [13 – 17]. The space of coexistence of phases arises when one stable state coexists with another stable state [18]. The appearance of such a space is a phase transition of the first kind, determined by Maxwell's principle. Two (or more) global minima of the potential function in such a space have the same depth [19]. The stable phase can become unstable at some points of the studied space, forming a bifurcation subspace [20]. Two phases in the critical region may become identical at some values of the order parameter. The emergence of identical phases may lead to the formation of a critical space of order two. In the presence of three or four identical phases, critical spaces of order three or four are formed, respectively [21]. The equation of state of the system specifies some n-dimensional manifold when describing phase transitions in the corresponding space. Thom's catastrophe theory can be used to estimate the features of the potential function of a self-organizing system in the case of using one order parameter. With this approach, catastrophe theory is considered as a generalized form of the Ginzburg-Landau phase transition theory [18]. However, to assess the conditions for the emergence of coexisting phases and to describe possible phase transitions in multicomponent systems, it is necessary to use approaches that allow one to analyze the features of potential functions of several order parameters. The properties of the Plebanski-Demianski island model [22] were studied using a non-orthogonal gradient tetrad. The Plebanski-

Demianski model (eight-parameter solution of vacuum Einstein-Maxwell equations) was studied as a model of Schwarzschild, which contains a local singularity [19, 20]. The technique of computer modeling of the process of formation of critical spaces in complex multicomponent systems based on the use of a differential topological approach can be used.

Lagrangian of the Plebanski-Demianski island model. In present communication we study the island model with Plebanski-Demianski type metric in the framework of Riemannian geometry with curvature flows of vacuum space-time. The difference between the equations obtained in our approach in the framework of this model and equations obtained in the framework of the Plebanski-Demianski model [22] is discussed for proposed of non-singular model obtaining. The class of space-time with signature (+, +, +, –) in the Plebiansky-Demiansky model is investigated,

described in coordinates $x^i = (p, q, \sigma, \tau)$:

$$ds^2 = \frac{1}{(p+q)^2}\{\frac{1+(pq)^2}{P}dp^2 + \frac{P}{1+(pq)^2}(d\sigma + q^2 d\tau)^2 + \frac{1+(pq)^2}{Q}dq^2 - \frac{Q}{1+(pq)^2}(d\tau - p^2 d\sigma)^2\} \quad (1)$$

where $P = P(p)$ and $Q = Q(q)$ are arbitrary structure functions depending on p and q, respectively.

The Lagrangian was constructed on the basis of gradient vectors to model critical phenomena in the system under consideration (1):

$$m_i = \frac{\partial x^0}{\partial x^i} = (1,0,0,0), \quad n_i = \frac{\partial x^1}{\partial x^i} = (0,1,0,0),$$
$$p_i = \frac{\partial x^2}{\partial x^i} = (0,0,1,0), \quad s_i = \frac{\partial x^3}{\partial x^i} = (0,0,0,1) \quad (2)$$

The local basis (2) in this case in the general case does not necessarily have to be orthogonal. The proposed approach allows us to obtain a metric tensor in the form of a bilinear combination of basis vectors, the coefficients of which will be functions, and the Lagrangian as a combination of these functions and their first derivatives. Thus, within the framework of the standard field theory, it is possible to obtain a Lagrangian for a rotating charged uniformly accelerated mass in GTR.

From (1) and (2) it follows that

$$x^0 = \tau, \quad x^1 = \sigma, \quad x^2 = p, \quad x^3 = q, \quad (3)$$

and the signature of the space has the form (–, –, –,+). Then, taking into account (3), expression (1) takes the form

$$ds^2 = \frac{1}{(p+q)^2}\{\frac{Q}{1+(pq)^2}(dx^0 - p^2 dx^1)^2 - \frac{P}{1+(pq)^2}(dx^1 + q^2 dx^0)^2 - \frac{1+(pq)^2}{P}dx^{2^2} - \frac{1+(pq)^2}{Q}dx^{3^2}\} \quad (4)$$

The metric tensor corresponding to (1) will then have the form [23]:

$g_{ik} = Am_i m_k - B(m_i n_k + m_k n_i) - Cn_i n_k - Dp_i p_k - Fs_i s_k,$

where

$$A = \frac{Q - q^2 P}{(p+q)^2(1+(pq)^2)}, \; B = 2\frac{p^2 Q + q^2 P}{(p+q)^2(1+(pq)^2)}, \quad (5)$$

$$C = -\frac{p^4 Q - P}{(p+q)^2(1+(pq)^2)}, \quad D = \frac{1+(pq)^2}{(p+q)^2 P}, \quad F = \frac{1+(pq)^2}{(p+q)^2 Q} \quad (6)$$

are functions of coordinates. The components of the metric tensor and basis vectors with superscripts were found in the form:

$$g_{kl}=\begin{pmatrix} A & -B & 0 & 0\\ -B & -C & 0 & 0\\ 0 & 0 & -D & 0\\ 0 & 0 & 0 & -F\end{pmatrix},\quad g^{ik}=\begin{pmatrix} \frac{AC}{A(B^2+AC)} & -\frac{B}{AC+B^2} & 0 & 0\\ -\frac{B}{B^2+AC} & -\frac{A}{AC+B^2} & 0 & 0\\ 0 & 0 & -1/D & 0\\ 0 & 0 & 0 & -1/F\end{pmatrix} \tag{7}$$

$$m^i=\left(\frac{AC}{A(B^2+AC)};-\frac{B}{B^2+AC};0;0\right),\ n^i=\left(-\frac{B}{AC+B^2};-\frac{A}{AC+B^2};0;0\right),$$
$$p^i=\left(0;0;-\frac{1}{D};0\right),\qquad s^i=\left(0;0;0;-\frac{1}{F}\right) \tag{8}$$

The Lagrangian of system (1) was represented as:

$$L=G=\Gamma^m_{il}\Gamma^l_{km}g^{ik}-\Gamma^m_{nm}\Gamma^n_{il}g^{il}=\Gamma^m_{il}\overset{(s)}{\Pi}{}^{il}_{m}-\overset{(as)}{\Pi}{}^{m}_{nm}\Gamma^n_{il}g^{il}, \tag{9}$$

where

$$\Gamma^m_{il}\overset{(s)}{\Pi}{}^{il}_{m}=\frac{1}{4}\{-\frac{2(D_mp^m)^2}{D}-\frac{2(F_ms^m)^2}{F}-\frac{1}{(B^2+AC)^2}[A^mA_mC^2+4A^mB_m-2A^mC_mB^2+2B^mB_m(B^2-AC)+4B^mC_mAB+C_mC^mA^2]-\frac{D_mD^m}{D^2}-\frac{F_mF^m}{F^2}\};$$

$$\Gamma^m_{il}\overset{(s)}{\Pi}{}^{il}_{m}=\frac{1}{4}\{\frac{F^{\Delta 2}}{F^3}+\frac{D^{*2}}{D^3}+\frac{D^{\Delta 2}}{FD^2}+\frac{F^{*2}}{DF^2}-\frac{2}{B^2+AC}(\frac{B^{*2}}{D}+\frac{B^{\Delta 2}}{F})+\frac{1}{(B^2+AC)^2}[A^2(\frac{C^{*2}}{D}+\frac{C^{\Delta 2}}{F})+C^2(\frac{A^{*2}}{D}+\frac{A^{\Delta 2}}{F})-2B^2(\frac{A^*C^*}{D}+\frac{A^{\Delta}C^{\Delta}}{F})+4BC(\frac{A^*B^*}{D}+\frac{A^{\Delta}B^{\Delta}}{F})+4AB(\frac{B^*C^*}{D}+\frac{B^{\Delta}C^{\Delta}}{F})]\};$$

$$\begin{aligned}\overset{(s)}{\Pi}{}^{m}_{nm}\Gamma^n_{il}g^{il}=&\frac{1}{4}\frac{1}{(B^2+AC)^2}[-A^2C^nC_n-4B^2B^nB_n-C^2A_nA^n-4CBA_nB^n\\&-2ACA_nC^n-4ABB_nC^n]\\&+\frac{1}{B^2+AC}\Big[-\frac{2A}{D}C^nD_n-\frac{4B}{D}B_nD^n-\frac{2C}{D}A_nD^n-\frac{2A}{F}C_nF^n\\&-\frac{4B}{F}B_nF^n-\frac{2C}{F}A_nF^n-2CA_ns^nF_ls^l-2CA_np^nD_lp^l\\&-4BB_np^nD_lp^l-4BB_ns^nF_ls^l-2AC_np^nD_lp^l-2AC_ns^nF_ls^l\Big]\\&-\frac{2(D_np^n)^2}{D}-\frac{2(F_ns^n)^2}{F}-\frac{2}{D}D_ns^nF_ls^l-\frac{2}{DF}D_nF^n-\frac{2}{F}D_lp^lF_np^n-\frac{1}{D^2}D_nD^n-\frac{1}{F^2}F^nF_n.\end{aligned} \tag{10}$$

$$\overset{(s)}{\Pi}{}^{m}_{nm}\Gamma^n_{il}g^{il}=\frac{1}{4}\{\frac{1}{(B^2+AC)^2}[A^2(\frac{C^{*2}}{D}+\frac{C^{\Delta 2}}{F})+4B^2(\frac{B^{*2}}{D}+\frac{B^{\Delta 2}}{F})+C^2(\frac{A^{*2}}{D}+\frac{A^{\Delta 2}}{F})+4CB(\frac{A^*B^*}{D}+\frac{A^{\Delta}B^{\Delta}}{F})+2AC(\frac{A^*C^*}{D}+\frac{A^{\Delta}C^{\Delta}}{F})+4AB(\frac{B^*C^*}{D}+\frac{B^{\Delta}C^{\Delta}}{F})]+\frac{1}{B^2+AC}[\frac{2A}{D}(\frac{C^*D^*}{D}+\frac{C^{\Delta}D^{\Delta}}{F})+\frac{4B}{D}(\frac{B^*D^*}{D}+\frac{B^{\Delta}D^{\Delta}}{F})+\frac{2C}{D}\left(\frac{A^*D^*}{D}+\frac{A^{\Delta}D^{\Delta}}{F}\right)+\frac{2A}{F}\left(\frac{C^*E^*}{D}+\frac{C^{\Delta}F^{\Delta}}{F}\right)+\frac{4B}{F}\left(\frac{B^*F^*}{D}+\frac{B^{\Delta}F^{\Delta}}{F}\right)+\frac{2C}{F}(\frac{A^*F^*}{D}+\frac{A^{\Delta}F^{\Delta}}{F})-\frac{2CA^{\Delta}F^{\Delta}}{F^2}-\frac{2CA^*D^*}{D^2}-\frac{4BB^*D^*}{D^2}-\frac{4BB^{\Delta}F^{\Delta}}{F^2}-\frac{2AC^*D^*}{D^2}-\frac{2AC^{\Delta}F^{\Delta}}{F^2}]-\frac{2D^{*2}}{D^3}-\frac{2F^{\Delta 2}}{F^3}+\frac{1}{D^2}(\frac{D^{*2}}{D}+\frac{D^{\Delta 2}}{F})+\frac{1}{F^2}(\frac{F^{*2}}{D}+\frac{F^{\Delta 2}}{F})\}$$

Taking into account the results (9) and (10), the following was obtained:

$$L = \frac{1}{2DF}\{-\frac{1}{(B^2+AC)^2}\left[B^2(FA^*\mathrm{C}^* + DA^{\Delta}\mathrm{C}^{\Delta}) + 2B^2\left(FB^{*2} + DB^{\Delta 2}\right)\right.$$
$$\left. + AC(FA^*\mathrm{C}^* + DA^{\Delta}\mathrm{C}^{\Delta})\right]$$
$$+ \frac{1}{(B^2+AC)}\left[AC^{\Delta}D^{\Delta} + 2BB^{\Delta}D^{\Delta} + CA^{\Delta}D^{\Delta} + AC^*F^* + 2BB^*F^*\right.$$
$$\left. + CA^*F^* - FB^{*2} - DB^{\Delta 2}\right] + \frac{FD^{*2}}{D^2} + \frac{DF^{\Delta 2}}{F^2}\} \tag{11}$$

The symbols * and Δ mean differentiation with respect to the coordinates p and q, respectively. The structure functions in the limit of flat space-time [22] were represented as:

$$P(p) = \frac{a}{s^2a^2+1}\left[a(1-p^4) - \frac{(s^2a^2-1)}{s}p^2\right]$$
$$Q(q) = \frac{a}{s^2a^2+1}\left[a(1-q^4) + \frac{(s^2a^2-1)}{s}q^2\right] \tag{12}$$

The parameter *s* is related to the rotation of space-time. Parameter *a* has the value of the acceleration.

Taking into account (12), functions (6) will take the form:

$$A = \frac{a\{as[1-q^4-q^2(1-p^4)]+(s^2a^2-1)(1+p^2)q^2\}}{s(s^2a^2+1)(p+q)^2(1+(pq)^2)}$$
$$B = \frac{2a^2\{p^2(1-q^4)+q^2(1-p^4)\}}{(s^2a^2+1)(p+q)^2(1+(pq)^2)}$$
$$C = -\frac{a\{sa[\,p^4(2-q^4)-1]+(s^2a^2-1)(1+q^2p^2)p^2\}}{s(s^2a^2+1)(p+q)^2(1+(pq)^2)}$$
$$D = \frac{s(1+(pq)^2)(s^2a^2+1)}{a[sa(1-p^4)-(a^2s^2-1)p^2](p+q)^2}$$
$$F = \frac{s(s^2a^2+1)(1+(pq)^2)}{a(p+q)^2[sa(1-q^4)+(a^2s^2-1)q^2]}$$

Predictive modeling of critical phenomena in island systems. Predictive modeling of critical phenomena of system (1) for the case a>0 and s>0 was carried out [22]. The position of the points in space at which the stability condition is satisfied was calculated from the system [20, 21]:

$$\left|\vec{\nabla}L\right| = 0; \quad det\frac{d^2L}{d\mathrm{X}^2} > 0, \tag{13}$$

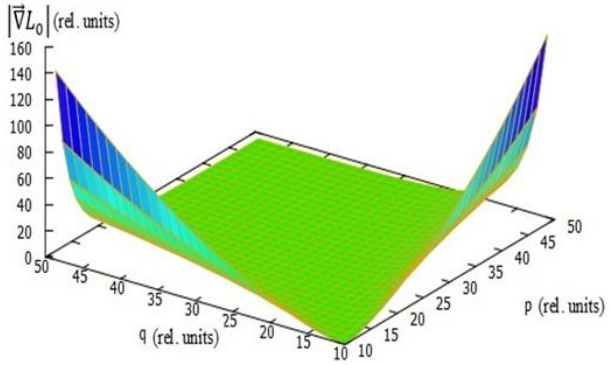


Fig.1a. Results of modeling the surface of the Lagrangian gradient modulus $\left|\vec{\nabla}L\right|$ in relative units

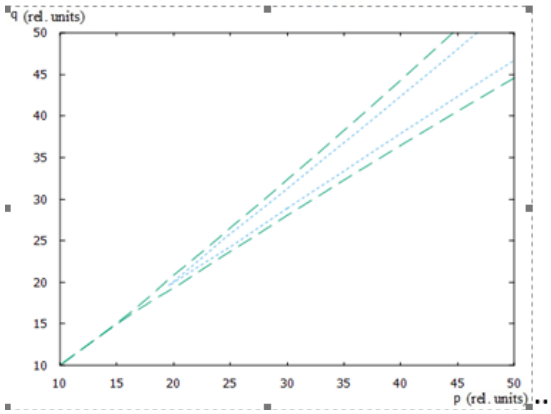


Fig.1b. Results of modeling the zero contour of the Lagrangian gradient modulus $\left|\vec{\nabla}L\right|$ in relative units

$$X = X(p;q), \qquad det\frac{d^2L}{dX^2} = det\begin{pmatrix} \frac{\partial^2(p,q)}{\partial p^2} & \frac{\partial^2 L(p,q)}{\partial p \partial q} \\ \frac{\partial^2 L(p,q)}{\partial q \partial p} & \frac{\partial^2 L(p,q)}{\partial q^2} \end{pmatrix}$$

The results of modeling the surface of the Lagrangian gradient modulus $\left|\vec{\nabla}L\right|$ and its zero contour in relative units are shown in Fig.1a and Fig.1b, respectively.

The results of modeling the surface of the determinant $det\frac{d^2L}{dX^2}$ of the second derivatives of the Lagrangian and its zero contour in relative units are shown in Fig.2a and Fig.2b, respectively.

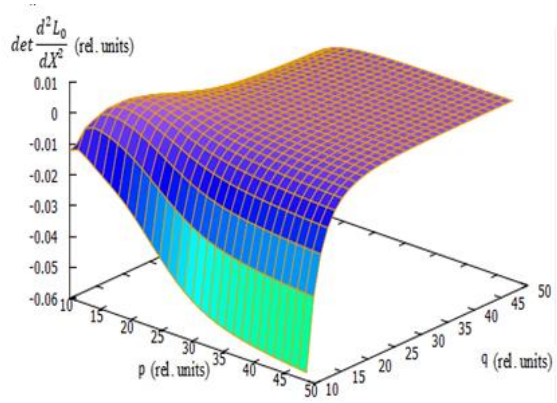


Fig.2a. Results of modeling the surface of the determinant of the second derivatives of the Lagrangian in relative units.

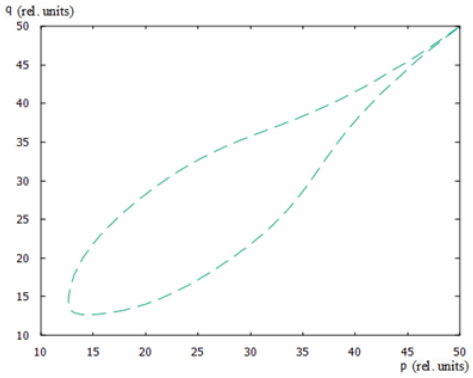


Fig.2b. Results of modeling the zero contour of the determinant of second derivatives in relative units

The position of the points at which the conditions for the emergence of the bifurcation space of the studied model (1) are fulfilled was calculated from the system of equations [22, 23]:

$$\left|\vec{\nabla}L\right| = 0; \quad det\frac{d^2L}{dX^2} = 0 \tag{14}$$

The zero contour of the determinant of the second derivatives ($det\frac{d^2L}{dX^2} = 0$) of the Lagrangian (9) is shown in Fig. 2b. The position of the points on the section of the phase diagram, in which the conditions for the emergence of a space of coexistence of two phases are fulfilled, was calculated from a system of equations and inequalities [22, 23]:

$$\left|\vec{\nabla}L\right| = 0, \quad det\frac{d^2L}{dX^2} = 0,\ det\frac{d^3L}{dX^3} = 0,\ det\frac{d^4L}{dX^4} > 0 \tag{15}$$

where $det\frac{d^3L}{dX^3}$ is the determinant of the third derivative of the Lagrangian with respect to the arguments p and q. The block matrix diagonalization algorithm was used to obtain the matrix of third derivatives of the Lagrangian. Analytical expressions of the third partial derivatives of the Lagrangian were obtained in the first step. Two matrices of partial derivatives of the components of the matrix of second derivatives of the Lagrangian with respect to arguments *p* and *q* were formed, respectively:

$$\frac{d^3L}{dp^3} = \begin{pmatrix} \frac{\partial^3 L(p,q)}{\partial p^3} & \frac{\partial^3 L(p,q)}{\partial p \partial q \partial p} \\ \frac{\partial^3 L(p,q)}{\partial q \partial p \partial p} & \frac{\partial^3 L(p,q)}{\partial q^2 \partial p} \end{pmatrix}, \quad \frac{d^3L}{dq^3} = \begin{pmatrix} \frac{\partial^3 L_0(p,q)}{\partial p^2 \partial q} & \frac{\partial^3 L_0(p,q)}{\partial p \partial q \partial q} \\ \frac{\partial^3 L_0(p,q)}{\partial q \partial p \partial q} & \frac{\partial^3 L_0(p,q)}{\partial q^3} \end{pmatrix} \tag{16}$$

The block-diagonal matrix of the third derivative of the Lagrangian of system (1) with respect to arguments p and q was obtained from (16) in the next step:

$$\frac{d^3L}{dX^3} = \begin{pmatrix} \frac{d^3L}{dp^3} & 0 \\ 0 & \frac{d^3L}{dq^3} \end{pmatrix} \tag{17}$$

The results of calculating the positions of the points of the surface of the determinant of the third derivative of the Lagrangian (9) and its zero contours are shown in Fig. 3a and Fig. 3b, respectively.

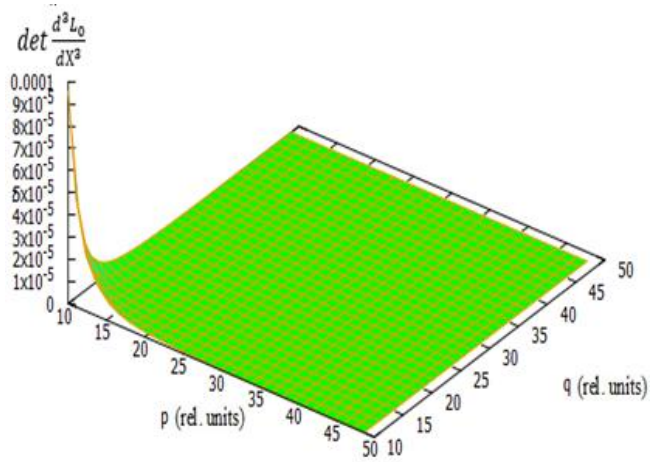


Fig. 3a. Results of calculating the surface of the determinant of the third derivative of the Lagrangian.

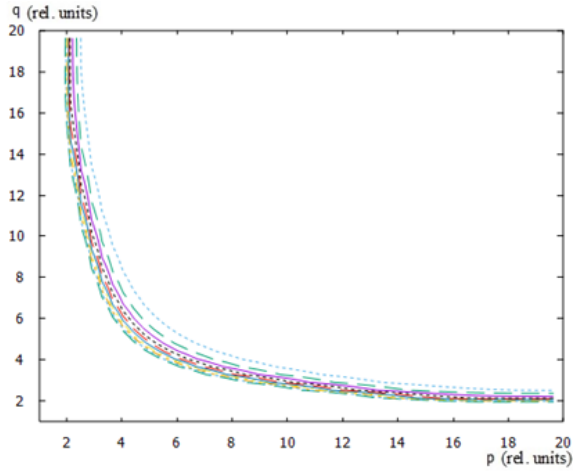


Fig. 3b. Results of calculation of zero contours of the determinant of the third derivative of the Lagrangian.

The calculated surface of the determinant of the fourth derivatives of the Lagrangian (9) on the studied interval is shown in Fig.4.

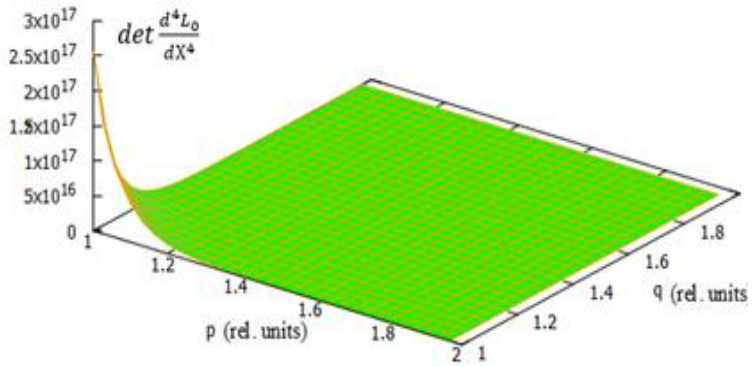


Fig. 4. Results of calculating the position of the points of the surface of the determinant of the fourth derivative of the Lagrangian in relative units

Analytical expressions of the fourth partial derivatives of the Lagrangian (1) with respect to $X(p,q)$ for calculating the determinant of the fourth derivative were obtained. Matrices of partial derivatives in the next step were composed:

$$\frac{d^4L}{dp^4}=\begin{pmatrix}\frac{\partial^4L(p,q)}{\partial p^4} & \frac{\partial^4L(p,q)}{\partial p\partial q\partial p^2}\\ \frac{\partial^4L(p,q)}{\partial q\partial p^3} & \frac{\partial^4L(p,q)}{\partial q^2\partial p^2}\end{pmatrix};\ \frac{d^4L}{dp^3q}=\begin{pmatrix}\frac{\partial^4L(p,q)}{\partial p^3\partial q} & \frac{\partial^4L(p,q)}{\partial p\partial q\partial p\partial q}\\ \frac{\partial^4L(p,q)}{\partial q\partial p^2\partial q} & \frac{\partial^4L(p,q)}{\partial q^2\partial p\partial q}\end{pmatrix}$$

$$\frac{d^4L}{dq^3p}=\begin{pmatrix}\frac{\partial^4L_0(p,q)}{\partial p^2\partial q\partial p} & \frac{\partial^4L_0(p,q)}{\partial p\partial q^2\partial p}\\ \frac{\partial^4L_0(p,q)}{\partial q\partial p\partial q\partial p} & \frac{\partial^4L_0(p,q)}{\partial q^3\partial p}\end{pmatrix};\ \frac{d^4L}{dq^4}=\begin{pmatrix}\frac{\partial^4L_0(p,q)}{\partial p^2\partial q^2} & \frac{\partial^4L_0(p,q)}{\partial p\partial q^3}\\ \frac{\partial^4L_0(p,q)}{\partial q\partial p\partial q^2} & \frac{\partial^4L_0(p,q)}{\partial q^4}\end{pmatrix}.$$

The block-diagonal matrix $\frac{d^4L_0}{dX^4}$ was composed from the obtained matrices at the next step:

$$\frac{d^4L_0}{dX^4} = \begin{pmatrix} \frac{d^4L}{dp^4} & 0 & 0 & 0 \\ 0 & \frac{d^4L}{dp^3q} & 0 & 0 \\ 0 & 0 & \frac{d^4L}{dq^3p} & 0 \\ 0 & 0 & 0 & \frac{d^4L}{dq^4} \end{pmatrix} \quad (18)$$

Analysis of the position of the points of the surface of the determinant of the fourth derivative of the Lagrangian (9) of the system under study (1) showed that the condition $det\frac{d^4L_0}{dX^4} > 0$, that is, the positive signature of the calculated points of the surface of the determinant of the fourth derivative of the Lagrangian, is satisfied over the entire range of the phase space under study. The differential-topological method for calculating the position of the points of the phase space of system (1) in which the conditions for the emergence of phase coexistence spaces of order two are satisfied was applied. The positions of the points on the phase space at which conditions (15) are simultaneously satisfied in the region under study were determined. Analytical expressions for first- to fourth-order derivatives and calculations of the position of the surface points of the determinants of the corresponding derivatives using the open computer algebra system MAXIMA [24] were determined. The positions of the points on the section of the phase diagram of the existence of the system (1), in which the condition of coexistence of second-order phases (15) is fulfilled, are shown in Fig. 6. The conditions of zero values R of the derivatives from the first to the third inclusive and positive values of the fourth derivative of the Lagrangian (9) of the system under study (1) at these points are fulfilled simultaneously. The points in the phase space where the two phases coexist are located along the boundary of the found region (Fig. 6). Condition (15) is fulfilled along the boundary of the found space. Thus, the simulation results predict the emergence of spaces of coexistence of two phases near the found boundary. System (1) will be in different phases on both sides of the found boundary.

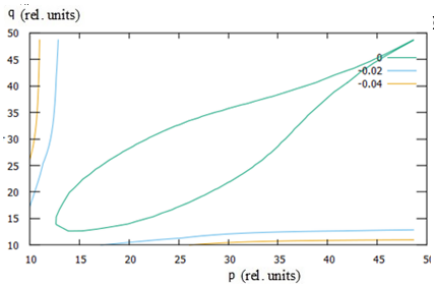


Fig. 6. Results of calculations of the section of the phase diagram of the system (1). The positions of the points at which the condition of coexistence of second-order phases is fulfilled are shown (in relative coordinates).

Conclusions. The results of modeling critical phenomena in island systems of the Plebanski-Demianski type indicate the existence of a space in which the stability condition of the system under consideration is met, as well as the possibility of the emergence of bifurcation regions under certain conditions. Calculations of sections of phase diagrams of the considered system show that at certain values of parameters and independent coordinates of the model, the conditions for the emergence of phase coexistence spaces of order two will be fulfilled. Such states are unstable and can lead to the degradation of the system by a jump. The relativity of coordinates allows us to adapt the proposed approach to predict the emergence of critical spaces on phase sections of existence diagrams of both various elementary particles and island macrosystems.

References

1. Ismail M., Ellithi A. Y., Adel A., Anwer H. Islands of stability and quasi-magic numbers for super- and ultra-heavy nuclei. *Chinese Phys*. 2016. P. 40. 124102.

2. Agbemava S., Afanasjev A., Ring P., Octupole deformation in the ground states of even-even nuclei: A global analysis within hthe covariant density functional theory. 2016. *Phys. Rev*. P. 93. 044304.
3. Schunck N., Robledo L. Microscopic theory of nuclear fission: a review. *Rep. Prog. Phys*. 2016. V.79. 116301
4. Agbemava S., Afanasjev A., Taninah A., Gyawali A.. Extension of the nuclear landscape to hyperheavy nuclei. *Phys.Rev.* 2019. V. 99. No. 3. 034316.
5. Afanasjev A., Agbemava S., Gyawali A. Hyperheavy nuclei: existence and stability. *Phys.Lett.B.* 2018. V.782. P.533-540.
6. Kosior A., Staszczak A., Wong C.Y. Toroidal Nuclear Matter Distributions of Superheavy Nuclei from Constrained Skyrme--HFB Calculations. *Acta Phys. Polon. Supp.* 2017. V.10, P.249.
7. Staszczak A., Wong C.Y., Kosior A. Toroidal high-spin isomers in the nucleus. *Phys. Rev*. C. 2017. V.95, No.5. 054315.
8. Agbemava S., Afanasjev A., Ring P. Octupole deformation in the ground states of even-even nuclei: a global analysis within the covariant density functional theory. *Phys. Rev. C*. 2016. V.93. No.4. 044304.
9. Afanasjev A., Agbemava S. Ray D., Ray P. Neutron drip line: Single-particle degrees of freedom and pairing properties as sources of theoretical uncertainties. *Phys. Rev. C*. 2015. V.91, No.1. 014324.
10. Ismail M., Ellithi A.Y., Adel A., Anwer H. On magic numbers for super- and ultraheavy systems and hypothetical spherical double-magic nuclei. *J. Phys. G* 43. 2016. No.1. 015101.
11. Afanasjev A. Agbemava S. Gyawali A. Hyperheavy nuclei: existence and stability. *Phys. Lett. B*. 2018. 782. P.533-540.
12. Giuliani S.A., Martinez-Pinedo G., Robledo L.M.. Fission properties of superheavy nuclei for r-process calculations. *Phys. Rev. C.* 2018. V.97. No. 3. 034323.
13. Fattoyev F., Horowitz C., Schuetrumpf B.. Quantum Nuclear Pasta and Nuclear Symmetry *Energy Phys. Rev. C*. 2017. V.95, No.5. 055804.
14. Radosław A. Kycia, Sebastian Kubis, Włodzimierz Wójcik. Topological analysis of nuclear pasta phases. *Phys.Rev. C*. 2017. V.96. No 2. 025803.
15. Kubis S., Wójcik W.. Geometric approach to nuclear pasta phases. *Phys.Rev.C.* 2016. V. 94 .No.6. 065805.
16. Schuetrumpf B., Klatt M.A., Iida K., Schroeder-Turk G.E., Maruhn J.A.. Appearance of the single gyroid network phase in "nuclear pasta" matter. *Phys. Rev. C*. 2015. *V.* 91.No.2. 025801
17. Malov L. Adamian G., Antonenko N., Lenske H. Landscape of the island of stability with self-consistent mean-field potentials. *Phys. Rev. C*. 2021.V.104. No 6.
18. Okada K. Classical calculations on the phase transition I. Phase diagram in four-dimensional space for the system with one order parameter. *J. Phys. Soc. Jap.* 1982. V. 51. No 10. P. 3250 – 3257.
19. Shapovalov H., Kazakov A. Oleynyk V. Simulation of critical phenomena in the island systems in general relativity with flows. *2nd International Conference on Innovative Solutions in Software Engineering. Ivano-Frankivsk, Ukraine*. 2023.
20. Shapovlov H. Kazakov A., Oleynyk V., Zorilo V. Matematical modeling of critical phenomena according to the Plebanski- Demianski metric. *Technologies, Innovative And Modern Theories Of Scientists. XX International Scientific and Practical Conference. Graz, Austria*. 2023. P. 434 – 438.
21. Kazakov A.I., Shapovalov G.V., Moskvin P.P.. Computer simulation for formation of critical spaces in II–VI solid solutions. *Journal of Crystal Growth*. 2019. V. 506. P. 201 – 205.

22. Plebanski J.F., Demianski M. Rotating, Charged, and Uniformly Accelerating Mass in General Relativity. *Ann. Phys*. 1976. V. 98, P. 98-127.
23. Olyeynik V.P. Problems of Atomic Science and Technology. *Nuclear Physics Investigations* 2012. V. 57. No. 1. P. 171-172.
24. Maxima. A Computer Algebra System. URL: http://maxima.sourceforge.net

МОДЕЛЮВАННЯ КРИТИЧНИХ ЯВИЩ В ОСТРІВНИХ СИСТЕМАХ ПЛЕБАНСЬКОГО-ДЕМ'ЯНСЬКОГО З УРАХУВАННЯМ ОБЕРТАННЯ ТА ПРИСКОРЕННЯ

Г.В. Шаповалов[1], А.І. Казаков[1], Ю. Мунтян[2], В. Олейник[3]

[1]Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[2]Одеська національна морська академія
8, Дідріхсона вул., Одеса, 65052, Україна
[3]Одеський національний університет
2, Змієнка вул., Одеса, 65026, Україна

Математичне моделювання критичних явищ у системах, що описуються острівними моделями, є актуальним. Це пов'язано з тим, що острівні моделі можуть бути використані для прогнозування нестійких станів елементарних частинок, що розширює можливості прогнозування процесів у сучасній ядерній енергетиці. Можна виконати моделювання фазового переходу вакуум-матерія на основі аналізу критичних явищ в острівних системах. Основні положення теорії катастроф Тома та фазових переходів Ландау були використані для прогнозування можливості виникнення критичних явищ в острівних системах. Розрахунки фазових станів були виконані з використанням диференціально-топологічного підходу. Результати розрахунків вказують на можливість виконання умов фазових переходів другого роду, коли дві різні фази системи можуть співіснувати одночасно. Система стає нестійкою та може переходити з однієї стабільної фази в іншу навіть з невеликими коливаннями за таких умов. Для розрахунку фазових станів острівних систем було досліджено модель острова Плебанського-Дем'янського з урахуванням обертання та прискорення.

Ключові слова: співіснування фаз, критичні явища, фазові простори, острівні системи, матричний визначник.

DOI 10.15276/imms.v16.no1.16
UDC 004.056.55

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 16-25

THE IMPACT OF CODEWORD SIZE ON THE ROBUSTNESS OF CODE-CONTROLLED STEGANOGRAPHIC METHODS

Sokolov A.V.[1], Pohorieltsev P.M[2]., Zhuk Ye.A.[3], Filipenko N.O.[2]

[1]National University "Odesa Law Academy"
23, Fontanska Road, Odesa, 65009, Ukraine
[2]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[3]Kharkiv National University of Radio Electronics
14, Nauky Ave., Kharkiv, 61166, Ukraine
Email: radiosquid@gmail.com[1]

The paper is devoted to a novel direction in digital steganography, the concept of code-controlled information embedding, which allows adaptive management of the embedding process based on the properties of specially designed codewords. In contrast to conventional spatial- or transform-domain techniques, the approach of code control enables precise localization of embedding effects in the frequency domain while maintaining minimal computational complexity. The research aims to determine how the size of the codeword affects the robustness of the steganographic message under identical conditions. To achieve this, a series of controlled experiments was performed using digital images subjected to JPEG compression at varying quality factors. Two embedding strategies were compared: embedding a single bit per smaller block and embedding multiple bits into a larger block at the same capacity. The results show that increasing the codeword size and embedding several bits per block can significantly improve robustness without degrading the reliability of perception, as confirmed by stable PSNR values. However, the experiments also reveal that the benefits of enlarging the codeword size tend to saturate beyond a certain threshold, since larger blocks become more susceptible to compression-induced distortions. The research provides new insights into the balance between robustness, reliability of perception, and embedding efficiency in code-controlled steganography. The results contribute to the optimization of block sizes and embedding strategies, offering practical guidelines for the development of next-generation steganographic systems. The results obtained not only enhance the resilience of hidden data but also lay the foundation for creating adaptive, intelligent, and computationally efficient information-hiding algorithms that can be integrated into modern cybersecurity infrastructures.
Keywords: digital steganography, code-controlled embedding, Walsh-Hadamard transform, robustness, reliability of perception, information hiding, block optimization, JPEG compression, cybersecurity.

Introduction and statement of the problem. In the modern digital era, the exponential growth of multimedia content – ranging from images and audio to video and interactive media – has created both opportunities and challenges for information security. While cryptography has long been recognized as a cornerstone for protecting the confidentiality and integrity of data, steganography is increasingly emerging as a complementary technique that addresses a different aspect of secure communication: the concealment of information itself. By embedding sensitive data within seemingly innocuous multimedia carriers, steganography not only adds a layer of secrecy but also enhances resilience against unauthorized detection and interception. As the volume of digital information continues to expand, and as sophisticated analytical tools become more prevalent, steganography is poised to become an indispensable component of modern information protection systems, operating together with cryptographic methods to ensure both secrecy and security.

Today, the main efforts of researchers in the field of steganography are focused on improving several key characteristics of steganographic methods. These include reliability of

perception, ensuring that the embedded information remains undetectable to human perception; capacity, maximizing the amount of hidden data that can be embedded without compromising the carrier; robustness against attacks, maintaining the integrity of the embedded message under various distortions or manipulations; and resistance to steganalysis, reducing the likelihood of detection by automated or statistical analysis tools. Optimizing these characteristics simultaneously remains a central challenge, guiding the development of both traditional and emerging steganographic techniques.

Today, steganographic techniques have become highly diverse, encompassing a wide range of approaches to embedding additional information into digital media. Traditional methods leverage transform domains [1], such as Discrete Cosine Transform (DCT) or wavelet transforms, to subtly modify carrier signals. At the same time, more recent approaches exploit machine learning and artificial intelligence to optimize embedding patterns and improve imperceptibility. Among these, code-controlled steganography has emerged as an auspicious direction. By using codewords to control the embedding process, these methods can achieve higher efficiency and robustness compared to many other techniques, even when operating directly in the spatial domain of the carrier. This capability allows for precise control over information hiding, making code-controlled methods a powerful tool in the modern steganography arsenal.

We provide a concise overview of recent advances in the aforementioned areas of steganography. Our focus will encompass traditional transformation-domain methods, machine learning- and Artificial Intelligence (AI) based techniques, as well as the emerging field of code-controlled steganography. By highlighting the strengths, limitations, and current trends in each approach, we intend to offer a clear perspective on the state-of-the-art, setting the stage for a deeper discussion on the optimization of code-controlled methods in terms of embedding efficiency and robustness.

A considerable body of recent research has focused on developing transform-domain steganographic methods that enhance the robustness and reliability of the perception of embedded data. Song et al. [2] proposed a robust JPEG steganographic scheme that combines the DCT and Singular Value Decomposition (SVD) within the nonsubsampled shearlet transform (NSST) domain, achieving improved resistance to compression and noise. Liu et al. [3] developed a method that integrates the wavelet-domain SVD with adaptive Quantization Index Modulation (QIM), effectively balancing embedding capacity and robustness for JPEG images. Subhedar [4] explored the use of the ridgelet transform together with SVD, demonstrating high imperceptibility in the spatial-frequency representation of images. Similarly, Singh and Singla [5] combined SVD and the Discrete Wavelet Transform (DWT) to create a multi-level embedding framework capable of preserving image quality while maintaining robustness against steganalysis detection. Collectively, these papers highlight the growing trend of hybrid transformation-based approaches that exploit both frequency-domain properties and matrix factorization techniques to enhance the overall performance of image steganography.

Recent advances in artificial intelligence have significantly influenced the development of next-generation steganographic systems. Chang and Echizen [6] introduced a pioneering concept of steganography beyond space and time using a chain of multimodal AI models capable of synchronizing semantic features across different media types, thereby redefining the boundaries of covert communication. Carol et al. [7] proposed an AI-powered adaptive steganography framework that dynamically selects embedding parameters based on content characteristics, improving both imperceptibility and adaptability to diverse media. Raja Rajeswari N. et al. [8] designed an AI-enhanced LSB steganography interface that leverages neural network feedback to optimize pixel-level embedding, leading to higher accuracy and security. In a comprehensive review, Wani and Sultan [9] analyzed deep learning-based image steganography methods, highlighting how convolutional and generative networks outperform traditional algorithms in balancing payload, reliability of perception, and resistance to

steganalysis. Collectively, these papers illustrate a paradigm shift toward intelligent, context-aware steganographic systems that integrate machine learning to autonomously optimize information hiding strategies.

The direction of code-controlled steganography represents a truly novel paradigm in the field of covert communication. Introduced by the authors, this concept enables embedding additional information directly in the spatial domain of the container, under code-controlled influence of selected carrier components, thereby combining the minimal computational complexity typical for spatial-domain schemes with the robustness advantages often found in transform-domain methods. In particular, the paper [10] demonstrates that by pre-coding the payload with specially designed codewords (for example, with specific Walsh-Hadamard transform characteristics), one can achieve impressive results both in terms of reliability of perception and resistance to attacks (for example, compression-attacks) with minimal embedding cost and low algorithmic overhead. Research [10] shows that carefully constructed classes of codewords localize the embedding disturbances in the targeted transform domain of the container and thus optimize the trade-off between capacity, reliability of perception, and robustness. The multi-level codewords extension [11] further enhances the method's resistance and throughput, making code-controlled steganography a compelling and practically efficient option in modern information-security systems. The most recent advancement in code-controlled steganography is the development of methods enabling blind decoding, where the embedded information can be reliably extracted without prior knowledge of the original container [12]. This approach significantly simplifies the decoding process while maintaining high imperceptibility and robustness against various attacks. By carefully designing the code structures and embedding strategies, these methods optimize the trade-off between computational efficiency, embedding capacity, and resistance to steganalysis, making blind code-controlled steganography an efficient and promising tool for modern secure information systems.

As demonstrated by the research results presented in this paper, the concept of code-controlled steganography not only enables the design of highly efficient embedding methods but also provides a framework for investigating the fundamental properties of steganographic embedding. This, in turn, allows for further refinement and optimization of practically applicable steganographic techniques. For instance, from coding theory, it is well known that the efficiency of error-correcting codes increases with the length of the code. However, there is a lack of publicly available data regarding the optimization of the block size used for embedding information in steganographic systems. In the present paper, we employ the concept of code control to explore this question and investigate which strategy is more effective: embedding multiple bits into a larger block or a single bit into a smaller one.

The *purpose* of this paper is to research the impact of codeword size on the robustness of steganographic messages against attacks on the embedded information, under otherwise equal conditions.

Specifically, the paper seeks to determine whether embedding multiple bits into larger blocks or single bits into smaller blocks provides superior robustness, thereby providing insights that can guide the development of more effective and practically applicable steganographic methods.

Code control concept. The code control concept represents a new paradigm in steganography that allows adaptive control of the embedding process based on the properties of the codewords used.

Let a digital image block X of size $N \times N$ 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

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix},\ H_1 = 1. \quad (2)$$

In addition to the two-dimensional Walsh-Hadamard Transform, its one-dimensional version is also commonly used for a vector Y

$$V = YH_N. \quad (3)$$

At the same time, in [10], a fundamental relationship was established between the two-dimensional and one-dimensional forms of the Walsh-Hadamard Transform, within which it was demonstrated that the two representations are mathematically equivalent and can be converted into each other through vectorization operations

$$\tilde{W} = \tilde{X}\, H_{N^2}, \quad (4)$$

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

$$\tilde{M} = \tilde{X} + \tilde{T}, \quad (5)$$

then

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

As follows from equation (6), the impact on the Walsh-Hadamard transform components of the container block is fully determined by the internal structure of the transform components of the selected codeword. Because each codeword interacts selectively with a specific transform component, this approach enables precise and localized embedding of additional information within the corresponding region of the transform domain.

In the framework of code-controlled embedding, there exists a fundamental flexibility in how codewords are employed within a container block. In the simplest scenario, a single codeword T can be used to represent one bit of additional information per block.

Formally, for a block X_k and a single bit $m_i \in \{-1, 1\}$, the embedding can be expressed as

$$M_k = X_k + m_i T, \quad (7)$$

where T is the codeword selected for the whole embedding process.

Alternatively, it is possible to embed multiple bits within a single block by using a set of codewords $\{T_0, T_1, ..., T_{2^L-1}\}$.

In this case, for a set of L bits $\boldsymbol{m} = \{m_0, m_1, ..., m_{\log L-1}\}$, the embedding is performed as

$$M_k = X_k + T_m. \quad (8)$$

where each codeword T_m selectively influences specific transform components of the block.

This formulation highlights the principled ability to control the number of embedded bits per block by choosing either a single codeword or a combination of multiple codewords, providing a flexible trade-off between embedding capacity and reliability of perception.

This paper addresses the fundamental question of which strategy is more effective under otherwise equal conditions: embedding a single bit into a smaller codeword (7), or embedding multiple bits into a larger codeword (8). By systematically analyzing these two approaches, the

research aims to provide practical guidance for optimizing code-controlled steganographic methods in terms of robustness, imperceptibility, and embedding efficiency.

Experimental Methodology. To ensure the correctness of the comparison between codewords of different lengths, the research is designed so that the experimental conditions remain as similar as possible for all variants. In particular, the embedding process is performed within the same frequency segment of the image representation, and the amplitude of the embedding signal is kept constant. In addition, the density of the additional information relative to the number of pixels in the container is maintained at the same level. This approach allows isolating the influence of the codeword length itself on the resulting resistance of the steganographic message to attacks against the embedded data.

In this research, we perform a comparative analysis of two embedding strategies. The first comparison considers embedding four bits into a single 8×8 codeword versus embedding one bit into a 4×4 codeword.

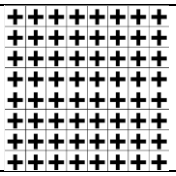
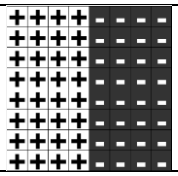
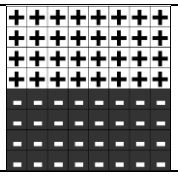
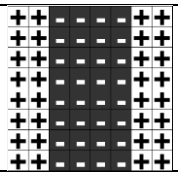
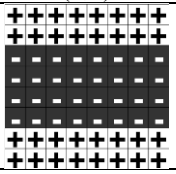
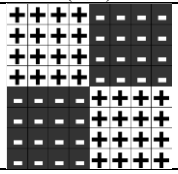
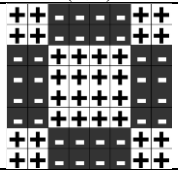
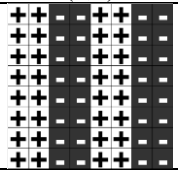
The second comparison evaluates the embedding of four bits in a 16×16 codeword against the embedding of one bit in an 8×8 codeword. These experiments are performed under identical embedding conditions, allowing a direct assessment of the impact of codeword size and the number of embedded bits on the robustness and perceptual quality of the steganographic message.

For the case of four bits embedded into 8×8 codewords, the codewords used are shown in Table 1. For brevity, only the non-inverted variants are presented, i.e., eight codewords, although the total number of such codewords is sixteen.

These codewords serve as the basis for the embedding process, selectively influencing specific low-frequency transform components within each container block. The code distance between these codewords is $d = 32$, ensuring sufficient separation to enhance robustness and reduce decoding errors.

Table 1.

Non-inverse codewords of size 8x8

			
(1,1)	(1,5)	(5,1)	(1,7)
			
(7,1)	(5,5)	(7,7)	(1,3)

In the experiment where a single bit of information is embedded into an 8×8 codeword from Table 1, the embedding specifically targets the (5,1) transform component.

In the experiments involving the embedding of information into 4×4 blocks, a single codeword was used for each block

$$T_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}. \quad (9)$$

In the experiment involving the embedding of four bits of additional information into 16×16 blocks, the codewords used are shown in Table 2. For brevity, only the non-inverted variants are presented, i.e., eight codewords, although the total number of such codewords is sixteen.

The code distance between these codewords is 128, providing significant separation to enhance robustness and reduce decoding errors. These codewords selectively influence specific

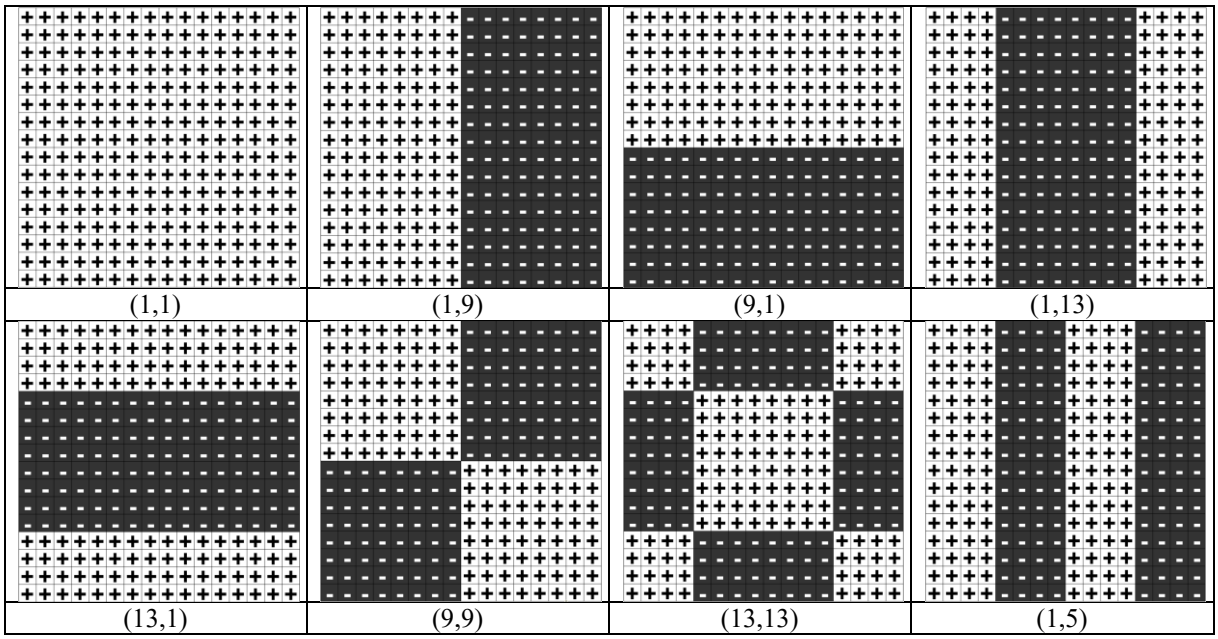
transform components within each block, ensuring controlled embedding while maintaining consistent amplitude and information density across all experiments.

For the experiments involving the embedding of a single bit of additional information into 8×8 blocks, the codeword from Table 2 was used. The embedding specifically targeted the (9,1) transform component of the codeword, ensuring controlled and localized modification of the container block.

It is worth noting that selecting an appropriate set of codewords for embedding additional information is an inherently complex task. The design and optimization of such codeword sets involve numerous considerations, including code distance, transformant selection, and robustness against steganalysis attacks, and therefore deserve dedicated and comprehensive research.

Table 2.

Non-inverse codewords of size 16x16



To evaluate the effectiveness of code-controlled embedding, a series of experiments was performed using digital images and different embedding strategies. The methodology can be summarized as follows:

1. Original color images were converted from the RGB to the YCbCr color space, and only the luminance component (Y) was used as the carrier. Images were cropped to a fixed size of 1200×1200 pixels to ensure uniformity across all experiments.
2. Random binary sequences were generated to represent the additional information to be embedded. For experiments with multi-bit embedding, each block contained 4 bits of information. Each 4-bit group was then mapped to a unique codeword from a predefined set, corresponding to the code-controlled embedding concept.
3. Two independent experimental comparisons were performed:
   - Experiment 1: embedding 1 bit per block in 4×4 codewords versus 4 bits per block in 8×8 codewords.
   - Experiment 2: embedding 1 bit per block in 8×8 codewords versus 4 bits per block in 16×16 codewords.

   In both cases, the overall embedding density (bits per pixel) and the embedding amplitude were kept constant to enable fair comparison.
4. For multibit 8×8 and 16×16 embedding, predefined sets of 16 codewords (8 original and 8 inverted) were employed. The Hamming distance between codewords was 32 and 128, respectively, ensuring high robustness and low decoding error probability. Each

codeword selectively influenced specific Walsh-Hadamard Transform components, allowing localized and controlled embedding.

5. Image blocks were sequentially modified according to the selected codeword and corresponding message bits. The modified luminance component was then recombined with chrominance channels, and the resulting steganographic image was saved in JPEG format with a predefined quality factor (QF).
6. For extraction, the difference between the steganographic and original blocks was computed. Correlations between this difference and all codewords were evaluated to determine the most likely embedded codeword, and the corresponding message bits were recovered. The error rate was calculated as the proportion of incorrectly recovered bits relative to the total number of embedded bits. The bit error rate was calculated as the ratio of incorrectly recovered bits to the total number of embedded bits.

Results of experiments. The results of all performed experiments are summarized in Table 3. This table presents a comprehensive comparison of various embedding strategies, including the use of different codeword sizes and the number of embedded bits per block. The metrics reported allow evaluation of the impact of codeword size and bit quantity on the robustness against compression attack.

Table 3.

Experimental results

Code-word size	Bits per block	Bit per pixel	PSNR, dB	QF									
				10	20	30	40	50	60	70	80	90	100
4x4	1	1/16	48.13	47.8	43.9	38.8	32.7	26.5	20.5	13.5	7.4	1.3	0
8x8	4	1/16	48.13	48.5	44.7	37.7	29.5	21.5	14.7	7.9	2.5	0.7	0.3
8x8	1	1/64	48.13	41.5	29.3	14.9	5.9	3.1	2	0.8	0.3	0	0
16x16	4	1/64	48.13	45.2	34.6	19.2	6.8	2.3	1.4	1	0.5	0.4	0.2

To further assess the robustness of the proposed embedding approach, we constructed Fig. 1, which represents a dependency graph of the percent of extraction errors on the JPEG compression quality factor (QF). This analysis was performed to compare two embedding strategies:

1. embedding one bit of additional information into 4×4 blocks, and
2. embedding four bits of additional information into 8×8 blocks.

Such a comparison enables the determination of which strategy provides a better balance between payload capacity and resistance to compression-induced distortions under otherwise identical embedding conditions.

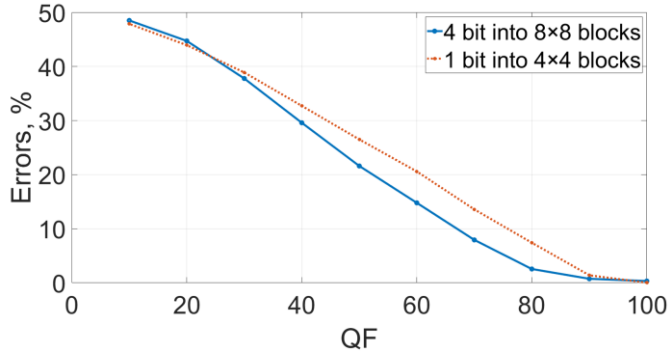


Fig. 1. A dependency graph of the percent of extraction errors on the JPEG compression quality factor (QF) for the case of embedding 1 bit in 4x4 blocks vs 4 bits in 8x8 blocks

A comparative analysis of the embedding results demonstrates a significant improvement in robustness when moving from 4×4 codewords with a single bit per block to 8×8 codewords with four bits per block at the same embedding rate (1/16 bit per pixel). As shown in Fig. 1, increasing the codeword size and the number of embedded bits substantially

reduces the error rate across all JPEG quality factors (QF). The improvement is especially pronounced at QF = 70, which is widely used in practice: the error rate for 8×8 codewords with 4 bits per block is 5.6% lower than that for 4×4 codewords with a single bit. Notably, this increase in robustness is achieved without any degradation of image quality, with PSNR values remaining 48.13 dB.

In this part of the paper, another scenario is examined, as the graph in Fig. 2 illustrates the relationship between the percentage of extraction errors and the JPEG compression quality factor (QF). The experiment compares two embedding strategies:

1. embedding one bit of additional information into 8×8 blocks, and
2. embedding four bits of additional information into 16×16 blocks.

This comparison is intended to evaluate whether increasing the codeword size further enhances the robustness of the embedded data when the embedding rate and all other conditions remain constant, or whether the improvement tends to saturate beyond a certain block size.

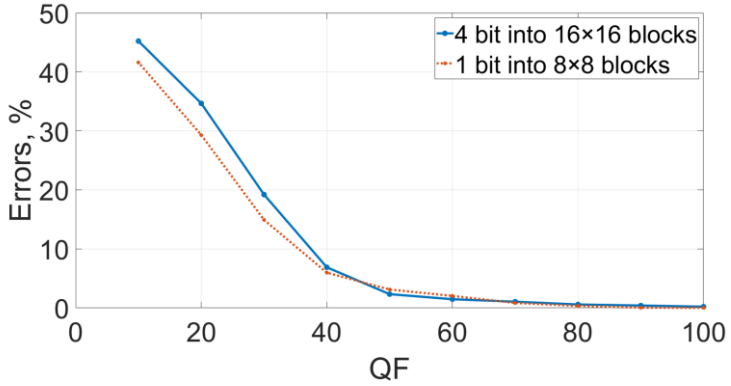


Fig. 2. A dependency graph of the percent of extraction errors on the JPEG compression quality factor (QF) for the case of embedding 1 bit in 8x8 blocks vs 4 bits in 16x16 blocks

A more detailed examination of the results reveals that a straightforward increase in codeword size does not necessarily lead to improved robustness. As shown in Fig. 2, when transitioning from 8×8 blocks with one bit per block to 16×16 blocks with four bits per block, the number of extraction errors decreases only slightly for intermediate JPEG compression levels (QF = 50 and 60). For all other compression levels, however, robustness either remains nearly the same or even decreases despite the larger block size.

This phenomenon can be explained by considering the interaction between block size and embedding capacity. While larger blocks allow embedding more bits per block, they also aggregate more image information, making each embedded bit more sensitive to compression-induced distortions. In other words, the benefits of increasing the codeword size saturate because the relative impact of JPEG quantization on each embedded bit becomes more pronounced as the block grows. Consequently, beyond a certain block size, further enlargement does not yield additional robustness and may even slightly degrade performance for higher compression levels.

Conclusions. The performed research confirms the efficiency of the code-controlled embedding concept as a promising paradigm in modern digital steganography. The approach provides flexible control of the embedding process through specially designed codewords, ensuring a precise balance between reliability of perception, robustness, and computational simplicity. Experimental analysis demonstrates that, under equal embedding density, increasing the codeword size and embedding multiple bits per block significantly improves robustness against compression attacks (especially for JPEG with QF ≈ 70), while maintaining high reliability of perception (PSNR ≈ 48 dB).

The obtained results reveal a saturation effect: beyond a certain block size, further growth of the codeword does not yield additional robustness gains and may even reduce performance at high compression levels. This phenomenon is caused by the cumulative influence of quantization noise on large transform blocks. Comparative evaluation of the tested

strategies indicates that the optimal configuration corresponds to embedding several bits per medium-sized block (e.g., 8×8), which offers the best trade-off between payload, resistance to distortion, and decoding accuracy.

The findings provide a theoretical and practical basis for optimizing block sizes and codeword structures in code-controlled steganography, enabling the development of efficient and adaptive algorithms for secure information hiding in modern cybersecurity systems.

References

1. Abdulla A. A. Digital image steganography: challenges, investigation, and recommendation for the future direction. *Soft Computing.* 2024. Vol. 2. No. 15. P. 8963-8976. DOI: 10.1007/s00500-023-09130-8
2. Song X. et al. Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain. *Multimedia Tools and Applications.* 2022. Vol. 81. No. 25. P. 36453-36472. DOI: 10.1007/s11042-022-13525-4
3. Liu J. et al. Robust jpeg image steganography using wavelet domain SVD and adaptive QIM. *8th International Conference on Signal and Image Processing (ICSIP). IEEE*, 2023. P. 434-438. DOI: 10.1109/icsip57908.2023.10270839
4. Subhedar M. Image steganography using ridgelet transform and SVD. *International e-Conference on Intelligent Systems and Signal Processing: e-ISSP. Singapore.* 2021. P. 81-91. DOI: 10.1007/978-981-16-2123-9_6
5. Singh J., Singla M. Image steganography technique based on singular value decomposition and discrete wavelet transform. *International Journal of Electrical and Electronics Research.* 2022. Vol. 10, No. 2. P. 122-125. DOI: 10.37391/ijeer.100212
6. Chang C. C., Echizen I. Steganography beyond space-time with chain of multimodal *AI. Scientific Reports.* 2025. Vol. 15. No. 1. P. 12908. DOI: 10.1038/s41598-025-97238-2
7. Carol I. K. S., Kumar D. K., Ragavan V. A. N. AI-Powered Adaptive Steganography. Smart System for Integrated Computing and Communication: First International Conference, ICSSICC 2024, Coimbatore, India, November 15–16, 2024, Proceedings. Springer Nature, 2025. P. 328.
8. Raja Rajeswari N. et al. AI-enhanced LSB steganography interface: concealed data embedding framework. *9th International Conference on Smart Structures and Systems (ICSSS). IEEE*. 2023. P. 1-4. DOI: 10.1109/icsss58085.2023.10407062
9. Wani M. A., Sultan B. Deep learning based image steganography: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery.* 2023. Vol. 13, No. 3. P. e1481. doi: 10.1002/widm.1481
10. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale*. 2021. No. 4 (52). P. 115-130. DOI: 10.52254/1857-0070.2021.4-52.11
11. 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. DOI: 10.3103/s0735272723040052
12. Sokolov A.V., Ihnatenko O.O., Balandina N.M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problems of regional energetics.* 2024. Vol. 62. No. 2. P. 121-137. DOI: 10.52254/1857-0070.2024.2-62.11

ВПЛИВ РОЗМІРУ КОДОВОГО СЛОВА НА СТІЙКІСТЬ СТЕГАНОГРАФІЧНИХ МЕТОДІВ З КОДОВИМ УПРАВЛІННЯМ

Соколов А.В.[1], Погорєльцев П.М.[2], Жук Є.А.[3], Філіпенко Н.О.[2]

[1]Національний університет «Одеська юридична академія»
23, Фонтанська дорога, Одеса, 65009, Україна
[2]Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[3]Харківський національний університет радіоелектроніки
14, Науки пр., Харків, 61166, Україна
Email: radiosquid@gmail.com[1]

Стаття присвячена новому напрямку в цифровій стеганографії – концепції вбудовування інформації з кодовим управлінням, яка дозволяє адаптивно керувати процесом вбудовування на основі властивостей спеціально розроблених кодових слів. На відміну від традиційних методів, що працюють у просторовій області, або в областях перетворень, концепція кодового управління дозволяє точно локалізувати ефекти вбудовування в частотній області, зберігаючи при цьому мінімальну обчислювальну складність. Мета дослідження – визначити, як розмір кодового слова впливає на стійкість стеганографічного повідомлення при інших однакових умовах. Для досягнення цієї мети було проведено серію контрольованих експериментів з використанням цифрових зображень, що піддавалися стисненню JPEG з різними коефіцієнтами якості. Було порівняно дві стратегії вбудовування: вбудовування одного біта в менший блок та вбудовування кількох бітів у більший блок з тією ж пропускною спроможністю. Результати показують, що збільшення розміру кодового слова та вбудовування кількох бітів у блок може значно покращити стійкість без погіршення надійності сприйняття, що підтверджується стабільними значеннями PSNR. Однак, експерименти також показують, що переваги збільшення розміру кодового слова мають тенденцію до насичення після досягнення певного порогу, оскільки більші блоки стають більш схильними до спотворень, викликаних стисненням. Дослідження дає нове розуміння балансу між стійкістю, надійністю сприйняття та ефективністю вбудовування в стеганографії з кодовим управлінням. Результати сприяють оптимізації розмірів блоків та стратегій вбудовування, пропонуючи практичні рекомендації для розробки стеганографічних систем наступного покоління. Отримані результати не тільки підвищують стійкість прихованих даних, але й закладають основу для створення адаптивних, інтелектуальних та обчислювально ефективних алгоритмів приховування інформації, які можна інтегрувати в сучасні інфраструктури кібербезпеки.

Ключові слова: цифрова стеганографія, вбудовування з кодовим управлінням, перетворення Уолша-Адамара, стійкість, надійність сприйняття, приховування інформації, блокова оптимізація, стиснення JPEG, кібербезпека.

DOI 10.15276/imms.v16.no1.26
UDC 004.621

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 26-33

COMPUTER-AID DESIGN TECHNOLOGIES IN HYBRID MODELING BASED ON INFORMATION MODELING IN AUTODESK FUSION

V.M. Tigariev, O.S. Lopakov, V.V. Kosmachevskiy

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

Currently, much attention is paid to the tasks of increasing the speed and quality of product design in modern CAD. The process of creating objects of complex shape requires solving a variety of tasks. Various modeling methods are used to implement them. The paper proposes using Autodesk Fusion to solve design tasks based on hybrid modeling. To implement these tasks, an information model of hybrid product modeling in Fusion is proposed. Hybrid modeling allows using top-down design technology. This type of design speeds up the development of products, especially with complex shapes. To optimize the shape, it is possible to use cloud technologies and artificial intelligence elements. All stages of the proposed model are sequentially considered. Using the information model of hybrid modeling allows you to analyze the creation of all product elements. Fusion simplifies design using parametric modeling, which provides quick setup, seamless iteration, and automated updates at the design and production stages — all within a single cloud platform. If necessary, we simulate the load on the model elements and optimize the possible choice of materials. To view the finished product, we perform rendering, which allows us to polish visual effects in order to present our design qualitatively or obtain client approval. When working in the cloud environment of the designer in Autodesk Fusion, the following tasks are performed using artificial intelligence: calculation of model elements, load testing, shape optimization, rendering and product viewing, drawing design, preparation of control programs for technological processes of manufacturing parts using various technologies, for example, additive. The paper provides an example of hybrid modeling of a game manipulator when designing in Fusion using the proposed information model. The use of all steps of the information model is shown in detail. The features of surface and solid modeling when creating an object of complex shape are presented. The developed information model can be adapted for various types of modeling when designing in Fusion.
Keywords: information model, hybrid modeling, surface model, solid model, design, Autodesk Fusion.

Introduction. Computer 3D modeling is a rapidly growing field of technology. Various modeling methods are constantly evolving and improving. Computer modeling significantly reduces the time required for the design process, providing incomparably greater opportunities. Hybrid modeling methods provide new opportunities for computer design technologies, and the development of information technologies gives them new meaning.

There are various types of modeling: solid, surface, frame, hybrid, and hybrid modeling. Each operation has its advantages and limitations, so it is wise to choose the best characteristics from each and use all methods simultaneously. This is the main assumption of hybrid modeling. The main obstacle may be a clear boundary between different types of modeling and the use of completely different commands/modules each time. But this is not a problem if we perform a single operation to trim a solid using a surface. True hybrid modeling significantly changes the concept of modeling and the very approach to computer-aided design, as well as increases work efficiency. With hybrid modeling, logical operations work with both types of geometry—solid and surface—which opens up new possibilities and imagination during the design process. For complex processes, it is not easy to change the shape by modifying the surface alone. Furthermore, simple hybrid modeling in most systems works with only one logical operation of the Boolean system, or the design environments are clearly divided into those specializing in solids and those specializing in surfaces. In fully hybrid modeling software, most operations

work for both solids and surfaces—there is no difference, so it is simply the same command. Hybrid modeling technology removes the barriers between modeling methods that limited many advanced features to professional design only. Hybrid modeling allows designers to save time-consuming repair work and focus on more creative tasks.

Hybrid modeling is not just a software feature. It is the core programming technology for all types of CAD. With this technology, designers do not need to consider whether they are working with solid or non-solid bodies, thereby simplifying the entire manufacturing process. Hybrid modeling in Fusion involves combining different modeling methods, primarily parametric solid modeling and direct or freeform surface modeling, to create complex designs more efficiently. This approach leverages the strengths of each method, such as the history and precision of parametric modeling for elements such as ribs and bosses, and the flexibility of free-form tools for organic shapes. The goal is to use the right tool for the right part of the design, integrating solid and surface modeling to maximize workflow and design exploration.

Product designers and engineers use several modeling methods: bottom-up modeling, top-down modeling, horizontal or middle modeling, and hybrid approaches that combine these methods. Several approaches to top-down modeling include multi-part modeling, parameter binding, and skeleton modeling, in which a “skeleton” sketch conveys the design intent, and designers model individual components around this common final assembly—potentially in a single CAD file. The top-down modeling method is particularly well suited for complex products such as automobiles and other vehicles, electronics, appliances, and machinery.

CAD software that supports top-down modeling reduces the risk of errors such as part mismatches, which can result from the traditional bottom-up approach. Autodesk Fusion uses a single design model that easily allows global parameter changes that update the entire project. To optimize the hybrid modeling process, it is necessary to develop an information model of this technology.

Analysis of recent studies and publications. Key aspects of hybrid modeling in Fusion. You can use parametric tools for fundamental parts of the design, such as the main body, and then switch to free-form tools (T-spline) for organic or complex surfaces [1-3].

Integration of solids and surfaces. The basic concept is to integrate both solid and surface modeling methods, for example, creating a complex surface model and then using a solid modeling command such as “shell” to cut it out for rapid prototyping [4].

Hybrid modeling is also crucial for hybrid manufacturing, where designs must consider both additive and subtractive processes. Fusion tools allow engineers to explore materials, dimensions, and design implications for both manufacturing methods in a single environment, as illustrated by examples of hybrid modeling in various fields such as dentistry, aerodynamics, and prosthetics [5,6]. Hybrid modeling allows you to create a more reliable and efficient workflow by switching between different modes as needed. For example, creating a complex, organic handle using free-form tools and then adding standard solid elements. Papers [7-11] explain how different types of modeling can be used when creating mechanical devices.

Paper [12] provides an overview and prospects for the use of hybrid modeling technologies. Works [13-16] explain the use of information models to optimize the design processes of various devices and technologies. Information models are used to structure data and ensure consistency, which improves data quality, facilitates interaction between systems, and simplifies the organization and search for information.

Purpose of the work. Currently, new objects in various fields are created using computer-aided design technologies that utilize cloud technologies. When creating an algorithm for designing new objects using computer technologies, it is important to use an information model. An information model generalizes the approach to design using various technologies.

Let's take a closer look at the information model of hybrid product modeling in Autodesk Fusion CAD (Fig. 1).

When creating and analyzing a product model, several sequential and interrelated steps must be performed. The proposed information model consists of two main components: surface modeling and solid modeling.

Let's consider the components of the proposed information model for hybrid design using Autodesk Fusion. The sequence of stages in the information model of hybrid design in Fusion corresponds to top-down design technology. In top-down modeling, designers and engineers start with a model that conveys the design concept for the entire assembly and defines the general relationships between the elements in the assembly.

The following steps are involved in surface modeling.

1. At the beginning of the work, we have the initial data for the future product model, for example, in the form of a cloud of boundary points of the conceptual model. We upload them to the Autodesk Fusion environment.
2. Formation of sketches of surface model elements. At this stage, 2D and 3D sketches of the boundary elements of the future conceptual model are formed.
3. The next stage is the formation of conceptual model elements using surface modeling, which includes various options for creating surfaces.
   a. Creating model elements using simple surface creation commands.
   b. Creating model elements using spline curves of surface frames.
   c. Creating a model using standard surface models

The type of model element creation is selected depending on the technology of further modeling.

4. Based on the selected modeling technology, a conceptual surface model is created and modified. This can be a modification of individual boundary surfaces or a single surface based on sketches or a standard surface model.

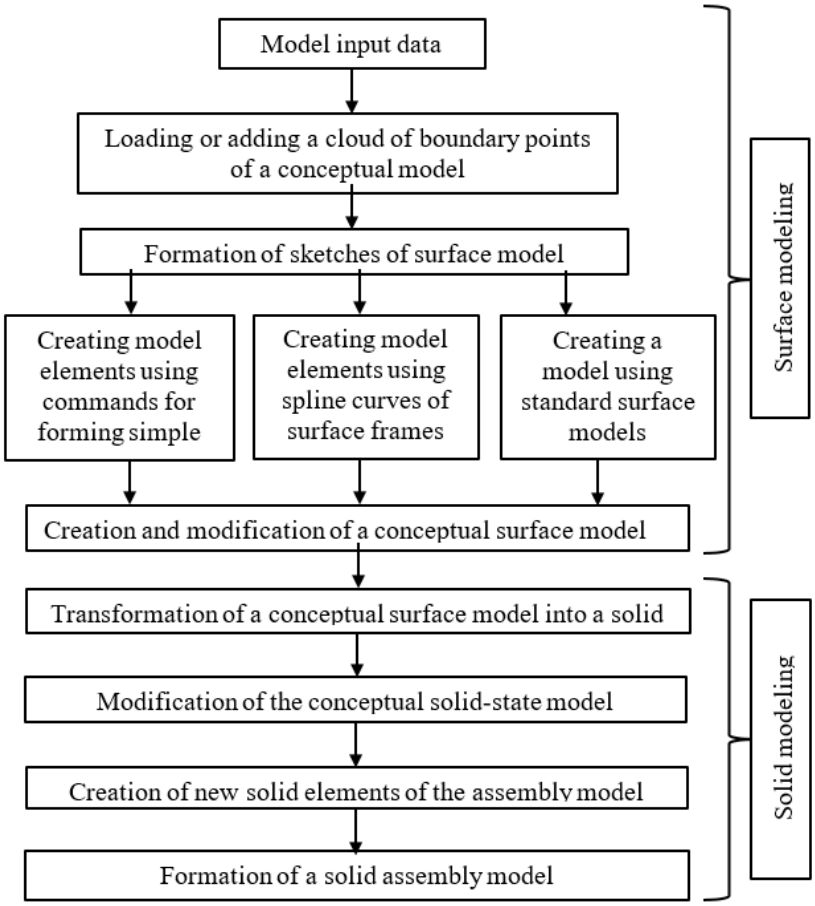


Fig. 1. Information model of hybrid design in Fusion

This completes the surface creation component of the conceptual model. After that, we move on to the solid parametric modeling component of the assembly model of the object.

1. Converting a conceptual surface model into a solid model. A surface model has no thickness. To convert such a model, you need to specify the thickness in the modeling parameters.
2. The next step is to modify the conceptual solid model. This can be done by dividing the model into separate elements or changing its shape. At this stage, we complete the formation of the structural elements of the assembly model of the product.
3. Creating new solid elements of the assembly model. Using solid modeling, we create additional assembly elements.
4. The final stage is the formation of a solid assembly model.

Fusion simplifies the design of an assembly model of an object using parametric modeling, which provides quick configuration, smooth iteration, and automated updates during the design and manufacturing stages—all within a single cloud platform.

Main section. Using the proposed information model, a hybrid model of a game manipulator was created.

At the initial level, we will create a conceptual surface model of the manipulator's body. We load the boundary points of the model. Based on these points, we form 2D and 3D sketches of the boundary elements of the conceptual model (Fig. 2).

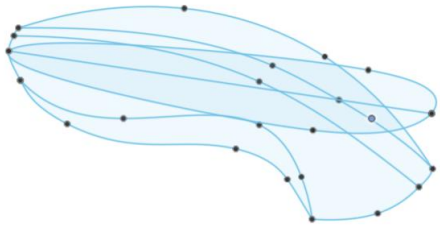


Fig. 2. 2D and 3D sketches of boundary elements of the conceptual model

Using the created sketches, it is possible to form a surface model in three ways.

The first is to create model elements using commands for forming simple surfaces, as shown in Fig. 3. This approach requires complex editing for objects with non-linear shapes.

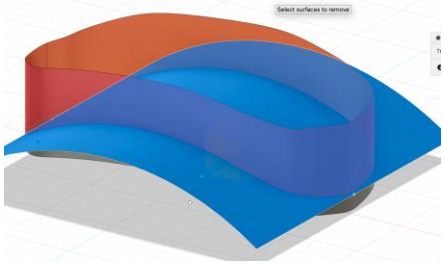


Fig. 3. Creating model elements using commands for forming simple surfaces

The second is to create a model using standard surface models as a base template (Fig. 4). This option can be used for objects with simple shapes.

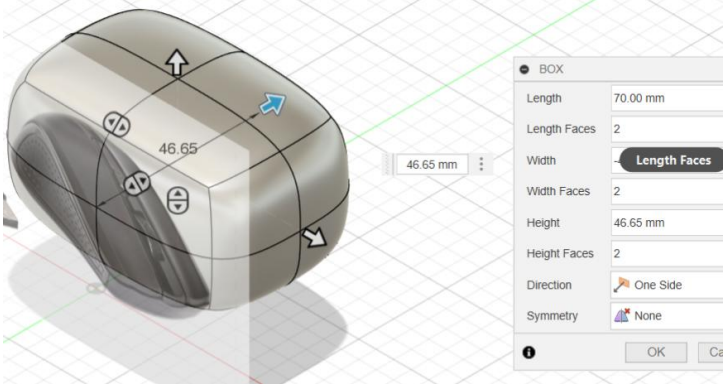


Fig. 4. Creating a model using standard surface models

The third is the creation of model elements using spline curves of surface frames. This technology allows for more optimal formation of complex surface models.
Let's take a closer look at hybrid modeling technology using spline curves.
Select the Sweep command to create a three-dimensional shape based on the sketches you have created. Select the necessary profiles to form the initial part of the manipulator. It is important to check that the profiles are correctly aligned and match the contour of the future model.

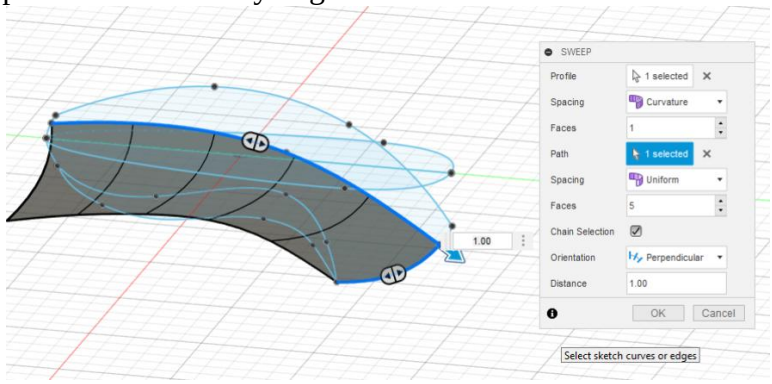


Fig. 5. Creating model elements using spline curves of surface frames

After editing and using the necessary intermediate sketches, we obtain an open conceptual surface (Fig. 6).

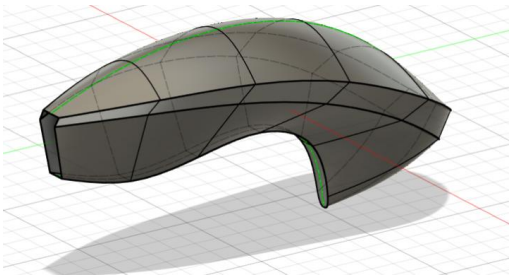


Fig. 6. Open conceptual surface

Adjust the position of the lower part of the surface using the Match command to align it with the specified profile. Combine the holes using the Bridge command to obtain a complete closed conceptual surface of the manipulator (Fig. 7). Use the Shell command to convert the shell into a solid object. Create a new sketch to divide the solid object into two parts. Use the Split Body command to cut the body into two parts (Fig. 8). Solid models of the manipulator body and cover have been created.

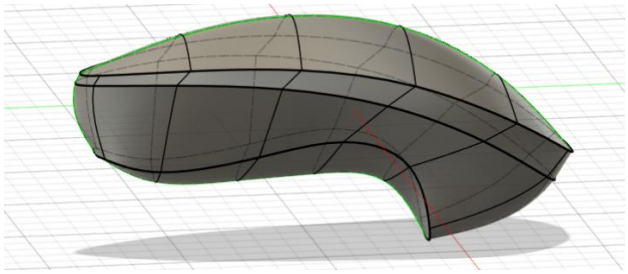


Fig. 7. Closed conceptual surface of the manipulator

Fig. 8. Cross-section of the model into 2 parts

We disable the visibility of the cover, and we will get only the body part on the screen. Fig. 9.

Fig. 9. Solid model of the manipulator body

Create a new solid component – a button. Using the created model of the new element, use the Split Body command to make a hole for the button (Fig. 10). Repeat these steps to create side buttons on the body and a joystick on the manipulator cover. We will get the finished model of the game manipulator (Fig. 11).

Fig. 10. Solid-state component button and button hole

If necessary, we apply materials to individual parts of the manipulator and visualize the created model (Fig. 12).

Fig. 11. Game controller model

Fig. 12. Visualization of the manipulator model

The model of the game manipulator created using computer-aided design technology in hybrid modeling mode was implemented in accordance with the proposed information model.

Conclusions. Designing objects based on hybrid modeling allows the use of top-down technology. This speeds up the design process. An information model has been proposed to optimize hybrid modeling. This model explains the relationship between the stages of surface and solid modeling. Possible options for surface modeling in modern CAD systems are

considered. The paper shows the implementation of hybrid modeling in the development of a game manipulator in Autodesk Fusion using an information model of design. The scientific novelty of the result lies in the fact that for the first time a hybrid modeling technology based on an information model of design is proposed. All stages of manipulator design based on the proposed information model in Fusion were considered. The practical significance of the results obtained lies in the fact that the use of the proposed information model will increase the speed, accuracy, and quality of design based on hybrid modeling. Prospects for further research lie in determining the conditions for interaction with other CAD programs. When designing complex shapes, optimal processes for their creation can be found.

References

1. Solid-Surface Hybrid Modeling: Future Trends of 3D CAD Modeling /ZW3D CAD/CAM. 2020. 11p. URL: https://zwcad.hu/wp-content/uploads/2020/07/33_ZW3D_White_Paper-Solid-Surface_Hybrid_Modeling.pdf
2. Wypysiński R. Hybrid modeling in CAD. *Advanced Technologies in Mechanics*. 2021.V. 2. No 1(2). P. 15–22. DOI: 10.17814/atim.2021.1(2).14
3. Świaczny. G, Wyleżoł M. Improving the topology of CAD models in the context of their susceptibility to design changes – model preparation stage. Part 1. *Mechanik.* 2020. No 8–9.DOI: https://doi.org/10.17814/mechanik.2020.8-9.16
4. Mroczkowski D., Wyleżoł M. Optimization of the shape of the heat shield in terms of natural frequency. *Mechanik*. 2022. No. 8–9. DOI: https://doi.org/10.17814/ mechanik.2022.8-9.15
5. ElGhawi R., Kraft B., Reimers Ch., Reichstein M., Korner M. Winkler1 Hybrid Modeling of Evapotranspiration: Inferring Stomatal and Aerodynamic Resistances Using Combined Physics-Based and Machine Learning. 2023. 35p. DOI: 10.1088/1748-9326/acbbe0
6. Wyleżoł M. Hybrid Modeling Methods of Cranial Implants. *Advances in Science and Technology Research Journal.* 2022. V. 12. No. 4. P. 35–47 https://doi.org/10.12913/ 22998624/99039
7. Ureta F. G., Tymms Ch., ZorinInteractive D. Modeling of Mechanical Objects. *Eurographics Symposium on Geometry Processing.* 2023. V. 35. No. 5. https://cims.nyu.edu/gcl/papers/gilureta2023imm.pdf
8. Leeuwen J. P., Wagter H., Oxman R.M. Information Modelling for Design Support a Feature-based approach. *Building Information Technology Proceedings of the 3rd Conference on Design and Decision Support Systems in Architecture and Urban Planning, Spa, Belgium*. 2020. P. 304-325.
9. Rudolph M., Kurz S., Rakitsch B. Hybrid Modeling Design Patterns. URL: https://doi.org/10.48550/arXiv.2401.00033
10. Веселовська Н. Р., Іскович-Лотоцький Р.Д. Використання гібридного моделювання при розробці гідроімпульсного привода віброударного пристрою. URL: http://ir.stu.cn.ua/handle/123456789/24965
11. Jun L., Dongyun W., Xiaobing X., Hualin R. Study on hybrid modeling of hydraulic excavator. *Mechanical and Control Engineering.* DOI: http://doi.org/10.26480/ wsmce.01.20723.30.33
12. Schweidtmann A.M., Zhang D., Stosch M. A review and perspective on hybrid modeling methodologies. *Digital Chemical Engineering*. DOI: 10.1016/j.dche.2023.100136
13. Lopakov O., Tigariev V., Tonkonogyi V., Kosmachevskiy V. Shape Optimization of an Object Using the Information Model. *Lecture Notes in Mechanical Engineering*. 2022. P. 88–97. DOI:10.1007/978-3-030-91327-4_9
14. Tigariev V., Lopakov O., Rybak O., Kosmachevskiy V., Cioată V. G. Design in modern information systems by applying cloud technologies. *Journal of Engineering Sciences*. 2023. V. 10(1). P. E8-E13, DOI: 10.21272/jes.2023.10(1).e2
15. Wagner G.: Information and Process Modeling for Simulation. *Journal of Simulation Engineering.* 2021. V.1(1). P. 1–25.

16. Tigariev V. M., Lopakov O. S., Koliada A. S., Kosmachevskiy V. V. Development of computerized technology for creating individual respiratory protection equipment using 3d modeling and cad. *Informatics and mathematical methods in simulation*. 2024. No. 4 V. 14, P. 296-304. DOI: 10.15276/imms.v14.no4.296.

ТЕХНОЛОГІЇ КОМП'ЮТЕРНОГО ПРОЄКТУВАННЯ В ГІБРИДНОМУ МОДЕЛЮВАННІ НА ОСНОВІ ІНФОРМАЦІЙНОЇ МОДЕЛІ У AUTODESK FUSION

В.М. Тігарєв, О.С. Лопаков, В.В. Космачевський

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

На даний час велика увага приділяється задачам підвищення швидкості та якості проєктування виробів у сучасних САПР. Процес створення об'єктів складної форми потребує вирішення різноманітних завдань. Для їх реалізації використовуються різноманітні методи моделювання. В роботі пропонується використовувати Autodesk Fusion для вирішення завдань проєктування на основі гібридного моделювання. Для реалізації цих завдань запропоновано інформаційна модель гібридного моделювання виробів у Fusion. Гібридне моделювання дозволяє використовувати технологію проєктування зверху вниз. Такий тип проєктування пришвидшує розробку виробів особливо зі складними формами. Для оптимізації форми можливо використання хмарних технології та елементів штучного інтелекту. Послідовно розглядаються всі етапи запропонованої моделі. Використання інформаційна модель гібридного моделювання дозволяє провести аналіз створення всіх елементів виробу. Fusion спрощує проєктування за допомогою параметричного моделювання, яке забезпечує швидке налаштування, безперебійну ітерацію та автоматизовані оновлення на етапах проєктування та виробництва — і все це в рамках єдиної хмарної платформи. При необхідності проводимо симуляцію навантаження на елементи моделі и виконуємо оптимізацію можливого вибору матеріалів. Для перегляду готового виробу проводимо рендеринг який дозволяє відшліфувати візуальні ефекти, щоб якісно представити свій дизайн або отримати схвалення клієнта. При роботі у хмарному середовище дизайнера в Autodesk Fusion виконуються наступні завдання з використанням штучного інтелекту: розрахунок елементів моделі, тестування навантажень, оптимізацію форми, рендеринг та перегляд виробу, оформлення креслеників, підготовку керуючих програм для технологічних процесів виготовлення деталей за різними технологіями, наприклад адитивні. У роботі наведено приклад гібридного моделювання ігрового маніпулятора при проектуванні у Fusion з використанням запропонованої інформаційної моделі. Деталізовано показано використання всіх кроків інформаційної моделі. Наведено особливості поверхневого та твердотільного моделювання при створенні об'єкту складної форми. Розроблена інформаційна модель може буте адаптована для різноманітних типів моделювання при проєктуванні у Fusion.

Ключові слова: інформаційна модель, гібридне моделювання, поверхнева модель, твердотільна модель, проєктування, Autodesk Fusion.

DOI 10.15276/imms.v16.no1.34
UDC 004.78

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 34-42

CONTEXT OBTAINING METHOD IN SUSTAINABLE WORKPLACES

M.I. Yakubovych, V.Y. Lyashkevych

Ivan Franko National University of Lviv
50, Drahomanova str., Lviv, 79005, Ukraine
Emails: maksym.yakubovych@lnu.edu.ua, vasyl.liashkevych@lnu.edu.ua

The modern workplace is rapidly transforming into a complex cyber-physical environment that combines people, technology systems, surroundings, production processes and knowledge. This multidimensionality claims to continuously obtain contextual information, including dynamic information about the status of space, equipment, people and processes, which determines the possibilities for adaptability, security and sustainable management. The paper identifies the role of context as a basic element of adaptive management, reveals the interdisciplinary nature of contextual data, and shows how its correct acquisition affects safety, energy efficiency, productivity and employee well-being. The research methodology includes an analysis of the literature and modern technological solutions, a systematization of context types, the construction of a comparative table of the advantages and disadvantages of existing methods, as well as the use of semantic, expert and simulation validation for a preliminary accelerated assessment. The main results show that each singular method has significant limitations: computer vision (CV) suffers from occlusions, wearable sensors from user unacceptability, digital twins (DTs) from modelling complexity and knowledge graphs (KGs) suffer from high requirements for ontology engineering. The proposed method, based on the hybrid approach, demonstrates the highest accuracy of context obtaining, robustness to data gaps and transparency of solutions based on explained models and semantic integration. The findings show that a combination of physical, semantic and behavioral sources of information provides the most complete picture of the workspace environment states. The proposed context obtaining method integrates heterogeneous data and increases the level of intelligence of workspace management systems. The work contributes to the development of scientific thought in the field of resilience, cyber-physical systems and intelligent monitoring, and also lays the foundation for building adaptive, human-centric decision support systems and automatic microclimate control systems, increasing production incidents and optimizing personnel workload in real workspaces.

Keywords: sustainable workplace, context obtaining, digital twin, knowledge graphs, machine learning, explainable artificial intelligence, computer vision.

Introduction. Today, human productivity has become a multifactorial system, and the modern work environment is determined not only by physiology but also by many other factors. Among such factors, one can list: cognitive load, emotional state, quality of interaction with information systems, nature of tasks performed, etc. It used to be believed that if an employee had warmth, light, and fresh air, they would automatically perform better, but today we know that this is not the case. Even ideal physical comfort does not compensate for excessive information noise, constant notifications, task inconsistency, digital fatigue, etc. It is obvious that physical parameters are no longer the main limiting factor of productivity and, accordingly, the criterion for evaluating the workplace and environment.

Only such a multifactor model can assess why productivity is falling or rising, and what really needs to be changed - intelligent monitoring that analyzes: physical parameters, behavioral patterns, digital patterns, social context, etc. Context in such environments is formed at the intersection of data about people, the environment, equipment, production processes, and regulatory requirements, which determines the critical need for methods for its accurate, timely, and explainable obtaining. Given the rapid digitalization of production, the growing role of IoT, DTs, and intelligent security systems, the formation of a reliable context is becoming the basis for effective and sustainable management.

Literature review. The concept of a sustainable, human-centric workspace is becoming increasingly relevant due to the growing ability of information systems to sense, interpret, and predict context in real time. Recent research on the persistence of cognitive and context-sensitive decision-making systems emphasizes that context is no longer a static attribute of the environment, but a dynamic, multidimensional signal that must be continuously acquired, integrated, and interpreted to maintain persistent intelligent environments [1]. The systemic overview of Industry 4.0 and intelligent product and service systems also highlights contextual awareness as a key capability of the cyber-physical manufacturing and service ecosystem, and emphasizes the need for robust architecture, interoperability, and semantic modeling [2-3].

Broadly speaking, within this broader area, methods for obtaining contextual information in the workplace can be summarized into several main research areas:

- environmental monitoring based on IoT sensors;
- workplace surveillance based on CV;
- wearable devices and methods for measuring human activity;
- cyber-physical modeling based on DTs;
- contextual modeling based on semantics and KGs.

Each approach has its own unique advantages and limitations when applied to sustainable workspaces (SWs) that must simultaneously ensure safety, resilience, productivity and well-being.

Many works treat context primarily as a function of environmental parameters such as temperature, humidity, air quality, occupancy and energy consumption, measured via dense IoT sensor networks. Thus, in [4], was considered energy conservation as one of the components of the smart sustainable management system using Arduino microcontroller. After, in [5], the autoregressive models have demonstrated high accuracy in predicting electricity consumption and monitoring, which allows for prompt response to inefficient use of resources and reduction of electricity costs.

Reviews of many other scientific resources note that IoT-based monitoring systems have been successfully deployed to collect environmental data using temperature, humidity, gas and motion sensors, enabling energy-efficient control of HVAC systems, predictive maintenance and optimization of production processes [6]. In the workplace domain, such systems are often integrated into “smart office” or “smart workplace” solutions that adjust lighting and microclimate to reduce energy use while maintaining basic comfort. However, sensor-only approaches capture mostly physical aspects of context and provide limited insight into cognitive load, work patterns, social interactions or task complexity. The considered types of context its measurement methods were listed in [7].

CV techniques extend context obtaining to visual observation of workers, tools, postures and activities. In industrial and construction settings, CV is widely used to monitor safety, detect unsafe behaviors and analyze human-machine interactions. For example, studies on driver behavior monitoring and intent interpretation have shown that video analytics can detect complex behavioral patterns, including inattention, fatigue, and high-risk maneuvers [8]. However, CV-based methods suffer from overlaps, limited camera angles, privacy concerns, and high computational requirements. In crowded offices or flexible hybrid workspaces, line-of-sight limitations and dynamic layouts further limit the reliability of purely visual context obtaining.

Recent research combines wearable device data with IoT infrastructure for human activity recognition (HAR), inferring behavioral patterns and assessing physical activity [8]. Nevertheless, there are issues with long-term user adoption, intrusiveness of the devices, the need for calibration, and sparse data when workers do not wear the devices continuously are consistently reported in various sources.

In the Ukrainian scientific community, DT technology is being actively researched as a fundamental platform for digital management and monitoring. For example, in [9], industrial DTs describes the twin as a proxy that aggregates sensor data and exposes it via APIs to

different business systems, thereby improving understanding of the current state and supporting lifecycle management of industrial assets. A collective monograph on the digital transformation of industrial management emphasizes the role of enterprise-level DTs as a "smart" carrier of digital management that enables integrated decision-making and collaboration [10-11]. Despite these advances, the DTs cannot yet fully replace other context obtaining methods.

KG-based machine learning enables context-aware intrusion detection in industrial systems. Results show that semantic integration can improve anomaly detection capabilities and resilience to data heterogeneity [12]. In the manufacturing sector, recent research combining digital twins with KGs has demonstrated how semantic layers can support flexible queries, advanced analytics, and more interpretable decision support [13]. From an architectural perspective, reviews on context-aware systems emphasize ontologies and semantic middleware as key enablers of interoperability and reusable context models across smart environments [2]. However, creating and maintaining high-quality ontologies for complex workspaces requires significant expert input and effective management. This creates a practical obstacle to the widespread adoption of KG-based approaches in daily workplace management.

Recent surveys explicitly connect context-awareness with sustainability and resilience. They, arguing that cognition and context-aware decision-making systems (CCA-DMS) must integrate multiple context modalities such as physical, behavioral, cognitive and organizational, to support sustainable smart environments [1]. In intelligent product service systems, a context-oriented design framework proposes to combine sensor data, user interaction logs, and semantic models to dynamically customize services and improve user experiences [2, 14-15]. In the Ukrainian context, eco-ergonomic research on the "safe and productive digital workplace" highlights the need to jointly consider ergonomic, ecological and organizational factors such as lighting, noise, microclimate, work–rest regimes, safety culture and digital workload, to support both sustainability and productivity [16].

Meanwhile, industry analyses of workplace sustainability and integrated workplace management systems (IWMS) show that modern platforms are increasingly integrating building management, space utilization, environmental monitoring, and employee comfort metrics into a single dashboard [17]. However, most of these solutions still rely on relatively superficial contextual features and do not fully utilize semantic integration or advanced explanation models. However, the paper [18] considers multidimensional trade-off modeling in sustainable workplace management as not only a methodological necessity, but also a strategic condition for achieving a balance between productivity, resource efficiency, and a high level of social responsibility.

Research objective. From scientific review, current research supports the claim that no single method of context obtaining is sufficient for sustainable workplaces. The biggest gap lies in hybrid, human-centric approaches that integrate heterogeneous physical, semantic and behavioral data streams using DTs and semantic models. Therefore, the creation of an appropriate method for obtaining accessible context in SWs is the main goal of this work.

Research results and their discussion. The results of the comparative analysis of methods taking into account the types of context listed in [7] are shown in Fig. 1. A comparative analysis of context types and obtaining methods clearly demonstrates that no single method can provide complete, accurate, and semantically meaningful context in a smart SW. Each approach only covers a part of the context and has limitations related to the subject area. For example:

- CV exceeds with spatial and behavioral context but fails in microclimate, physiology, machine wear and semantics;
- wearables work well physiologically, but cannot monitor the environment, device, etc.
- DT models physical process state well, but it is not a real sensor and requires data from other sources.
- KG provides semantics and compliance rules, but cannot observe reality, which depends on input from CV, IoT, wearables or DT.

- interpretable anomaly detection (XAI-AD) can reveal anomalies, but cannot interpret their causes or apply physical and semantic constraints.

Table 1.

Comparison of observed methods vs types of context in SWs

Type of Context	CV	Wearables	DT	KG	XAI-AD
Environmental / Physical	Proc: Good at detecting lighting, smoke, occupancy, physical hazards. Cons: Cannot measure CO_2, noise; it is bad in lighting, occlusions.	Proc: Can capture body temperature, limited environmental exposure signals. Cons: Cannot measure microclimate; limited long-term accuracy.	Proc: Models HVAC, energy flows, air quality dynamics. Cons: Requires validated physical models; expensive to maintain.	Proc: Adds semantic rules (comfort, safety thresholds). Cons: Needs accurate sensor integration; cannot observe itself.	Proc: Detects anomalies in temperature/noise/energy patterns. Cons: Needs reliable telemetry; cannot sense SW directly.
Worker Behavior	Proc: Excellent for posture, gestures, unsafe movements, ergonomic risks. Cons: Occlusion; privacy issues.	Proc: Perfect for fatigue, overload, motion patterns (IMU). Cons: Requires user acceptance; battery limitations.	Proc: Can simulate typical movements and ergonomic load. Cons: Not real-time unless paired with CV/wearables.	Proc: Adds semantic interpretation (unsafe gesture). Cons: Depends on correct classification from CV/wearables.	Proc: Flags anomalous behaviors using temporal sequences. Cons: Needs training data; may miss subtle context.
Physiological / Psycho-physiological	Proc: Indirect signs only (face stress, movement). Cons: Cannot measure HRV/EEG/EDA directly.	Proc: Best source for HRV/EEG/EDA, stress, fatigue, cognitive load. Cons: Privacy-sensitive; may be intrusive.	Proc: Can simulate fatigue or stress impact on tasks. Cons: Simulation ≠ actual state; no direct measurements.	Proc: Semantic modeling of stress rules (limits, safety bounds). Cons: Needs physiological input.	Proc: Detects anomalies in physiological patterns. Cons: Needs training from wearable data.
Social-Collaborative	Proc: Detects interactions, contact density, group behavior. Cons: Occlusions; multi-person tracking complexity.	Proc: Can detect proximity via BLE/IMU. Cons: Limited spatial accuracy; no team-level semantics.	Proc: Models team workflows, resource allocation. Cons: Does not observe real social dynamics.	Proc: Captures roles, responsibilities, coordination rules. Cons: Needs real-time data input.	Proc: Detects anomalous team-level patterns (overload). Cons: Requires time-series data from multiple sensors.
Equipment & Machinery	Proc: Identifies visual damage, overheating, missing guards. Cons: Cannot detect vibration.	Proc: Can monitor vibration via wrist-worn devices (indirect). Cons: Not reliable for machine states.	Proc: Best for predictive maintenance; simulates wear, load, cycle times. Cons: Requires detailed machine models.	Proc: Enables semantic rules. Cons: Needs correct telemetry mapping.	Proc: Detects anomalies in SCADA/PLC signals. Cons: Sensitive to telemetry loss.
Process / Production Context	Proc: Recognizes operation stages visually (assembly steps). Cons: Visibility; cannot interpret digital flow.	Proc: Captures worker motion contribution in process. Cons: No understanding of process logic.	Proc: Perfect for full process flow simulation, cycle times. Cons: Needs detailed model with calibration.	Proc: Encodes rules (ISO, SOP), workflow logic. Cons: Requires full ontology.	Proc: Detects process anomalies. Cons: Cannot explain high-level semantics alone.
Safety & Risk	Proc: Detects hazards, unsafe zones, falls, PPE misuse. Cons: May miss invisible risks (gas, CO_2).	Proc: Detects physiological and micro-behavioral risk precursors. Cons: Limited environmental hazard sensing.	Proc: Simulates hazards, emergency scenarios. Cons: Not real hazard detection; only model-based.	Proc: Risk reasoning (cause–effect rules). Cons: Needs integration with sensor systems.	Proc: Excellent for anomaly-based safety alerts. Cons: Requires robust training and thresholds.
Resilience & Resource	Proc: Detects occupancy for HVAC optimization. Cons: Cannot measure energy flows.	Proc: Indirectly detects fatigue for productivity trends. Cons: Not suited for resource data.	Proc: Strong for energy, water, waste, CO_2 modeling. Cons: Accuracy depends on model precision.	Proc: Encodes ESG thresholds, sustainability policies. Cons: Needs rich metadata.	Proc: Detects anomalies in consumption patterns. Cons: Only statistical; lacks semantics.
Semantic / Ontological	Proc: Provides raw visual events. Cons: Cannot apply standards or reasoning.	Proc: Captures bio-signals. Cons: Not semantic.	Proc: Calculates physical state, but not norms. Cons: Does not handle ontologies.	Proc: Applies rules, standards, SHACL, compliance. Cons: Needs ontology engineering.	Proc: Adds explainability to decisions. Cons: No standalone semantics.

Therefore, we chose a hybrid approach that integrates DT, KG and XAI-AD into a single workflow since this is the minimum number of methods to cover all types of context. The method (Fig. 1) intertwines sensing, modelling, reasoning, and explainable intelligence to orchestrate a sustainable workplace. It all starts with a deliberately mixed collection of raw data: CV data, wearable telemetry data, IoT tags, programmable logic controller (PLC) or supervisory control and data acquisition (SCADA) control logs and even analog agents from Webot.

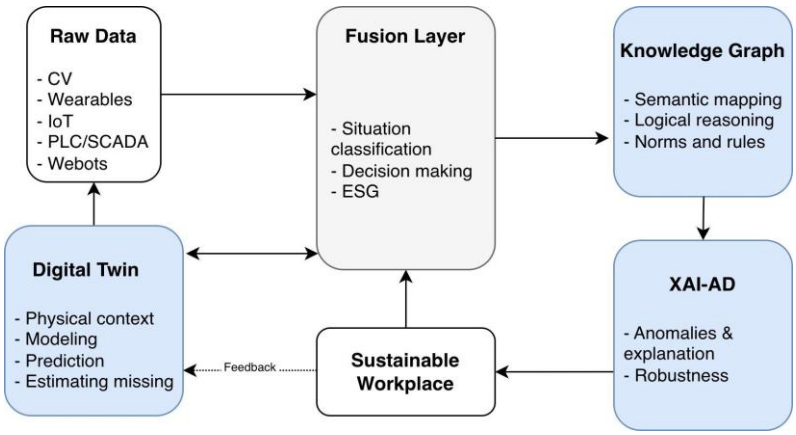


Fig. 1. Context obtaining method in SW

These data streams, which are shown in a PlantUML sequence diagram (Fig. 2), are not treated as independent channels. Instead, they enter a fusion layer that aligns them temporally and semantically, so that a single situation can be identified even if the data patterns differ, such as an operator entering a high-risk area while starting a machine. At this combined level, classification algorithms interpret the operational state, and a decision-making engine weighs responses based on environmental, social and governance objectives, thereby effectively embedding ESG standards into daily operational logic. The integration layer is not isolated. It uses a KG that encodes shared semantics, regulatory rules, and logical relationships between processes, devices, personnel roles, and regulatory obligations.

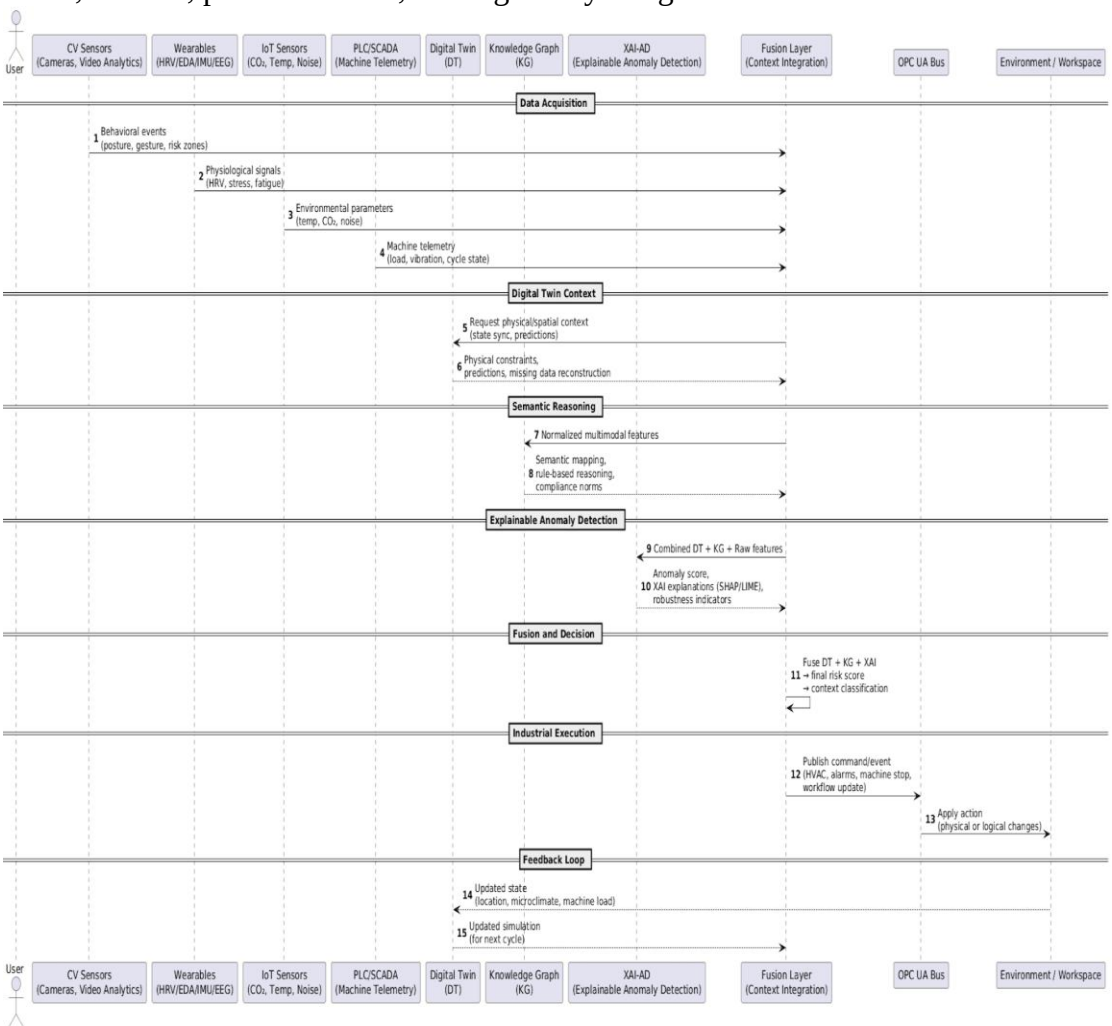


Fig. 2. PlantUML sequence diagram of the proposed method

By projecting the comprehensive observations in a chart, the system gains the ability to infer causal relationships, preconditions and corresponding points. This knowledge system can stabilize the interpretation of events across parts and prevent model deviations when terminology or processes change. This allows for transferring a contextual understanding to the XAI-AD. The XAI-AD component does more than just flag anomalies. It also generates human-readable descriptions, tracks which rules were violated, which sensors contributed most to the alerts, and how confident the system is in detecting violations.

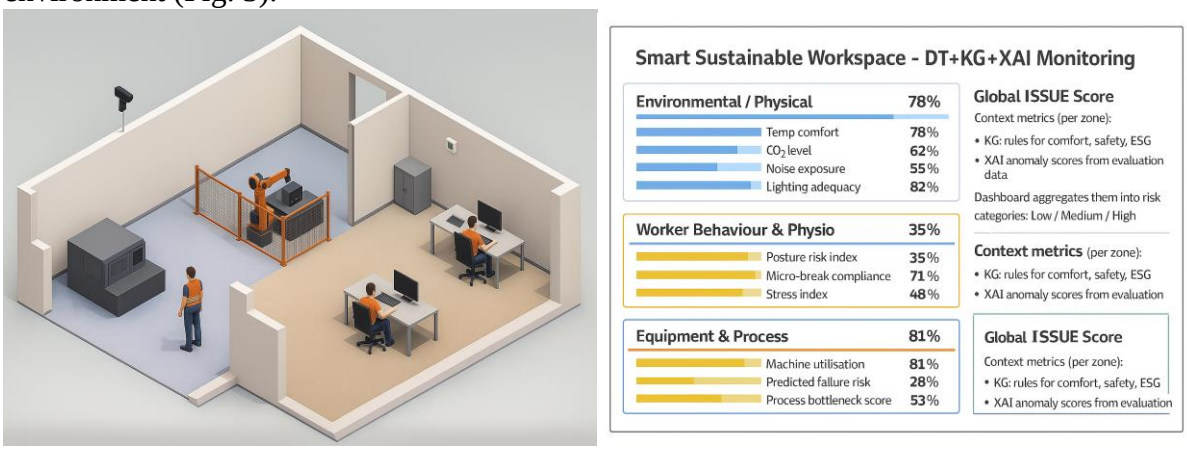
Along with cognitive elements, DTs encapsulate the physical workplace. By receiving the same raw data, they can accurately represent the status of machines, the flow of materials, the movement of personnel and others. When a sensor fails, the DT can fill the gap, predict short-term conditions such as peak energy consumption, and test mitigation strategies without interrupting actual operations. Double-feedback data analysis connects the integration layer and the SW control center, creating a feedback loop that continuously adjusts policies, proactively organizes maintenance, and ensures a balance between productivity, well-being and environmental impact.

The biggest advantage of the proposed method lies in overall transparency because the decisions are made based on a single intelligent system, not isolated dashboards. Prediction and control signals became clearer, resource use aligned with sustainability commitments and interpretable warnings strengthened accountability.

However, integrating all these components (Fig. 2) is no easy task. Coordinating data quality between traditional PLC systems and modern wearable devices is costly, and the knowledge graph requires ongoing management to maintain consistency with the enterprise's classification system. DTs must synchronize almost instantly, which poses challenges for network infrastructure and network security practices. Furthermore, supporting ESG-compliant decision-making standards requires cross-functional coordination. If management shifts priorities or data privacy regulations tighten, the system will adapt quickly or issues being phased out.

Despite the aforementioned challenges, this method provides a solid foundation for continuous improvement. By combining rich contextual information, XAI and virtualization experiments, organizations can gradually create efficient and secure SWs.

To prove the applicability of the proposed method, we did some simulations in the Webots environment (Fig. 3).



a) b)

Fig. 3. Simulations in the Webots environment: a) SW; b) Dashboard with measurements.

For simulation in Webots (Fig. 4a), two key components were created in the environment: DT of the SW with factory and office spaces. Also, two controllers were created: one for data generation and the other for building a dashboard.

The first controller, "context_supervisor.py", simulates the operation of sensors. It reads environmental parameters such as temperature, CO_2, noise, machine load, and worker stress

every clock cycle and writes them to CSV. This creates a data stream similar to real IoT systems. There are 10000 generated records which used for the simulation (Fig. 4).

The second controller, "dashboard_controller.py", operates in Supervisor mode, has a “Display device”, which updates the graphical elements in real time. It reads CSV, calculates normalized contextual metrics, generates an integral Global ISSUE Score, defines categories (Low/Medium/High), and draws appropriate blocks on the dashboard (Fig. 4b).

Thus, Webots can simultaneously perform physical room simulation, generate DT data and display analysis results on a dashboard, providing instant and complete simulation of the operation of an intelligent monitoring system.

Discussion of the results obtained. The scientific novelty of the proposed method lies in the creation of a unified hybrid architecture, integrating DT, KG and XAI, which for the first time combines spatiotemporal physical modeling, semantic ontological interpretation and XAI-AD for comprehensive context extraction in SWs.

Unlike existing similar approaches, the method provides multimodal integration of consolidated data, its semantic normalization using KG and reliable deviation detection using XAI models.

It is shown for the first time that the combination of DT and KG allows for compensation for the loss of sensor data, and the addition of XAI provides interpretability, self-explanatoryness and robustness to anomalies.

The method forms a new class of context-oriented systems capable of supporting real-time decision-making taking into account physical, behavioral, psychophysiological, process and normative dependencies.

Conclusions. The paper presents a comparative analysis of modern context obtaining methods from which it follows that no single method can fully capture the diverse and multidimensional context required in smart SWs. The hybrid integration of DTs, KGs and XAI-AD bridges these gaps by combining physical modeling, semantic thinking and robust anomaly detection. This synergy provides high accuracy, interpretability, and robustness to missing or noisy data and a future-ready framework for context-aware decision-making in SW management. The applicability of the proposed method was assessed by using semantic, expert and simulation validation for preliminary accelerated evaluation.

References

1. Violos J., Mamanis G., Kompatsiaris I. Cognition and context-aware decision-making systems for a sustainable planet: a survey on recent advancements, applications and open challenges. *Discov Sustain.* 2025. No.6.P. 235. URL: https://doi.org/10.1007/s43621-025-00954-y.
2. Santos A., Lima C., Pinto T., Reis A., Barroso J. Context-Aware Systems Architecture in Industry 4.0: A Systematic Literature Review. *Applied Sciences*. 2025. No.15(11). P. 5863. URL: https://doi.org/10.3390/app15115863.
3. Carrera-Rivera A., Larrinaga F., Lasa G. Context-awareness for the design of smart-product service systems: Literature review. *Computers in Industry.* 2022. V. 142, 103730. URL: https://doi.org/10.1016/j.compind.2022.103730.
4. Yakubovych M.Y., Lyashkevych V.L., Shuvar R.Y. Energy Conservation as One of the Components of the Management System for the Smart Sustainable Workspaces. *Electronics and Information Technologies*. 2025. V.29. P.79-94. URL: https://doi.org/10.30970/eli.29.8
5. Yakubovych, M.Y., Lyashkevych, V.L., & Shuvar, R.Y. Modern methods of energy conservation management in a smart sustainable workplace. *Herald of Khmelnytskyi National University. Technical Sciences*. 2025. V. 357. No.5.2, P.236-246. URL: https://doi.org/10.31891/2307-5732-2025-357-90
6. Moghrabi, I. A. R., Bhat, S. A., Szczuko, P., AlKhaled, R. A., & Dar, M. A. (2023). Digital Transformation and Its Influence on Sustainable Manufacturing and Business Practices. Sustainability, 15(4), 3010. URL: https://doi.org/10.3390/su15043010.

7. Yakubovych M., Lyashkevych V. Modern Challenges For Real-Time Context Monitoring In Smart Sustainable Workspaces. Modern Perspectives on Science and Economic Progress: *2nd International Scientific and Practical Conference. 2025. Vilnius, Lithuania* .P. 464-468. URL: https://doi.org/10.70286/isu-05.11.2025.007
8. Chen Yu, Li J., Blasch E., Qu Q. Future Outdoor Safety Monitoring: Integrating Human Activity Recognition with the Internet of Physical-Virtual Things. 2025. URL: https://doi.org/10.20944/preprints202503.0415.v1
9. Digital Twins for Industrial Applications (Ukrainian translation of white paper). Kyiv: I. Sikorsky Kyiv Polytechnic Institute, 2020. URL: https://atep.kpi.ua/wp-content/uploads/2021/12/iic_digital_twins_industrial_apps_white_paper_2020-02-18-ukr.pdf?utm_source=chatgpt.com
10. Ostrovska H.Y. Digital transformation of industry. In Digital transformation of the industrial sector. Kyiv: NAS of Ukraine, 2024. P. 31–48 URL: https://nasplib.isofts.kiev.ua/server/api/core/bitstreams/44c7cd94-2cba-47a4-96dc-ca11b39a214f/content?utm_source=chatgpt.com
11. Voronkova, V. H. Digital Transformation of Industrial Management: Theory and Practice. 2023. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/13677/1/ 0054482.pdf? utm_source=chatgpt.com
12. Garrido J.S. Machine learning on knowledge graphs for context-aware security. arXiv preprint arXiv:2105.08741. 2021. URL: https://doi.org/10.1109/CSR51186.2021.9527927.
13. Stavropoulou G, Tsitseklis K, Mavraidi L, Chang K-I, Zafeiropoulos A, Karyotis V, Papavassiliou S. Digital Twin Meets Knowledge Graph for Intelligent Manufacturing Processes. *Sensors.* 2024. No.24(8). P.2618. URL: https://doi.org/10.3390/s24082618.
14. Yuan W., Chang D., Han T. A context-aware smart product-service system development approach and application case. *Computers & Industrial Engineering*. 2023. P.183. 109468. URL: https://doi.org/10.1016/j.cie.2023.109468.
15. Mirshafiee N, Han J, Ahmed-Kristensen S. The DHSmart model for smart product-service system (smart PSS): dynamic, data-driven, human-centred. *Proceedings of the Design Society*. 2024. 4:2149-2158. URL: https://doi.org/10.1017/pds.2024.217.
16. Protasenko O., Ivashura A., Yermolenko O., Ponomarenko Ye. (). Safe and productive digital workplace: Eco-ergonomic principles of organisation. *Innovation and Sustainability.* 2025. No.5(1). P.83–91. URL: https://repository.hneu.edu.ua/handle/123456789/36598? utm_source=chatgpt.com
17. Horizant. Sustainability and employee comfort: A synergy with IWMS. 2025. URL: https://www.horizantinsights.com/article/sustainability-and-employee-comfort-a-synergy-with-iwms/
18. Yakubovich M.I., Lyashkevych V.Ya. Justification of multidimensional trade-off modeling in the management of sustainable workplaces. *Problems of informatics and computer technology. XIV International Scientific and Practical Conference*. 2025. P. 149-151. URL: https://drive.google.com/file/d/12FGgnfM6NA8HPo66h0TgVrfbPHAYDMFC/view

M.I. Yakubovych, V.Y. Lyashkevych

МЕТОД ВИДОБУВАННЯ КОНТЕКСТУ В СТІЙКИХ РОБОЧИХ ПРИМІЩЕННЯХ

М.І. Якубович, В.Я. Ляшкевич

Львівський національний університет імені Івана Франка
50, Драгоманова вул., Львів, 79005, Україна
Emails: maksym.yakubovych@lnu.edu.ua, vasyl.liashkevych@lnu.edu.ua

Сучасне робоче місце швидко трансформується у складне кіберфізичне середовище, яке поєднує людей, технологічні системи, оточення, виробничі процеси та знання. Ця багатовимірність вимагає безперервне видобування контекстуальної інформації, включаючи динамічну інформацію про стан простору, обладнання, людей та процесів, що визначає можливості адаптивності, безпеки та стійкого управління. У статті визначено роль контексту як базового елемента адаптивного управління, розкрито міждисциплінарний характер контекстуальних даних та показано, як їх правильне врахування впливає на безпеку, енергоефективність, продуктивність та добробут працівників. Методологія дослідження включає аналіз літератури та сучасних технологічних рішень, систематизацію типів контексту, побудову порівняльної таблиці переваг і недоліків існуючих методів, а також використання семантичної, експертної та симуляційної валідації для попередньої прискореної оцінки. Основні результати показують, що подібні методи мають суттєві обмеження: комп'ютерний зір страждає від перекритів, наручні сенсори від неприйнятності для користувача, цифрові двійники від складності моделювання, а графи знань від високих вимог до інженерії знань. Запропонований метод, базується на гібридному підході та демонструє найвищу точність видобування контексту, стійкість до прогалин у даних та прозорість рішень на основі моделей зрозумілого штучного інтелекту та семантичної інтеграції. Результати показують, що поєднання фізичних, семантичних та поведінкових джерел інформації забезпечує найповнішу картину стану робочого середовища. Запропонований метод видобування контексту інтегрує різнорідні дані та підвищує рівень інтелекту систем управління робочим простором. Робота сприяє розвитку наукової думки в галузі стійкості, кіберфізичних систем та інтелектуального моніторингу, а також закладає основу для побудови адаптивної, людиноцентричної системи підтримки рішень та системи автоматичного контролю мікроклімату, збільшення кількості виробничих інцидентів, оптимізації навантаження персоналу в реальних робочих просторах.

Ключові слова: стійкий робочий простір, видобування контексту, цифровий двійник, графи знань, машинне навчання, зрозумілий штучний інтелект, комп’ютерний зір.

DOI 10.15276/imms.v16.no1.43
UDC 004.4`4: 004.23

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 43-51

PROBLEMS OF AUTOMATIC CODE OPTIMIZATION BY THE COMPILER

I. Zhulkovska[1], O. Zhulkovskyi[1],
T. Rudianova[2], O. Lebid[2], M. Mormul[2]

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

Rational use of modern compiler capabilities, in particular automatic SIMD vectorization, enables significant improvements in computational performance for tasks involving data-array processing and computer modeling of complex processes and systems. The growing demand for software performance in scientific computing, big-data analysis, artificial intelligence, and machine learning emphasizes the importance of exploiting hardware-level data parallelism. This study investigates the efficiency of automatic SIMD vectorization provided by the Microsoft Visual C++ compiler in comparison with manual optimization implemented through AVX2 instructions. To evaluate performance, three implementations were developed: a scalar baseline version, a compiler-optimized automatic SIMD code, and a manually vectorized SIMD version using intrinsic functions. Computational experiments were conducted using the SAXPY operation for arrays sized from 10^5 to 10^9. The results demonstrated that automatic SIMD vectorization provides up to a 7.5x speedup with an efficiency of 0.94 for small- and medium-scale problems, effectively utilizing processor resources through aggressive optimizations such as loop unrolling and efficient use of FMA pipelines Manual SIMD optimization showed stable acceleration of up to 3. for large arrays but with lower efficiency (0.28–0.49 due to memory-bandwidth limitations and less aggressive compiler-level transformations. The comparison revealed that automatic methods are more convenient for developers, significantly reducing the effort required for writing SIMD code, while manual optimizations remain relevant when scaling to large data volumes. The findings indicate that the optimal strategy is a combined use of automatic and manual SIMD transformations, allowing a balance between performance, accuracy, and development effort, thus ensuring both efficiency and scalability of software solutions in high-performance computing and computer modeling. Future research will focus on expanding the experimental base across various processor architectures, analyzing the interaction of SIMD vectorization with other compiler transformations, and applying ML-based methods for adaptive optimization-strategy selection.

Keywords: automatic SIMD vectorization, manual SIMD optimization, AVX2, MSVC compiler, high-performance computing.

Introduction. The rapid development of computing technology [1] and software has significantly increased the requirements for software performance, particularly in scientific computing, computer modeling, big-data analysis, and tasks related to artificial intelligence (AI) and machine learning (ML) [2, 3]. Execution efficiency is critical for high-performance computing (HPC), as well as for engineering and industrial systems, where computation speed and result accuracy directly affect the quality of forecasts and decision-making processes [4].

For a long time, performance growth was achieved by reducing transistor sizes and increasing processor clock frequencies. However, physical limitations rendered this approach ineffective, leading to alternative solutions [1], such as multi-core architectures, parallel computing, and the use of SIMD (Single Instruction, Multiple Data) hardware capabilities.

One of the key directions in improving performance is automatic compiler-based code optimization, which improves execution performance without modifying the source code. Modern compilers implement a wide range of optimizations, including vectorization, loop

unrolling and loop fusion, dead-code elimination, function inlining, constant propagation, and others [5].

Special attention is given to SIMD vectorization, which enables efficient exploitation of data-level parallelism (DLP) [6]. This approach allows a single instruction to be executed simultaneously across an entire vector of elements, significantly accelerating array-based data processing. Such methods are particularly relevant for modeling complex technological processes and systems [4], as well as for numerical algorithms used in large-scale data analysis and AI models.

Until recently, most SIMD optimizations were performed manually by programmers, requiring deep knowledge of hardware architecture and being a labor-intensive process. However, the advancement of modern compilers has gradually enabled automation of this process, making it possible to compare the efficiency of manual and automatic SIMD vectorization.

In this context, the present study focuses on analyzing modern approaches to automatic SIMD vectorization by compilers and comparing them with the outcomes of manual optimization in order to assess the advantages and limitations of both approaches. This allows identification of development trends in code-optimization technologies and directions for their further improvement.

Related works. Modern compilers perform multistage program transformations at different representation levels (source – intermediate representation (IR) – machine code), applying a set of optimization passes. The objective of these passes is to improve execution performance and hardware-resource utilization without altering the program's semantics. In recent years, compiler developers have emphasized combining program data-flow analysis with processor architectural features to automatically select and tune optimizations [7].

A particularly important direction involves optimizations aimed at exploiting DLP parallelism [8, 9]. These include [5]: vectorization, SLP transformations (Superword-Level Parallelism), loop unrolling/fusion, and related transformations that reduce the number of instructions and improve the utilization of vector-register resources in modern CPUs (SSE, AVX/AVX2/AVX-512 for Intel, NEON for ARM architectures, etc.). The practical effectiveness of such transformations depends on the accuracy of dependence analysis within loops, the availability of memory-aliasing information, and support for a specific Instruction Set Architecture (ISA) [10].

The assessment of compilers' automatic vectorization capabilities is an active area of research. In [5], a systematic methodology for evaluating auto-vectorizers was proposed, demonstrating that the presence or absence of useful information in the code strongly affects the results of auto-vectorization. Moreover, synthetic benchmarks (e.g., the Test Suite for Vectorizing Compilers, TSVC) do not always capture the practical constraints of real-world applications. This underlines the necessity of thorough testing and specialized approaches for measuring compiler capabilities.

An important direction of development involves combining SIMD vectorization with other compiler transformations, such as loop tiling (which improves cache locality and the utilization efficiency of the memory hierarchy), software pipelining (which overlaps data dependencies and balances instruction pipeline utilization), and memory-access optimizations aimed at reducing latency and avoiding memory-bank conflicts. As shown in [11], the integrated application of these approaches enables performance levels approaching those of manual optimization, confirming the potential of multilevel strategies for program-code optimization.

Recent studies increasingly focus on the application of ML methods for selecting optimization passes. In [12], an ML model was proposed that predicts the suitability of vectorization and other optimizations based on code characteristics, allowing compilers to dynamically adapt their strategies. This opens new opportunities for creating «intelligent

compilers», capable of learning from examples and accounting for both code properties and hardware features.

Although modern compilers implement multistage optimization passes and achieve significant acceleration in many cases, the literature review identifies a number of systemic limitations that substantially affect the effectiveness of automatic transformations.

For instance, automatic vectorization is effective for regular access patterns, such as linear matrix indices. However, complex address expressions, indirect indexing through arrays, or branches within loops limit the compiler's ability to generate efficient vector code [13]. Preliminary data transformations (e.g., tiling, data-layout adjustments) are often required, complicating automation.

The generation of efficient code also depends on the specific hardware architecture, including vector width, instruction set, and support for predication. Optimizations designed for the AVX2 architecture may not deliver performance gains on platforms with ARM SVE, and vice versa. This complicates the creation of universal auto-vectorizers, since each architecture has unique characteristics that influence vectorization efficiency [14].

Finding the optimal combination of passes and compiler parameter settings considerably increases compilation time. In ML-based approaches, additional offline training of models is required to predict the usefulness of optimization passes. This increases build time and necessitates a trade-off between code quality and compilation cost, especially in industrial workflows [7].

While ML-based methods for compiler optimization-pass selection show promising results, the main challenge lies in the need for large training datasets, which may be difficult to obtain in specific domains or for new architectures. Furthermore, ML models may have limited generalization ability to unseen programs, reducing their effectiveness in real-world scenarios. The lack of transparency in decision-making (explainability) within complex ML models further complicates their integration into industrial compilers, as predicting and controlling their behavior across different scenarios becomes difficult. These factors increase the risk of overfitting, where a model performs well on training data but fails to efficiently handle new or unexpected inputs. Thus, although ML approaches promise improved optimization efficiency, their application requires careful dataset collection, model tuning, and ensuring transparency of decisions [15].

All optimization transformations must preserve program semantics. Aggressive transformations, such as memory-access reordering or speculative vectorization, may require additional control mechanisms – including memory fences or runtime assertions – to prevent correctness violations. However, introducing such safeguards can reduce runtime performance and partially offset the benefits of automatic optimizations [16].

Research Objective. Computational efficiency in computer-modeling tasks largely depends on the use of SIMD instructions, which enable data-level parallelism in array processing. The traditional approach of manual vectorization (explicit SIMD) ensures a high degree of control but requires considerable time investment and architectural expertise. In contrast, modern compilers – particularly Microsoft Visual Studio C++ (MSVC) – implement automatic vectorization (implicit SIMD), which can significantly reduce development effort.

The purpose of this study is to investigate the efficiency of automatic SIMD vectorization in modern compilers using MSVC as a case study and to compare it with manual code optimization. The work aims to identify the advantages and limitations of automatic and manual optimization strategies, as well as to develop practical recommendations for improving program performance in high-performance computing, particularly in the computer modeling of complex processes and systems.

Main Part. Vectorization is the process of transforming sequential scalar instructions into vector instructions, which – unlike multithreading models – implements data-level parallelism (DLP) within a single processor core. This allows a single instruction to be executed over multiple elements simultaneously, using SIMD instructions as the hardware foundation.

Modern processors support SIMD through the following extensions [17]: SSE (Streaming SIMD Extensions) – 128 bit, AVX/AVX2 (Advanced Vector Extensions) – 256 bit, AVX-512 – 512 bit, ARM NEON, and SVE (Scalable Vector Extension).

Theoretical acceleration (S_{max}) depends on the ratio of the vector-register width to the size of the data element (W_{reg} / W_{elem}). For example, for AVX2 with 32-bit elements, up to eight operations can be performed per clock cycle.

Two approaches to SIMD are distinguished: explicit vectorization (explicit SIMD) – using intrinsic functions and inline assembly – and automatic vectorization (implicit SIMD, auto-vectorization), in which the compiler automatically analyzes and transforms the appropriate code into vectorized instructions without changes to the program source text. Explicit vectorization ensures full control but requires deep knowledge of the Instruction Set Architecture (ISA) and reduces code portability. The advantage of automatic vectorization is reduced development effort; however, its efficiency depends on dependence analysis algorithms and support for the specific hardware architecture.

The conditions for effective vectorization include regular memory access, the absence of loop-carried dependencies, proper data alignment, and correct pointer handling (alias analysis).

The primary performance metrics are execution time (τ), speedup (S), and acceleration efficiency (E, $0 \le E \le 1$):

$$S = \tau_{scal} / \tau_{vec},$$

$$E = S / S_{max},$$

where τ_{scal}, τ_{vec} – are the execution times of the scalar (non-vectorized) and vectorized versions, respectively.

Most modern compilers implement multi-level optimization – from high-level transformation (source – IR) to machine-code generation. Vectorization is a component of loop optimizations and machine-dependent optimizations.

GCC supports auto-vectorization at optimization level -O3 and with options such as -ftree-vectorize and -funroll-loops. It also has good integration with OpenMP SIMD.

Clang/LLVM provides a Loop Vectorizer and an SLP Vectorizer and is oriented toward flexible tuning. It is widely used in scientific computing projects and AI frameworks.

Intel ICC/ICX is regarded as a reference standard for high-performance computing, offering advanced heuristics for dependence analysis and optimized generation of AVX/AVX-512 instructions.

MSVC supports auto-vectorization for loops when using the /O2 or /Ox. optimization flags. Built-in intrinsic functions in <immintrin.h> allow for explicit SIMD implementation.

Starting with C++17, MSVC also integrates parallel STL algorithms (Parallel Patterns Library), which combine multithreading with vectorization. This represents a higher level of automation, relying not only on the compiler's internal optimization mechanisms but also on library-level abstractions.

In MSVC, vectorization is implemented based on loop analysis in an SSA-style intermediate representation (IR). The algorithm checks for loop-iteration independence, the feasibility of applying predication to conditional branches, the regularity of array indexing, and proper memory-access alignment. If alignment cannot be guaranteed, the compiler inserts so-called «safe loads» to ensure correctness.

MSVC applies a combination of strip-mining and vectorization – splitting the loop into a «vector» part and a «remainder» (tail) executed in scalar mode. This ensures correctness even for arrays whose length is not a multiple of the vector width. A distinctive feature of MSVC is its integration of the auto-vectorizer with the Profile-Guided Optimization (PGO) system: during preliminary program runs, execution statistics are collected, allowing the compiler to more accurately select loops for vectorization.

To evaluate the efficiency of compiler auto-vectorization and manual SIMD optimization, three groups of tests were implemented:

1) a scalar baseline implementation of array-processing algorithms;

2) an automatically optimized implementation compiled with the /O2 and /Ox, optimization flags that activate MSVC's auto-vectorizer;

3) a manual SIMD implementation, where the same algorithms were vectorized using AVX2 instructions from the <immintrin.h> library.

As an example, the SAXPY operation (Single-Precision A×X Plus Y) was computed:

$$y_i = \alpha x_i + y_i, i = 1,..., N,$$

where N is the array size, α – a constant, x, y – are vectors.

In the scalar baseline version (C++):

```
for (int i = 0; i < N; ++i) y[i] = a * x[i] + y[i];
```

The loop contains a simple linear indexing pattern, no conditional branches, and regular memory access, making it suitable for automatic SIMD vectorization.

When applying automatic optimization, the Microsoft Visual C++ compiler transforms the scalar loop into a vectorized loop using AVX2 SIMD instructions. The basic approach involves loading eight float elements into a 256-bit YMM register and performing multiplication and addition in vectorized form.

However, in practical implementations within the MSVC IDE, the compiler applies a more aggressive strategy – loop unrolling and scheduling multiple vector blocks per iteration. This means that, instead of processing only eight elements at a time, MSVC simultaneously processes several groups of eight elements, distributing them across different YMM registers (e.g., ymm1, ymm2, ymm3, etc.). Such an approach reduces loop-control overhead, maximally loads processor pipelines capable of executing several SIMD operations in parallel, and more effectively exploits FMA (fused multiply-add) instructions, which combine multiplication and addition in a single cycle.

Thus, automatically generated MSVC code not only vectorizes computations but also applies advanced optimizations at both the memory and instruction-flow levels. This approach can be characterized as an aggressive SIMD-vectorization strategy.

SIMD version (AVX2):

```
1   __m256 avx_a = _mm256_set1_ps(a);
2   int i;
3   for (i = 0; i + 7 < N; i += 8)  // vector loop
4   {
5       __m256 avx_x = _mm256_loadu_ps(&x[i]);
6       __m256 avx_y = _mm256_loadu_ps(&y[i]);
7       avx_y = _mm256_fmadd_ps(avx_a, avx_x, avx_y);
8       _mm256_storeu_ps(&y[i], avx_y);
9   }
10  for (; i < N; ++i) y[i] = a * x[i] + y[i]; // tail loop
```

In this implementation, vectorization of computations is carried out using AVX2 SIMD intrinsics from Intel. A 256-bit vector type __m256 s employed, corresponding to the hardware YMM registers of the Intel architecture [18, 19]. Each YMM register can hold eight single-precision floating-point numbers (float), enabling the simultaneous processing of eight elements of a float array within a single instruction.

At the beginning, a broadcast operation is performed using _mm256_set1_ps(a) (line 1), which loads the scalar coefficient a into all eight positions of the vector register avx_a. Next, the vectorized loop (lines 3–9) is executed: _mm256_loadu_ps(&x[i]) and _mm256_loadu_ps(&y[i]) (lines 5 and 6, respectively) load contiguous subarrays of x and y into YMM registers. The instruction _mm256_fmadd_ps(avx_a, avx_x, avx_y) implements the fused multiply-add (FMA) operation (line 7), which is executed in hardware without intermediate storage of the product, thereby reducing execution overhead and improving computational accuracy. The result is stored back into memory using _mm256_storeu_ps (line 8).

Since the array length N may not be a multiple of the vector register size (eight elements), a tail loop is used to process the remainder with scalar instructions. This guarantees correctness for any input size. The same principle is applied in automatic compiler optimization.

The presented code illustrates a typical SIMD-programming structure, where vector processing of the main data portion using YMM registers is combined with a tail section for residual elements. Such an approach efficiently exploits hardware-level data-parallelism (DLP) while maintaining universal applicability.

Thus, manual SIMD code is optimal in terms of the «purity» and simplicity of SIMD, but it does not exploit the potential of loop unrolling. By contrast, MSVC auto-vectorization generates more complex yet more aggressive code, capable of delivering higher performance on modern CPUs thanks to loop unrolling and maximized utilization of FMA pipelines.

Results and Discussion. The experiments were conducted on a laptop equipped with a 12th Gen Intel Core i5-12500H 2.50 GHz processor (12 cores / 16 threads), 16 GB of DDR4-3200 MHz RAM, running Microsoft Windows 10. Program development and compilation were performed in MSVC 2022, targeting the 64-bit (x64) architecture with SIMD AVX2 extensions enabled. Execution time was measured using the standard clock() function from the <time.h> library.

The program was implemented in MSVC with the following settings:

– Enable Enhanced Instruction Set = Advanced Vector Extensions 2 (x86/x64) (/arch:AVX2);

– Floating Point Model = Fast (/fp:fast)

Analysis of the obtained results (Table 1) reveals significant differences between scalar execution, manual SIMD vectorization, and compiler auto-optimization. The execution time in the scalar version grows nearly linearly with increasing problem size, reaching 4.493 seconds for $N = 10^9$ (Fig. 1). This is expected, since the absence of data-level parallelism limits performance to sequential execution of instructions.

Table 1.

Performance metrics of computational implementations

N	1.0×10^5	1.0×10^6	1.0×10^7	1.0×10^8	1.0×10^9
τ_{scal}	0.000121	0.00135	0.01445	0.10685	4.493
τ_{vec}	0.000046	0.00049	0.00656	0.04635	1.157
τ_{auto}	0.000016	0.00035	0.00433	0.04599	0.855
S_{vec}	2.61	2.76	2.20	2.31	3.88
S_{auto}	7.50	3.92	3.34	2.32	5.25
E_{vec}	0.33	0.34	0.28	0.29	0.49
E_{auto}	0.94	0.49	0.41	0.29	0.66

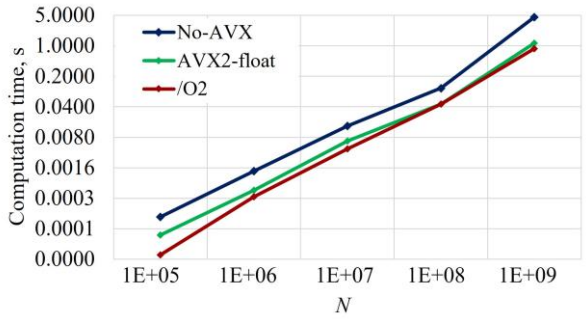


Fig. 1. Execution-time dependence on problem size

Manual SIMD vectorization provides substantial acceleration. For $N = 10^9$, execution time is reduced almost fourfold compared to the baseline scalar version. The corresponding speedup ranges from 2.2 to 3.88 depending on the problem size (Fig. 2). At the same time,

hardware-utilization efficiency remains in the range of 0.28–0.49, indicating incomplete loading of vector registers and potential performance losses due to irregular memory access or synchronization overheads.

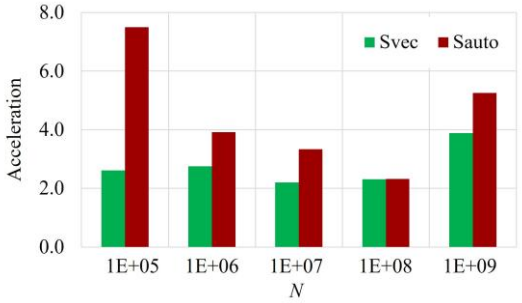


Fig. 2. Comparison of manual and automatic vectorization performance

Compiler auto-optimization demonstrates even higher performance for small and medium problem sizes. For $N = 10^5$, a maximum speedup of 7.5x is achieved with efficiency of 0.94, which is close to the theoretical limit (Fig. 3). However, as data size increases, efficiency decreases. For instance, at $N = 10^8$ it drops to only 0.29, which can be attributed to memory-bandwidth limitations and the influence of data-layout organization on the performance of vector computations.

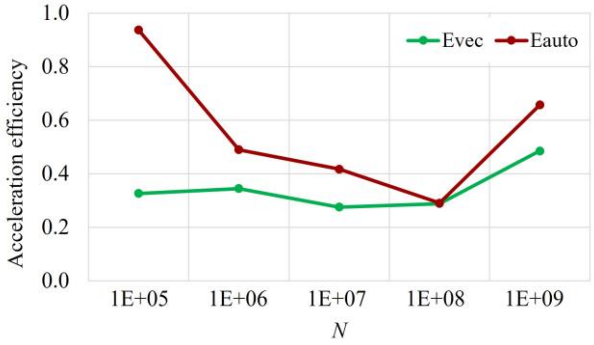


Fig. 3. Comparison of SIMD-resource-utilization efficiency

The results indicate that automatic SIMD vectorization in modern compilers can deliver performance comparable to or even exceeding manual optimization, particularly for small- and medium-sized tasks. At the same time, when scaling to larger datasets, the advantages of manual optimization become more evident due to its ability to better account for memory-organization specifics and to fine-tune loop parameters. These findings confirm the necessity of a combined approach, integrating automatic optimization with selective manual SIMD techniques in performance-critical code sections.

Conclusions. This study analyzed the efficiency of automatic and manual SIMD vectorization for array-processing tasks in the MSVC environment using AVX2 extension instructions.

Automatic vectorization in modern compilers demonstrates a high level of performance, particularly for small- and medium-scale tasks. The achieved speedup of up to 7.5x with an efficiency of 0.94 highlights MSVC's ability to fully utilize processor SIMD resources through aggressive optimizations, including loop unrolling and the effective use of FMA pipelines.

Manual SIMD optimization provides stable performance gains when scaling to larger problem sizes, achieving up to 3.88x acceleration for large arrays. However, its efficiency remains lower (0.28–0.49) due to memory-bandwidth limitations and the less aggressive nature of the transformations compared to automatic compiler optimizations.

The optimal strategy for high-performance applications is a combined use of automatic and manual SIMD optimization methods, which enables a balance between

performance and development effort, while ensuring the scalability of software solutions in computational modeling of complex processes and systems.

Future research directions include expanding the experimental base to cover various processor architectures (Intel, AMD, ARM), analyzing the interaction of SIMD vectorization with other compiler transformations, and applying ML-based methods for the adaptive selection of optimization strategies in HPC and computational modeling tasks.

References

1. Hennessy J.L., Patterson D.A. A New Golden Age for Computer Architecture. *Communications of the ACM.* 2019. Vol. 62, №2. P. 48–60. DOI: https://doi.org/10.1145/3282307
2. Bouras M., Idrissi A. A Survey of Parallel Computing: Challenges, Methods and Directions. *Modern Artificial Intelligence and Data Science. Studies in Computational Intelligence.* 2023. Vol. 102. P. 67–81. DOI: https://doi.org/10.1007/978-3-031-33309-5_6
3. Imbert C. Computer Simulations and Computational Models in Science. In: *Springer Handbook of Model-Based Science. Springer Handbooks.* Cham: Springer, 2017. P. 735–781. DOI: https://doi.org/10.1007/978-3-319-30526-4_34
4. Zhulkovskii O., Panteikov S., Zhulkovskaya I. Information-Modeling Forecasting System for Thermal Mode of Top Converter Lance. *Steel in Translation.* 2022. Vol. 52, №5. P. 495–502. DOI: https://doi.org/10.3103/s0967091222050138
5. Siso S., Armour W., Thiyagalingam J. Evaluating Auto-Vectorizing Compilers Through Objective Withdrawal of Useful Information. *ACM Transactions on Architecture and Code Optimization.* 2019. Vol. 16, No.4. Article 40. P. 1–23. https://doi.org/10.1145/3356842
6. Zheng R., Pai S. Efficient Execution of Graph Algorithms on CPU with SIMD Extensions. In: *2021 IEEE/ACM International Symposium on Code Generation and Optimization (CGO).* 2021. P. 262–276. DOI: https://doi.org/10.1109/CGO51591.2021.9370326
7. Haj Ali A. Machine Learning in Compiler Optimization. Berkeley: EECS Department, University of California, 2021. URL: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2021/EECS-2021-2.html
8. Zhulkovskyi O., Zhulkovska I., Vokhmianin H., et al. Application of SIMD-Instructions to Increase the Efficiency of Numerical Methods for Solving SLAE. *Computer Systems and Information Technologies.* 2024. No.4. P. 126–133. DOI: https://doi.org/10.31891/csit-2024-4-15
9. Zhulkovskyi O.O., Vokhmianin H.Ya., Zhulkovska I.I., et al. Acceleration of Image Processing Algorithms Using SIMD Technology. *Informatics and Mathematical Methods in Simulation.* 2025. Vol. 15, №1. P. 15–23. DOI: https://doi.org/10.15276/imms.V15.Vo1.15
10. Feng J., He Y., Tao Q. Evaluation of Compilers' Capability of Automatic Vectorization Based on Source Code Analysis. *Scientific Programming.* 2021. P. 1–15. DOI: https://doi.org/10.1155/2021/3264624
11. Aleen F., Zakharin V.P., Krishnaiyer R., et al. Automated Compiler Optimization of Multiple Vector Loads/Stores. *International Journal of Parallel Programming.* 2018. Vol. 46. P. 471–503. DOI: https://doi.org/10.1007/s10766-016-0485-7
12. Ashouri A.H., Killian W., Cavazos J., et al. A Survey on Compiler Autotuning Using Machine Learning. *ACM Computing Surveys.* 2018. Vol. 51, №5. Article 96. P. 1–42. DOI: https://doi.org/10.1145/3197978
13. Cho D., Pasricha S., Issenin I., et al. Compiler Driven Data Layout Optimization for Regular/Irregular Array Access Patterns. *ACM SIGPLAN Notices.* 2008. Vol. 43, №7. P. 41–50. https://doi.org/10.1145/1379023.1375664

14. Sakib N., Prabhu T., Santhi N., et al. Comparison of Vectorization Capabilities of Different Compilers for x86 and ARM CPUs. *arXiv*. 2025. DOI: https://doi.org/10.48550/arXiv.2502.11906
15. Wang Z., O'Boyle M. Machine Learning in Compiler Optimization. In: *Proceedings of the IEEE*. 2018. Vol. 106, №11. P. 1879–1901. DOI: https://doi.org/10.1109/JPROC.2018.2817118
16. Vu S.T., Heydemann K., de Grandmaison A., Cohen A. Secure Delivery of Program Properties Through Optimizing Compilation. In: *Proceedings of the 29th International Conference on Compiler Construction (CC 2020).* 2020. P. 14–26. DOI: https://doi.org/10.1145/3377555.3377897
17. Wang J., Yu L., Zhuang W., Yang X., Zhang S., Qin Z. Research on Vector Extension of Instruction Set Architecture. In: *2024 3rd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE).* Hangzhou, China, 2024. P. 378–385. DOI: https://doi.org/10.1109/CBASE64041.2024.10824427
18. Van Hoey J. AVX. In: *Beginning x64 Assembly Programming.* Berkeley, CA: Apress, 2019. P. 307–315. https://doi.org/10.1007/978-1-4842-5076-1_35
19. Intel Intrinsics Guide. Intel. URL: https://www.intel.com/content/www/us/en/docs/intrinsics-guide/index.html

ПРОБЛЕМИ АВТОМАТИЧНОЇ ОПТИМІЗАЦІЇ ПРОГРАМНОГО КОДУ КОМПІЛЯТОРОМ

І.І. Жульковська[1], О.О. Жульковський[1],
Т.М. Рудянова[2], О.Ю. Лебідь[2], М.Ф. Мормуль[2]

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

Раціональне використання можливостей сучасних компіляторів, зокрема автоматичної SIMD-векторизації, дозволяє значно підвищити продуктивність обчислень у задачах обробки масивів даних, комп'ютерного моделювання складних процесів та систем. Зростання вимог до продуктивності програмного забезпечення у наукових обчисленнях, аналізі великих даних, задачах штучного інтелекту та машинного навчання робить актуальним використання апаратного паралелізму на рівні даних.

У роботі досліджується ефективність автоматичної SIMD-векторизації компілятором Microsoft Visual C++ у порівнянні з ручною оптимізацією, що реалізується через AVX2-інструкції. Для оцінки продуктивності були розроблені три реалізації обчислень: скалярна базова версія, автоматично оптимізований код компілятора, а також ручна SIMD-версія із застосуванням intrinsic-функцій. Обчислювальні експерименти проведено на прикладі операції SAXPY для масивів розміром 10^5–10^9.

Результати показали, що автоматична SIMD-векторизація забезпечує прискорення до 7.5x із ефективністю 0.94 для задач малої та середньої розмірності, максимально використовуючи ресурси процесора завдяки агресивним оптимізаціям, таким як розгортання циклів та ефективне використання FMA-конвеєрів. Ручна SIMD-оптимізація демонструє стабільне прискорення до 3.88x для великих масивів, проте з нижчою ефективністю (0.28–0.49) через обмеження пропускної здатності пам'яті та меншу агресивність трансформацій. Порівняння показало, що автоматичні методи є більш зручними для розробника, дозволяючи значно зменшити трудомісткість написання SIMD-коду. Водночас ручні оптимізації залишаються актуальними при масштабуванні задач на великі обсяги даних. Результати роботи свідчать, що оптимальною стратегією є комбіноване застосування автоматичних і ручних SIMD-трансформацій, що дозволяє досягти балансу між продуктивністю, точністю та зручністю розробки, забезпечуючи ефективність і масштабованість програмних рішень у високопродуктивних обчисленнях і комп'ютерному моделюванні. Перспективи подальших досліджень пов'язані з розширенням експериментальної бази на різні архітектури процесорів, аналізом взаємодії SIMD-векторизації з іншими компіляторними трансформаціями та застосуванням ML-методів для адаптивного вибору оптимізаційних стратегій.

DOI 10.15276/imms.v16.no1.52
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 52-57

МАТЕМАТИКА В КІБЕРБЕЗПЕЦІ

І.І. Борисенко, Л.М. Тимошенко, І.С. Вінковська

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

Кількість користувачів мережі Інтернет зростає експоненціально кожного року. В той же час кожного дня з'являються десятки тисяч кіберзлочинців, які, використовуючи слабкі місця інформаційної системи, здатні викрадати дані, тому тема протистояння кібератакам є та буде актуальною зараз і, напевне, ще не одне десятиріччя. Сучасні технології з використанням математичного аналізу даних дозволяють протидіяти протиправним діям в мережі та характеризують наш сучасний етап розвитку. Кібербезпека – комплекс заходів, який спрямований на здійснення захисту різноманітних інформаційних систем та мереж від кібератак. Здійснення охорони даних базується на передових технологіях та методах захисту інформації, які в свою чергу базуються на фундаментальних знаннях математики. Саме такі розділи математики як логіка, комбінаторика, матричний аналіз, а особливо теорія графів, або графові технології, мають великий вплив та значення серед усієї кількості математичних методів. Стрункa система спеціальних термінів і позначень математики дозволяє просто і доступно описувати складні і тонкі речі як геометрично (графи), так і алгебраїчно (мариці). Аналіз наукових праць дозволив визначити основні напрями застосування властивостей, характеристик графів та графових алгоритмів в інформаційній та кібернетичній безпеці. Серед них виділено дослідження, пов'язані із застосуванням графів в інформаційних системах та у програмуванні, з моделюванням, аналізом та застосуванням графів атак, з криптографічними та стеганографічними перетвореннями, з побудовою дерева рішень у задачах прийняття рішень в умовах ризику і невизначеності. Увагу вчених і науковців привернули і інші математичні напрями. Цифрове зображення, яке в стеганографії обирається як контейнер, математично представляється матрицею. Повідомлення, яке вбудовується в контейнер, і не являється зображенням, можна представити в матричному вигляді, або виконати його препроцесінг, застосовуючи алгоритми роботи з послідовностями. Отже, широке застосування математики в інформаційній та кібербезпеці, математичний підхід до розробки нових та модифікації існуючих застосунків кібербезпеки робить обґрунтованим вибір та актуальність даного дослідження.

Ключові слова: математичні методи, кібербезпека, графові алгоритми, криптографія, стеганографія.

Вступ. У сучасному світі теорія графів є однією з актуальних та ефективних, серед математичних технологій, оскільки сфера її застосування охоплює різні області діяльності людства, зокрема у інформаційній та кібернетичній безпеці.

Аналіз наукової літератури свідчить про наявність глибокої зацікавленості вчених до проблеми використання графових технологій у кібербезпеці. Сформувалися наступні напрями застосування теорії графів:

- криптографічні перетворення за допомогою теорії графів;
- графи в стеганографії;
- графи в інформаційній системі та у програмуванні;
- моделювання;
- аналіз та застосування графів атак.

І це ще не повний перелік.

Не меншою популярністю та затребуваністю, особливо в стеганографії, користується лінійна алгебра, матричний аналіз та операції над послідовностями. А саме:

- використання систем алгебраїчних рівнянь [1,2];
- використання спектрального та сингулярного розкладу матриць [3-5];
- створення крипто-стеганографічних шифрів [6].

Постановка задачі. *Метою* роботи є аналіз та дослідження існуючих математичних методів, використання їх в області захисту інформації, визначення шляхів подальшого їх розвитку та використання в кібербезпеці.

Рамки роботи обмежені описом основних напрямків застосування графових технологій та матричного аналізу в інформаційній та кібернетичній безпеці.

Розглянемо питання щодо застосування графів в інформаційних системах.

Для розробки та опису схеми інформаційних потоків в інформаційній системі зручно використовувати теорію графів. Будують інформаційну систему як орієнтований граф, який містить скінченну кількість вузлів – це компоненти інформаційної системи, та дуг, які відображають інформаційні потоки, тобто взаємозв’язки між ними. Опис схеми інформаційних потоків можна змоделювати за допомогою маршрутів графа, послідовно перерахувавши: джерело інформації, проміжну апаратура та отримувача інформації, а також вид інформації, яка передається. Суміжність компонентів інформаційної системи буде визначати матриця суміжності, а матриця інцидентності – зв’язок між компонентами та інформаційними потоками. На основі даних цих матриць можна передбачити засоби захисту інформації, наприклад, розмежування доступу до інформації [3].

Велика кількість наукових досліджень присвячена розробці та удосконаленню моделей атак у вигляді графів для задач моніторингу кібербезпеки з метою захисту інформації.

В роботі [3] представлена графово - матрична модель супротивника інформаційно-технологічної системи для розробки методу перевірки стійкості системи захисту інформації до передбачуваної загрози.

Будується матриця суміжності зваженого графа інформаційної системи, на головній діагоналі якої знаходиться вага вершин, інші елементи це 1, якщо вершини зв’язані ребром і 0 в противному разі.

Розглядається можливий спосіб моделювання атаки з використанням сукупної моделі інформаційно-технологічної системи й супротивника. Припускається, що здійснення впливу супротивника буде спрямовано безпосередньо на засоби захисту (листки в графі системи), і вплив здійснюється членами-виконавцями організації супротивника. Атака моделюється, вводячи новий зв'язок між вершиною, відповідною до активного члена-супротивника, і тим листком у графі інформаційної системи, який відповідає атакованому засобу захисту, що відобразиться у збуренні матриці суміжності сукупного графа.

У статті [7] розглядається комплексна модель кібератаки на основі теорії графів, яка поєднує класичні уявлення щодо моделювання складних атак з розширеннями, що враховують залежності уразливостей окремих компонентів системи та мережевий статус компонентів. Наведено приклад оцінювання сценарію атаки та зроблено висновки щодо можливості застосування моделі для прогнозування наслідків атаки.

У роботі [8], на відміну [7], використовується орієнтований граф і на його основі побудовано графову модель противника інформаційної системи та показано, як зручне укладання графа, отримане завдяки розбивці графа на класи еквівалентності та порядку, може відігравати принципово важливу роль у вирішенні задачі знищення або обмеження діяльності злочинної групи.

В роботі [9] вирішено задачу підвищення ефективності стеганосистеми шляхом розробки модифікації методу вбудовування повідомлення, запропонованого в [10].

Підвищення ефективності вдалося досягти завдяки запропонованому методу знаходження максимального паросполучення, як основи алгоритму вбудовування повідомлень на основі теорії графів.

Основна частина. Розглянемо приклад, як можна застосувати розвинуту в стеганографії теорію графів до алгоритмів, які вже мають практичне застосування, тобто як і надалі можна розвивати практичну теорію графів.

В роботі [11] пропонується стеганографічний алгоритм просторової області вбудовування в цифрове зображення. Основним принципом розробки є мінімізація впливів вбудованого повідомлення на контейнер. В основу алгоритму покладено порівняння бітових послідовностей контейнера та повідомлення, модифікація елементів контейнера виконується тільки у випадку, коли виявлено неспівпадіння відповідних бітів. Алгоритм дозволяє зменшити викривлення контейнера, зберегти статистики першого порядку та забезпечити стійкість до найбільш відомих статистичних атак.

Повідомлення і пікселі контейнера розбиваються на підпослідовності. Початок підпослідовностей контейнера, в які вбудовується повідомлення, фіксуються в ключі *K*. Але саме цю задачу можна вирішити за допомогою графа.

Розглянемо, яким чином можна фіксувати за допомогою графа підпослідовності контейнера, в які вбудована інформація, яку треба передати адресату. Окрім цього, пропонується дублювати інформацію, яку треба переслати. За рахунок клонування відліків інформації, що вбудовується, алгоритм підвищить свою стійкість не тільки до статистичних але і до інших видів атак таких як, наприклад, зашумлення стегоконтейнера, а в окремих випадках до геометричних атак, таких як поворот та обрізання.

Вузли графа – це стартові відліки підпослідовностей контейнера, в які вбудоване повідомлення, ребра – показують, з якої вершини графа потрібно перемістити в іншу, а саме ту вершину, щоб одержати зв’язне повідомлення.

Оскільки є клони кожного відліку повідомлення, то граф буде представляти собою не ланцюг, а дерево – рис.1.

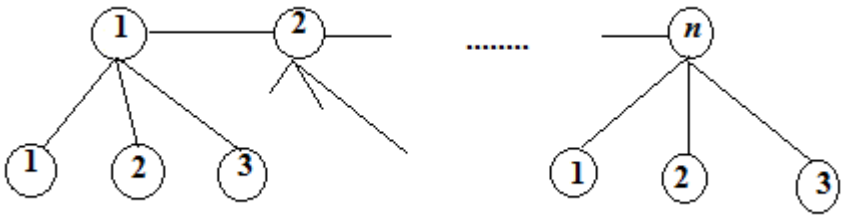


Рис. 1. Граф-дерево розміщення повідомлення

При декодуванні повідомлення, якщо ланцюг графа 1-2-…-*n* не дає зв’язного тексту (шум в каналі зв’язку або навмисно накладений шум, як атака на стегоконтейнер, інші види атак), то є можливість використати листи графа 11, 12 або 13 і так далі *n*1, *n*2, *n*3.

Дублювання окремих блоків інформації дещо перевантажує контейнер, але дає можливість протистояти атакам, які вносять збурення в контейнер, навіть помітні оку, наприклад, накладання шуму достатньо високого рівня, або ж геометричним атакам.

Характеристики алгоритмів, що оперують із графами, зазвичай дуже чутливі до способу їх представлення.

Однією з найбільш простих схем зберігання графа [12] є *таблиця зв'язків* - двовимірний масив, який має n рядків і m стовпців, де m — максимальна степінь вершин в графі $G=(X,E)$. Список суміжності $i-$го вузла зберігається в $i-$ рядку.

Дана схема зберігання надзвичайно проста при реалізації, доступ до списку суміжності чергового вузла — доступ до відповідного рядка матриці, модифікація графа приводить до зміни елементів відповідних рядків матриці без порушення

загальної структури (якщо при модифікації не змінюється m). Однак ця схема може бути надзвичайно неефективною, якщо велика кількість вузлів графа має степінь, меншу (значно), ніж вершина з максимальною степінню, оскільки її (схеми) вимоги до пам'яті визначаються як mn «збережених» елементів.

Найбільш зручною з погляду можливостей проведення модифікацій графа є схема, що використовує *поле зв'язків*. Дана схема містить три одновимірні масиви A, A_s, A_{ind}, перші два з яких мають довжини $2|E|$, останній — $|X|$. Значенням покажчика $A_{ind}(i)$ є початок списку суміжності $i-$го вузла в масиві A. Якщо $A(k)$ — це черговий сусід $i-$го вузла, то $A_s(k)$ — покажчик розташування наступного його сусіда в масиві A. Від'ємне значення $A_s(k)$ говорить про закінчення списку суміжності вузла, що розглядається.

Загальна довжина масивів при такому способі представлення графа — $4|E|+|X|$, що значно більше, ніж у першій схемі. Однак модифікація графа вимагає лише незначних змін у вже сформованій частині масивів.

Другий аспект використання математики в кібербезпеці – це розвиток матричного аналізу в стеганографії (спектральний і сингулярний розклад (SVD) матриці контейнера, в якості якого обирається зображення), який ґрунтовно і докладно представлено в [3].

Наприклад, в роботі [13] оцінюється збурення контейнера, при його стеганоперетвореннi, через оцінку збурень сингулярних чисел його SVD.

В роботі [5] досліджується і обґрунтовується зв'язок чутливості стегоповідомлення і збурень власних векторів матриці контейнера.

Ще одне суттєве використання математики – це застосування в криптографії таких інструментів як модулярні обчислення, теореми Ейлера та Ферма, застосування еліптичних кривих для створення цифрових підписів, використання однонаправлених функцій для хешування паролів та інші.

Розглянемо як можна відомий криптографічний шифр транспозиції модифікувати за допомогою математичних операцій над перестановками та адаптувати його до стеганографії. Оскільки транспозиційний шифр не змінює частоту окремих літер, він все ще сприйнятливий до частотного аналізу, хоча транспозиція дійсно усуває інформацію з пар літер. Тому подальший розвиток цього виду шифру є актуальним.

Для будь-яких перестановок μ і g визначена операція їх добутку $\mu \circ g$, а також операція перестановки оберненої до даної μ^{-1}.

Для реалізації алгоритму, що пропонується, потрібно вміти розв'язувати рівняння, елементами якого є перестановки. Розглянемо рівняння:

$$\mu \circ x = g \tag{1}$$

Оскільки існує така перестановка x для якої виконується рівність (1) і вона єдина, то розв'язком рівняння (1) є:

$$x = \mu^{-1} \circ g \tag{2}$$

До безпосереднього процесу вбудовування повідомлення потрібно виконати препроцесінг і самого повідомлення і контейнера, в якості якого виступає цифрове зображення в градаціях сірого, або ж синя складова кольорового зображення, оскільки зорова система людини менш чутлива до синього кольору.

Елементи повідомлення кодуються цифрами, які належать деякій множині $M = \{1, 2, ..., k\}$. Елементи контейнера послідовно групуються у блоки розміром $1x\ n$. При вбудовуванні повідомлення використовується деякий допоміжний масив *masiv*, в якому знаходиться k перестановок довжини n. Всі перестановки занумеровані. При вбудовуванні елемента повідомлення з кодом i в масиві *masiv* знаходимо перестановку з номером i, перемножуємо її на ключ μ, одержуємо перестановку g. Масив *masiv* не

містить перестановки, добуток якої з ключем μ дає тотожну перестановку. Блоки контейнера, які складаються з однакових елементів, випускаються. Елементи інших блоків переставляються згідно перестановці g тільки в тому випадку, якщо для будь-якої пари елементів, які обмінюються місцями, різниця їх значень не перевищує деяке число d.

Запропонований алгоритм не являється «сліпим», тому для декодування повідомлення потрібна наявність контейнера.

Щоб декодувати повідомлення треба розбити матрицю контейнера та стеганоконтейнера на блоки того самого розміру, що і при вбудовуванні. Порівняти відповідні блоки контейнера та стего, якщо вони співпали, то це означає, що в блок повідомлення не вбудовувалося. У противному разі треба обчислити перестановку μ^{-1}, обернену до ключа μ, та обчислити добуток $h = \mu^{-1} \circ g$. Одержану перестановку h знайти в масиві *masiv*. Порядковий номер, який відповідає h, є кодом елемента вбудованого повідомлення.

Висновок. Математика – це наука, яка дає широке розмаїття інструментів за допомогою яких можна створювати все нові, більш ефективні, методи захисту інформації. Тому її значення та застосування у різних напрямках наукових досліджень, зокрема у сфері інформаційної та кібернетичної безпеки, буде розвиватися і надалі.

В роботі проведено аналіз та дослідження деяких існуючих математичних методів та запропоновано два нових алгоритми, як практична реалізація можливостей математики для модифікації вже існуючих методів.

Розглянуті підходи до застосування теорії графів, матричного аналізу, дискретної математики в інформаційній та кібернетичній безпеці можуть бути впроваджені під час вивчення дисципліни «Математичні основи кібербезпеки», «Основи криптографії», «Основи стеганографії» та інших дисциплін для студентів спеціальності 125 Кібербезпека, а також при підготовці фахівців у процесі науково-дослідної роботи або курсової чи дипломної роботи.

Список літератури

1. Кобозева А.А., Коломийчук А.В. Стеганографический метод, основанный на решении систем линейных алгебраических уравнений. *Праці УНДІРТ*. 2006. №1(45). С. 104–108.
2. Борисенко И.И., Кобозева А.А. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений. *Праці УНДІРТ*. 2006. №3(47). С. 78–83.
3. Кобозева А.А, Хорошко В.А. Анализ информационной безопасности. К.: ГУИКТ, 2009. 251 с.
4. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах. *Вісник Східноукр. нац. ун-ту ім. В.Даля.* 2006. №9(103). Ч.1. С.74–82.
5. Нариманова Е.В., Кобозева А.А. Оценка чувствительности стегосообщений к возмущающим воздействиям. *Системні дослідження та інформаційні технології*. 2008. №3. С. 52–65.
6. Борисенко И.И., Трифонова Е.А. Система передачи секретных данных основанная на криптостеганографической технике. *Сучасний захист інформації*. 2020. №1. С. 58–61.
7. Моделювання кібератак засобами теорії графів/ В.А. Савченко та ін. *Сучасний захист інформації*. 2019. №4(40). С. 6–11.
8. Борисенко И.И. Еще один подход к моделированию противника информационной системы с использованием теории графов. *Информатика и математические методы в моделировании*. 2012. №1. С. 70–76.

9. Борисенко І.І., Вінковська І.С. Теорія графів як основа методів вбудовування інформації. *Математика та математичні методи в моделюванні*. 2025. Том 15, №1. С. 39–47.
10. Hetzl S., Mutzel P. A graph-theoretic approach to steganography. *Proc. Communication and Multimedia security.* 2005. P.119–128.
11. Борисенко І.І. Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень. *Сучасна спеціальна техніка*. 2014. №2. С. 110–115.
12. Харари Ф. Теория графов. М.: Мир. 1973. 300 с.
13. Борисенко И.И. Оценка возмущения контейнера при его стеганопреобразовании. *Високі технології в машинобудуванні*. 2015. №1. С. 27–32.

MATHEMATICS IN CYBERSECURITY

I.I. Borysenko, L.M.Timoshenko, I.S. Vinkovska

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

The number of Internet users is growing exponentially every year. At the same time, tens of thousands of cybercriminals emerge every day, who, exploiting the weaknesses of information systems, are capable of stealing data. Therefore, the topic of countering cyberattacks is and will remain relevant now and, most likely, for decades to come. Modern technologies using mathematical data analysis make it possible to counter illegal activities online and characterize our current stage of development. Cybersecurity is a set of measures aimed at protecting various information systems and networks from cyberattacks. The protection of data is based on advanced technologies and information security methods, which in turn are based on fundamental mathematical knowledge. It is precisely branches of mathematics such as logic, combinatorics, matrix analysis, and especially graph theory, or graph technologies, that have a significant influence and importance among all mathematical methods. The structured system of specialized mathematical terms and notations allows complex and subtle concepts to be described simply and accessibly, both geometrically (graphs) and algebraically (matrices). The analysis of scientific works made it possible to identify the main directions for applying the properties, characteristics of graphs, and graph algorithms in information and cyber security. Among them, research related to the use of graphs in information systems and programming, modeling, analysis and application of attack graphs, cryptographic and steganographic transformations, and building decision trees in decision-making tasks under conditions of risk and uncertainty was highlighted. The attention of scientists and researchers was also drawn to other mathematical areas. A digital image chosen as a container in steganography is mathematically represented by a matrix. A message embedded in the container, which is not an image, can be represented in matrix form, or preprocessed using algorithms for working with sequences. Thus, the extensive use of mathematics in information and cybersecurity, and the mathematical approach to developing new and modifying existing cybersecurity applications, makes the choice and relevance of this research justified.
Keywords: mathematical methods, cybersecurity, graph algorithms, cryptography, steganography.

DOI 10.15276/imms.v16.no1.58
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 58-73

РОЗРОБКА ЗАСТОСУНКУ ДЛЯ КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ІСТОРІЇ ВЕББРАУЗЕРА

М.В. Відін[1], О.А. Стопакевич[1], А.О. Стопакевич[2]

[1]Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[2]Державний університет інтелектуальних технологій та зв'язку
1, Кузнечна вул., Одеса, 65023, Україна
Email: stopakevich@gmail.com

Веббраузери є одним з основних джерел цифрових доказів в сучасній криміналістиці. Існуючі інструменти для криміналістичного аналізу профілів веббраузерів є недостатньо ефективними, оскільки відтворюють закладену в браузери модель даних, орієнтовану на швидкість рендерингу та оптимізацію роботи з окремими URL-адресами. Експерти-криміналісти змушені працювати з «сирими» списками, що містять тисячі записів, витрачаючи значний час на відтворення послідовності дій користувача, ручну фільтрацію технічних редиректів, трекерів, реклами та службових запитів. Мета роботи полягає у розробці алгоритмів та програмного застосунку для криміналістичного аналізу історії веббраузера Microsoft Edge, який трансформує розрізнені дані профілю у структуровану інформацію, придатну для оперативного виявлення інцидентів та реконструкції дій користувача. В основу розробки покладено перехід від класичної URL-орієнтованої моделі (характерної для структури баз даних Chromium) до хост-орієнтованої моделі представлення даних. Цей підхід дозволяє агрегувати тільки значимі артефакти активності (історію відвідувань, файли cookie, завантажені файли тощо) в хронологічному порядку навколо унікального імені хоста. Архітектурно рішення розділене на дві частини: модуль збору та агрегації даних, реалізований мовою Python з використанням асинхронних запитів для швидкої обробки масивів інформації, та модуль візуалізації на базі бібліотеки Webix, що забезпечує високу продуктивність інтерфейсу при роботі з великими даними. Графічний інтерфейс застосунку дозволяє експерту проводити багатопріоритетне сортування та фільтрацію записів за багатьма критеріями. Особливу увагу приділено візуалізації ланцюжків переходів, що дає змогу відтворити послідовність дій підозрюваного на конкретному ресурсі. Тестування підтвердило здатність застосунку швидко обробляти дані та виявляти релевантні докази, значно скорочуючи час, необхідний для експертизи, порівняно зі звичайним ручним аналізом «сирих» даних. Він забезпечує наочне представлення цифрових доказів та мінімізує ймовірність пропуску важливої інформації під час розслідувань.

Ключові слова: криміналістика; аналіз; браузер; історія; профіль; агрегація; застосунок; хост-орієнтована модель даних; SQLite; JSON; Python; JavaScript; Webix.

Вступ. Дослідження в галузі цифрової криміналістики веббраузерів переважно зосереджуються на аналізі та відновленні збережених в них даних з метою ідентифікації та збору важливих доказів щодо онлайн-поведінки об'єкта розслідування. Практично всі дії, які здійснює підозрюваний під час використання веббраузера, можуть залишити сліди на його комп'ютері. Тому вивчення цих доказів на пристрої підозрюваного може надати цінну інформацію для слідчих. Вилучення таких даних, як історія, файли cookie, списки завантажень, кеш, збережені паролі з веббраузера проводиться за допомогою спеціальних програмних засобів, огляд найбільш поширених з яких приведено в [1].

Зараз експерти-криміналісти мають вручну аналізувати велику кількість вебадрес (URL адрес), які зберігаються в профілі браузера. Їх доволі важко аналізувати вручну, оскільки типовий користувач відвідує від 100 до 500 сайтів на місяць в залежності від його сфери професійної діяльності, а кількість URL, звісно, буде в рази більшою.

Ручний аналіз історії браузера за місяць активності може займати у експерта від 4 до 8 годин робочого часу. Існуючі інструменти часто видають технічні таблиці, які містять перелік URL в хронологічному порядку. Для роботи з деякими програмами потрібні знання про структуру протоколів, вебпрограмування, будову браузерів тощо для правильної інтерпретації. Значний час уходить на фільтрацію сміттєвих вебадрес, реклами, трекерів, технічних редіректів тощо.

Основна причина полягає в тому, що внутрішній формат зберігання даних в браузерах розроблено виходячи з критеріїв швидкості виконання певних функцій. Основною одиницею даних є URL. Це зручно для браузера, наприклад, щоб виділити покликання, які були вже відвідані чи продовжити URL при введені його початку в адресний рядок. Проте не зручно для користувача який отримує перелік URL, які відкривав браузер, без систематизації й з сортуванням за датою останнього виклику. Бази даних профілю з метою пришвидшення не застосовують механізми забезпечення цілісності – ключі, вбудовані процедури, перевірки тощо. При цьому докладна інформація для оперативного доступу зберігається тільки для URL, які відвідувались за останні 3 місяця. Інформація про URL, останній доступ яких був понад три місяця, стирається з основних таблиць, але залишається в другорядних. Оскільки формат зберігання орієнтований на ефективність браузера, то єдиним шляхом зробити її ручним для людини є спеціальна обробка даних, агрегація зі зміною основної одиниці, що наявні утиліти не роблять.

Як універсальні програми для збору доказів, для яких аналіз даних профілів – лише одна з функцій, так й спеціалізовані утиліти для цієї задачі, у цілому недостатньо зручні. Вони просто представляють дані, виходячи зі схем, в яких вони зберігаються в профілі браузера. Як правило як перші, так й другі видають "сирі" списки URL, лишаючи інтерпретацію людині. При цьому ряд утиліт навіть не мають графічного інтерфейсу й призначені щоб експортувати дані в Excel, XML, HTML тощо.

Ця робота присвячена розробці застосунку, який дозволяє аналізувати активність користувача браузера більш зручним чином, ніж це пропонується в наявних програмних застосунках. Це дозволить оптимізувати процес: зменшити кількість часу на аналіз й скоротити ймовірність пропуску важливих даних.

Мета та задачі дослідження. Мета дослідження – розробити необхідні алгоритми та зробити принципові програмні рішення, які пов'язані з перетворенням інформації, яка зберігається в профілі веббраузера у інформацію, яка за схемою даних та видом представлення є більш структурованою та придатною для криміналістичного аналізу. Як веббраузер виберемо Microsoft Edge під ОС Microsoft Windows.

Задачі дослідження.

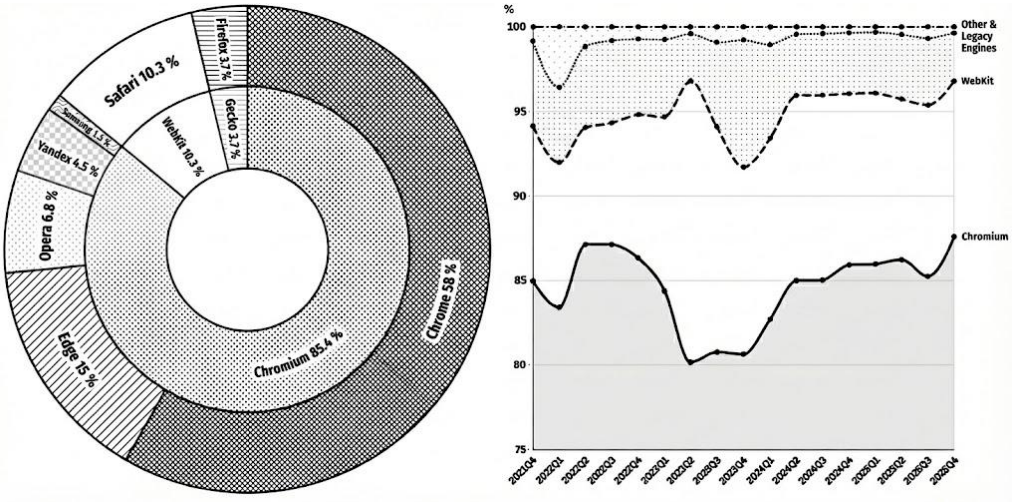
1. Короткий огляд архітектури сучасних браузерів на платформі Chromium.
2. Короткий огляд принципів роботи та функціональних можливостей наявних застосунків для аналізу профілів користувачів.
3. Формулювання переліку вимог до нового застосунку.
4. Вибір необхідних інструментів та бібліотек для виконання задачі розробки застосунку.
5. Розробка частини збору даних застосунку.
6. Розробка частини візуалізації застосунку.
7. Тестування застосунку на реальному профілі веббраузера.

Архітектура сучасних браузерів на платформі Chromium. Браузери на базі платформі Chromium найбільш популярні світі. Розподіл користувачів браузерів на початок 2025 р. й за останні 4 роки проілюстрований на рис. 1.

Якщо аналізувати певні тенденції, то можемо виявити наступні: доля браузерів на платформі Chromium ~ 85% й зростає; лідирує Chrome, Edge, Safari; втрачає позиції Firefox. Користувачі Safari – це користувачі пристроїв Apple, а користувачі Firefox – це

значною мірою користувачі Linux, деякі ІТівці й ті, хто прагне бути незалежними від великих корпорацій.

Технічно всі браузери на платформі Chromium мало відрізняються один від одного [2]. Все, що стосується основи — рендерингу, історії, кукі (cookies), обраного, внутрішніх настройок в них ідентично. Проєкт Chromium є формально незалежним й розробляє відкритий програмний код, який розробники браузерів (Google, Microsoft, Opera Software тощо) на базі цієї платформи доповнюють своїми патчами й додатковими модулями. Розробники браузерів додають різноманітний функціонал, наприклад інтеграцію двигуна ШІ, прив'язки акаунту до певних сервісів розробника браузера, синхронізацію даних між браузерами одного користувача на різних пристроях, підтримку VPN/оптимізатора/фільтру трафіку, підвищення рівня захисту, ефективності використання ресурсів тощо.



а) DataReportal 2025 р. б) StatCounter 2021-25 рр.

Рис.1. Розподіл між браузерами серед користувачів України

Браузер Edge має певні переваги, які проявляються переважно тільки в ОС Windows: тісна інтеграція з Windows, Office, Microsoft 365, економія батареї, економія ресурсів ОС, SmartScreen, ізоляція вкладок (більш безпечний механізм, ніж Sandbox реалізований в Chrome), Copilot як ШІ-помічник, найбільша кількість функціональних можливостей графічного інтерфейсу в порівнянні з аналогами. Достатньо об'єктивне та повне порівняння Edge та Chrome може бути переглянуте за [3]. Огляд можливостей інших браузерів на платформі Chromium приведений в [4].

У цілому в профілі браузерів на платформі Chromium основна інформація про відвідування зберігається в форматі баз даних SQLLite, а про настройки браузерів – в JSON. Частина даних (локальне сховище сайтів тощо) зберігається в інших форматах, наприклад IndexedDB. Схема зберігання даних кожного браузера зазвичай додає певні параметри й дані, але не видаляє й не змінює сенс тих, які реалізуються в вихідному коді платформи Chromium. Детальний огляд схеми даних браузера Edge, проведений нами в [1].

Принципи роботи та функціональні можливості наявних застосунків для аналізу профілів користувачів. Проблема безпеки даних, які зберігаються в даних, розглянута в [5]. Автори показують, що майже всі популярні браузери (крім Tor) зберігають критично важливі дані у домашніх директоріях без особливого захисту. Механізми шифрування паролів і cookies можна обійти, а HTTPS – зламати шляхом ін’єкції шкідливих кореневих сертифікатів. Таким чином, якщо є доступ до акаунту Windows користувача, отримати весь зміст профілю з домашньої папки не є складною задачею. Значною мірою

застосування стандартних підходів до зберігання й шифрування даних в профілі пояснюється тим, що вихідний код браузерів на базі платформ Chromium, WebKit, Gecko є загальнодоступним. Велика кількість можливостей сучасних браузерів, які застосовуються не тільки для сайтів, але й для реалізації застосунків з графічним інтерфейсів на десктопі та мобільних пристроях, призводить до потенційних вразливостей. В зазначеній роботі приведені приклади кібератак, які їх можуть експлуатувати.

Вилучати дані з профілю браузера можна 4 основними типами інструментів:

– спеціальні утиліти (в тому числі написані власноруч) , які збирають дані й записують їх в один з зручних форматів (Excel, HTML звіт тощо);

– утиліти для доступу до даних різних форматів (графічне середовище для роботи з БД SQLite, спеціалізовані редактори JSON, аналізатори дампу пам'яті тощо);

– комплексні застосунки для збору криміналістичних даних з ОС та різних програм, встановлених на диску користувача;

– спеціальні утиліти з графічним інтерфейсом, які призначені для роботи з профілями (повністю чи з конкретним аспектом) конкретних браузерів.

Огляд на наш погляд найбільш зручних утиліт трьох типів для браузерів на платформі Chromium проведений як в роботі [1], так і в роботах [6-8]. В цих роботах розглянуті програми для комплексного збору доказів й інші спеціальні утиліти, виділені основні їх можливості та зроблений порівняльний аналіз.

Формулювання переліку вимог до нового застосунку. Наша мета – розробити новий застосунок для роботи з профілями браузера Edge під ОС Windows, в якому за базу класифікації інформації з якою працює користувач буде взято ім'я хоста. Тому перед видаванням інформації в графічний інтерфейс користувача необхідно провести попередню агрегацію: сформувати на базі розкиданих даних цілісну базу даних для аналізу, яка буде зручною для перегляду та роботи. Застосунок має відповідати наступному переліку вимог:

– в основному орієнтація на ОС Windows, проте адаптація для других популярних ОС має бути тривіальною;

– інтерфейс має бути зрозумілим будь-якому IT-спеціалісту, неочевидні питання мають бути розкриті в довідці, яка доступна безпосередньо в інтерфейсі;

– основна мова – українська, якщо застосовуються невідомі англомовні терміни/скорочення, то їх пояснення українською мовою має реалізуватись через підказку при наведенні (tooltip);

– можливість швидкої роботи з даними обсягом до 50 тис. хостів й 500 тис. URL;

– результатом парсингу БД та JSON файлів профіля є JSON файл з агрегованими даними;

– частина візуалізації має виконуватись на Desktop й дозволяти відмічати цікаві та нецікаві записи й зберігати помітки при перезавантаженні сторінки/браузера;

– частина візуалізації має забезпечити швидку та зручну роботу з даними, що передбачає реалізацію функцій сортування (в тому числі багатопріоритетне) й фільтрування даних;

– частина візуалізації має мати адаптивний інтерфейс, який враховує можливості екрана в межах розмірів Desktop (мобільна версія чи версія для планшетів не передбачається);

– частина візуалізації має складатись з 4 вкладок: "Відвідування" (таблиця хостів + інформації про сесії відвідування їх URL за запитом), "Пошукові запити" (запити пошукових систем), "Про користувача" (інформація про акаунт, паролі, мовні вподобання), "Профіль" (контрольні суми, розмір, статистична інформація про файли профілю).

Вибір необхідних інструментів та бібліотек для виконання задачі розробки застосунку. В основу застосунку покладена хост-орієнтована модель представлення

даних. На відміну від оригінальної, URL-орієнтованої структури Chromium, ця модель агрегує всі розрізнені артефакти (історію, файли cookie, дані форм, кеш) навколо імені хоста. Це значно підвищує зручність, швидкість та глибину аналізу, дозволяючи аналітику-криміналісту отримати повну картину взаємодії користувача з кожним сайтом. Таким чином, застосунок розділяється на дві частини: частини збору та агрегування інформації та частину візуалізації з функціями пошуку, яка працює не з даними профілю, а з агрегованою інформацією.

Застосунок розділимо на дві окремі частини, які будуть реалізовуватись різними мовами програмування: частину агрегації та частину графічного інтерфейсу.

Перша частина застосунку реалізує набір алгоритмів для вилучення, очищення, перетворення та агрегації даних з профілю браузера у описаний специфікований формат JSON. Модуль враховує реальні проблеми цілісності даних, усуває неінформативний «шум» (локальні адреси, дані розширення) та додає інформацію, пов'язану з геолокацією хоста. Для реалізації першої частини застосунку будемо використовувати дистрибутив Anaconda на базі Python 3.12.

Серед стандартних бібліотек будемо використовувати: asyncio для ефективної роботи з сотнями одночасних мережевих з'єднань, datetime, ipaddress для перевірки зони (локальна, глобальна) IPv4, json, os, re, socket, sqlite3, typing, urllib для розбиття URL на компоненти (схема, хост, порт, шлях, параметри) й для нормалізації та перевірки їх коректності.

Серед нестандартних бібліотек будемо використовувати: Cipher – для вилучення паролів з профілю, ifaddr для визначення переліку IP-адрес мережевих карт, задіяних ОС, maxminddb для роботи з локальними геолокаційними базами даних MaxMind, pythonping для реалізації ping-запитів з можливістю настройки припустимого часу та інших параметрів, simple_cache для кешування результатів виконання витратних за часом функцій (мережевих запитів), для виклику криптографічних функцій Windows з метою дешифрації паролю.

Друга частина реалізує вебінтерфейс для візуалізації та аналізу отриманих даних. Для реалізації вебінтерфейсу будемо застосовувати мову JavaScript з комплексною бібліотекою компонентів, оскільки нам потрібно реалізовувати інтерфейс десктоп-застосунку. Основним компонентом є таблиця даних, зміст якої має генеруватись динамічно при прокрутці з метою підвищення ефективності роботи. Прокрутка, фільтрація, сортування з даними обсягами в десятки тисяч записів має бути миттєвою. У цілому критеріями для вибору бібліотеки графічних компонентів будуть:

- наявність ключових компонентів та їх функціональні можливості;
- продуктивність таблиць: віртуалізація, ефективність застосування DOM браузера, підтримка великих даних й рівень масштабованості;
- потрібний функціонал має бути безкоштовним й не ставити вимоги до програмного коду, який використовує бібліотеку;
- розмір бібліотеки;
- наявність додаткових інструментів, які спрощують розробку;
- можливості стилізації;
- якість документації.

Проведений порівняльний аналіз ряду бібліотек (Webix, Kendo UI, Ext JS, DevExtreme тощо) зупинив наш вибір на Webix. Згідно з даними дослідження [9] datatable цієї бібліотеки забезпечує порівняний з іншими рішеннями рівень продуктивності й відповідає вимогам масштабованості. Теж саме підтверджується в експериментальному дослідженні українських вчених [10]. В цілому Webix, безкоштовна версія, має достатню для наших задач функціональність.

Розробка частини збору даних застосунку. Схема даних для збору інформації, орієнтована на хост проілюстрована на UML-діаграмі класів (рис. 2).

Заповнення цієї схеми виконується згідно з розробленим алгоритмом.

Алгоритм виходить з визначення глобального IP, коректного хоста та коректного url.

Глобальний IP – це IP, який: 1) є коректною IPv4 адресою; 2) не є IP адресою адаптерів внутрішньої мережі; 3) не входить до переліку внутрішніх адрес, на кшталт 0.0.0.0, 127.0.0.1, 192.168.. тощо.

Коректний хост – це хост, який: 1) якщо містить IP, то це глобальний IP; 2) якщо це ім'я, то воно посилається на глобальний IP; 3) не містить ідентифікатор модуля Edge, тобто не відповідає "^[a-z]{32}$"; 4) не є внутрішньою сторінкою Edge, тобто не входить до переліку: "about", "edge-urls", "accessibility", "apps", "app-service-internals" тощо.

Коректний URL – це URL, який: 1) починається зі схеми http / https / ftp; 2) містить ім'я хоста чи ipv4 адресу й цей хост коректний; 3) у цілому відповідає структурі RFC 3986.

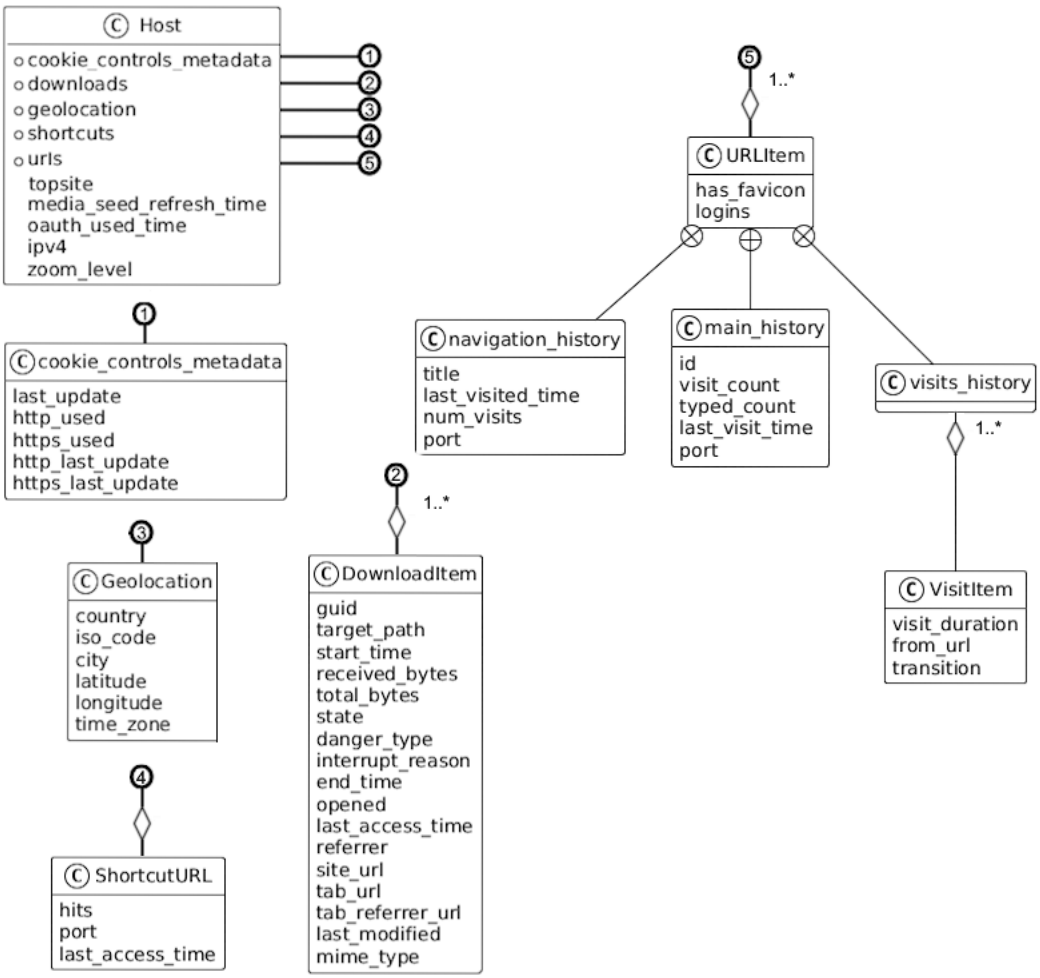


Рис. 2. UML діаграма схеми даних, яку заповнює парсер

Кроки виконання алгоритму.

К1. Збір усіх унікальних URL адрес з баз даних. Для цього застосовується SQL команда SELECT DISTINCT. Вибірка проводиться з webassist.navigation_history.url, history.urls.url, favicons.icon_mapping.page_url, topsites.top_sites.url.

К2. Виділення коректних URL та хостів. Для цього виконується.

1. Формування об'єднаного переліку всіх URL all_url_list з видаленням дублікатів.
2. Розділення переліку на перелік коректних та некоректних URL.
3. Виділення з переліку коректних URL переліку унікальних хостів з портами.
4. Розділення переліку на перелік коректних та некоректних хостів з портами.
5. Видалення хостів відомих трекерів, рекламних систем тощо.

6. Видалення локальних IP адрес та хостів, з ними пов'язаних. IP адреси збираються з кожного мережевого пристрою з використанням функцій бібліотеки ifaddr. Далі вони перевіряються на доступність за допомогою ping (бібліотека pythonping). Останній етап - отримуються хости, пов'язані з IP за допомогою socket.gethostbyaddr(ipaddr).

К3. Заповнення словника search_queries_dict переліком запитів до пошукових систем (Google, Bing тощо). Запити отримуються шляхом декодування URL, в яких записані пошукові запити в форматі RFC 1738. Всі додані в словник URL видаляються з зібраних первинних даних.

К4. Заповнення словника site_dict первинними даними відносно хостів (за рис. 2)

К5. Завантаження з файлу JSON preferences інформації про останні оновлення кукі відносно наявних хостів (з врахуванням протоколу). Конкретні значення кукі не завантажуються. Це нам дозволяє отримати дату останнього відвідування хоста.

К6. Завантаження з файлу JSON preferences збережених режимів масштабування для кожного хоста. Збереження величини проводиться в поле zoom_level запису про хост в словнику. Це непрямий вказівник на те, що інформація користувачем уважно читалась.

К7. Завантаження з файлу JSON preferences часу авторизації та URL з якого була проведена авторизація за механізмом OAUTH. Збереження часу проводиться в поле oauth_used_time запису про хост в словнику site_dict.

К8. Завантаження з таблиці БД topsites.top_sites переліку найбільш відвідуваних сайтів. Збереження результату проводиться в topsite запису про хост в словнику site_dict.

К9. Завантаження з БД history.downloads переліку збережених завантажень. Збереження результату проводиться в поле downloads запису про хост в словнику site_dict.

К10. Завантаження з БД media_device.media_device_salts переліку хостів, яким дозволено доступ до мультимедіа пристроїв. При обробці треба звернути увагу, що в storage_key може бути присутньо одночасно декілька хостів через ^0. Наприклад, це може бути https://linguacoach.appspot.com/^0https://pronunciationchecker.com. Збереження дати останньої генерації солі проводиться в поле media_seed_refresh_time запису про хост в словнику.

К11. Отримання для всіх хостів з доменними іменами IP адрес з використанням стратегії асинхронного отримання IP-адрес для списку доменних імен з обмеженням швидкості запитів, паралельним виконанням та кешуванням результатів.

Отримання IP адрес проводиться наступним чином:

1. Ініціалізація об'єкта обмеження швидкості (AsyncRateLimiter):
   - приймає регламент роботи "Token Bucket";
   - запускає фоновий цикл поповнення токенів (_refill_loop) через asyncio.create_task();
   - поповнення відбувається кожні 0.1 сек з інкрементом rate_per_sec * 0.1;
   - метод acquire() блокує виконання до отримання токена через цикл перевірки з asyncio.sleep(0.005).
2. Підготовка даних у resolve_hosts_ipv4_async:
   - уніфікація списку хостів зі збереженням порядку через dict.fromkeys();
   - розділення на кешовані/некешовані хости з використанням глобального словника dns_cache;
   - ініціалізація DNS-резолвера бібліотеки dns
     ```
     resolver = dns.asyncresolver.Resolver(configure=False)
     resolver.nameservers = [dns_server]
     ```
3. Паралельне встановлення відповідності (резолвінг):
   - створення семафора asyncio.Semaphore(concurrency) для обмеження одночасних запитів;
   - запуск асинхронних worker'ів через asyncio.create_task() для кожного некешованого хоста;

- використання asyncio.gather() для очікування завершення всіх задач.

4. Обробка результатів:
   - для IP-адрес прямим записом у результати (резолвінг не потрібен), дані мають фільтруватись на вході, це для безпеки;
   - для доменів – виклик_resolve_one з очікуванням токена limiter.acquire() та асинхронним запитом до DNS через resolver.resolve(host, 'A').
5. Збереження результатів у кеш за допомогою simple_cache.save_key().
6. Завершення роботи:
   - зупинка обмежувача через limiter.close() з відміною задачі_refill_task.cancel();
   - об'єднання кешованих і нових результатів.

В результаті отримаємо словник формату {хост: IPv4-адреса}.

К12. Отримання інформації щодо геолокації хостів з використанням локальної БД. При наявності нової версії БД програма має її завантажувати. Запити мають кешуватись. Збереження результату проводиться в поле geolocation запису про хост в словнику site_dict.

К13. Заповнення полів navigation_history, main_history, favicon за наявності інформації про відповідний запис URL, який створюється в запису відповідного хоста в словнику site_dict.

К14. Завантаження з БД history переліку відвідувань, який записується за наявності інформації в відповідний запис URL, який створюється в запису відповідного хоста. Необхідний SQL-запит наступний:

```
SELECT
u.url         AS url,
v.visit_time  AS visit_time,
printf('%d:%02d:%06.3f',
    cast((v.visit_duration/1000000) / 3600 as integer),
    cast(((v.visit_duration/1000000) % 3600) / 60 as integer),
    (v.visit_duration/1000000.0) % 60.0
) AS visit_duration,
COALESCE(u_from.url, '')  AS from_url,
v.transition as transition
FROM visits v
JOIN urls u ON u.id = v.url
LEFT JOIN visits v_from ON v_from.id = v.from_visit
LEFT JOIN urls u_from ON u_from.id = v_from.url
ORDER BY u.url, v.visit_time DESC;
```

К15. Завантаження з БД shortcuts лічильників ручного введення адреси, який записується за наявності інформації в відповідний запис URL, який створюється в запису відповідного хоста. Необхідний SQL-запит наступний:

```
SELECT url, SUM(number_of_hits) as noh, max(last_access_time) as lat
FROM omni_box_shortcuts WHERE keyword=""  GROUP BY url ORDER BY noh
DESC
```

К16. Завантаження з БД logindata переліку збережених паролів, якщо дослідження проводиться з використанням облікового запису користувача.

Спочатку завантажуємо ключ з файлу Local State

```
with open(storage_path + "Local State", 'r') as file:
    enc_key = json.loads(file.read())['os_crypt']['encrypted_key']
enc_key = base64.b64decode(enc_key)
enc_key = enc_key[5:]
dec_key = win32crypt.CryptUnprotectData(enc_key, None, None, None,
0)[1]
```

Далі отримуємо пароль для потрібного значення поля password_value таблиці logins

```
cipher = AES.new(dec_key, AES.MODE_GCM, nonce=enc_pwd[3:3+12])
```

```
dec_password=cipher.decrypt_and_verify(enc_pwd[3+12:-16], enc_pwd[-16:])
```

К17. Створення словника user_data_dict.

К18. Запис в словник інформації про файли досліджуваного профілю (дата, розмір, контрольна сума).

К19. Завантаження з файла за json_preferences_path інформації про власника акаунта Microsoft, який підключений до Edge.

К20. Завантаження з JSON файла preferences інформації про мовні вподобання користувача.

К21. Завантаження з JSON файлу preferences інформації про закладки користувача.

К22. Завантаження з БД shortcuts інформації про пошукові запити користувача. SQL-запит має наступний вигляд:

```
SELECT url, contents, keyword, SUM(number_of_hits) as noh, max(last_access_time) as lat
FROM omni_box_shortcuts WHERE keyword!="" GROUP BY url ORDER BY noh DESC
```

В БД зберігаються лише дані за 3 місяця. Але цей перелік можна об'єднати з інформацією, яка записана в search_queries_dict за весь період профілю (вилучити запити з URL хостів пошукових систем, які не мають обмежений термін збереження).

К23. Агрегація даних зі словників таким чином, щоб записати інформацію про відвідування URL завантаження в хостах в хронологічному порядку за сесіями з розшифровкою кодів transition (причина переходу).

К24. Запис агрегованих даних в JSON файл для подальшої роботи через графічний інтерфейс.

Розробка частини візуалізації застосунку. Графічний інтерфейс застосунку має бути зручним робочим інструментом для криміналіста та спеціаліста з кібербезпеки, який виконує низку задач, які необхідні для дослідження. Основна мета застосунку - візуалізація даних, кількість яких може бути доволі значною. Застосунок має виконуватись на ПК (Desktop).

Серед великої кількості відвіданих URL цікавими можуть виявитись доволі небагато. Якщо криміналіст знає що шукати (час, сайти), то система фільтрів має допомогти якнайшвидше отримати позитивний результат. Якщо ж ні, то система фільтрів має дозволити не заблукати в безлічі непотрібної інформації. Застосунок не має передбачати виконання якісь інтелектуальних операцій, його задача - знайти цікаві записи вручну. Подальший їх аналіз – це вже справа людини-спеціаліста.

Деталізуємо зміст 4 вкладок інтерфейсу, перелік яких зазначений в вимогах.

Вкладка "Відвідування" має містити:

1. таблицю з інформацією про хости, яка має:
   - поля: хост, статус, дата останнього відвідування (час відображається в підказці при наведенні), кількість візитів, локація фізичної точки доступу (Access Point), IPv4 адреса, кількість завантажень, наявність в топ 20 (признак), коефіцієнт масштабування, наявність авторизації (признак), наявність авторизації через OAUTH (признак), дозвіл на застосування мультимедіа пристроїв (признак), введення з адресного рядка хоча би в одному випадку (признак);
   - багатопріоритетне сортування з врахуванням типу даних, яке за замовчуванням ведеться по даті останнього відвідування в зворотному порядку;
   - відображати всі дані без розбивання на сторінки;
   - дозволяти отримати інформацію про IP адресу/Геолокацію за допомогою наявних сервісів шляхом клацання по відповідній комірці запису;

- можливість встановлювати позначку для кожного запису прямо в таблиці: цікаво, не цікаво, не дивився;
- можливість відкривати інформацію про відвідування конкретного хоста

2. фільтри для таблиці з інформацією про хости, які розділяються на:
   - бінарні (показувати/не показувати): цікаві, переглянуті, не переглянуті, поза TOP 20, без логіну (тобто такі, на які користувач не авторизувався);
   - інтервальні (дата з, дата по);
   - текстові з використанням регулярних виразів (хост, заголовок, IP);
   - інші (країна фізичної точки доступу хоста тощо).
3. деревовидну таблицю з інформацією про відвідування URL з хоста, яка:
   - заповнюється коли обирається конкретний хост в таблиці (клацають по його імені);
   - візуалізує ієрархію виду сайт -> ланцюжок -> url;
   - є меншою за висотою таблиці з інформацією про хости, проте може бути за потреби розширена на весь екран;
   - відображає за допомогою дерев інформацію, відсортовану за ланцюжками відвідувань в зворотному хронологічному порядку;
   - в кожному ланцюжку відображає шлях URL, заголовок сторінки, додаткову інформацію з поясненнями, час відвідування кожного URL та фінальний час відвідування ланцюжка;
   - дозволяти користувачеві перейти на певні сторінки клацанням, але з попередженням про необхідність зробити це обмірковано.
4. фільтри для деревовидної таблиці з інформацією про відвідування URL з хоста за заголовком та URL.

   Вкладка "Пошукові запити" має містити таблицю, яка:

- містить поля: запит, статус, дата, кількість запитів, пошуковик;
- відображає всі дані без сторінок;
- дозволяє реалізувати текстовий пошук по запитам;
- дозволяє робити вибірку по окремому статусу та пошуковику;
- дозволяє проводити багатопріоритетне сортування.

Вкладка "Про користувача" має містити 4 таблиці:

- параметри акаунта Edge;
- збережені паролі (візуалізувати не потрібно, але при необхідності вони можуть бути скопійовані в буфер обміну);
- мовні вподобання (мова, кількість переглядів, кількість перекладів),
- закладки.

Вкладка "Профіль" має містити таблицю "Зміст досліджуваного профілю" з інформацією про файли профілю, з яких отримано інформацію з такими полями: назва елементу, шлях, тип (папка/JSON/SQLite), дата створення та останньої зміни, хеш файла в форматі SHA-256.

При проєктуванні графічного інтерфейсу будемо орієнтуватись на застосування на десктоп моніторах. Це означає наявність монітору, який працює в альбомній розгортці з відношенням роздільної здатності близьким до 16:9.

Як базу візьмемо класичний інтерфейс з білим фоном. Шрифт – Roboto або будь-який інший sans-serif. Базовий розмір– 16 px (~12 pt в нормальному масштабі). Стандартний колір шрифта – чорний. Стандартний колір елементів впливу – світлоголубий (#1CA1C1). Стандартний колір рядку заголовків таблиці – світлофіолетовий (#F4F5F9).

У цілому за базу візьмемо стандартне оформлення компонентів з таблиці стилів webix без особливих налаштувань. Як джерело графічних іконок будемо застосовувати

іконки з колекції Material Design (mdi) [11]. Як джерело іконок, реалізованих за допомогою шрифта, будемо застосовувати іконки з колекції Font Awesome (fa) [12].

Ми маємо розробити 4 екрани, які будуть в межах одного вікна. Для перемикання між екранами використаємо вкладки (Tabs), проте не стиснені, а розгорнуті на весь екран. Ці вкладки будуть розміщуватись зверху 4 екранів, підкреслення буде ідентифікувати саме на якій вкладці ми зараз знаходимось.

Перевірка роботи застосунку на тестовому профілі. На комп'ютері з початку травня 2025 р. була встановлена операційна система Windows з браузером Edge, яка надалі оновлювалась автоматично. Профіль накопичувався з травня до кінця вересня 2025 р. В той час працювала 132 версія браузера. Протягом зазначеного періоду переглядались новини, читалась пошта, проводилась покупка техніки, робились пошукові запити та відвідувались сайти з метою опановування асемблера x86, системи верстки Typst. З кінця серпня частково в цьому браузері шукалась та читалась інформація, пов'язана за тематикою магістерської роботи.

Після збору інформації були сформовані два JSON файли, які містять інформацію про 216 хостів та 103 пошукових запита.

Далі з цими даними можна працювати через візуальну частину застосунку.

Копія екрана з вікном користувача після запуску візуальної частини застосунку показана на рис. 3.

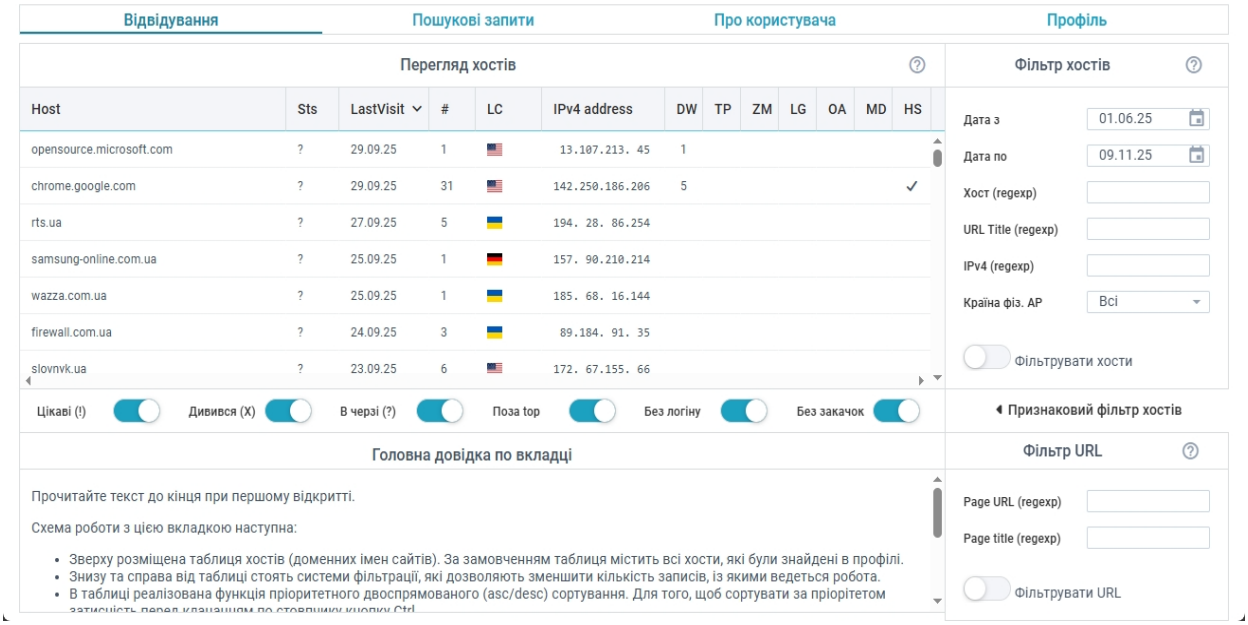


Рис. 3. Вікно інтерфейсу користувача після першого завантаження інформації, зібраної з профіля

В першому рядку показаний загальний заголовок застосунку з його назвою та інформацією про розробника.

В другому рядку показані доступні вкладки (таби) й відмічено що зараз відкрита вкладка "Відвідування".

В третьому рядку розміщена сітка 5x2. В подальшому будемо посилатись на її елементи як (рядок, стовпець).

В (1,1) і (1,2) сітки розміщені заголовки фреймів. В (2,1) розміщена таблиця з повним переліком хостів.

В заголовку таблиці "LastVisit" показано спрямування вниз, що означає сортування в зворотному (desc) порядку. IP адреси відображені так, щоб було зручно виділяти октет чи групи октетів в адресі (сортування за потребою проводиться послідовно за октетами). Бачимо, що з двох хостів були скачані файли (DW), а при

введенні chrome.google.com застосовувалась підказка в адресному рядку, тобто адреса вводилась вручну.

В (2,2) розміщені небінарні фільтри таблиці хостів, за замовчуванням вони всі відключені одним вимикачем. Інтервал встановлюється за замовчуванням від першого знайденого запису до поточної дати.

В (3,1) розміщені бінарні фільтри таблиці хостів. Вони реалізовані як окремі вимикачі й за замовчуванням всі знаходяться в стані "увімкнено" (1).

В (4,1) розміщено інформаційне повідомлення для користувача, приведене в повному вигляді в попередньому підрозділі.

В (4,2) розміщені фільтри для URL. Вони також, як і в (3,1) мають один вимикач.

Для відмічення цікавих сайтів середи тих, в яких була авторизація, встановимо фільтр для їх відображення. Відмітимо, наприклад, не знімаючи фільтр, як цікаві хости discord.com і rozetka.com.ua, а як нецікаві – my.plag.com.ua і account.ukr.net. В результаті ці зміни будуть зафіксовані на екрані й відновляться при наступному запуску. Результат вибірки показаний на рис. 4.

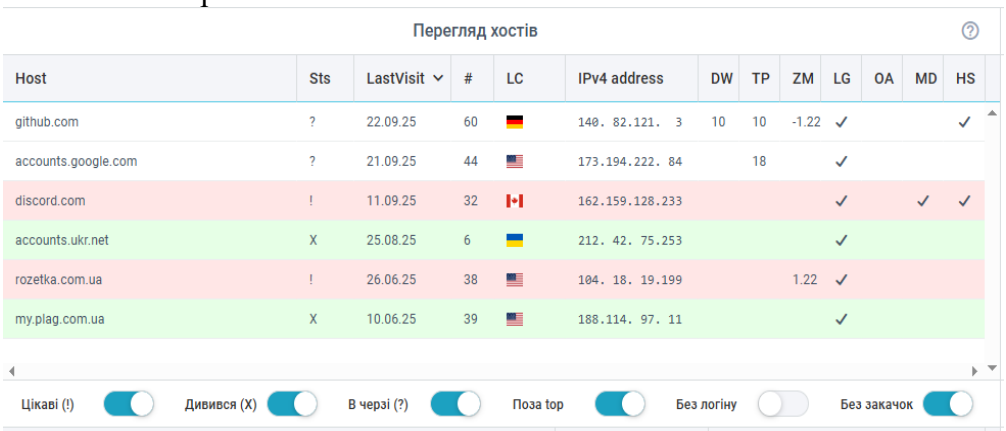


Рис. 4. Вибірка хостів, в яких була авторизація та встановлення оцінок цікавості інформації

Виберемо за допомогою фільтру хостів всіх хости, які відповідають регулярному виразу ^n.*?soft. Результат вибірки показаний на рис. 5

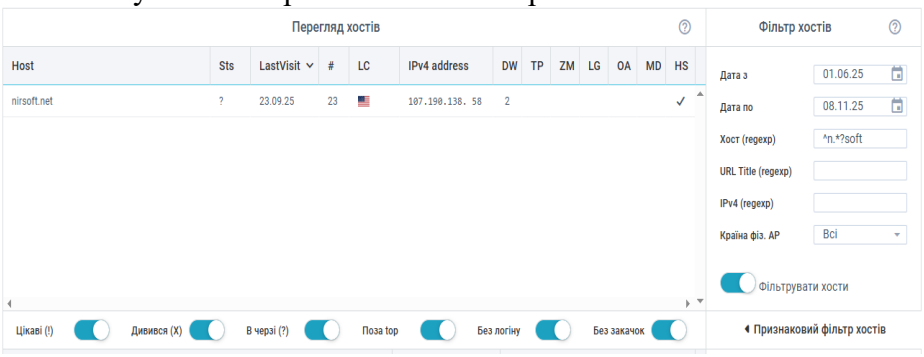


Рис. 5. Відображення всіх хостів, які відповідають регулярному виразу ^n.*?soft.

Натиснемо на ім'я хоста й переглянемо нижній фрейм. Результат показаний на рис. 6.

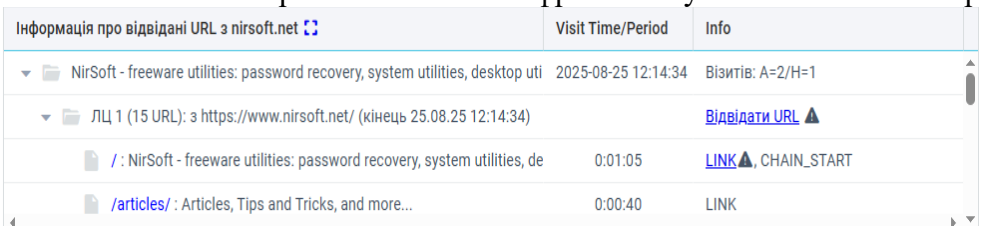


Рис. 6. Відображення інформації про відвідування URL в нижньому фреймі вкладки

Перемкнемось в повноекранний режим, натиснувши на іконку в заголовку таблиці й відкриємо дерев першого ланцюжка, результат за яким показаний на рис. 7.

Інформація про відвідані URL з nirsoft.net	Visit Time/Period	Info
ЛЦ 1 (15 URL): з https://www.nirsoft.net/ (кінець 25.08.25 12:14:34)		Відвідати URL
/ : NirSoft - freeware utilities: password recovery, system utilities, desktop utilities	0:01:05	LINK, CHAIN_START
/articles/ : Articles, Tips and Tricks, and more...	0:00:40	LINK
/articles/view-edge-history.html : View Edge Web browser history with BrowsingHistoryView tool	0:01:10	LINK
/utils/browsing_history_view.html : BrowsingHistoryView - View browsing history of your Web browsers	0:01:50	LINK
/utils/chrome_cache_view.html : BrowsingHistoryView - View browsing history of your Web browsers	0:01:32	LINK
/utils/chromecacheview.zip : успішно 542 кб	0:00:04	Скопіювати в буфер обміну
/web_browser_tools.html : Web Browser Tools Package	0:02:15	LINK
/utils/chrome_history_view.html : ChromeHistoryView - View the browsing history of Chrome Web brow	0:01:11	LINK
/utils/chromehistoryview.zip : успішно 692 кб	0:00:05	Скопіювати в буфер обміну
/utils/chrome_history_view.html : ChromeHistoryView - View the browsing history of Chrome Web brow	0:00:05	BACK
/web_browser_tools.html : Web Browser Tools Package	0:0:19	BACK
/utils/my_last_search.html : My Last Search Package	0:00:30	LINK
/web_browser_tools.html : Web Browser Tools Package	0:00:19	BACK
/computer_forensic_software.html : Computer forenistic software	0:02:10	LINK, CHAIN_END

Рис. 7. Перегляд ланцюжка відвідування URL хоста nirsoft

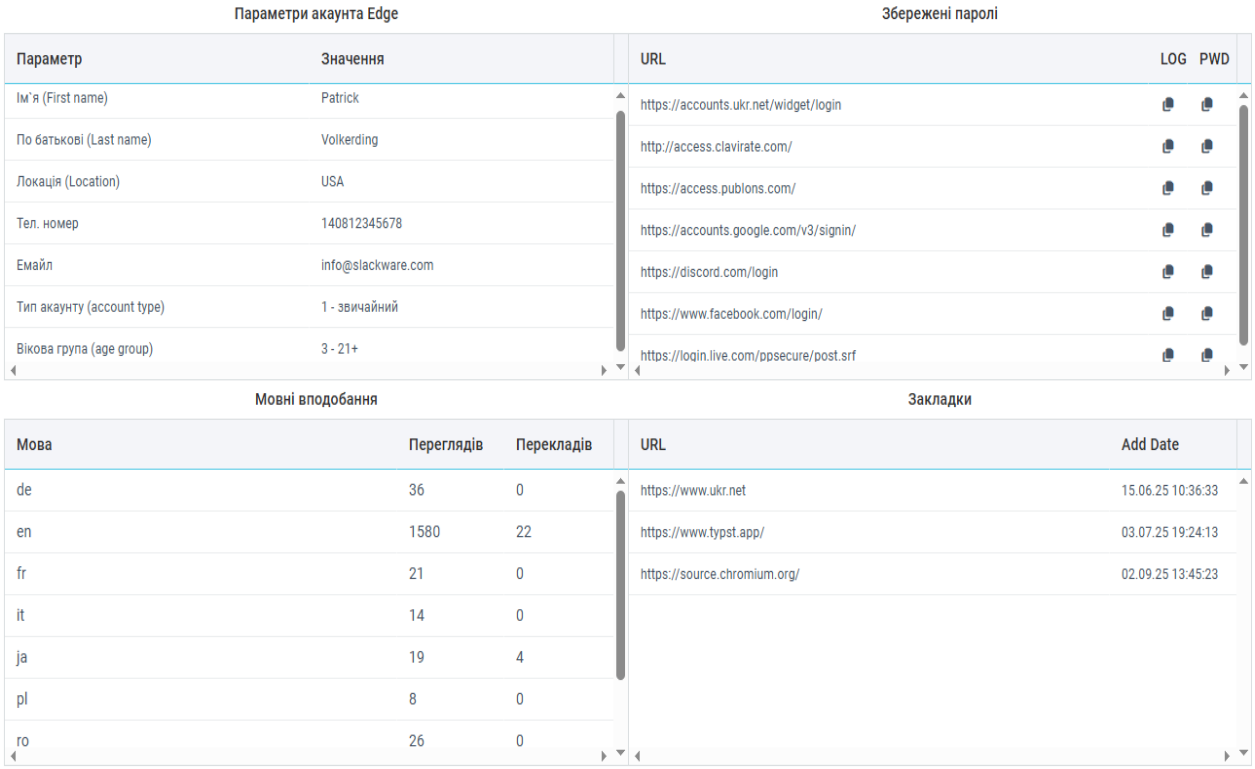
Перемкнемо поточну вкладку на "Пошукові запити", встановимо фільтр "typst" й відмітимо всі записи як нецікаві. Результат запиту показаний на рис. 8.

Перегляд пошукових запитів

Запит	Sts	Дата	#	Пошуковик
typst				
bib to dict typst	X	01.09.25	1	google.com
join sequence typst	X	03.09.25	1	google.com
page numbers typst	X	04.09.25	1	google.com
typst 1.5 line spacing	X	31.08.25	1	google.com
typst app	X	06.09.25	1	google.com
typst bibliography post edit	X	01.09.25	1	google.com
typst check block paragraph	X	26.08.25	1	google.com
typst create package	X	06.09.25	1	google.com
typst dash	X	04.09.25	1	google.com
typst equation align left	X	04.09.25	1	google.com
typst link properties	X	26.08.25	1	google.com

Рис. 8. Результат позначення пошукових запитів користувача, які містять слово "typst" як нецікаві

Зміст вкладки "Про користувача" показаний на рис. 9. Система зібрало достатньо інформації – не тільки телефон й емейл (які мали бути на час реєстрації дійсними, замазані для безпеки), але й розшифрувала ряд паролів (їх можна скопіювати в буфер).



Параметри акаунта Edge

Параметр	Значення
Ім`я (First name)	Patrick
По батькові (Last name)	Volkerding
Локація (Location)	USA
Тел. номер	140812345678
Емайл	info@slackware.com
Тип акаунту (account type)	1 - звичайний
Вікова група (age group)	3 - 21+

Збережені паролі

URL	LOG	PWD
https://accounts.ukr.net/widget/login		
http://access.clavirate.com/		
https://access.publons.com/		
https://accounts.google.com/v3/signin/		
https://discord.com/login		
https://www.facebook.com/login/		
https://login.live.com/ppsecure/post.srf		

Мовні вподобання

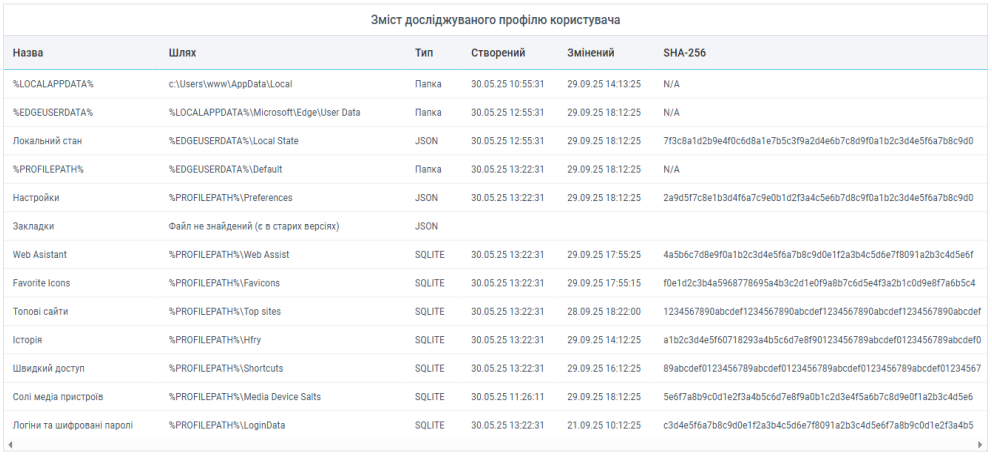
Мова	Переглядів	Перекладів
de	36	0
en	1580	22
fr	21	0
it	14	0
ja	19	4
pl	8	0
ro	26	0

Закладки

URL	Add Date
https://www.ukr.net	15.06.25 10:36:33
https://www.typst.app/	03.07.25 19:24:13
https://source.chromium.org/	02.09.25 13:45:23

Рис. 9. Зміст екрана "Про користувача"

Нарешті, зміст вкладки "Профіль" показаний на рис. 10. Наявність хешів та дат файлів дозволить захиститись від підміни профілю.



Зміст досліджуваного профілю користувача

Назва	Шлях	Тип	Створений	Змінений	SHA-256
%LOCALAPPDATA%	c:\Users\www\AppData\Local	Папка	30.05.25 10:55:31	29.09.25 14:13:25	N/A
%EDGEUSERDATA%	%LOCALAPPDATA%\Microsoft\Edge\User Data	Папка	30.05.25 12:55:31	29.09.25 18:12:25	N/A
Локальний стан	%EDGEUSERDATA%\Local State	JSON	30.05.25 12:55:31	29.09.25 18:12:25	7f3c8a1d2b9e4f0c6d8a1e7b5c3f9a2d4e6b7c8d9f0a1b2c3d4e5f6a7b8c9d0
%PROFILEPATH%	%EDGEUSERDATA%\Default	Папка	30.05.25 13:22:31	29.09.25 18:12:25	N/A
Настройки	%PROFILEPATH%\Preferences	JSON	30.05.25 13:22:31	29.09.25 18:12:25	2a9d5f7c8e1b3d4f6a7c9e0b1d2f3a4c5e6b7d8c9f0a1b2c3d4e5f6a7b8c9d0
Закладки	Файл не знайдений (є в старих версіях)	JSON			
Web Asistant	%PROFILEPATH%\Web Assist	SQLITE	30.05.25 13:22:31	29.09.25 17:55:25	4a5b6c7d8e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8091a2b3c4d5e6f
Favorite Icons	%PROFILEPATH%\Favicons	SQLITE	30.05.25 13:22:31	29.09.25 17:55:15	f0e1d2c3b4a5968778695a4b3c2d1e0f9a8b7c6d5e4f3a2b1c0d9e8f7a6b5c4
Топові сайти	%PROFILEPATH%\Top sites	SQLITE	30.05.25 13:22:31	28.09.25 18:22:00	1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
Історія	%PROFILEPATH%\Hfry	SQLITE	30.05.25 13:22:31	29.09.25 14:12:25	a1b2c3d4e5f60718293a4b5c6d7e8f90123456789abcdef0123456789abcdef0
Швидкий доступ	%PROFILEPATH%\Shortcuts	SQLITE	30.05.25 13:22:31	29.09.25 16:12:25	89abcdef0123456789abcdef0123456789abcdef0123456789abcdef01234567
Солі медіа пристроїв	%PROFILEPATH%\Media Device Salts	SQLITE	30.05.25 11:26:11	29.09.25 18:12:25	5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6
Логіни та шифровані паролі	%PROFILEPATH%\LoginData	SQLITE	30.05.25 13:22:31	21.09.25 10:12:25	c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8091a2b3c4d5e6f7a8b9c0d1e2f3a4b5

Рис. 10. Зміст вкладки "Профіль"

Таким чином, усі сформовані вимоги застосунок виконує. Тестування показало працездатність усіх функцій, що продемонстровано на рисунках.

Висновки. Проведена розробка застосунку для криміналістичного аналізу профілю браузера Microsoft Edge. В основу застосунку покладена хост-орієнтована модель представлення даних. На відміну від оригінальної, URL-орієнтованої структури моделі даних платформи Chromium, ця модель агрегує всі розрізнені артефакти (історію, файли cookie, дані форм, кеш) навколо імені хоста. Це значно підвищує зручність, швидкість та глибину аналізу, дозволяючи аналітику-криміналісту отримати повну картину взаємодії користувача з кожним сайтом. Таким чином, застосунок розділяється на дві частини: частини збору та агрегування інформації та частину візуалізації з функціями пошуку, яка працює не з даними профілю, а з агрегованою інформацією. Перша частина застосунку написана мовою Python й реалізує набір алгоритмів для вилучення, очищення,

перетворення та агрегації даних з профілю браузера у описаний специфікований формат JSON. Модуль враховує реальні проблеми цілісності даних, усуває неінформативний «шум» (локальні адреси, дані розширення) та додає інформацію, пов'язану з геолокацією хоста. Друга частина реалізує вебінтерфейс для візуалізації та аналізу отриманих даних. Обрана як база для інтерфейсу комплексна бібліотека компонентів Webix підтвердила свою ефективність для роботи з великими обсягами даних (до 50 000 записів) без значних затримок при зміні фільтрів. Проведене тестування підтвердило, що розроблений застосунок повністю відповідає вимогам, сформульованим виходячи з аналізу переваг й недоліків існуючих інструментів. Застосунок призначено для фахівців з кібербезпеки та правоохоронних органів України. Його використання дозволить пришвидшити процес криміналістичного аналізу, забезпечуючи більш повне та наочне представлення цифрових доказів, що важливо для судового процесу. Подальшим розвитком застосунку може бути адаптація до інших браузерів на базі Chromium, окремий аналіз діяльності розширень (зараз вона вилучається), аналіз синхронізованих не декількох пристроях профілів, аналіз змісту закешованих даних браузера, аналіз змісту хосту без його відвідування користувачем з застосуванням ШІ.

Список літератури

1. Відін М.В., Стопакевич О.А., Стопакевич А.О. Аналіз проблеми криміналістичного дослідження історії веббраузера. *Інформатика та математичні методи в моделюванні*. 2025. Т. 15, №. 4. С. 518-534.
2. Chromium design documents. URL: https://www.chromium.org/developers/design-documents/
3. Zacks S. Edge vs. Chrome: Two Great Browsers, but Which is Best in 2025? *Private Internet access*. 2025. URL: https://www.privateinternetaccess.com/blog/edge-vs-chrome/
4. 6 Lesser-Known Chromium Based Browsers Worth Exploring. *MoreLogin*. 2025. URL: https://www.morelogin.com/blog/chromium-based-browser
5. Somé D.F., Airan M., Durumeric Zakir, Staicu C.-A. User Profiles: The Achilles' Heel of Web Browsers. *arXiv*. 2025. DOI: 10.48550/ARXIV.2504.17692
6. Chand R.R., Sharma N.A., Kabir M.A. Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques. *Springer Science Computer Science*. 2025. V. 6. P. 355. DOI: 10.1007/s42979-025-03921-6
7. Akintola G.B. Performance Evaluation of four Different Forensic Tools for Web Browser Analysis. *Int. J. of Scientific Research in Multidisciplinary Studies.* 2024. V. 1, No. 10. P.68-82.
8. Adamu H., Ahmad A.A., Hassan A., Gambasha S.B. A Survey of Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis. *Int. J. of Research and Innovation in Applied Science*. 2021. Vol. 6. No. 5. P. 103-107.
9. Chenrnyk M. Webix JS DataTable Best-in-class Performance. URL: https://blog.webix.com/webix-js-datatable-best-in-class-performance/
10. Сергієнко А. В., Балалаєва О. Ю., Гребенькова А. В. Розробка веб-додатку для обліку фінансів та господарської діяльності за допомогою бібліотек Webix UI Library та DHTMLX для системи на основі М-технологій. *Наука та виробництво*. 2023. №25. С. 75-86. DOI: 10.31498/2522-9990252023286712
11. Material Design Icon Collection – Pictogrammers. URL: https://pictogrammers.com/library/mdi/
12. Classic Solid Style icons – Font Awesome. URL: https://fontawesome.com/search?f=classic&s=solid&o=r

DEVELOPMENT OF AN APPLICATION FOR FORENSIC ANALYSIS OF WEB BROWSER HISTORY

M.V. Vidin[1], O.A. Stopakevych[1], A.O. Stopakevych[2]

[1]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
[2]State University of Intellectual Technologies and Telecommunications
1, Kuznechna, Odesa, 65023, Ukraine
Email: stopakevich@gmail.com

Web browsers are one of the main sources of digital evidence in modern forensics. Existing tools for forensic analysis of web browser profiles are not effective enough. This is because they reproduce the data model embedded in browsers. This model is focused on rendering speed and optimization of work with individual URLs. Consequently, forensic experts must work with "raw" lists containing thousands of entries, spending considerable time recreating the sequence of user actions and manually filtering technical redirects, trackers, advertisements, and service requests. This study aims to develop algorithms and software applications for the forensic analysis of Microsoft Edge web browser history. These will transform fragmented profile data into structured information suitable for rapid incident detection and user action reconstruction. The development is based on transitioning from the classic, URL-oriented model characteristic of the Chromium database structure to a host-oriented data representation model. This approach allows significant activity artifacts, such as visit history, cookies, and downloaded files, to be aggregated in chronological order around a unique host name. The architectural solution is divided into two parts: a data collection and aggregation module implemented in Python using asynchronous requests for fast processing of large amounts of information, and a visualization module based on the Webix library, which ensures high interface performance when working with large data sets. The application's graphical interface allows experts to perform multi-priority sorting and filtering of records according to multiple criteria. Particular attention is paid to the visualization of transition chains, which makes it possible to recreate the sequence of actions of a suspect on a specific resource. Testing has confirmed the application's ability to quickly process data and identify relevant evidence, significantly reducing the time required for examination compared to conventional manual analysis of “raw” data. It provides a clear representation of digital evidence and minimizes the likelihood of missing important information during investigations.

Keywords: forensics; analysis; browser; history; profile; aggregation; application; host-oriented data model; SQLite; JSON; Python; JavaScript; Webix.

DOI 10.15276/imms.v16.no1.74
УДК 681.536.55

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 74-84

ДОСЛІДЖЕННЯ ПРОЦЕСУ КЕРУВАННЯ ТЕПЛОВИМ КОМФОРТОМ У ПРИМІЩЕННІ

Є. К. Воскобойник[1], О. О. Бойко[2]

Національний технічний університет «Дніпровська політехніка»
19, Дмитра Яворницького пр., Дніпро, 49000, Україна,
Emails: voskoboinyk.ye.k@nmu.one[1], boiko.o.o@nmu.one[2]

Побудована структура системи керування тепловим комфортом Розроблено моделі у графічному середовищі імітаційного моделювання. Проведено імітаційні експерименти із врахуванням змін: типу одягу, швидкості обміну речовин, середньої температури випромінювання, відносної швидкості руху повітря, відносної вологості. Запропонована система забезпечує підтримку прогнозованої середньої оцінки PMV на заданому рівні за нормальних умов. При погіршенні умов енерговитрати залишаються на рівні традиційної системи керування температурою. При покращенні умов система опалення автоматично відключається, що зменшує енерговитрати. Врахування відносної вологості дозволяє обмежувати енерговитрати шляхом корекції обмеженої прогнозованої оцінки PMV. Зменшення відсотка відхилення при перемиканні зворотного зв'язку підвищує якість функціонування системи. За найгірших умов система підтримує параметри мікроклімату на рівні традиційного керування температурою, що підтверджує її надійність. Запропоновано структуру системи керування тепловим комфортом з використанням індексу PMV як керованої змінної. Обґрунтовано необхідність врахування відносної вологості при розрахунку обмеженої прогнозованої оцінки PMV. Визначено механізм підвищення якості функціонування системи за рахунок адаптивного перемикання зворотного зв'язку між дійсним та обмеженим значенням PMV. Використання системи дозволяє зменшити енерговитрати або підтримувати їх на рівні традиційних систем керування температурою. Рішення може бути застосоване у багатокімнатних будівлях для підвищення енергоефективності та комфорту користувачів. Розробка методики налаштування параметрів системи та перспективна реалізація безперервного керування відкриває можливості для інтеграції у сучасні системи «розумного будинку».

Ключові слова: тепловий комфорт; двопозиційний регулятор; енергоефективність; імітаційне моделювання; математична модель; ідентифікація; автоматизоване керування.

Вступ. На європейській біржі EPEX SPOT 12 грудня 2024 року на піку ціна електроенергії у Федеративній Республіці Німеччина становила 936 € за МВт·год., у Французькій Республіці де джерелом електрики є атомна енергетика 275 €, а у Республіці Польща електрика якої виробляється станціями працюючими на бурому вугіллі 164 € [1]. Кратне підвищення ціни у Німеччині пов'язано з низькою вітряністю в Європі, що у свою чергу дозволило наростити виробіток електроенергії у Франції на 56 атомних реакторах до пікових 51960 МВт [2] та збільшити прибутки за рахунок високої волотильності на ринку. Незважаючи на надлишки електроенергії у деяких постачальників структура ринку Європейського Союзу призвела до глобального збільшення цін у більшості країн членів.

Окрім французьких АЕС для компенсації падіння вироблення електроенергії з відновлюваних джерел у Німеччині використовуються газові станції, що призводить до збільшення попиту на даний енергоресурс. У зв'язку з цим компанія постачальник природного газу Eon Energy підвищила ціни на 24,3 %. Рахунок звичайної німецької роди, яка споживає біля 1800 м3 природного газу збільшився з 2530 € до 3145 € [3]. Середня ціна за електроенергію для населення у Німеччині становить біля 400 € за МВт·год. [4]. У свою чергу Федеральне відомство із захисту населення вже закликало готуватися до довгострокових відключень електроенергії [5], після чого відбулося знеструмлення центрального району міста Тюбінген [6].

Проблеми деяких країн Європейського Союзу з електроенергією погіршуються у зв'язку з перспективою зменшення або відмови від її постачання сусідами. Так Норвегія яка не входить до складу ЄС та не обмежена його законодавством розглядає питання відмови від поставок електроенергії до інших країн у зв'язку з підвищенням внутрішніх цін на неї [7]. Швеція звинувачує Німеччину у збільшенні цін на електроенергію у зв'язку з закриттям її АЕС однак не може зупинити поставки по інтерконекторам так як це забороняється законодавством ЄС [8].

У ситуації, що склалася єдиним шляхом економії енергоресурсів у домогосподарстві залишається зменшення їх використання. Враховуючи, що головним споживачем енергії у даному випадку є система опалення найпростішим шляхом зменшення витрат являється підвищення ефективності керування нею. Таким чином питання дослідження процесу керування тепловим комфортом у приміщенні з метою зменшення енерговитрат є актуальним.

Мета. Розробка та дослідження системи керування тепловим комфортом у приміщенні на базі двопозиційного регулятора з урахуванням прогнозованої середньої оцінки PMV (Predicted Mean Vote), що дозволяє забезпечити енергоефективність та підтримку мікроклімату відповідно до індивідуальних та змінних умов перебування людини.

Основна частина. Дослідження процесу керування тепловим комфортом у приміщенні вимагає визначення діапазонів зміни прогнозованої середньої оцінки PMV, прогнозованого процента невдоволених PDD, споживаної потужності та температури у приміщенні при різних значеннях налаштувань системи керування. У реальних умовах для цього потрібно мати приміщення з підтримкою параметрів мікроклімату на заданому рівні. Окрім того час таких досліджень вимірюється десятками діб та потребує значних витрат енергоресурсів. Виходячи з цього більш ефективнішим є проведення досліджень у всьому діапазоні налаштувань системи керування шляхом моделювання.

Враховуючи вище означене та результати досліджень можливості зниження енерговитрат за рахунок керування системою опалення на підставі теплового комфорту [9] розроблена структура моделі системи керування тепловим комфортом у приміщенні на базі двопозиційного регулятора (рис. 1).

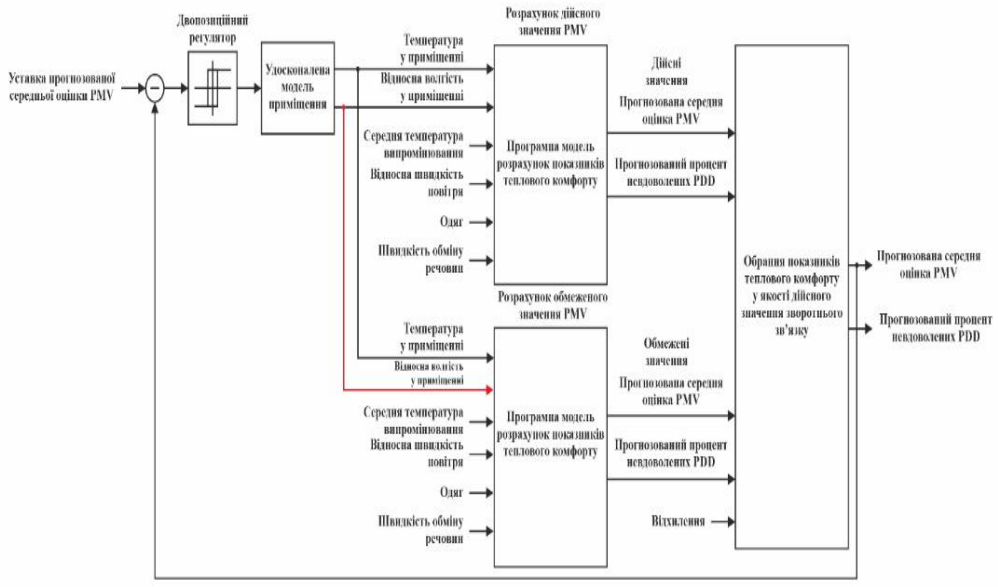


Рис. 1. Структурна схема моделі системи керування тепловим комфортом у приміщенні на базі двопозиційного регулятора

Побудова системи на базі двопозиційного регулятора пов'язана з тим, що більшість сучасних побутових електрообігрівачів мають регулятор потужності та працюють у режимі включений/виключений. З 4773 масляних обігрівачів зареєстрованих в Інтернет магазині

Розетка 35 мають програмне керування, до складу 104 входить датчик температури та тільки найдорожчі – ціна яких у два три рази вища за звичайні моделі та сягає 10000 грв. реалізують безперервне керування [10].

Відповідно до попередніх досліджень авторів [9] при розробці моделі системи керування тепловим комфортом у приміщенні на базі двопозиційного регулятора врахована необхідність створення механізму обмеження споживання енергоресурсів (рис. 1). Обмежуюче значення прогнозованої середньої оцінки PMV розраховується на підставі вхідних параметрів відповідних типовим умовам – роботі традиційної системи керування температурою у приміщенні [9]. Доки дійсне значення PMV дорівнює або більше обмежуючого у якості зворотного зв'язку використовується воно. Коли дійсне значення PMV стає меншим за обмежуюче на відсоток відхилення споживання енергоресурсів збільшується у порівнянні з традиційною системою, тому у якості зворотного зв'язку використовується обмежуюче значення, що забезпечує споживання енергоресурсів на рівні традиційної системи.

Досліджування виконувалося шляхом варіювання параметрів системи керування: типу одягу, швидкості обміну речовин, середньої температури випромінювання, відносної швидкості повітря, початкової відносної вологості повітря, початкової температури у приміщенні, відсотка відхилення, уставки прогнозованої середньої оцінки PMV.

У таблиці 1 наведені результати моделювання зміни типу одягу у діапазоні 0,30÷2,00 кло. Дані які не впливають на характер процесу керування вилучені для зменшення обсягу таблиці та полегшення аналізу. PMV відповідає середньому значенню прогнозованої середньої оцінки, PDD середньому значенню прогнозованого процента невдоволених, Тмін. мінімальній температурі у приміщенні, Тмакс. максимальній температурі у приміщенні, Е споживаній енергії, ΔЕ різниці споживаної енергії системи керування тепловим комфортом та традиційної. Детальніше діапазон 0,80÷1,20 кло наведено на рис. 2.

Таблиця 1.

Результати моделювання зміни типу одягу

№	Тип одягу, кло	PMV обмежений	PMV дійсний	PDD	Тмін., °С	Тмакс., °С	Е, кВт·год.	ΔЕ, кВт·год.
1	0,30	-0,23	-2,00	76,61	16,96	17,91	0,36	-0,03
2	0,90	-0,23	-0,39	8,25	16,96	17,91	0,36	-0,03
3	0,95	-0,14	-0,23	6,11	17,59	18,48	0,48	0,09
4	1,00	-0,22	-0,23	6,12	16,99	17,95	0,39	0,00
5	1,05	-0,30	-0,23	6,14	16,40	17,44	0,21	-0,18
6	1,10	-0,43	-0,27	6,55	16,00	16,00	0,00	-0,39
7	2,00	-0,43	0,58	12,03	16,00	16,00	0,00	-0,39

У діапазоні 0,30÷0,90 кло розбіжність між дійсною прогнозованою оцінкою PMV та обмеженням перевищує 5 % (чорна та червона характеристики), що відповідає збільшенню енерговитрат по відношенню до традиційної системи. Тому на даній ділянці система керування використовує в якості зворотного зв'язку обмежену PMV. У діапазоні 0,90÷1,10 кло система підтримує дійсну PMV на рівні уставки -0,2 відповідно до налаштування двопозиційного регулятора при цьому енерговитрати не перевищують витрати традиційної системи. У діапазоні 1,10÷2,00 кло дійсна PMV перевищує значення уставки системи керування, опалення не працює, енерговитрати відсутні. Зміна налаштування відхилення з 5 % до 1 % (рис. 3, синя характеристика) зменшує енерговитрати у діапазоні 0,90÷1,00 кло до рівня традиційної системи.

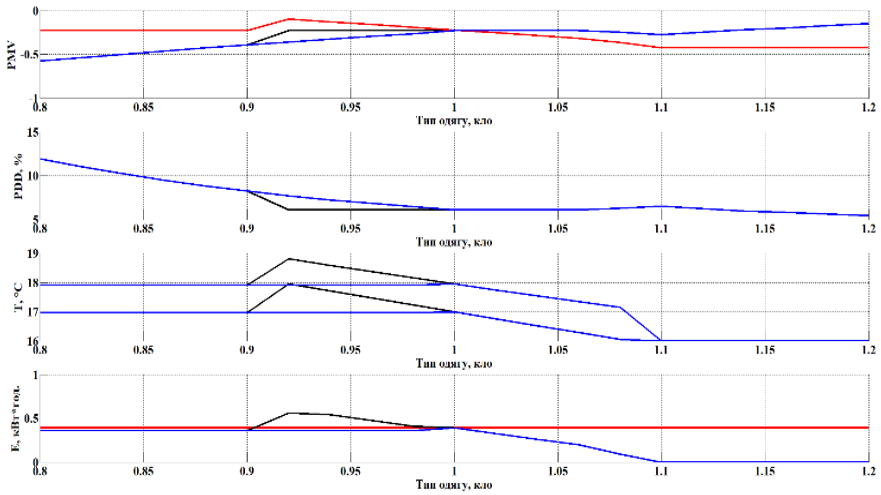


Рис. 2. Результат моделювання зміни типу одягу

На рис.2 чорна характеристика відповідає дійсній PMV при відхиленні 5 %; синя – дійсній PMV при відхиленні 1 %; червона – обмеженій PMV.

Результати моделювання зміни швидкості обміну речовин наведені у табл. 2. Значення параметру поділяється на три діапазони: 0,80÷1,10 мет – збільшення енерговитрат по відношенню до традиційної системи, обмеження PMV, 1,10÷1,25 мет – відпрацювання зміни параметру для підтримки заданої уставки PMV та 1,25÷2,20 кло – дійсна PMV перевищує значення уставки системи керування, опалення не працює. Детальніше діапазон 1,00÷1,30 кло наведено на рис. 3.

Таблиця 2.

Результати моделювання зміни швидкості обміну речовин

№	Швидкість обміну речовин, мет	PMV обмежений	PMV дійсний	PDD	Тмін., °C	Тмакс., °C	E, кВт·год.	ΔE, кВт·год.
1	0,80	-0,23	-1,86	69,93	16,96	17,91	0,36	-0,03
2	1,10	-0,23	-0,38	8,07	16,96	17,91	0,36	-0,03
3	1,15	-0,19	-0,23	6,10	17,24	18,17	0,41	0,02
4	1,20	-0,30	-0,23	6,14	16,40	17,44	0,21	-0,18
5	1,25	-0,43	-0,24	6,23	16,00	16,00	0,00	-0,39
6	2,00	-0,43	0,69	15,10	16,00	16,00	0,00	-0,39

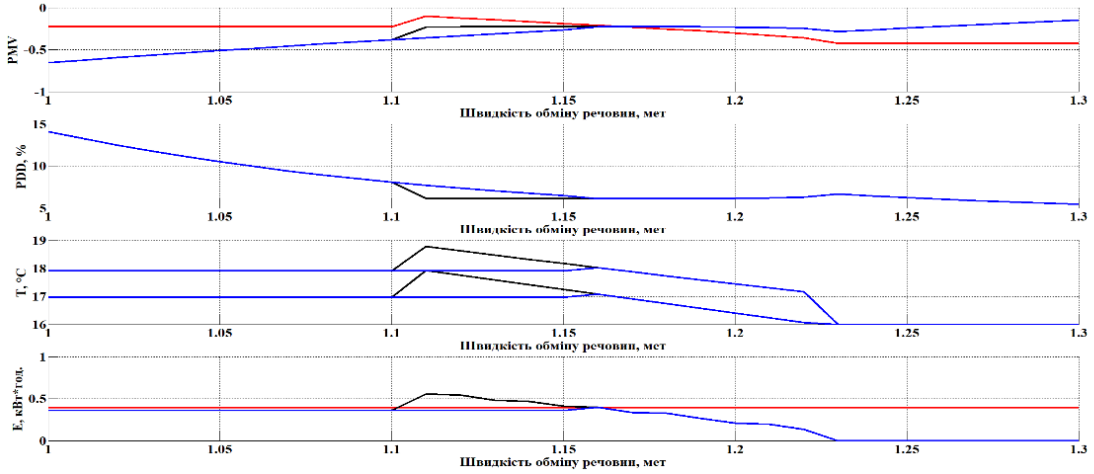


Рис. 3. Результат моделювання зміни швидкості обміну речовин

Результати моделювання зміни середньої температури випромінювання наведені у таблиці 3. Значення параметру поділяється на три діапазони: 16÷23 °С – збільшення енерговитрат по відношенню до традиційної системи, обмеження PMV, 23÷25 °С – відпрацювання зміни параметру для підтримки заданої уставки PMV та 25÷35 °С – дійсна PMV перевищує значення уставки системи керування, опалення не працює. Детальніше діапазон 21÷27 °С наведено на рис. 4.

Таблиця 3

Результати моделювання зміни середньої температури випромінювання

№	Середня температура випромінювання, °С	PMV обмежений	PMV дійсний	PDD	Тмін., °С	Тмакс., °С	E, кВт·год.	ΔE, кВт·год.
1	16,00	-0,23	-0,98	25,43	16,96	17,91	0,36	-0,03
2	22,00	-0,23	-0,44	9,09	16,96	17,91	0,36	-0,03
3	23,00	-0,10	-0,23	6,13	17,92	18,82	0,57	0,18
4	24,00	-0,20	-0,23	6,12	17,13	18,09	0,41	0,02
5	25,00	-0,30	-0,23	6,14	16,40	17,44	0,21	-0,18
6	26,00	-0,43	-0,26	6,35	16,00	16,00	0,00	-0,39
7	35,00	-0,43	0,60	12,53	16,00	16,00	0,00	-0,39

При виконанні дослідження удосконалена модель приміщення використана без динамічної зміни середньої температури випромінювання. Для цього вилучена її частина, яка забезпечує імітацію включення та виключення обладнання у приміщенні [9]. Це пов’язано з тим, що у даному дослідженні усі показники визначається в усталеному режимі. Таким чином статичне значення середньої температури випромінювання забезпечує більшу наочність та спрощує аналіз його впливу на процес керування.

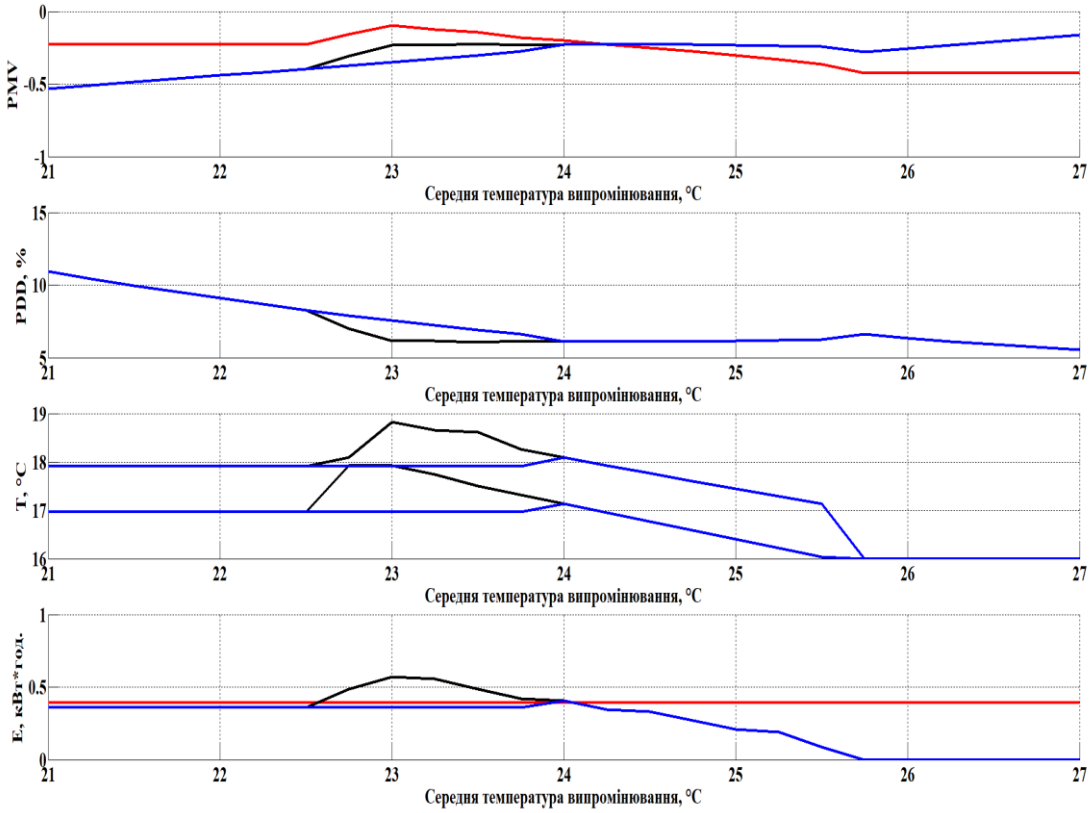


Рис.4. Результат моделювання зміни середньої температури випромінювання

Результати моделювання зміни відносної швидкості повітря наведені у таблиці 4 та на рис. 5. Значення параметру поділяється на три діапазони: 0,05÷0,10 м/с – відпрацювання постійної дійсної прогнозованої середньої оцінки PMV, 0,10÷0,15 м/с – відпрацювання зміни параметру для підтримки заданої уставки PMV та 0,15÷0,3 м/с – збільшення енерговитрат по відношенню до традиційної системи, обмеження PMV.

Таблиця 4.

Результати моделювання зміни відносної швидкості повітря

№	Відносна швидкість повітря, м/с	PMV обмежений	PMV дійсний	PDD	Тмін., °С	Тмакс., °С	E, кВт·год.	ΔE, кВт·год.
1	0,05	-0,30	-0,23	6,15	16,46	17,49	0,26	-0,13
2	0,10	-0,30	-0,23	6,14	16,40	17,44	0,21	-0,18
3	0,15	-0,17	-0,23	6,14	17,37	18,33	0,48	0,09
4	0,20	-0,23	-0,41	8,59	16,96	17,91	0,36	-0,03
5	0,25	-0,23	-0,52	10,66	16,96	17,91	0,36	-0,03
6	0,30	-0,23	-0,61	12,75	16,96	17,91	0,36	-0,03

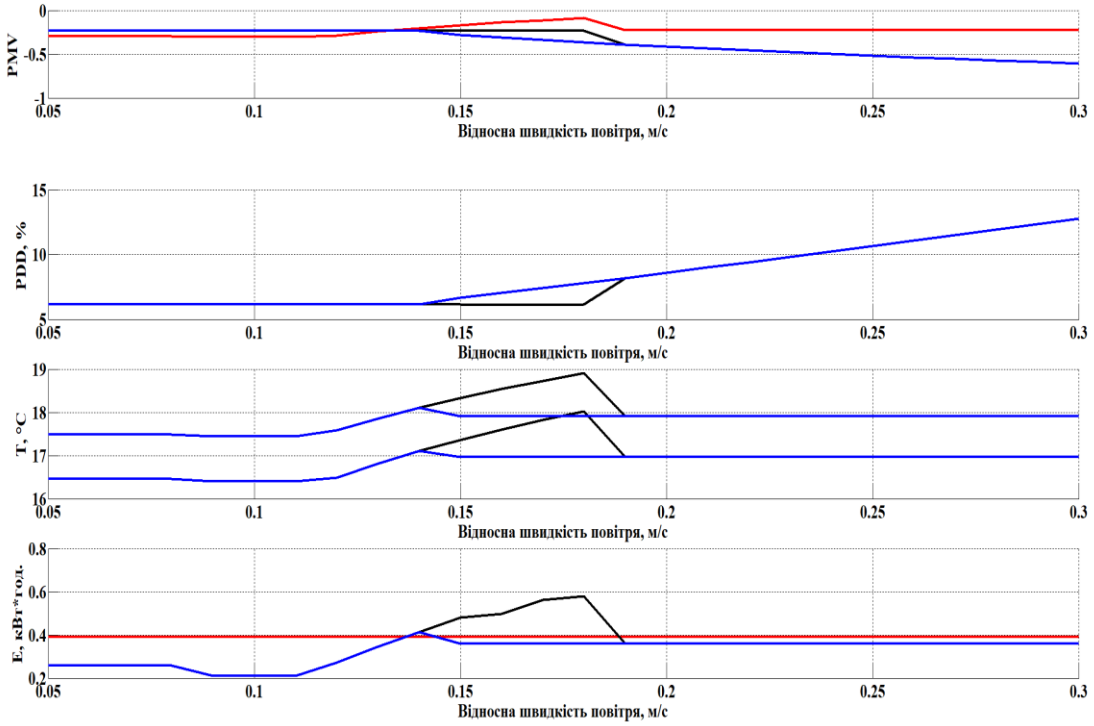


Рис. 5. Результат моделювання зміни відносної швидкості повітря

Результати моделювання зміни початкової відносної вологості повітря наведені на рис. 6. Падіння значення обмеження прогнозованої середньої оцінки PMV пов’язано із зменшенням температури при збільшенні значення відносної вологості, що призводить до розбіжності з дійсною PMV до 5 % та відсутності обмеження. Значення параметру поділяється на два діапазони 20,0÷54,0 % – відпрацювання зміни параметру для підтримки заданої уставки PMV та 55,0÷60,0 % – опалення не працює.

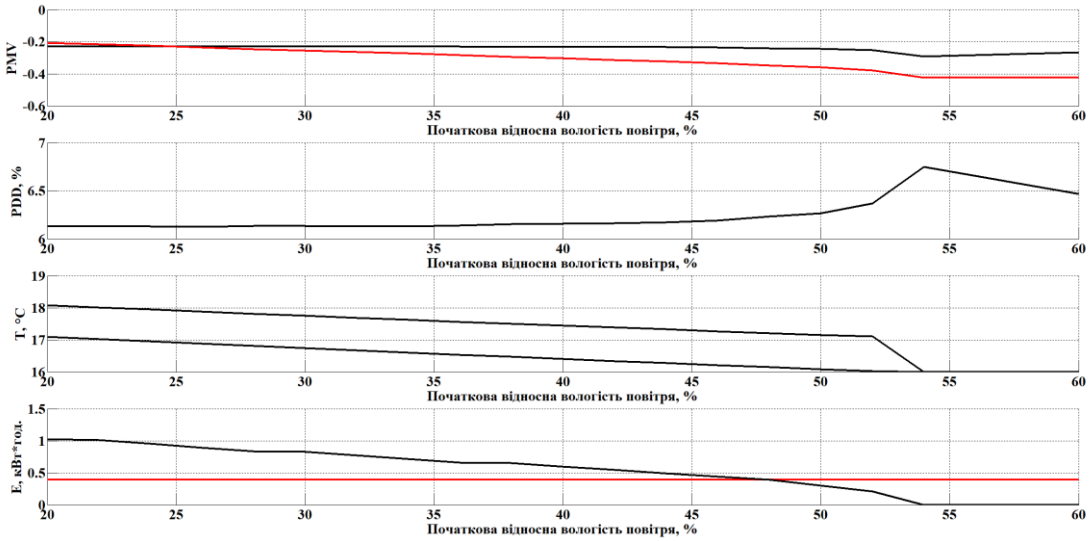


Рис. 6. Результат моделювання зміни початкової відносної вологості повітря

За результатами аналізу отриманих даних експерименту встановлено, що при розрахунку обмеження PMV необхідно враховувати поточне значення відносної вологості повітря для забезпечення обмеження витрат енергоресурсів у всьому діапазоні зміни даного параметру. Результати моделювань з урахуванням запропонованих змін наведені на рис. 7. Порівняння моделювань зміни інших параметрів з результатами, що враховують дійсне значення відносної вологості показало їх відповідність.

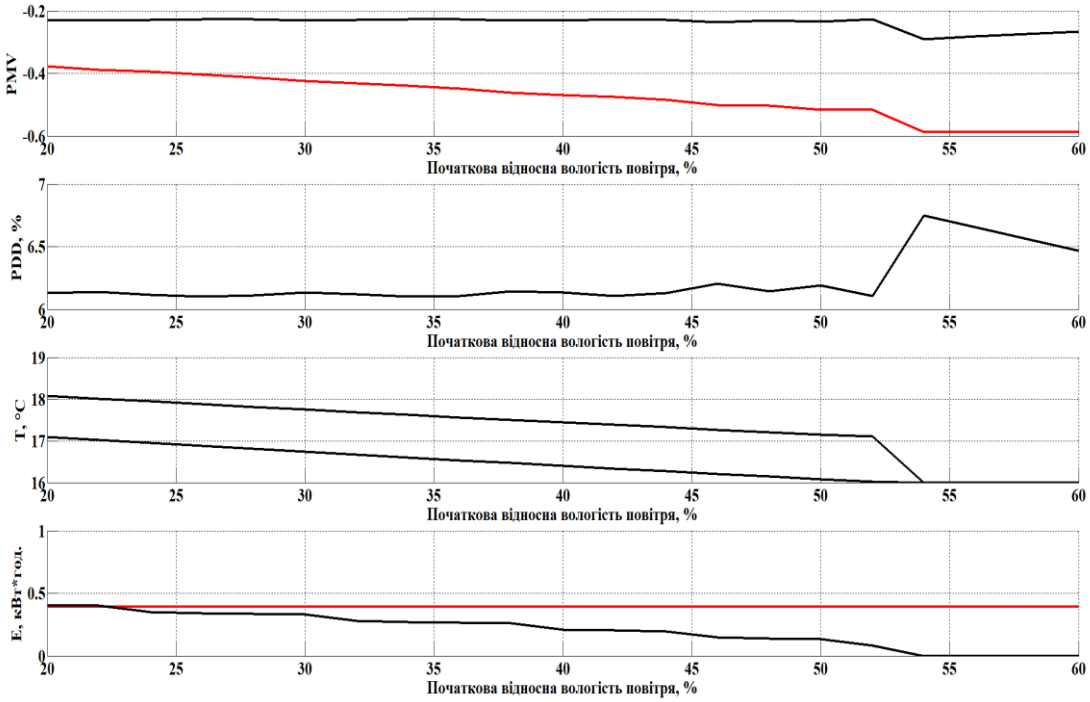


Рис. 7. Результат моделювання зміни початкової відносної вологості повітря з урахуванням при розрахунку обмеження PMV відносної вологості повітря

Результати моделювання зміни початкової температури повітря наведені у таблиці 5 та на рис. 8. Значення параметру поділяється на два діапазони 10,0÷16,5 °С – відпрацювання зміни параметру для підтримки заданої уставки PMV та 16,5÷20,0 °С – опалення не працює.

Таблиця 5.

Результати моделювання зміни початкової температури повітря

№	Початкова температура повітря, °С	PMV обмежений	PMV дійсний	PDD	Тмін., °С	Тмакс., °С	E, кВт·год.	ΔE, кВт·год.
1	10,00	-0,30	-0,25	6,30	16,51	17,28	1,58	-0,24
2	10,50	-0,30	-0,25	6,28	16,50	17,28	1,45	-0,25
3	11,00	-0,30	-0,25	6,27	16,50	17,27	1,34	-0,25
4	11,50	-0,30	-0,24	6,26	16,49	17,27	1,27	-0,22
5	12,00	-0,30	-0,24	6,24	16,48	17,27	1,15	-0,23
6	12,50	-0,30	-0,24	6,22	16,47	17,28	1,04	-0,24
7	13,00	-0,30	-0,24	6,20	16,47	17,28	0,93	-0,22
8	13,50	-0,30	-0,24	6,18	16,46	17,30	0,82	-0,23
9	14,00	-0,30	-0,23	6,16	16,45	17,31	0,72	-0,21
10	14,50	-0,30	-0,23	6,12	16,44	17,33	0,57	-0,27
11	15,00	-0,30	-0,23	6,11	16,43	17,36	0,48	-0,25
12	15,50	-0,30	-0,23	6,10	16,41	17,40	0,34	-0,27
13	16,00	-0,30	-0,23	6,14	16,40	17,44	0,21	-0,30
14	16,50	-0,36	-0,28	6,65	16,50	16,50	0,00	-0,41
15	20,00	0,10	0,16	5,53	20,00	20,00	0,00	-0,29

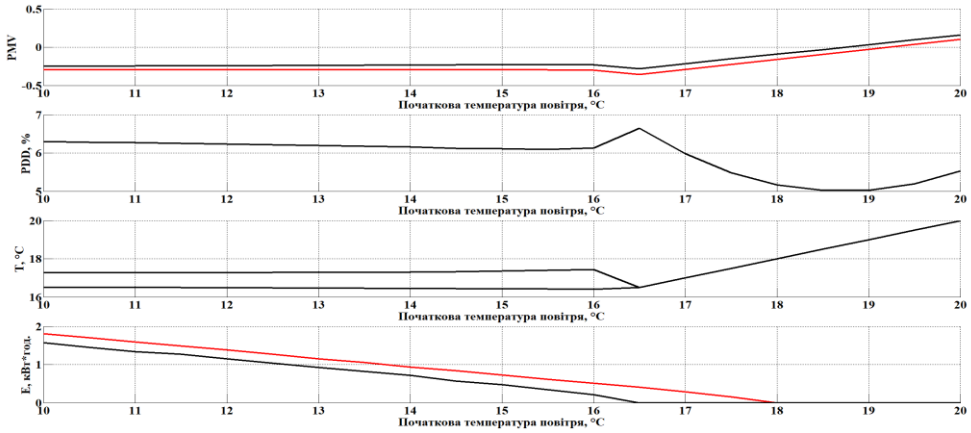


Рис. 8. Результат моделювання зміни початкової температури повітря

Результати моделювання зміни уставки прогнозованої середньої оцінки PMV наведені у таблиці 6 та на рис. 9. Значення параметру поділяється на два діапазони -1,0÷-0,3 – опалення не працює та -0,3÷1,0 – відпрацювання зміни параметру для підтримки заданої уставки PMV.

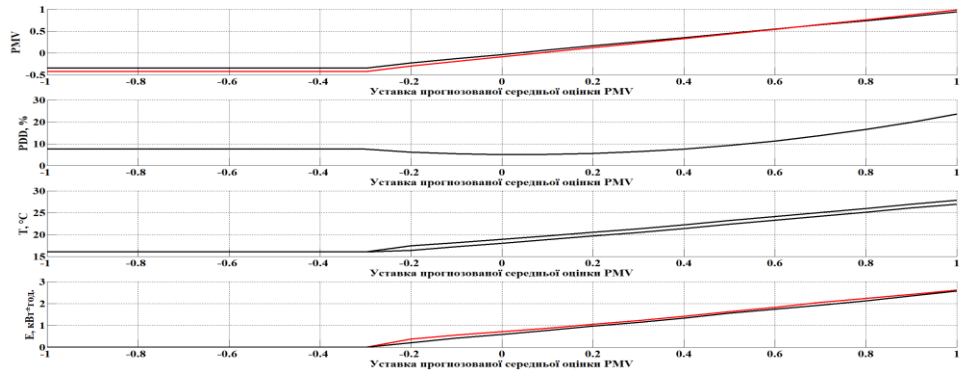


Рис. 9. Результат моделювання зміни уставки прогнозованої середньої оцінки PMV

Таблиця 6.

Результати моделювання зміни уставки прогнозованої середньої оцінки PMV

№	Уставка PMV	PMV обмежений	PMV дійсний	PDD	Тмін., °С	Тмакс., °С	E, кВт·год.	ΔE, кВт·год.
1	-1,00	-0,43	-0,35	7,50	16,00	16,00	0,00	0,00
2	-0,30	-0,43	-0,35	7,50	16,00	16,00	0,00	0,00
3	-0,20	-0,30	-0,23	6,14	16,40	17,44	0,21	0,00
4	-0,10	-0,19	-0,13	5,36	17,19	18,15	0,41	0,00
5	0,00	-0,09	-0,04	5,05	17,99	18,89	0,58	0,00
6	0,10	0,02	0,06	5,11	18,85	19,70	0,76	0,00
7	0,20	0,13	0,16	5,59	19,67	20,50	0,96	0,00
8	0,30	0,22	0,25	6,37	20,43	21,30	1,13	0,00
9	0,40	0,33	0,35	7,59	21,37	22,22	1,34	-0,17
10	0,50	0,44	0,45	9,23	22,37	23,20	1,55	-0,14
11	0,60	0,54	0,55	11,26	23,29	24,12	1,73	-0,14
12	0,70	0,65	0,64	13,71	24,21	25,04	1,92	-0,10
13	0,80	0,76	0,74	16,48	25,14	25,97	2,12	-0,10
14	0,90	0,87	0,84	19,81	26,09	26,91	2,34	-0,09
15	1,00	0,98	0,94	23,61	26,92	27,84	2,58	-0,08

Дослідження впливу відсотка відхилення (рис. 10, табл. 7) показали, що йогозначення у діапазоні 0,50÷4,00 % забезпечує енерговитрати на рівні традиційної системи керування температурою у приміщенні. Характеристики відповідні відхиленню 1 % для кожного з розглянутих параметрів наведені на рисунках 3-6.

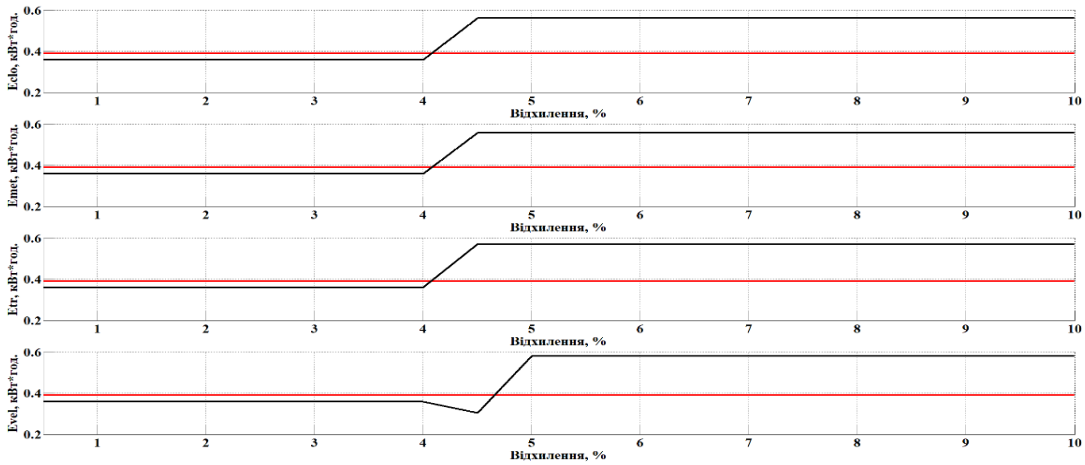


Рис. 10. Результати моделювання зміни відхилення

Таблиця 7.

Результати моделювання зміни відхилення

№	Відхилення, %	Eclo, кВт·год.	Emet, кВт·год.	Etr, кВт·год.	Evel, кВт·год.
1	0,50	0,36	0,36	0,36	0,36
2	1,00	0,36	0,36	0,36	0,36
3	4,00	0,36	0,36	0,36	0,36
4	4,50	0,56	0,56	0,57	0,30
5	5,00	0,56	0,56	0,57	0,58
6	10,00	0,56	0,56	0,57	0,58

Моделювання за найскладніших умов у приміщенні відповідно до стандарту [11] коли уставка PMV дорівнює 0,0, тип одягу 0,3 кло, швидкість обміну речовин 0,8 мет, середнє значення випромінювання 10 °С [12], відносна швидкість повітря 0,3 м/с, початкове значення температури 10 °С та відносна вологість повітря 20 % показало, що система не в змозі за рахунок керування тільки обігрівачем досягти теплового

комфорту тому керування виконується за обмеженою прогнозованою середньою оцінкою PMV. Дійсне значення PMV виходить за діапазон допустимого інтервалу використання +2÷-2, температура у приміщенні підтримується на рівні 19,6 °С, енерговитрати становлять 2,12 кВт.·год.

За результатом досліджень встановлено, що розроблена система керування тепловим комфортом у приміщенні на базі двопозиційного регулятора забезпечує підтримку теплового комфорту на заданому рівні за нормальних умов. За умов підвищених енерговитрат для підтримки теплового комфорту по відношенню до традиційної системи керування температурою, виконується обмеження прогнозованої середньої оцінки PMV таким чином щоб рівень енерговитрат був аналогічний до традиційної системи. За умов встановлення дійсного значення прогнозованої середньої оцінки PMV вище уставки з урахуванням налаштування двопозиційного регулятора опалення вимикається. Таким чином дана система забезпечує керування тепловим комфортом у приміщенні так щоб рівень енерговитрат був нижчім або аналогічним до традиційної системи керування температурою у приміщенні.

Висновки.

1. Обґрунтована та запропонована структура системи керування тепловим комфортом у приміщенні на базі двопозиційного регулятора на підставі якої розроблена модель у графічному середовищі імітаційного моделювання Simulink для математичного пакету MATLAB.
2. Проведено дослідження процесу керування тепловим комфортом за умови зміни типу одягу, швидкості обміну речовин, середньої температури випромінювання, відносної швидкості та вологості повітря. Визначено, що запропонована система керування за нормальних умов у приміщенні забезпечує підтримку прогнозованої середньої оцінки PMV на заданому рівні, при погіршені умов енерговитрати підтримуються на рівні традиційної системи керування температурою у приміщенні, а при покращенні система опалення не працює.
3. Використання запропонованої системи керування тепловим комфортом забезпечує зменшення енерговитрат або підтримку їх на рівні традиційної системи.
4. Для обмеження енерговитрат відповідно до зміни відносної вологості повітря її значення необхідно враховувати при розрахунку обмеженої прогнозованої середньої оцінки PMV.
5. Підвищення якості функціонування системи керування тепловим комфортом забезпечується за рахунок зменшення відсотка відхилення який відповідає за перемикання зворотного зв’язку між дійсним значенням прогнозованої середньої оцінки PMV та обмеженим.
6. Запропоноване рішення за найгірших умов у приміщенні забезпечує підтримку параметрів мікроклімату на рівні традиційної системи керування температурою у зв’язку з неможливістю досягнення теплового комфорту тільки за рахунок керування опаленням.
7. Подальшим напрямком дослідження є розробка методики налаштування параметрів системи керування тепловим комфортом у приміщенні на базі двопозиційного регулятора та розробка безперервної системи керування тепловим комфортом.

Список літератури

1. Market Results. *Epex spot*. URL: https://is.gd/dxxwJP
2. French Nuclear Output Rises to Highest Since February. *Bloomberg.* 2020. URL: https://is.gd/jkki5e
3. Eon erhöht Gaspreis in NRW um 24 Prozent. *Rheinische Post*. URL: https://is.gd/1OeLCq
4. Cold without wind: German ‘dunkelflaute’ brings electricity prices to crisis levels and depletes gas reserves. *El Pais*. URL: https://is.gd/dBuTSG.

5. Bereiten Sie sich auf Notlagen vor. URL: https://is.gd/TCDxkZ
6. Stromausfall in Tübingen - Altstadt mit Weihnachtsmarkt betroffen. *Tagesschau*. URL. https://is.gd/gpgfNp
7. Norway campaigns to cut energy links to Europe as power prices soar. *Financial Times*. 2024. URL: https://www.ft.com/content/f0b621a1-54f2-49fc-acc1-a660e9131740
8. Swedish minister open to new measures to tackle energy crisis, blames German nuclear +phase-out. *Euractiv*. URL: https://is.gd/UpdNxj
9. Voskoboinyk Ye., Boyko O., Slavinskyi D., Cheberiachko Y. Research on the possibility of reducing energy consumption by controlling the heating system based on thermal comfort. *Computer Engineering and Automation*. *Scientific Papers of Donetsk National Technical University*. 2025. No. 3,4 (36). P. 5–12. DOI: https://doi.org/10.32782/2786-9024/v3i4(36).331266
10. Масляні обігрівачі / Розетка. URL: https://is.gd/bm71zZ.
11. ДСТУ Б EN ISO 7730: 2011. Ергономіка теплового середовища. Аналітичне визначення та інтерпретація теплового комфорту на основі розрахунків показників PMV і PPD і критеріїв локального теплового комфорту. Київ: Мінрегіон України, 2012
12. Бойко О., Воскобойник Є., Чеберячко Ю. Удосконалена модель приміщення для дослідження процесу керування тепловим комфортом. *Електромеханічні і енергозберігаючі системи*. 2025. № 1 (68). С. 15-22. URL: https://doi.org/10.32782/2072-2052.2025.1.68.2

RESEARCH ON THE PROCESS OF CONTROLLING THERMAL COMFORT IN A ROOM

Ye. K. Voskoboinyk[1], O. O. Boyko[2]

Dnipro University of Technology
19, Dmytra Yavornytskoho Ave., Dnipro, 49000, Ukraine
Emails: voskoboinyk.ye.k@nmu.one[1], boiko.o.o@nmu.one[2]

The structure of the thermal comfort control system is designed. Simulation experiments taking into account changes in clothing type, metabolic rate, average radiation temperature, relative air velocity, relative humidity is conducted. the system operation with traditional indoor temperature control is compared. The proposed system ensures the maintenance of the predicted average PMV estimate at a given level under normal conditions. When conditions deteriorate, energy consumption remains at the level of the traditional temperature control system. When conditions improve, the heating system is automatically turned off, which reduces energy consumption. Taking into account the relative humidity allows you to limit energy consumption by correcting the limited predicted PMV estimate. Reducing the percentage of deviation when switching feedback improves the quality of system operation. Under the worst conditions, the system maintains microclimate parameters at the level of traditional temperature control, which confirms its reliability. The structure of a thermal comfort control system based on a two-position regulator using the PMV index as a control variable is proposed. The need to take into account relative humidity when calculating the limited predicted PMV estimate is justified. A mechanism for improving the quality of system operation is determined by adaptive switching of feedback between the actual and limited PMV values. The use of the system allows reducing energy consumption or maintaining it at the level of traditional temperature control systems. The solution can be used in multi-room buildings to increase energy efficiency and user comfort. The development of a method for setting system parameters and the prospective implementation of continuous control opens up opportunities for integration into modern "smart home" systems.

Keywords: thermal comfort; two-position regulator; energy efficiency; simulation modeling; mathematical model; identification; automated control.

DOI 10.15276/imms.v16.no1.85
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 85-95

АНАЛІЗ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ АТАК З ВИКОРИСТАННЯМ WAZUH SIEM

Є.О. Севастєєв[1], М.О. Довгань[1], І.В. Лімарь[2]

[1]Державний університет інтелектуальних технологій і зв'язку
1, Кузнечна вул., Одеса, 65023, Україна
[2]Інженерно-технологічний інститут «Біотехніка» Національної академії аграрних наук
26, Маяцька дорога, Хлібодарське, Одеський район, 67667, Україна
Emails: zdelan2018@gmail.com, seva.odessa@gmail.com, quantum.biology@outlook.com

У роботі проведено комплексний аналіз ефективності SIEM-системи Wazuh для моніторингу та виявлення кібератак в інформаційних системах. Досліджено архітектуру системи, принципи її роботи, включаючи процес кореляції подій, та функціональні можливості. Змодельовано чотири типові атаки: SQL-ін'єкція, ShellShock, неавторизований прихований процес та DDoS на кінцеві точки, під'єднані до Wazuh. Проаналізовано логи, правила кореляції та результати детектування. Встановлено, що Wazuh ефективно виявляє веб-атаки за вбудованими правилами (100% успіху для SQL-ін'єкції та ShellShock), але для неавторизованих процесів потрібні кастомні правила, а DDoS не детектується без додаткових механізмів (HIDS, ШІ або комплексних правил кореляції). Актуальність зумовлена зростанням кіберзагроз: за даними досліджень, Wazuh демонструє високу ефективність у хмарних середовищах, генеруючи тисячі алертів при симуляції атак. Практичне значення роботи полягає у впровадженні методології комплексного аналізу ефективності SIEM-систем на прикладі Wazuh для підвищення рівня захищеності інформаційних систем. Отримані результати дозволяють оптимізувати процеси моніторингу, кореляції подій безпеки та реагування на інциденти в корпоративних середовищах. Запропоновані рішення щодо вдосконалення правил детектування та інтеграції додаткових механізмів безпеки можуть бути використані при побудові багаторівневої системи кіберзахисту.
Основні завдання: вивчення архітектури Wazuh, моделювання типових кібератак, аналіз результатів детектування, оцінка ефективності вбудованих та кастомних правил кореляції, а також формування висновків. Результати можуть застосовуватися для оптимізації кібербезпеки в корпоративних мережах, освітніх програмах та аудитах.
Ключові слова: SIEM, Wazuh, виявлення атак, моніторинг безпеки, кореляція подій, управління інцидентами.

Вступ. У сучасному цифровому середовищі такі кібератаки, як SQL-ін'єкції, ShellShock, приховані процеси та DDoS, продовжують залишатися серйозною загрозою для інформаційних систем. Згідно з дослідженнями, загальна кількість кібератак значно зросла у 2024 році, причому веб-вразливості та атаки на доступність посідають серед найпоширеніших векторів нападу [1]. Ці типи атак характеризуються високою ефективністю та можуть завдати значної шкоди організаціям, що висуває вимоги до своєчасного виявлення та оперативного реагування на них. SIEM-системи, зокрема Wazuh, забезпечують комплексний підхід до моніторингу подій безпеки, аналізу логів і реагування на інциденти в реальному часі. Wazuh, заснована на OSSEC, інтегрується з Elastic Stack (Elasticsearch, Kibana, Filebeat) і підтримує функції HIDS, FIM та SCA, що робить її привабливою для організацій [2].
Проблема полягає в тому, що ефективність Wazuh залежить від якості налаштування правил кореляції та інтеграції додаткових інструментів для складних атак, таких як DDoS. Дослідження показують, що вбудовані правила ефективні для веб-атак, але для DDoS потрібні спеціалізовані механізми, включаючи аналіз мережевого трафіку або ШІ [3].

Мета дослідження. Метою даного дослідження є комплексна оцінка ефективності SIEM-системи Wazuh у виявленні кібератак. У рамках дослідження передбачено аналіз архітектурних особливостей та принципів функціонування даної системи. Проводиться моделювання характерних типів атак, включаючи SQL-ін'єкцію, ShellShock, несанкціоновані приховані процеси та DDoS. Виконується аналіз логів та оцінка ефективності вбудованих і кастомних правил кореляції. На основі отриманих результатів формуються практичні рекомендації щодо оптимізації використання системи безпеки.

Аналіз останніх джерел. SIEM-системи відіграють ключову роль у виявленні та реагуванні на кіберзагрози, як зазначено в дослідженнях, що підкреслюють необхідність кореляції подій для відповідності стандартам PCI DSS, GDPR і NIST [4]. Wazuh вирізняється відкритим кодом, агентами для моніторингу кінцевих точок і можливістю інтеграції з Elastic Stack, що забезпечує гнучкість у розгортанні [5].

Дослідження показує, що Wazuh демонструє значну ефективність у виявленні веб-атак, зокрема SQL-ін'єкцій та ShellShock. Це забезпечується завдяки розширеному набору вбудованих правил кореляції, що базуються на сигнатурному аналізі та враховують сучасні вектори атак [6]. Система здатна оперативно ідентифікувати стандартні шаблони атак, що робить її ефективним інструментом для захисту веб-інфраструктури. Проте для DDoS-атак Wazuh має обмеження через відсутність вбудованого аналізу мережевого трафіку, що вимагає інтеграції з інструментами, такими як Suricata або ШІ-моделі [7]. У контексті України, де кібербезпека критичної інфраструктури є пріоритетом, Wazuh розглядається як економічно вигідне рішення для організацій [8].

Перспективні напрями включають використання машинного навчання для аномалійного детектування через інтеграцію з Elasticsearch або OpenSearch, що може підвищити ефективність виявлення складних атак [9]. Крім того, дослідження наголошують на важливості поєднання технічних рішень із навчанням користувачів принципам кібергігієни [10].

Архітектура та принцип роботи Wazuh. Wazuh – це сучасна SIEM-система з відкритим кодом, розроблена на основі OSSEC (Host-based Intrusion Detection System). Її модульна архітектура забезпечує масштабованість, гнучкість і високу продуктивність при обробці великих обсягів подій безпеки. Є чотири основні компоненти системи [4].

Агенти Wazuh – це легковісні програмні компоненти, що встановлюються на кінцеві точки (сервери, робочі станції, хмарні інстанції). Відповідають за збір даних у реальному часі, включаючи системні логи, інтеграцію з ОС для моніторингу файлової цілісності (FIM), перевірку конфігурацій (SCA) та інвентаризацію програмного забезпечення. Агенти безпечно передають ці дані на сервер Wazuh через зашифрований канал.

Сервер Wazuh (Manager) виконує функцію центрального компоненту для прийому даних від агентів. Забезпечується процес декодування, нормалізації та аналізу вхідної інформації з використанням механізму кореляції на основі правил. До ключових функцій сервера належить аналіз логів шляхом порівняння отриманих подій із базою сигнатур для ідентифікації відомих загроз. Реалізується кореляція подій, що дозволяє виявляти складні багатоетапні атаки через аналіз послідовностей взаємопов'язаних подій. Передбачено функціонал автоматизованої відповіді на інциденти, який включає запуск сценаріїв реагування при виявленні загроз, зокрема блокування IP-адрес.

Індексатор Wazuh (Indexer) виконує роль сховища даних. Він індексує, зберігає та забезпечує швидкий пошук усіх нормалізованих подій безпеки та алертів, що надходять від сервера Wazuh. Побудований на основі OpenSearch/Elasticsearch, що забезпечує надійність і горизонтальну масштабованість.

Дашборд Wazuh (Dashboard) – це веб-інтерфейс для візуалізації даних, побудований на базі Kibana. Надає адміністраторам інтуїтивно зрозумілі панелі керування, графіки та інструменти для моніторингу стану безпеки, розслідування інцидентів і аналізу тенденцій.

Взаємодія компонентів відбувається наступним чином. Агенти збирають дані та передають їх на сервер Wazuh. Сервер аналізує інформацію, застосовує правила кореляції та генерує алерти. Ці алерти через інтегрований Filebeat відправляються до Індексатора для зберігання. Дашборд, у свою чергу, запитує дані з Індексатора через REST API і відображає їх користувачеві. Вся комунікація між компонентами захищена за допомогою шифрування TLS, а для конфіденційних даних використовується алгоритм AES-128. Архітектура, побудована на основі стеку Elastic (або OpenSearch), забезпечує не лише високу продуктивність, але й легкість інтеграції з іншими інструментами та платформами, що вказано на рис.1.

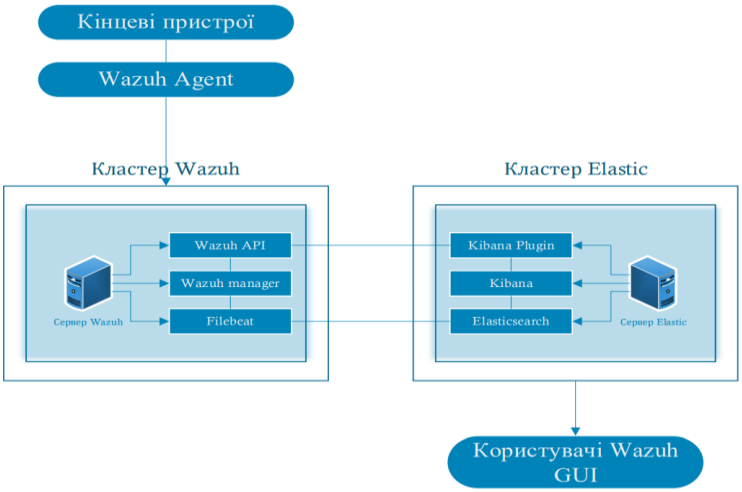


Рис. 1. Архітектура Wazuh

Загальний алгоритм функціонування SIEM-системи Wazuh (рис. 2) є багатоетапним циклічним процесом, спрямованим на перетворення сирих даних з різних джерел у структуровані та пріоритезовані сповіщення про загрози. Його можна умовно поділити на чотири основні фази.

Фаза збору та підготовки даних – процес ініціюється після початкового налаштування (конфігурації) системи адміністратором. Агенти Wazuh, встановлені на кінцевих точках, безперервно збирають системні логи, метрики безпеки та іншу релевантну інформацію. Ці дані передаються на сервер Wazuh, де вони проходять етап верифікації та перевірки на актуальність. Неактуальні або пошкоджені дані відкидаються. Коректні події потім проходять передобробку та нормалізацію, де їх приводиться до єдиного стандартизованого формату, зрозумілого для подальшого аналізу, незалежно від початкового джерела.

Фаза аналізу та кореляції становить концептуальне ядро функціонування SIEM-системи. На цьому етапі здійснюється низка послідовних процедур аналітичної обробки нормалізованих даних. Проводиться агрегація та фільтрація подій, що дозволяє усунути дублювання інформації та відфільтрувати статистичний шум. Виконується реконструкція послідовності дій зловмисника шляхом об'єднання розрізнених подій у єдиний сценарій атаки з ідентифікації її сесії. Найбільш складною процедурою виступає багатокрокова кореляція, яка ґрунтується на застосуванні правил і евристичних алгоритмів для виявлення складних багатоетапних сценаріїв компрометації. Метою багатокрокової кореляції є ідентифікація взаємозв'язків між різнорідними подіями безпеки, що належать до єдиного вектора атаки. Типовим прикладом може служити кореляція спроби несанкціонованого доступу з подальшим впровадженням шкідливого програмного забезпечення, що дозволяє ідентифікувати скоординовані дії зловмисника в інформаційній системі.

Фаза оцінки ризиків та пріоритезації. Після ідентифікації потенційних загроз система здійснює оцінку їх критичності. На даному етапі виконується аналіз

потенційного впливу атак на інфраструктуру з метою визначення масштабів можливих збитків. Проводиться пріоритезація виявлених загроз шляхом їх розподілу за рівнями небезпеки відповідно до заданих політик безпеки. Здійснюється фільтрація подій на основі ранжування для елімінації малозначущих сповіщень. Це забезпечує концентрацію уваги на найкритичніших загрозах та підвищує ефективність реагування на інциденти.

Фаза генерації результату. Події, що пройшли всі попередні етапи та були ідентифіковані як загрози, порівнюються з базою правил. У разі збігу генерується алерт, який зберігається в індексаторі та відображається в дашборді. Фінальним кроком є сповіщення адміністратора про виявлений інцидент через налаштовані канали зв'язку (електронна пошта, месенджери тощо).

Таким чином, принцип роботи Wazuh забезпечує не лише пасивний збор логів, але й активний, інтелектуальний аналіз безпеки, що дозволяє виявляти як прості, так і складні координовані атаки, що детально показано на рис.2.

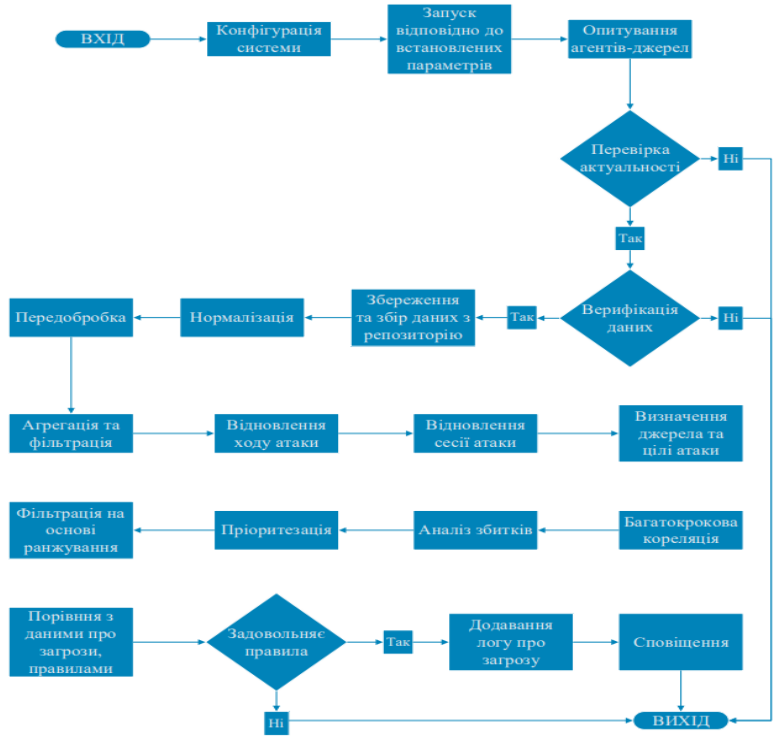


Рис. 2. Принцип роботи Wazuh

Моделювання атак та аналіз результатів. Для експериментальної оцінки ефективності SIEM-системи Wazuh було розгорнуто спеціалізоване тестове середовище, схема якого представлена на рис. 3. Його архітектура була реалізована на базі платформи віртуалізації VirtualBox та імітувала типовий сегмент корпоративної мережі, що включає критичні компоненти інфраструктури. Такий підхід дозволив у контрольованих умовах відтворити реальні сценарії кібератак без ризику для продуктивних систем.

Основним компонентом стенду виступив серверний кластер Wazuh, розгорнутий на віртуальній машині з операційною системою CentOS. Цей кластер включав три ключові модулі: Wazuh Indexer для індексації та зберігання подій безпеки, Wazuh Server (Manager) для аналізу та кореляції вхідних даних, а також Wazuh Dashboard на базі Kibana для візуалізації алертів і моніторингу. Окремо була налаштована кінцева точка під управлінням ОС Ubuntu, на якій був встановлений легковісний агент Wazuh. Цей агент відповідав за збір системних логів, моніторинг активності та передачу всієї інформації на центральний сервер для подальшого аналізу.

Для моделювання атакуючої діяльності використовувалася віртуальна машина з дистрибутивом Kali Linux, який є стандартним інструментом пентестерів і містить необхідний арсенал утиліт для проведення кібератак. Ця машина, що імітувала

зловмисника в глобальній мережі, була використана для послідовного проведення чотирьох типів атак на захищену кінцеву точку (Ubuntu): SQL-ін'єкції, ShellShock, запуску неавторизованого прихованого процесу та DDoS-атаки. Вся мережева взаємодія між компонентами була зосереджена в межах ізольованої локальної мережі (LAN), що забезпечило чистоту експерименту.

Адміністратор системи здійснював моніторинг подій та аналізував результати детектування через веб-інтерфейс Wazuh Dashboard. Така конфігурація стенду дозволила комплексно оцінити здатність Wazuh виявляти різнорідні загрози – від цільових веб-атак до складних мережевих нападів, а також визначити межі його вбудованого функціоналу. Структурна схема розгорнутого віртуального середовища показана на рис.3.

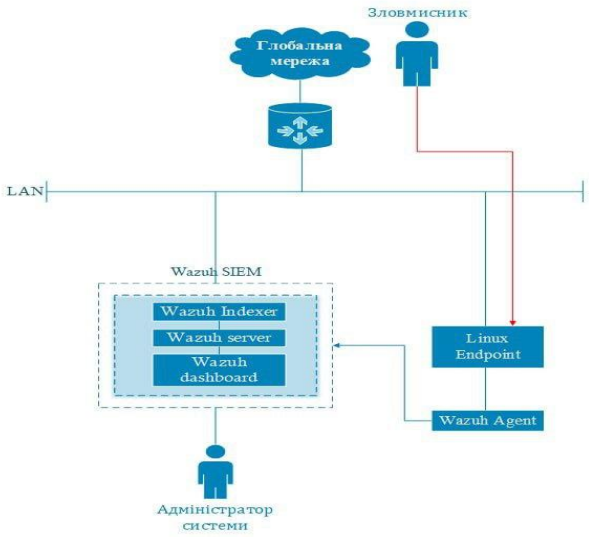


Рис. 3. Тестове середовище

Для комплексної оцінки можливостей детектування SIEM-системи Wazuh було змодельовано чотири типи кібератак, що репрезентують різні класи загроз: від поширених веб-вразливостей до складних мережевих атак. Метою експерименту була кількісна оцінка ефективності виявлення цих атак вбудованими та кастомними засобами Wazuh, а також якісний аналіз характеристик генерованих подій безпеки, таких як рівень критичності, відповідність нормативним вимогам та інформативність логів.

Першою змодельованою атакою була SQL-ін'єкція. На кінцевій точці з агентом Wazuh було розгорнуто веб-сервер Apache. Для імітації атаки з машини зловмисника (Kali Linux) було використано утиліту curl для відправки спеціально сформованого HTTP-запиту за адресою http://<IP_цілі>/users/?id=SELECT+*+FROM+users. Цей запит містив вставку SQL-коду, типовий для експлуатації вразливостей веб-додатків. Завданням Wazuh було проаналізувати логи доступу Apache та ідентифікувати ознаки ін'єкції.

Далі було відтворено експлуатацію вразливості ShellShock. Ця атака спрямована на багатокомпонентну оболонку Bash. Для її моделювання також було застосовано curl, але з модифікованим заголовком User-Agent, який містив шкідливий код: () { :; }; /bin/cat /etc/passwd. Ця конструкція, надіслана на веб-сервер, що використовує уразливі версії Bash, дозволяє виконувати довільні команди на сервері. Метою було перевірити, чи здатний Wazuh виявити такий нетривіальний вектор атаки в потоці мережевих логів.

Третім етапом стало виявлення неавторизованого прихованого процесу. На кінцевій точці було запущено службу netcat (nc) у режимі прослуховування порту (nc -l 8000), що імітувало бекдор або несанкціонований сервіс. Оскільки вбудовані правила Wazuh не орієнтовані на детектування подібних подій за замовчуванням, для цієї мети

було попередньо розроблено та додано кастомне правило кореляції (ID 100051), яке аналізувало вивід команди ps на наявність підозрілих процесів.

Четвертою та фінальною атакою була емуляція DDoS. Для її проведення з атакуючої машини було використано утиліту hping3 із параметрами -S –flood -p 80 <IP_цілі>. Ця команда ініціювала масове надсилання SYN-пакетів на 80-й порт цілі, створюючи навантаження, характерне для атаки типу "відмова в обслуговуванні". Цей експеримент мав на меті визначити межі можливостей Wazuh в детектуванні мережевих аномалій без залучення спеціалізованих модулів аналізу трафіку, таких як NIDS.

Таблиця 1.

Результати виявлення атак

Атака	Виявлено	Правило	Рівень	Відповідність вимогам
SQL-ін'єкція	Так	31103	7	PCI DSS, GDPR, NIST
ShellShock	Так	31168	15	PCI DSS, GDPR, NIST
Прихований процес	Так	100051	7	Немає
DDoS	Ні	-	-	-

Аналіз логів та аудит. Експериментально підтверджено ефективність SIEM-системи Wazuh у виявленні атак типу SQL-ін'єкція. Аналіз журналу подій зафіксував успішну ідентифікацію запиту за правилом кореляції 31103 з рівнем загрози 7. Протягом 24-годинного моніторингу зареєстровано 277 подій безпеки, з яких SQL-ін'єкція становила 0,36% від загальної кількості інцидентів. Система забезпечила повну фіксацію параметрів атаки, включаючи IP-адресу джерела (192.168.8.102), метод запиту (GET) та цільовий URL. Часовий аналіз виявив нерівномірність навантаження з піковими періодами активності о 08:00, 09:00, 12:00 та 15:00. Вбудована відповідність правила 31103 міжнародним стандартам безпеки (PCI DSS, GDPR, NIST 800-53) робить його особливо актуальним для організацій з підвищеними вимогами до захисту інформації. На рис. 4 представлено статистику виявлення атаки SQL-ін'єкції.

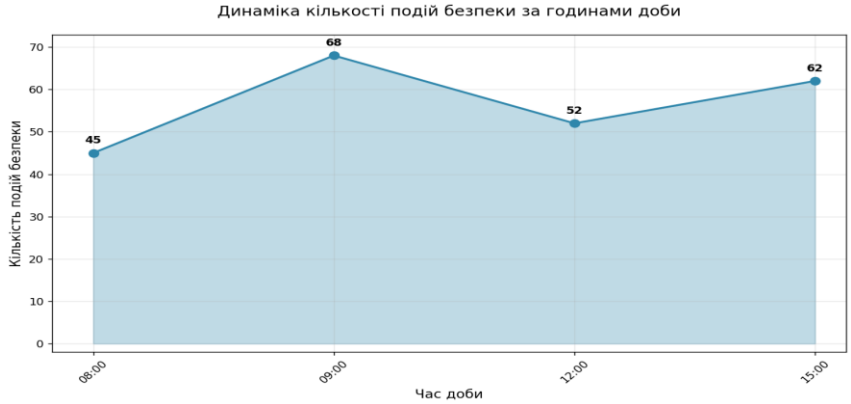


Рис. 4. Статистика виявлення атаки SQL-ін'єкції системою Wazuh

Лінійний графік демонструє чітко виражену нерівномірність у розподілі подій безпеки протягом доби. Максимальна активність зафіксована о 09:00 годині, коли система зареєструвала 68 інцидентів. Другий пік спостерігається о 15:00 годині (62 події), що може бути пов'язане з підвищеною активністю користувачів у робочий час. Період з 08:00 до 09:00 характеризується різким зростанням кількості подій на 51%, що відповідає початку робочого дня та активізації мережевої активності. У період з 09:00 до 12:00 спостерігається плавне зниження показників до 52 подій, з подальшим зростанням до 62 подій о 15:00 годині. Отримані дані підтверджують необхідність адаптивного налаштування правил кореляції SIEM-системи Wazuh з урахуванням часових особливостей мережевої активності. Періоди пікового навантаження вимагають підвищеної уваги до якості детектування та оперативності реагування на загрози.

Експериментально підтверджено ефективність SIEM-системи Wazuh у виявленні критичних вразливостей командного інтерпретатора bash. Зафіксовано успішну ідентифікацію атаки ShellShock за правилом кореляції 31168 з присвоєнням максимального рівня загрози 15. Статистичний аналіз засвідчив рівномірний розподіл подій безпеки протягом доби із середньою інтенсивністю 4,4G подій за 24-годинний період моніторингу. Система забезпечила комплексну фіксацію параметрів атаки, включаючи реєстрацію часових міток, ідентифікацію агента моніторингу та детальну класифікацію типу загрози. Аналіз динаміки подій безпеки виявив стабільну активність із незначними коливаннями протягом періоду з 18:00 до 15:00 наступної доби. Встановлено комплексну відповідність правила 31168 міжнародним стандартам інформаційної безпеки, включаючи PCI DSS, GDPR, NIST 800-53, TSC та MITRE ATT&CK framework. Присвоєння максимального рівня загрози (15) свідчить про класифікацію даного типу атаки як критично небезпечної з високим потенціалом компрометації системи.

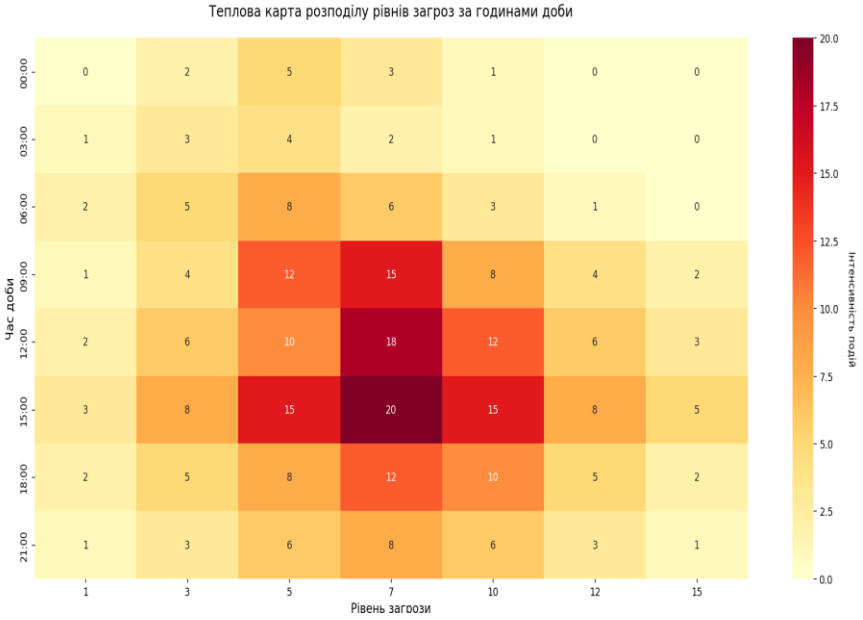


Рис. 5. Статистика виявлення атаки ShellShock системою Wazuh

Теплова карта демонструє чітку кореляцію між часом доби та інтенсивністю загроз безпеки. Максимальна концентрація подій високого рівня загроз (12-15) спостерігається в період з 12:00 до 15:00 годин, що відповідає піку бізнес-активності. Період з 09:00 до 18:00 характеризується стабільно високою частотою подій середнього та високого рівнів загроз (7-15), що становить приблизно 65% від загальної кількості інцидентів. Найвища інтенсивність зафіксована о 15:00 годині для рівня загрози 15, що підтверджує критичність даного періоду для системи безпеки. Нічний період (00:00-06:00) демонструє мінімальну активність з переважанням подій низького та середнього рівнів загроз (1-7). Отримані дані підтверджують необхідність адаптивної політики безпеки з динамічним налаштуванням правил кореляції відповідно до часових особливостей мережевої активності.

Експериментально встановлено необхідність спеціалізованих правил кореляції для детектування неавторизованих мережевих служб. Створення кастомного правила 100051 забезпечило технічну можливість ідентифікації процесу netcat (nc -l 8000). Статистичний аналіз зафіксував 4,4 мільйони подій безпеки протягом 24-годинного періоду, з яких 0,002% становили інциденти, виявлені кастомними правилами. Система забезпечила комплексну фіксацію параметрів інциденту, включаючи часову мітку, ідентифікацію агента моніторингу та класифікацію типу загрози. Аналіз часового розподілу активності виявив рівномірну інтенсивність подій із незначними коливаннями в період з 18:00 до 15:00 наступної доби.

Порівняльний аналіз підтвердив суттєву різницю між вбудованими та кастомними рішеннями. Правило 100051, демонструючи технічну ефективність, не відповідає міжнародним стандартам інформаційної безпеки (PCI DSS, GDPR, NIST 800-53), що обмежує його застосування в організаціях з високими регуляторними вимогами. Отримані результати обґрунтовують необхідність стандартизованих підходів до розробки кастомних правил кореляції.

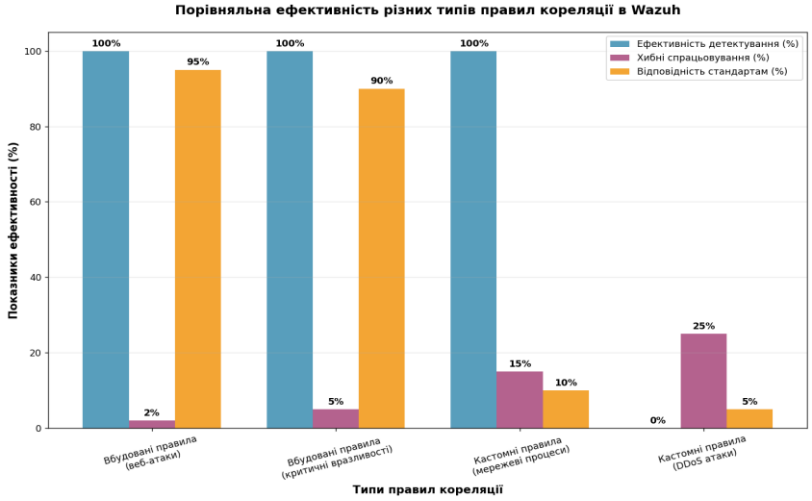


Рис. 6. Статистика виявлення неавторизованого прихованого процесу

Порівняльний аналіз ефективності правил кореляції виявляє суттєві відмінності між категоріями. Вбудовані правила для веб-атак демонструють оптимальні показники ефективності детектування (100%) при низькому рівні хибних спрацьовувань (2%) та високій відповідності стандартам (95%). Кастомні правила для виявлення мережевих процесів, незважаючи на технічну ефективність (100%), характеризуються підвищеним рівнем хибних спрацьовувань (15%) та обмеженою відповідністю регуляторним вимогам (10%). Найнижчі показники ефективності зафіксовано у кастомних правил для детектування DDoS-атак: нульова ефективність детектування (0%) при високому рівні хибних спрацьовувань (25%) та мінімальній відповідності стандартам (5%).

Експериментальне дослідження можливостей Wazuh щодо ідентифікації DDoS-атак проводилося з використанням утиліти hping3. Генерація інтенсивного потоку SYN-пакетів на порт 80 з інтенсивністю понад 40 пакетів/с не викликала реакції системи безпеки. Моніторинг активності протягом тестового періоду зафіксував повну відсутність детектування атаки, навіть після імплементації спеціалізованих кастомних правил кореляції. Отримані результати свідчать про структурні обмеження архітектури Wazuh в аналізі мережевого трафіку реального часу, що зумовлено орієнтацією системи на аналіз подій на рівні хоста та додатків. Результати дослідження підтверджують необхідність розробки стандартизованих підходів до створення кастомних правил кореляції та інтеграції з спеціалізованими системами аналізу мережевого трафіку. Для ефективного виявлення складних мережевих атак рекомендовано впровадження механізмів машинного навчання та інтеграцію з системами виявлення вторгнень (NIDS).

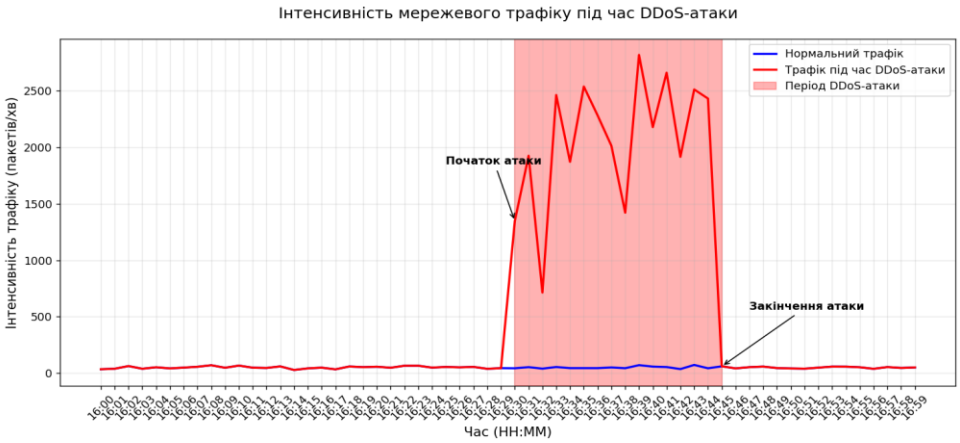


Рис. 7. Результат виконання DDoS-атаки за допомогою утиліти hping3

Графік демонструє різку зміну інтенсивності мережевого трафіку під час DDoS-атаки в період з 16:30 до 16:45. Середня інтенсивність трафіку зросла з нормальних 50 пакетів за хвилину до понад 2000 пакетів за хвилину, що становить збільшення на приблизно 4000%. Період атаки характеризується стабільно високою інтенсивністю трафіку з незначними флуктуаціями, що типовий для скоординованих DDoS-атак. Після завершення атаки о 16:45 спостерігається різке повернення до нормального рівня трафіку. Отримані дані підтверджують, що традиційні правила кореляції Wazuh, орієнтовані на аналіз подій на рівні хоста, є неефективними для виявлення аномалій мережевого трафіку. Відсутність реакції системи на 4000% зростання трафіку свідчить про необхідність інтеграції з спеціалізованими системами моніторингу мережевої активності.

Висновки. Проведене дослідження дозволило встановити комплексну оцінку ефективності SIEM-системи Wazuh у виявленні різних типів кібератак. Експериментальним шляхом доведено високу результативність системи щодо ідентифікації веб-загроз, зокрема SQL-ін'єкцій та атак типу ShellShock. Ця ефективність забезпечується розвиненою системою вбудованих правил кореляції, що відповідають міжнародним стандартам інформаційної безпеки, включаючи PCI DSS, GDPR та NIST 800-53. Системний аналіз архітектури Wazuh виявив значні обмеження щодо детектування складних мережевих атак. Експериментально підтверджено повну відсутність реакції системи на DDoS-атаки навіть при використанні спеціально розроблених кастомних правил кореляції. Встановлено, що це обмеження зумовлене фундаментальними особливостями архітектури, орієнтованої переважно на аналіз подій на рівні хоста та додатків.

Детальний аналіз ефективності різних типів правил кореляції показав, що кастомні правила для виявлення несанкціонованих процесів, незважаючи на технічну ефективність, характеризуються високим рівнем хибних спрацьовувань (15%) та мінімальною відповідністю регуляторним вимогам (10%). Це суттєво обмежує їх застусування в організаціях з високими вимогами до відповідності стандартам. На основі отриманих результатів розроблено комплекс рекомендацій щодо підвищення ефективності системи безпеки. Запропоновано архітектурні рішення щодо інтеграції Wazuh з спеціалізованими системами аналізу мережевого трафіку, такими як Suricata та Zeek. Обґрунтовано доцільність впровадження механізмів машинного навчання на базі Elasticsearch/OpenSearch для проактивного виявлення аномалій.

Визначено перспективні напрями подальших досліджень, серед яких пріоритетними є: розробка стандартизованих методів створення кастомних правил кореляції, що забезпечать відповідність міжнародним стандартам; створення адаптивних алгоритмів для виявлення складних багатоетапних атак; впровадження інтелектуальних

систем моніторингу мережевої активності. Отримані результати свідчать, що Wazuh є ефективним рішенням для побудови системи безпеки, проте його максимальна ефективність досягається лише при реалізації комплексного підходу до інтеграції з додатковими інструментами моніторингу. Запропонована методологія дозволяє створити багаторівневу систему захисту, здатну ефективно протидіяти різноманітним кіберзагрозам сучасного цифрового середовища.

Список літератури

1. Manzoor J., Waleed A., Jamali A.F., Masood A. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS One.* 2024. DOI: 10.1371/journal.pone.0301183.
2. Ahmed W.S., AL-Ta'I Z.T.M. Analysis of Wazuh SIEM's Effectiveness in Cloud Security Monitoring. *Journal of Cybersecurity and Information Management.* 2025. V. 15. No. 01. P. 244-250. DOI: 10.54216/JCIM.150119.
3. Chamkar S.A., Zaydi M., Maleh Y., Gherabi N. Improving Threat Detection in Wazuh Using Machine Learning Techniques. *Journal of Cybersecurity and Privacy.* 2025. V. 5. No. 2. P. 34. DOI: 10.3390/jcp5020034.
4. Jumiaty S. B. SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive. *International Journal of Advanced Computer Science and Applications*. 2024. V. 15. No. 9. P. 239-251.
5. Wibowo B., Nurrohman A., Hafiz L. Deep Learning in Wazuh Intrusion Detection System to Identify Advanced Persistent Threat (APT) Attacks. *International Journal of Science Education and Cultural Studies.* 2025. V. 4. No. 1. DOI: 10.58291/ijsecs.v4i1.311.
6. Stankovic S., Petrovic R. A. Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis. 2022. URL: https://www.researchgate.net/publication/364172770_A_Review_of_Wazuh_Tool_Capabilities_for_Detecting_Attacks_Based_on_Log_Analysis.
7. The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh. *IEEE Xplore*. 2023. DOI: 10.1109/ICETRAN10052950.2023.
8. Wazuh Security Event Response with Retrieval-Augmented Generation. *MDPI Sensors*. 2025. V. 25. No. 3. P. 870. DOI: 10.3390/s25030870.
9. Detection of DDoS attack in OpenStack cloud using Wazuh. *AIP Conference Proceedings*. 2025. V. 3227. P. 060004. DOI: 10.1063/5.0213456.
10. Exploration of Open Source SIEM Tools and Deployment of an Efficient System. Semantics Scholar. 2024. URL: https://www.semanticscholar.org/paper/d027ddda72142e332cc8c757d86f021d95e5cf6b.

ANALYSIS OF THE EFFECTIVENESS OF DETECTING ATTACKS USING WAZUH SIEM

Y.O. Sevastieiev[1], M.O. Dovgan[1], I.V. Limar[2]

[1]State University of Intelligent Technologies and Telecommunications
1, Kuznechnaya St., Odessa, 65023, Ukraine
[2]Engineering and Technology Institute «Biotechnica» of National Academy of Agrarian Science
26, Mayakska road, Hlibodarske, Odesa Raion, 67667, Ukraine
Emails: zdelan2018@gmail.com, seva.odessa@gmail.com, quantum.biology@outlook.com

This paper provides a comprehensive analysis of the effectiveness of the Wazuh SIEM system for monitoring and detecting cyberattacks in information systems. The architecture of the system, its operating principles, including the event correlation process, and its functional capabilities are examined. Four typical attacks are simulated: SQL injection, ShellShock, unauthorized hidden process, and DDoS on endpoints connected to Wazuh. Logs, correlation rules, and detection results are analyzed. It was found that Wazuh effectively detects web attacks using built-in rules (100% success for SQL injection and ShellShock), but custom rules are required for unauthorized processes, and DDoS is not detected without additional mechanisms (HIDS, AI, or complex correlation rules). The relevance is due to the growth of cyber threats: according to research, Wazuh demonstrates high efficiency in cloud environments, generating thousands of alerts during attack simulations. The practical significance of the work lies in the implementation of a methodology for comprehensive analysis of the effectiveness of SIEM systems using Wazuh as an example to improve the security level of information systems. The results obtained allow optimizing the processes of monitoring, correlating security events, and responding to incidents in corporate environments. The proposed solutions for improving detection rules and integrating additional security mechanisms can be used in building a multi-level cyber defense system. The main tasks are to study the architecture of Wazuh, model typical cyberattacks, analyze detection results, evaluate the effectiveness of built-in and custom correlation rules, and draw conclusions. The results can be used to optimize cybersecurity in corporate networks, educational programs, and audits.

Keywords: SIEM, Wazuh, attack detection, security monitoring, event correlation, incident management.

DOI 10.15276/imms.v16.no1.106
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 106-115

ОЦІНКА СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ДЛЯ РІЗНИХ КЛАСІВ КОНТЕЙНЕРІВ

В. В. Кілко, А. В. Соколов

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: vladimyr.kilko@gmail.com

Представлено результати експериментального дослідження впливу вибору кодового слова на надійність сприйняття та стійкість стеганографічного вбудовування в зображення. Робота орієнтована на підхід із кодовим управлінням, який дозволяє контролювати процес приховування інформації через параметри кодових структур без зміни області представлення даних. Дослідження виконано на наборі з 500 зображень, класифікованих за рівнем текстурованості (гладкі, середньотекстуровані, високодеталізовані та змішані), що дало змогу встановити закономірності між типом контейнера, вибором кодового слова та відновлюваністю прихованого повідомлення після JPEG-стиску. У межах експерименту розглядалися шість типів кодових слів: постійне (Const), низькочастотне (LF), комбіноване низькочастотне (LF-C), середньочастотне (MF), високочастотне (HF) та Bent. Для кожного зображення здійснювалося вбудовування і подальше відновлення даних після стиску на рівнях якості QF=10…100, а ефективність оцінювалася за показником бітових помилок відновлення. Отримані результати підтвердили, що вибір кодового слова має визначальний вплив на стійкість прихованої інформації, тоді як різниця між класами зображень-контейнерів справляє відчутний, але непорівнянний за масштабом ефект. Встановлено, що низькочастотне кодове слово забезпечує оптимальну стійкість для QF>20, тоді як постійне кодове слово є ефективним при жорсткому стиску (QF≤20). Високочастотне кодове слово доцільно застосовувати лише у сценаріях, де пріоритетом є збереження максимальної візуальної якості, а стійкість не є критичною. Bent кодове слово продемонструвало найменший розкид показників відсотку помилок при вилученні серед усіх класів зображень, підтверджуючи свою універсальність і рівномірний енергетичний розподіл у просторі Уолша-Адамара. Запропоновані рекомендації дозволяють формувати адаптивні системи стеганографії з кодовим управлінням, здатні автоматично підбирати частотний профіль кодового слова відповідно до властивостей контейнера та рівня очікуваного стиску. Отримані результати можуть бути використані для підвищення ефективності й надійності стеганографічних методів у практичних системах.

Ключові слова: стеганографія, JPEG, кодове управління, кодове слово, перетворення Уолша-Адамара, бент-функції, стійкість.

Вступ. У сучасну епоху стрімкого розвитку цифрових технологій частка мультимедійних даних у світовому трафіку постійно зростає. Зображення, аудіо- та відеофайли стали основними носіями інформації в соціальних мережах, засобах масової комунікації, електронній комерції та наукових платформах. Така тенденція відкриває нові можливості для обміну даними, але водночас створює серйозні виклики у сфері інформаційної безпеки.

Одним із найефективніших напрямів захисту інформації в мультимедійних середовищах є стеганографія – наука про приховування факту передавання повідомлення. На відміну від криптографії, що маскує зміст даних, стеганографія дозволяє приховати сам факт їх існування, вбудовуючи секретну інформацію у звичайні медіаоб’єкти. Завдяки цьому вона набуває особливого значення у контексті захисту комунікацій, цифрових прав, а також протидії інформаційним атакам.

Сучасні стеганографічні методи розвиваються в умовах підвищених вимог до їх ефективності. Оцінювання якості таких методів базується на сукупності критеріїв, що визначають практичну придатність алгоритму у реальних умовах використання.

По-перше, важливою характеристикою є надійність сприйняття (perceptual reliability) – здатність стеганоповідомлення зберігати високий рівень візуальної чи акустичної якості після вбудовування додаткової інформації. Будь-які спотворення, помітні для людини чи детектовані автоматизованими засобами контролю якості, можуть свідчити про наявність прихованої інформації та знижують ефективність системи.

Другим критерієм є пропускна здатність (capacity), тобто кількість інформації, яку можливо приховати без порушення надійності сприйняття та стійкості. Висока пропускна здатність забезпечує можливість передавання значних обсягів даних, однак часто супроводжується компромісом із дотриманням інших критеріїв стеганографічної якості.

Третій аспект – стійкість до атак проти вбудованого повідомлення (robustness). У практичних сценаріях мультимедійні файли можуть піддаватися стисненню, фільтрації, перетворенням чи перекодуванню. Ефективний стеганографічний метод повинен гарантувати відновлення прихованого повідомлення навіть після таких спотворень.

Нарешті, не менш важливим критерієм є стійкість до стеганоаналізу (undetectability), тобто здатність алгоритму протидіяти статистичним і машинним методам виявлення факту приховування. Саме цей параметр визначає реальну стійкість стеганосистеми та її здатність забезпечувати непомітний обмін інформацією у ворожому середовищі.

Для більшості сучасних стеганографічних методів досягнення оптимального балансу між надійністю сприйняття, пропускною здатністю та стійкістю до атак проти вбудованого повідомлення забезпечується шляхом використання областей перетворень – таких як дискретне косинусне перетворення (DCT), дискретне вейвлет-перетворення (DWT) або сингулярний розклад (SVD). Робота в цих просторах дозволяє ефективно розподіляти зміни у прихованому носії, зменшуючи візуальні спотворення та підвищуючи стійкість до атак.

Однак такий підхід має низку суттєвих недоліків. Виконання перетворень вимагає значних обчислювальних ресурсів, особливо при роботі з високороздільними мультимедійними об’єктами. Крім того, багаторівнева структура алгоритмів ускладнює реалізацію та аналіз методів, знижує їх швидкодію та створює труднощі під час адаптації до різних форматів даних.

Альтернативним шляхом підвищення ефективності є використання концепції кодового управління (code-based control), яка дозволяє впливати на процес вбудовування не через зміну області представлення даних, а через керування внутрішніми кодовими структурами самого повідомлення. Суть підходу полягає у тому, що вибір кодових слів, їхня комбінація та спосіб розподілу в контейнері можуть визначати, яким саме чином здійснюється вбудовування, забезпечуючи оптимальний компроміс між надійністю сприйняття, стійкістю до атак проти вбудованого повідомлення та пропускною здатністю.

Кодове управління відкриває можливість формування адаптивних стеганографічних систем, у яких поведінка алгоритму визначається не лише параметрами сигналу, а й властивостями кодових конструкцій. Це дозволяє будувати легші, швидші та водночас більш гнучкі методи, які можуть підлаштовуватися під умови середовища або тип загрози без необхідності обчислювано складних переходів до інших просторів.

Проте, існуючі дослідження методів з кодовим управлінням проводилися без урахування особливостей контейнерів. Зазвичай аналіз здійснювався на узагальненій вибірці зображень, без диференціації за їх структурними або статистичними

характеристиками. Такий підхід дозволяє оцінити загальні тенденції, однак не враховує, що властивості окремих зображень можуть істотно впливати на ефективність алгоритму вбудовування.

Особливий інтерес становить питання, як різні контейнери забезпечують стійкість до атак, спрямованих проти прихованого повідомлення, насамперед – до атак стисненням (наприклад, JPEG-компресії). Саме стиснення є однією із найпоширеніших типів впливу на мультимедійні дані, тому воно має вирішальне значення для практичної оцінки надійності стеганографічного методу.

Водночас вплив різних кодових слів на стійкість повідомлення при використанні різних типів контейнерів до цього часу залишається практично недослідженим. Невідомо, чи існують закономірності, які пов'язують структуру контейнера з рівнем збереження вбудованої інформації після атак стисненням, і чи можна цю залежність використати для підвищення ефективності системи кодового управління.

Метою роботи є аналіз впливу різних кодових слів на стійкість стеганографічного методу з кодовим управлінням у контексті використання різних типів зображень-контейнерів.

Дослідження спрямоване на виявлення залежностей між структурними характеристиками кодових слів, властивостями контейнера та рівнем збереження прихованої інформації після дії атак, зокрема – атак стисненням.

Аналіз літературних джерел. У сучасній науковій літературі представлено значну кількість робіт, присвячених дослідженню стеганографії, її методів та підходів до захисту інформації у цифрових носіях. Дослідники зосереджують увагу на різних аспектах цієї проблеми: від розробки алгоритмів вбудовування повідомлень у просторовій області та областях перетворень до комбінованих гібридних схем, інтеграції шифрування, а також застосування глибокого навчання для підвищення надійності сприйняття та інших характеристик методу. У більшості публікацій підкреслюється важливість забезпечення одночасно високої пропускної здатності, надійності відновлення повідомлення та стійкості до атак, однак існує суттєва прогалина у дослідженнях, що диференціюють поведінку алгоритмів залежно від типу контейнера і структури кодових слів. Саме ці аспекти становлять актуальний інтерес для подальшого розвитку стеганографічних методів з кодовим управлінням.

Робота Chinnusami M. та співавторів [1] пропонує гібридну схему IWT+SVD і демонструє, що поєднання цілочисельного вейвлет-перетворення із сингулярним розкладом підвищує надійність сприйняття і стійкість вбудованого зображення в умовах різних шумових моделей; автори також надали GUI для візуальної й кількісної оцінки результатів, що підвищує відтворюваність їхніх експериментів. Водночас у статті відсутній системний розгляд впливу різних класів контейнерів (наприклад, гладкі або високочастотні зображення) на поведінку алгоритму, і питання ролі структури кодових слів у забезпеченні стійкості до конкретних атак (зокрема стисненням) практично не піднімається, через що результати важко екстраполювати на задачу диференціації контейнерів.

Kumar N.N. і співавтори у статті [2] поєднують 2D-SWT з хаотичними техніками для попереднього шифрування перед вбудовуванням, що є корисною ідеєю для підвищення захищеності повідомлення; прототип показує практичність підходу для швидкого дослідження інтегрованих схем шифрування і стеганографії. Однак формат і обсяг роботи обмежують глибину експериментального аналізу: автори використовують невеликі/стандартні набори тестових зображень і базові метрики (PSNR/SSIM), не проводячи дослідження залежності від типів контейнерів або детального аналізу поведінки після різних рівнів стиснення.

Mandal P.C. і співавтори пропонують у [3] основану на IWT схему QVD-LSB з акцентом на високу ємність вбудовування і демонструють ретельні експерименти, що дає міцну технічну основу для методології і показує, як оптимізувати bpp без

катастрофічного погіршення якості. Водночас, як і в багатьох подібних роботах, перевірка виконана на типовому наборі зображень і не включає статистичної класифікації контейнерів за їхніми властивостями, а також не аналізує, як різні конструкції кодових слів (наприклад, різні коди виправлення помилок чи розподілу бітів) впливають на відновлення після стиснення.

Матеріали дослідження Nagini R. V. S. S. S. та співавторів [4] про multi-image стеганографію демонструють перспективність підходу розподілу додаткової інформації між кількома носіями як способу підвищити загальну стійкість і надійність сприйняття, проте практичні експерименти здебільшого виконуються на гомогенних або синтетичних множинах зображень; до того ж застосування DNN/складних стратегій розподілу ускладнює інтерпретацію того, яка саме властивість контейнера (текстура, спектр частот тощо) відповідає за кращу стійкість до стиснення. Через це multi-image підхід дає корисні ідеї для підвищення характеристик стеганографічних методів, але не дозволяє оцінити взаємозалежності типу «структура кодового слова – тип контейнера – відсоток помилок після стиснення».

Систематичний огляд Apau R. та співавторів [5] дає широкий структурований огляд сучасних підходів до протидії статистичному стеганоаналізу, підкреслюючи усталені тренди та методологічні прогалини: зокрема, автори прямо зазначають недостатню різноманітність тестових наборів і брак досліджень, що диференціюють поведінку алгоритмів за типом контейнерів. Це оглядове джерело слугує важливим підґрунтям для формулювання аргументу про недостатність досліджень саме в питанні взаємодії кодових слів і властивостей контейнера при атаках стисненням.

Нарешті, робота Angulakshmi M. й Deepa M. [6] подає ґрунтовний огляд сучасних нейромережевих підходів до стеганографії, включаючи архітектури типу енкодер/декодер та GAN-моделі, які демонструють високу продуктивність і надійність сприйняття. Проте такі методи, попри свої переваги у глибокому приховуванні інформації, залишаються здебільшого «чорними скриньками» з обмеженою інтерпретованістю. Тому для цілей аналітичного дослідження впливу структури кодових слів, закономірностей їх взаємодії з типом контейнера та пошуку контрольованих параметрів вбудовування більш придатними залишаються класичні, добре формалізовані методи (IWT, SVD, QVD-LSB тощо), які забезпечують можливість математичного опису та відтворюваного аналізу.

Новий напрям у стеганографії пов’язаний із використанням методів з кодовим управлінням, які дозволяють керувати процесом вбудовування інформації на рівні окремих кодових слів який був вперше представлений в роботі [7]. В роботі [8] запропоновано стеганографічний метод на основі багаторівневих кодових слів, що забезпечує підвищену стійкість до атак і дозволяє гнучко розподіляти навантаження між різними елементами контейнера, одночасно зберігаючи високу якість зображення. В роботі [9] розширено концепцію на цифрове відео та запропоновано сліпе декодування, що дає змогу відновлювати вбудовану інформацію без доступу до оригінального контейнера, підвищуючи практичну застосовність методу у реальних системах передачі даних. У подальшій роботі [10] детально досліджено ефективність сліпого декодування і показано, що оптимізація структури кодових слів і алгоритму вбудовування дозволяє значно зменшити ймовірність помилок відновлення при різних умовах атак та рівнях стиснення. Ці дослідження окреслюють перспективи розвитку стеганографії нового покоління, де кодове управління виступає ключовим механізмом підвищення стійкості та ефективності вбудовування інформації.

Незважаючи на наявність сучасних робіт, присвячених методам стеганографії з кодовим управлінням та їхню ефективність, у науковій літературі відсутні систематичні дослідження, які б детально аналізували вплив типу контейнера на характеристики таких методів. Зокрема, не розглянуто, як різні властивості зображень чи відео – текстура, спектральні компоненти, частота деталей – взаємодіють із структурою

кодових слів і визначають стійкість до атак, включно з стисненням та іншими поширеними методами втручання. Це створює помітну прогалину, яку актуально заповнити для розуміння реальної ефективності стеганографії з кодовим управлінням у різнорідних цифрових контейнерах.

Опис експерименту. Метою експерименту було з'ясувати, як вибір кодового слова для вбудовування впливає на стійкість прихованої інформації до JPEG-стиску в зображеннях різних типів. Дослідження спрямовувалося на встановлення взаємозв'язку між структурними особливостями зображень, характеристиками кодових слів і точністю відновлення повідомлення після стиску. В експерименті використано 500 зображень формату PNG, розподілених на чотири класи (pic_png1…pic_png4) відповідно до рівня їх текстурованості: гладкі, середньотекстуровані, високодеталізовані та змішані. Така класифікація дала змогу охопити широкий спектр структурних і спектральних характеристик зображень, що є важливим для коректної оцінки впливу вибору кодового слова на стійкість прихованої інформації. Розглядалися шість варіантів вибору кодових слів, які наведені в табл. 1 із відповідним кожному кодовому слову перетворенням Уолша-Адамара: постійна (Const), низькочастотна (LF), низькочастотна комбінована (LF-C), середньочастотна (MF), високочастотна (HF) та Bent. Ці варіанти визначають, які саме коефіцієнти частотної області зазнають модифікації під час вбудовування, формуючи таким чином різні профілі компромісу між надійністю сприйняття стеганоповідомлення та його стійкістю до спотворень, спричинених стиском. Усі кодові слова побудовано на основі функцій Уолша, що забезпечує рівномірний розподіл впливу на задану трансформанту перетворення Уолша-Адамара. Така побудова гарантує контрольоване і збалансоване втручання у структуру зображення. Винятком є бент-кодове слово (Bent), яке сформоване на основі бент-функції – спеціального класу максимально невзаємнокорельованих булевих функцій [11, 12]. Його енергія рівномірно розсіюється по всіх трансформантах простору Уолша-Адамара, створюючи майже ізотропний вплив на частотну область. Саме тому Bent-кодове слово може вважатися еталонним прикладом балансу між хаотичністю та гармонійною рівновагою в частотному представленні.

Для кожного з класу зображень проводилося вбудовування додаткової інформації з використанням послідовно кожного з шести варіантів кодових слів (Const, LF, LF-C, MF, HF та Bent). Кожне зображення-контейнер отримувало однаковий обсяг прихованих даних, що дозволяло порівнювати ефективність різних кодових конструкцій у однакових умовах.

Після вбудовування кожне стеганоповідомлення піддавалося JPEG-стиску з визначеними рівнями якості, що імітувало типові спотворення, до яких можуть потрапляти мультимедійні файли у реальних умовах передачі. Після стиснення проводилося відновлення прихованої інформації, і для кожного експериментального сценарію обчислювався відсоток бітових помилок відновлення.

Таким чином, процедура дозволяла систематично оцінити вплив вибору кодового слова на стійкість прихованої інформації, а також простежити, як тип зображення-контейнера (гладке, середньотекстуроване, високодеталізоване або змішане) модулює ефективність вбудовування та відновлення. Цей підхід забезпечив репрезентативний і контрольований експериментальний майданчик для порівняльного аналізу кодових конструкцій у контексті різних спектральних профілів контейнера.

Таблиця 1

Кодові слова, що брали участь в експерименті і їх перетворення Уолша-Адамара

Кодове слово, що брало участь в експерименті	Перетворення Уолша-Адамара
$Const = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{Const} = \begin{bmatrix} 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$LF = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}$	$W_{LF} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$LFC = \begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{LFC} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$MF = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$	$W_{MF} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$HF = \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}$	$W_{HF} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 64 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$Bent = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$	$W_{Bent} = \begin{bmatrix} 8 & 8 & 8 & 8 & 8 & 8 & -8 & -8 \\ 8 & -8 & 8 & -8 & 8 & -8 & -8 & 8 \\ 8 & 8 & 8 & 8 & 8 & 8 & -8 & -8 \\ 8 & -8 & 8 & -8 & 8 & -8 & -8 & 8 \\ 8 & 8 & 8 & 8 & 8 & 8 & -8 & -8 \\ 8 & -8 & 8 & -8 & 8 & -8 & -8 & 8 \\ -8 & -8 & -8 & -8 & -8 & -8 & 8 & 8 \\ -8 & 8 & -8 & 8 & -8 & 8 & 8 & -8 \end{bmatrix}$

Результати та обговорення. Далі ми представляємо результати дослідження впливу вибору кодових слів на стійкість стеганоперетворення до JPEG-стиску для різних класів зображень. Для кожного експериментального сценарію обчислювався відсоток бітових помилок відновлення після стиску. Узагальнені дані за всіма класами зображень та варіантами кодових слів наведені у табл. 2, що дозволяє порівняти ефективність кожної кодової конструкції та простежити закономірності взаємодії між структурними характеристиками контейнера і типом кодового слова.

Таблиця 2.

Відсоток бітових помилок для кожного класу зображень із застосуванням різних кодових слів

Матриця	Група зображень	JPEG Стиск									
		10	20	30	40	50	60	70	80	90	100
Постійна (Const)	pic_png1	40.2	31	22.8	15.9	10.9	7.3	3.9	1	0.3	0.1
	pic_png2	40.3	31.2	23.4	16.9	12	8.5	5	2	0.9	0.4
	pic_png3	40.1	30.6	22.8	16.3	10.9	8	4.9	2.2	1.2	0.7
	pic_png4	40.2	30.8	22.7	16.2	11	7.8	4.8	2	1.1	0.5
Низькочастотна (LF)	pic_png1	42.3	31.4	20.2	11.28	7.2	5	2.8	1.3	0.2	0
	pic_png2	42	31.6	21.3	12.9	8.6	6.4	3.8	2	0.4	0.2
	pic_png3	41.8	30.8	19.6	10	5.7	3.8	1.8	0.8	0.1	0
	pic_png4	42.2	30.8	19.6	10.3	6.1	4.2	1.9	0.9	0.2	0
Низькочастотна комбінована (LF-C)	pic_png1	44.7	36.4	26.5	15.9	9.3	6.7	4.5	2.8	0.8	0
	pic_png2	44.7	36.1	26.8	17.4	10.8	8.2	5.7	3.6	1	0.2
	pic_png3	44.5	35.6	26.2	15.4	7.5	4.9	2.9	1.5	0.3	0
	pic_png4	45.1	36.2	25.9	15.2	7.9	5.3	3.2	1.6	0.4	0
Середньочастотна (MF)	pic_png1	45.6	38	28.2	18.4	8.8	5.9	4.4	3	0.8	0
	pic_png2	45.5	37.6	28.4	20	10.9	7.9	6	4.2	1.3	0.2
	pic_png3	45.3	37.1	27.6	18.8	7.3	4.6	3	1.7	0.4	0
	pic_png4	46	38	27.7	17.8	7.4	4.6	3	1.8	0.5	0
Високочастотна (HF)	pic_png1	49.8	49.6	49.4	49.3	49.2	49	48.6	47.9	43.9	0
	pic_png2	49.8	49.7	49.5	49.3	49.2	48.9	48.4	47.3	41.2	0
	pic_png3	49.8	49.7	49.5	49.3	49.2	48.9	48.6	47.6	42	0
	pic_png4	49.8	49.7	49.5	49.4	49.2	49	48.6	47.7	42	0
Бент (Bent)	pic_png1	46.1	42	37.9	34.3	30.4	26.9	21.4	14.4	4	0
	pic_png2	46.3	42.1	38.2	34.7	31	27.9	22.6	15.4	4.4	0.2
	pic_png3	46.1	41.8	37.9	34.5	30.8	27.4	21.7	13.9	3.1	0
	pic_png4	46.2	41.9	37.9	34.4	31	27.6	22.4	14.9	3.5	0

Аналіз результатів експерименту дозволяє зробити кілька ключових висновків. По-перше, як видно з даних табл. 1.2, зеленим кольором виділені найбільш ефективні кодові слова, які демонструють найнижчий рівень бітових помилок відновлення і можуть бути рекомендовані для практичного використання в системах стеганографії з кодовим управлінням. По-друге, якщо не очікується впливу атак стисненням, доцільно використовувати високочастотне кодове слово, оскільки воно забезпечує максимальну надійність сприйняття контейнера і мінімальні візуальні спотворення, однак його стійкість до JPEG-стиску та інших втручань практично відсутня. По-третє, низькочастотне кодове слово показує високу ефективність при середніх рівнях стиснення до QF=20; для ще більш жорсткого стиску більш доцільним стає застосування кодового слова, що впливає на постійну складову, оскільки воно зберігає відновлюваність бітів навіть у сильно стиснутих зображеннях.

Розподіл ефективності кодових слів також залежить від класу зображень. Для гладких зображень (pic_png1) низько- та середньочастотні кодові слова забезпечують стабільно низький відсоток помилок, тоді як високочастотні компоненти майже одразу втрачають вбудовану інформацію при стиску. У середньотекстурованих та високодеталізованих зображеннях (pic_png2–pic_png3) перевага кодових слів, що впливають на низькі та середні частоти, менш помітна, проте вони все одно перевершують високочастотні варіанти за стійкістю. Зображення змішаного типу (pic_png4) демонструють проміжні результати, при цьому Bent-кодове слово зберігає передбачуваний рівень відновлення для всіх груп, що свідчить про його універсальність.

Bent-кодове слово, бувши реалізацією максимально невзаємнокорельованих булевих функцій, забезпечує рівномірний розподіл енергії по всіх трансформантах Уолша-Адамара. Завдяки цьому воно демонструє високу стійкість незалежно від спектрального профілю зображення та рівня стиску, поступово знижуючи кількість помилок зі збільшенням коефіцієнта якості JPEG.

Висновки. У роботі проведено системне експериментальне дослідження впливу вибору частотного кодового слова на стійкість стеганографічного вбудовування в зображеннях різних типів. Результати показали, що структура кодового слова істотно впливає на бітову похибку відновлення після стиску, а характер залежності змінюється залежно від класу зображення. Вплив типу контейнера на стійкість також виявлено, однак він є відчутно меншим порівняно з ефектом вибору кодового слова:

1. Встановлено, що низькочастотне кодове слово забезпечує найкращий баланс між надійністю сприйняття та стійкістю для зображень при рівнях якості JPEG QF > 20. Для жорстких умов стиску (QF ≤ 20) ефективнішим є кодове слово, що впливає на постійну складову (Const), оскільки воно дозволяє зберігати відновлюваність прихованих даних навіть у сильно стиснутих контейнерах.

2. Для сценаріїв, де стійкість до атак не є критичною, доцільно використовувати високочастотне кодове слово, що забезпечує мінімальні візуальні спотворення контейнера та високу надійність сприйняття.

3. Bent-кодове слово продемонструвало стабільні результати для всіх типів зображень і рівнів стиску, причому розкид відсотків помилок виявився найменшим. Це підтверджує універсальний характер його спектрального розподілу та можливість використання Bent-кодових слів як еталонних або контрольних конструкцій у системах стеганографії з кодовим управлінням.

4. У цілому можна стверджувати, що вибір кодового слова слід здійснювати адаптивно:

- для QF > 20 – перевага низькочастотних кодових слів;
- для QF ≤ 20 – постійне кодове слово;
- якщо важливою є незалежність стійкості стеганоповідомлення від класу контейнера – Bent кодове слово демонструє такі властивості.

Отримані результати формують основу для подальшої розробки адаптивних стеганографічних систем з кодовим управлінням, де вибір частотного профілю кодового слова може автоматично підлаштовуватися під спектральні властивості контейнера та очікуваний рівень стиску.

Список літератури

1. Chinnusami M. Analysis of hybrid integer wavelet transform and singular value decomposition for image steganography under various noise conditions. *Scientific Reports*. 2025. Vol. 15, No. 1. P. 31610. DOI: 10.1038/s41598-025-17020-2
2. Kumar N. N., Viswanathan R., Kumar P. S. An Efficient Approach on Image Encryption Steganography based on 2D SWT with Chaotic Techniques. *4th International Conference*

on Soft Computing for Security Applications. IEEE. 2024. P. 479-486. DOI: 10.1109/icscsa64454.2024.00083

3. Mandal P.C., Mukherjee I., Chatterji B.N. Integer wavelet transform based high performance secure steganography scheme QVD-LSB. *Multimedia Tools and Applications.* 2024. Vol. 83, No. 23. P. 62651-62675. DOI:10.1007/s11042-023-17927-w
4. Nagini R.V. Advancing communication security through multi-image steganography. AIP Conference Proceedings. *AIP Publishing LLC*. 2025. Vol. 3263, No. 1. P. 150001. DOI: 10.1063/5.0261581
5. Apau R. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PloS one.* 2024. Vol. 19, No. 9. P. e0308807. DOI: 10.1371/journal.pone.0308807
6. Angulakshmi M., Deepa M. Image Stenography Using Deep Learning Techniques. Enhancing Steganography Through Deep Learning Approaches. *IGI Global*. 2025. P. 53-74. DOI: 10.4018/979-8-3693-2223-9.ch003
7. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale.* 2021. No. 4 (52). P. 115-130. DOI:: 10.52254/1857-0070.2021.4-52.11
8. Кобозєва А.А., Соколов А.В. Стеганографічний метод з кодовим управлінням вбудовуванням інформації на основі багаторівневих кодових слів. *Вісті вищих учбових закладів. Радіоелектроніка.* 2023. Т. 66, №4. С. 205-222. DOI: 10.20535/s0021347023040052
9. Кілко В.В., Соколов А.В., Баландіна Н.М. Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео. *Кібербезпека та комп'ютерно-інтегровані технології.* 2024. С. 110-114.
10. Sokolov A.V., Ihnatenko O.O., Balandina N.M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problems of regional energetics.* 2024. Vol. 62, No. 2. P. 121-137. DOI: 10.52254/1857-0070.2024.2-62.11
11. Rothaus O. S. On "bent" functions. *Journal of Combinatorial Theory, Series A.* 1976. Vol. 20, No. 3. P. 300-305. DOI: 10.1016/0097-3165(76)90024-8
12. Sokolov A.V., Tsevukh I.V. Construction Method for Infinite Families of Bent Sequences. *Journal of Telecommunication, Electronic and Computer Engineering*. 2018. Vol. 10, No. 2. P. 51-54.

ASSESSMENT OF THE ROBUSTNESS OF A STEGANOGRAPHIC METHOD WITH CODE-BASED CONTROL FOR DIFFERENT CLASSES OF CONTAINERS

Kilko V.V., Sokolov A.V.

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine

The paper presents the results of experimental research on the influence of the choice of codeword on the reliability of perception and robustness of steganographic embedding in images. The paper focuses on an approach with code control, which enables the control of information hiding through code structure parameters without altering the data representation domain. The research was conducted on a set of 500 images classified by texture level (smooth, medium-textured, highly detailed, and mixed), which enabled the establishment of patterns between the type of container, the choice of codeword, and the recoverability of the hidden message after JPEG compression. Six types of codewords were considered in the experiment: constant (Const), low-frequency (LF), combined low-frequency (LF-C), medium-frequency (MF), high-frequency (HF), and Bent. For each image, embedding and subsequent recovery of data after compression were performed at quality levels QF=10…100, and the efficiency was evaluated by the recovery bit error rate. The results confirmed that the choice of codeword has a decisive influence on the stability of the hidden information, while the difference between the classes of container images has a noticeable but incomparable effect in scale. It was found that the low-frequency codeword provides the optimal robustness for QF>20, while the constant codeword is effective for hard compression (QF≤20). The high-frequency codeword is advisable to use only in scenarios where the priority is to preserve maximum reliability of perception, and robustness is not critical. The bent codeword demonstrated the smallest spread in the percentage of errors during extraction among all image classes, confirming its universality and uniform energy distribution in the Walsh-Hadamard domain. The proposed recommendations allow the formation of adaptive steganography systems with code control, capable of automatically selecting the frequency profile of the codeword according to the properties of the container and the level of expected compression. The results obtained can be used to improve the efficiency and reliability of steganographic methods in practical systems.

Keywords: steganography, JPEG, code control, codeword, Walsh-Hadamard transform, bent functions, robustness.

DOI 10.15276/imms.v16.no1.116
УДК 623.746:534.6:004.942

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 116-125

МОДЕЛЮВАННЯ КОМБІНОВАНОЇ АКУСТИЧНОЇ СИСТЕМИ ВИЯВЛЕННЯ ТА АКТИВНОЇ ПРОТИДІЇ ПОВІТРЯНИМ ЦІЛЯМ

П.К. Ніколюк, Д.Ю. Кохан

Донецький національний університет імені Василя Стуса
21, 600-річчя вул., Вінниця, 21021, Україна
Emails: p.nikolyuk@donnu.edu.ua, kokxan.d@donnu.edu.ua

Представлено результати розробки та моделювання інтегрованої симуляційної системи, що поєднує підсистему пасивної акустичної локації та підсистему активної протидії повітряним цілям. Запропоновано гетерогенну архітектуру сенсорного масиву, яка складається з двох вузькоспрямованих («shotgun») та двох всеспрямованих («omni») мікрофонів, і алгоритмічно реалізується з використанням зваженого методу найменших квадратів (WLS). Проведено порівняльний аналіз точності локалізації для WLS і класичного OLS у діапазоні співвідношення сигнал/шум від –10 до +20 дБ. Доведено, що WLS забезпечує зниження середньоквадратичної похибки локалізації більш ніж удвічі за низького SNR. Друга частина роботи присвячена оцінюванню бойової ефективності адаптивного методу наведення «Pure Pursuit» у реалістичних умовах із шумами, часовими затримками та обмеженням маневреності ракети. Результати підтверджують критичну роль точності локалізації та динамічного наведення у формуванні загальної ефективності системи «виявлення – ураження».
Ключові слова: пасивна акустична локація, зенітно-ракетний комплекс, зважений метод найменших квадратів, Pure Pursuit, ймовірність ураження, симуляційне моделювання.

Вступ. Сучасні умови ведення бойових дій та охорони критичної інфраструктури висувають підвищені вимоги до засобів виявлення повітряних загроз. Особливу небезпеку становлять малорозмірні низьколітаючі об’єкти, зокрема безпілотні літальні апарати та крилаті ракети, що ускладнює їх виявлення традиційними радіолокаційними системами через малу ефективну площу розсіювання та можливість маневрування поблизу рельєфу місцевості [1].

У цій ситуації пасивні акустичні системи локалізації розглядаються як перспективна альтернатива або доповнення до радіолокації. Пасивна акустика забезпечує прихованість роботи, відносно низьку вартість розгортання та певну стійкість до радіоелектронних засобів придушення, що робить її привабливою для застосувань у системах протидії малим повітряним цілям [2]. Ефективність акустичних підходів значною мірою залежить від архітектури сенсорного масиву та методів обробки сигналів, зокрема від оцінювання різниць часу приходу сигналів (TDOA) і використання статистично обґрунтованих процедур оцінювання положення [3].

Більшість існуючих досліджень зосереджено на задачах локалізації та оцінювання точності визначення положення цілі, при цьому рідко проводиться кількісний аналіз впливу вибору конфігурації сенсорів і алгоритмів оцінювання на кінцеву бойову ефективність інтегрованої системи «виявлення — ураження». Залишається недостатньо вивченим, яким чином зміни в архітектурі масиву та в процедурах зважування вимірювань транслюються у зміну ймовірності ураження цілі за реалістичних умов оперативної роботи засобу протидії [4].

У роботі запропоновано комплексну симуляційну модель, що поєднує підсистему пасивного акустичного виявлення, алгоритми локалізації на базі TDOA та динамічну модель засобу активної протидії. У межах цієї моделі досліджено вплив комбінованих конфігурацій мікрофонних масивів (вузькоспрямовані «shotgun» і всеспрямовані «omni») та застосування зваженого методу найменших квадратів (WLS) на точність

локалізації (RMSE) при різних рівнях співвідношення сигнал/шум (SNR). Додатково оцінено ефективність методу наведення ракети типу «Pure Pursuit» у задачі перехоплення за реалістичних обмежень маневреності ракети та наявності стохастичних похибок у вимірюваннях.

Мета роботи. Основною метою даної роботи є розробка, валідація та дослідження комплексної симуляційної моделі інтегрованої системи «акустична локація — засіб активної протидії», яка дозволяє кількісно оцінювати вплив архітектурних і алгоритмічних рішень підсистеми виявлення на кінцеву оперативно-бойову ефективність комплексу. Модель побудована так, щоб відтворювати реалістичні умови оперативного застосування: варіації співвідношення сигнал/шум, стохастичні похибки вимірювань, а також кінематичні й тактичні обмеження засобу ураження. Поставлена мета передбачає отримання кількісних метрик (зокрема RMSE локалізації та ймовірності ураження) й системний аналіз залежностей між параметрами сенсорної підсистеми, методами обробки даних та результатом перехоплення.

Для досягнення цієї мети сформульовано та реалізовано низку науково-технічних задач. Перша задача полягає в розробці та порівняльній оцінці методів локалізації для двох сенсорних конфігурацій: контрольної (чотири всеспрямовані мікрофони – «omni») з використанням класичного методу найменших квадратів (OLS) та пропонованої комбінованої конфігурації (дві вузькоспрямовані і дві всеспрямовані) із застосуванням статистично обґрунтованого зваженого методу найменших квадратів (WLS). Для обох варіантів передбачається чисельний експеримент у широкому діапазоні SNR із метою оцінки стабільності алгоритмів, розподілу похибки та статистичних характеристик оцінок положення цілі.

Друга задача спрямована на кількісну оцінку кінцевої бойової ефективності засобу активної протидії при використанні адаптивного алгоритму наведення ракети типу «Pure Pursuit». У межах цієї задачі моделюються реалістичні обмеження: обмежена маневреність і енергетичний ліміт ракети, випадкові втрати супроводу цілі та занижений рівень SNR у сенсорній підсистемі. Вивчається залежність ймовірності ураження від ключових параметрів сценарію, зокрема від швидкості цілі, та взаємозв’язок між точністю локалізації й успішністю перехоплення.

Очікуваний результат роботи – надання кількісних доказів ефективності інтегрованого підходу: показати, наскільки застосування комбінованого масиву й WLS знижує похибку локалізації порівняно з класичною архітектурою, і як це, у свою чергу, підвищує ймовірність ураження при реалістичних умовах. Крім того, робота має окреслити практичні рекомендації щодо проєктування сенсорної підсистеми та вибору алгоритмів наведення для систем протидії малим повітряним цілям, а також визначити напрями подальших досліджень і вдосконалення моделі.

Основна частина. Для досягнення поставленої мети було розроблено комплексну двовимірну симуляційну модель, яка імітує повний цикл роботи інтегрованої системи протидії. Архітектурно модель складається з трьох ключових, взаємопов’язаних підсистем.

Першою є підсистема акустичного виявлення, що відповідає за моделювання фізичного рівня. Вона імітує генерацію тонального акустичного сигналу повітряною ціллю, його поширення в середовищі з урахуванням геометричного затухання (обернено пропорційно відстані) та додавання адитивного білого гаусового шуму, що визначається заданим рівнем співвідношення сигнал/шум (SNR). Ця підсистема також моделює прийом сигналу мікрофонним масивом, застосовуючи до нього відповідні діаграми спрямованості.

Другою є підсистема локалізації, яка виконує первинну та вторинну обробку даних. Вона отримує змодельовані сигнали з мікрофонів, здійснює оцінку різниць часу прибуття (TDOA) між парами сенсорів та, на основі цих даних, виконує обчислення 2D-координат цілі. Ця підсистема реалізує два різні алгоритми мультилатерації для

порівняльного аналізу: звичайний метод найменших квадратів (OLS) та зважений метод найменших квадратів (WLS).

Третьою є підсистема активної протидії, що імітує логіку та динаміку мобільного зенітно-ракетного комплексу (ЗРК). Вона функціонує як скінченний автомат [5], отримуючи координати від підсистеми локалізації. На основі цих даних та власної логіки, ЗРК приймає рішення про перехоплення, моделює політ ракети за заданим методом наведення та визначає факт ураження або промаху [6].

Загальний вигляд головного вікна симуляційної моделі, що візуалізує одночасну роботу всіх трьох підсистем, наведено на рисунку 1. На ньому відображено 2D-карту оперативної обстановки з позиціями мікрофонів (М1 – М4), засобу ураження (ЗРК) та його зоною ефективності, а також реальні (отримані від моделі руху) та оцінені (отримані від підсистеми локалізації) траєкторії цілей.

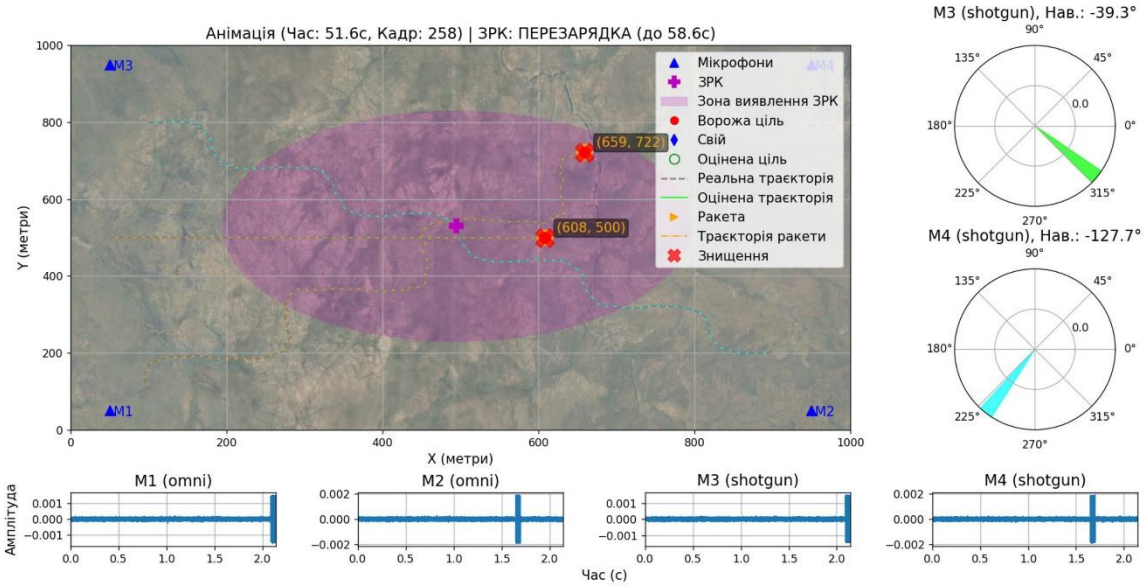


Рис. 1. Загальний вигляд симуляційної моделі інтегрованої системи «виявлення – ураження»

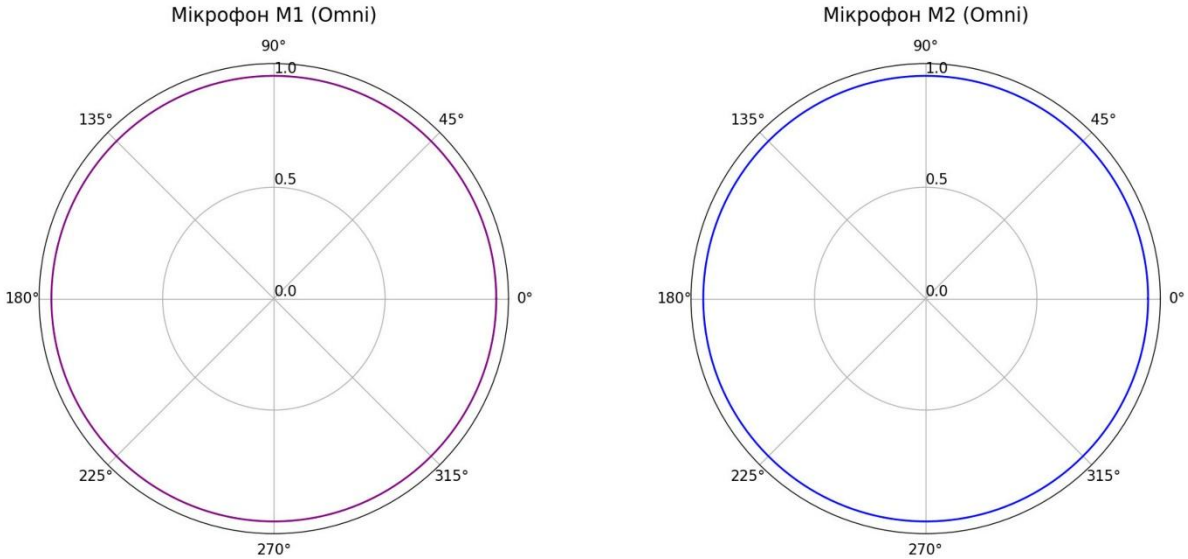


Рис. 2. Діаграми спрямованості всеспрямованих мікрофонів (М1 та М2) у полярній системі координат

В основі моделі виявлення лежить припущення, що повітряна ціль (БПЛА) генерує тональний акустичний сигнал на домінантній частоті f_0. Для простоти, у моделі цей сигнал представлено у вигляді синусоїди з амплітудою A:

$$s(t) = A\sin(2\pi f_0 t) \tag{1}$$

Поширюючись від джерела (цілі) з координатами (x_T, y_T) до k-го мікрофона, розташованого в точці (x_k, y_k), сигнал зазнає двох основних впливів: затухання, обернено пропорційного відстані d_k, та часової затримки τ_k. Крім того, на вході кожного мікрофона додається адитивний білий гаусів шум $n_k(t)$. Таким чином, прийнятий k-м мікрофоном сигнал $r_k(t)$ описується рівнянням:

$$r_k(t) = \frac{A}{d_k}\sin(2\pi f_0(t-\tau_k)) + n_k(t) \tag{2}$$

де відстань d_k та часова затримка τ_k визначаються як:

$$d_k = \sqrt{(x_T - x_k)^2 + (y_T - y_k)^2},\ \tau_k = d_k / c \tag{3}$$

причому c – швидкість звуку, а $n_k(t)$ – адитивний білий гаусів шум. Потужність шуму $n_k(t)$ визначається через параметр співвідношення сигнал/шум (SNR), що задається у децибелах (дБ):

$$SNR_{\text{dB}} = 10\log_{10}(P_s / P_n) \tag{4}$$

де P_s та P_n — середня потужність сигналу та шуму відповідно.

Визначення координат цілі базується на методі TDOA. Для цього спочатку необхідно оцінити різниці в часі прибуття сигналу $\Delta t_{k,0}$ між кожним k-м мікрофоном та опорним мікрофоном (в даній роботі – мікрофон з індексом 0). Ця оцінка $\hat{\tau}_{k,0}$ знаходиться за допомогою методу узагальненої взаємної кореляції (GCC-PHAT), який шукає часовий зсув τ, що максимізує функцію кореляції між сигналами [7]:

$$\hat{\tau}_{k,0} = \underset{\tau}{\operatorname{argmax}} \int_{-\infty}^{\infty} r_0(t) r_k(t+\tau) dt \tag{5}$$

де $r_0(t)$ та $r_k(t)$ — сигнали, прийняті опорним та k-м мікрофоном відповідно. Отриманий масив часових затримок $[\hat{\tau}_{1,0}, \hat{\tau}_{2,0}, \ldots, \hat{\tau}_{N-1,0}]$ є вхідними даними для підсистеми локалізації.

Отриманий набір оцінок різниць часу прибуття $[\hat{\tau}_{1,0}, \ldots, \hat{\tau}_{N-1,0}]$ є вхідними даними для задачі мультилатерації, яка полягає у розв'язанні системи нелінійних рівнянь відносно невідомих координат цілі (x, y). Кожне рівняння k в системі описує гіперболічну криву, що відповідає виміряній часовій затримці $\hat{\tau}_{k,0}$:

$$\sqrt{(x-x_k)^2 + (y-y_k)^2} - \sqrt{(x-x_0)^2 + (y-y_0)^2} = c \cdot \hat{\tau}_{k,0} \tag{6}$$

де k пробігає значення від 1 до $N-1$ (кількість мікрофонів мінус опорний). Ця система є надлишковою і розв'язується чисельними методами, мінімізуючи сукупну похибку [8]. Ключовим аспектом даної роботи є порівняння двох різних підходів до розв'язання цієї системи, що безпосередньо пов'язані з двома різними конфігураціями сенсорного масиву.

Перша конфігурація, контрольна, складається з чотирьох ідентичних всеспрямованих мікрофонів. Вони приймають сигнал та навколишній шум однаково з усіх напрямків. Для цієї однорідної системи вимірювань природно застосовувати звичайний метод найменших квадратів (OLS). Цей метод мінімізує суму квадратів різниць (нев'язок) між розрахованими та виміряними TDOA, припускаючи, що всі вимірювання $\hat{\tau}_{k,0}$ мають однакову надійність (однакову дисперсію похибки) [9]:

$$R_{\text{OLS}}(x,y) = \sum_{k=1}^{N-1} \left((\tau_k(x,y) - \tau_0(x,y)) - \hat{\tau}_{k,0} \right)^2 \to \min \tag{7}$$

де $\tau_k(x,y)$ та $\tau_0(x,y)$ — це теоретичні часи прибуття (розраховані з d_k / c та d_0 / c), а $\hat{\tau}_{k,0}$ — виміряна TDOA.

Друга конфігурація, пропонована, є комбінованою та складається з двох всеспрямованих («omni») та двох вузькоспрямованих мікрофонів типу «shotgun». Вузькоспрямовані мікрофони мають вузький головний пелюсток, що дозволяє їм досягати значного коефіцієнту підсилення сигналу та придушення шуму з-поза осі. В моделі ці мікрофони динамічно наводяться на попередню оцінену позицію цілі, що забезпечує значне локальне покращення SNR [10] (в даній моделі оцінене як +15.6 дБ).

Це створює неоднорідну систему вимірювань: оцінки TDOA, отримані з використанням «shotgun» мікрофонів, є значно надійнішими (мають меншу дисперсію похибки), ніж оцінки від «omni» мікрофонів, особливо при низьких загальних SNR.

Застосування OLS до такої системи є статистично неефективним, оскільки він ігнорує цю різницю в надійності. Тому для комбінованої конфігурації пропонується зважений метод найменших квадратів (WLS) [11, 12]. WLS мінімізує суму квадратів нев'язок, зважених за їхньою надійністю. Ваговий коефіцієнт w_k для кожної TDOA-оцінки $\hat{\tau}_{k,0}$ обирається обернено пропорційним до її дисперсії $\sigma^2_{\text{TDOA},k}$ [13]:

$$w_k = \frac{1}{\sigma^2_{\text{TDOA},k}} \tag{8}$$

Дисперсія похибки TDOA $\sigma^2_{\text{TDOA},k}$ залежить від суми дисперсій похибок сигналів на опорному (σ_0^2) та k-му мікрофоні (σ_k^2). Кожна з цих дисперсій, у свою чергу, обернено пропорційна ефективному SNR на даному мікрофоні [7]:

$$\sigma^2_{\text{TDOA},k} = \sigma_0^2 + \sigma_k^2 \quad , \quad \sigma_i^2 \propto \frac{1}{\text{SNR}_i} \tag{9}$$

Таким чином, TDOA-оцінки, отримані з пари «shotgun»-мікрофонів, матимуть найменшу дисперсію і, відповідно, найбільшу вагу w_k. Це дозволяє алгоритму WLS приділяти більше уваги надійним даним і менше — зашумленим. Функція втрат WLS, що мінімізується, має вигляд:

$$R_{\text{WLS}}(x,y) = \sum_{k=1}^{N-1} w_k \left((\tau_k(x,y) - \tau_0(x,y)) - \hat{\tau}_{k,0} \right)^2 \to \min \tag{10}$$

Цей підхід дозволяє коректно інтегрувати переваги вузькоспрямованих сенсорів на алгоритмічному рівні, що є ключовою гіпотезою першої частини дослідження.

Оцінені координати цілі (x, y), отримані від підсистеми локалізації, слугують вхідними даними цілевказання для третьої ключової компоненти моделі — підсистеми активної протидії. Ця підсистема імітує поведінку та кінематику зенітно-ракетного комплексу (ЗРК) в рамках реалістичного сценарію перехоплення.

Логіка роботи ЗРК описується у вигляді скінченного автомату (Finite State Machine, FSM) [6, 14], що є поширеним підходом для моделювання автономних систем. Автомат визначає операційний цикл ЗРК через низку послідовних станів. Базовим станом є «Очікування» (Idle), в якому ЗРК готовий до дії та безперервно отримує оновлені дані про ціль. Коли ціль потрапляє у зону ураження, відбувається перехід у стан «Захоплення» (Engaging), де імітується тактична затримка на підготовку до пуску $T_{\text{launch\_delay}}$, що вносить елемент варіативності. Після затримки відбувається «Пуск» (Launched), і з цього моменту активується модель кінематики та наведення ракети. Незалежно від результату атаки (ураження чи промах), ЗРК переходить у стан «Перезарядка» (Reloading), де він неактивний протягом фіксованого часу, імітуючи час, необхідний на підготовку до наступного перехоплення.

Ключовим елементом другої задачі дослідження є модель наведення ракети, що активується у стані «Пуск». Для кількісної оцінки ефективності використовується адаптивний метод пропорційного переслідування, або «Pure Pursuit». На відміну від примітивних методів, що спрямовують ракету у статичну точку, розраховану в момент пуску, «Pure Pursuit» є динамічним процесом. На кожному кроці симуляції Δt, система наведення ракети обчислює бажаний вектор напрямку $\vec{d}_{\text{des}}(t)$, що веде від поточної позиції ракети $\vec{P}_m(t)$ до поточної оціненої позиції цілі $\vec{P}_T(t)$:

$$\vec{d}_{\text{des}}(t) = \frac{\vec{P}_T(t) - \vec{P}_m(t)}{\left\|\vec{P}_T(t) - \vec{P}_m(t)\right\|} \tag{11}$$

Для забезпечення реалістичності моделі, на кінематику ракети накладено два фундаментальних обмеження. По-перше, ракета має фіксовану швидкість v_m (у даній роботі 180 м/с). По-друге, введено обмежену маневреність: ракета не може миттєво змінити свій поточний вектор напрямку $\vec{v}_{\text{dir}}(t)$ на бажаний $\vec{d}_{\text{des}}(t)$. Введено максимальну кутову швидкість розвороту ракети $\omega_{\max}$. Це означає, що за крок Δt, вектор напрямку може повернутися лише на максимальний кут $\theta_{\max} = \omega_{\max} \cdot \Delta t$. Фактичний новий напрямок $\vec{v}_{\text{dir}}(t + \Delta t)$ знаходиться шляхом повороту $\vec{v}_{\text{dir}}(t)$ в бік $\vec{d}_{\text{des}}(t)$ на кут, що не перевищує $\theta_{\max}$.

Таким чином, оновлення позиції ракети на кожному кроці відбувається за виразом:

$$\vec{P}_m(t + \Delta t) = \vec{P}_m(t) + \vec{v}_{\text{dir}}(t + \Delta t) \cdot v_m \cdot \Delta t \tag{12}$$

Крім кінематичних, у модель другого експерименту введено й інші «реалістичні» стохастичні та тактичні фактори. Ефективність ЗРК тестується в умовах суттєво зашумлених вхідних даних, що відповідає низькому SNR (SNR = -5 дБ). Крім того, існує ненульова ймовірність втрати супроводу цілі, що на поточному кроці підсистема локалізації не надасть оновлених координат, змушуючи ракету летіти "всліпу" до останньої відомої позиції. Нарешті, ракета має обмеження палива і може перебувати в польоті лише обмежений час, після чого атака вважається невдалою. Перехоплення вважається успішним, якщо відстань між ракетою та реальною позицією цілі стає меншою за заданий радіус ураження R_k.

Результати моделювання та їх аналіз. Для валідації розробленої моделі та кількісного порівняння алгоритмічних та архітектурних рішень було проведено два ключових обчислювальних експерименти. Перший з них, присвячений вирішенню першої задачі дослідження, полягав в оцінці точності та стабільності підсистеми локалізації шляхом порівняння двох системних конфігурацій. Перша конфігурація, контрольна, складалася з чотирьох всеспрямованих сенсорів («4 'omni'») з обробкою даних за допомогою звичайного методу найменших квадратів (OLS). Друга, пропонована, включала комбінований масив («2 'shotgun' + 2 'omni'») з обробкою за допомогою зваженого методу найменших квадратів (WLS).

Для обох конфігурацій було проведено серію з 10 симуляцій на кожній тестовій точці для усереднення результатів. Моделювання проводилося у широкому діапазоні співвідношення сигнал/шум (SNR) – від -10 дБ (дуже складні умови виявлення) до +20 дБ (сприятливі умови). Як інтегральну метрику якості використовувалася середньоквадратична похибка (RMSE) локалізації, що показує середнє відхилення оціненої позиції від реальної.

Результати обчислювального експерименту зведено у Таблиці 1 та візуалізовано на рисунку 3.

Таблиця 1.

Порівняльні результати точності локалізації для конфігурацій WLS та OLS

SNR (дБ)	RMSE 2 «shotgun + 2 omni (WLS)» (м)	STD «2 shotgun + 2 omni (WLS)» (м)	RMSE «4 omni (OLS)» (м)	STD «4 omni (OLS)» (м)
-10	1.248	0.075	2.713	0.162
-5	0.702	0.034	1.559	0.062
0	0.395	0.033	0.890	0.041
5	0.224	0.010	0.483	0.029
10	0.124	0.006	0.274	0.010
15	0.070	0.004	0.154	0.008
20	0.040	0.003	0.084	0.005

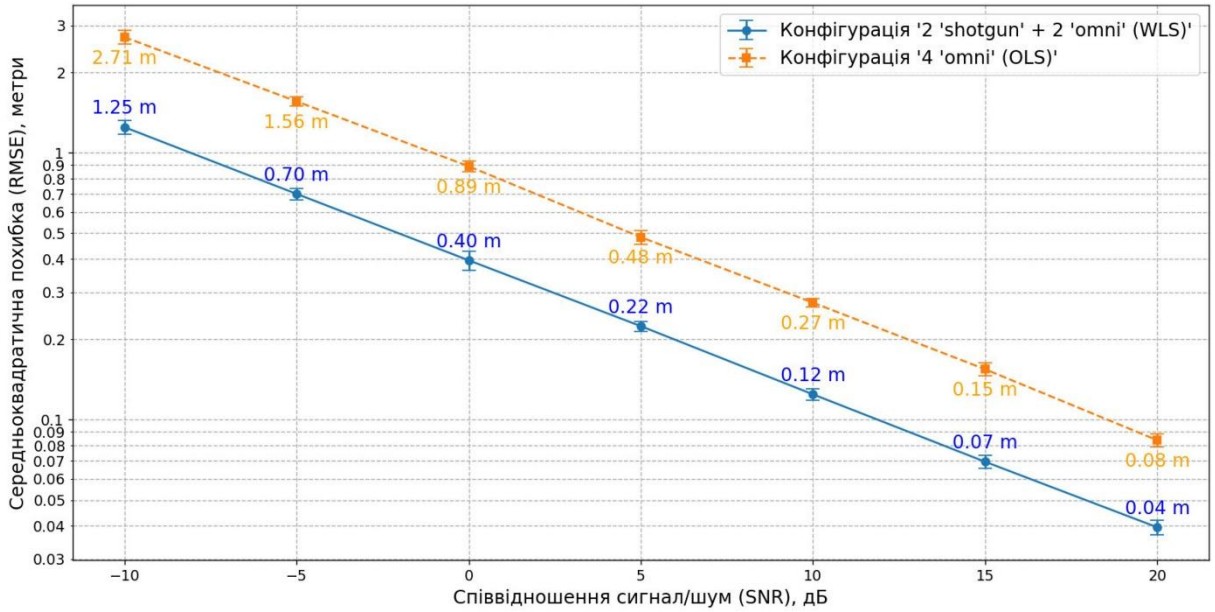


Рис. 3. Залежність точності локалізації (RMSE) від SNR

Аналіз отриманих даних дозволяє зробити кілька ключових висновків. Пропонована конфігурація «2+2 WLS» демонструє суттєво вищу точність локалізації порівняно з контрольною «4 omni OLS» в усьому досліджуваному діапазоні SNR.

Найбільш показовою є різниця в області низьких значень SNR, яка є найскладнішою і водночас найважливішою для пасивних акустичних систем. При SNR = -10 дБ, пропонована система (RMSE 1.248 м) забезпечує точність у 2.17 рази вищу, ніж контрольна (RMSE 2.713 м). Це підтверджує основну гіпотезу: зважений метод найменших квадратів (WLS) ефективно використовує переваги гетерогенного масиву. Алгоритм коректно ідентифікує TDOA-вимірювання, отримані з «shotgun» мікрофонів (де ефективний SNR значно вищий завдяки придушенню шуму), і надає їм більшої ваги при розв'язанні системи рівнянь. На противагу, OLS однаково враховує всі вимірювання, дозволяючи «шумним» даним від «omni» сенсорів погіршувати загальну точність оцінки. Зі зростанням SNR перевага WLS-системи зберігається, хоча абсолютна різниця похибок зменшується, оскільки обидві системи починають працювати в умовах високої достовірності вимірювань.

Отримані у першому експерименті дані підтверджують, що комбінована архітектура сенсорів у поєднанні з WLS-обробкою здатна забезпечити високу точність цілевказання навіть за вкрай несприятливих акустичних умов. Це дає змогу перейти до вирішення другої задачі дослідження: з'ясувати, чи достатньо цієї точності для ефективного перехоплення цілі, та як ця ефективність залежить від параметрів самої цілі.

Для цього було проведено другий обчислювальний експеримент, що моделює повний цикл перехоплення з використанням адаптивного методу наведення. Щоб

наблизити умови до реалістичних, у модель було свідомо введено низку «жорстких» тактичних та кінематичних обмежень, описаних у методології. Зокрема, моделювання проводилося при низькому SNR (-5 дБ); використовувалася повільна ракета ($v_m = 180$ м/с) з обмеженою маневреністю та обмеженим часом польоту (20 сек); також було введено 5% ймовірність зриву супроводу цілі на кожному кроці.

У цьому експерименті оцінювалася ймовірність ураження цілі залежно від її власної швидкості, яка варіювалася від 40 м/с до 120 м/с. Для кожної точки швидкості було проведено 300 симуляційних прогонів для отримання статистично значущої оцінки. Результати наведено у таблиці 2 та на рисунку 4.

Таблиця 2.

Ймовірність ураження цілі при використанні адаптивного методу наведення

Швидкість цілі (м/с)	P_p (%)
40	91%
50	87%
60	87%
70	63%
80	81%
90	79%
100	69%
110	49%
120	29%

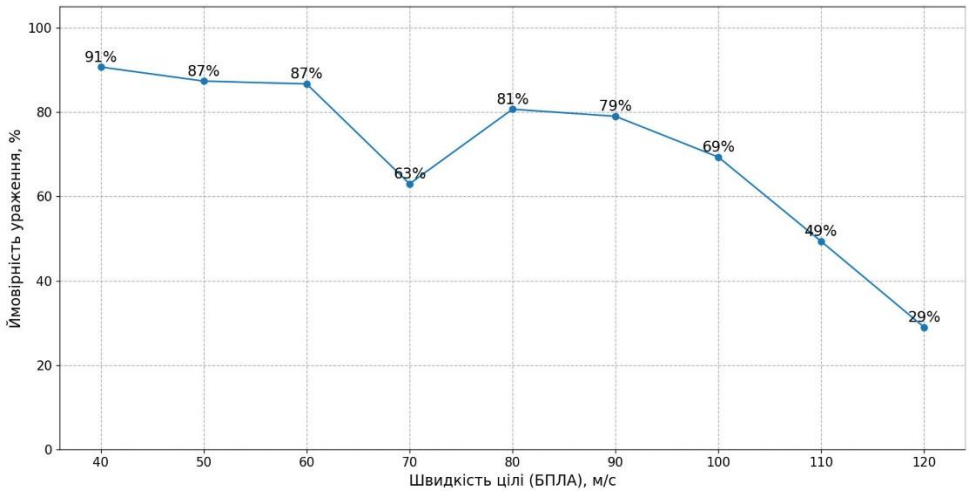


Рис. 4. Залежність ймовірності перехоплення від швидкості цілі для адаптивного методу наведення

Аналіз результатів другого експерименту підтверджує критичну важливість використання адаптивного методу наведення. Навіть за сукупності несприятливих факторів, метод «Pure Pursuit» демонструє високу ефективність проти цілей, що рухаються з відносно низькою швидкістю, досягаючи 91% ймовірності перехоплення для цілі зі швидкістю 40 м/с.

Зі зростанням швидкості цілі спостерігається очікуване, але нелінійне зниження ефективності. Це падіння ймовірності перехоплення (наприклад, до 29% при 120 м/с) пояснюється не стільки похибками локалізації, скільки суто кінематичними обмеженнями самої ракети. Повільна ракета з обмеженою маневреністю фізично не встигає компенсувати швидке переміщення цілі та вийти в точку перехоплення в межах свого енергетичного ліміту. Невеликий стрибок ефективності в районі 80-90 м/с може бути пов’язаний зі стохастичною природою моделі та особливостями геометрії перехоплення у конкретному сценарії.

Загалом, результати другого експерименту доводять, що високої точності локалізації (досягнутої завдяки WLS) недостатньо самій по собі. Для реалізації цієї точності у високий показник ймовірності перехоплення необхідно використовувати адаптивні методи наведення, здатні компенсувати похибки вимірювань та маневри цілі в реальному часі.

Висновки. У ході виконаного дослідження було розроблено та валідовано комплексну симуляційну модель, що інтегрує підсистему пасивної акустичної локації та підсистему активної протидії повітряним цілям. Розроблена модель дозволила кількісно оцінити та порівняти ключові архітектурні та алгоритмічні рішення, що впливають на загальну ефективність системи «виявлення-ураження».

За результатами першого обчислювального експерименту було кількісно доведено перевагу пропонованої комбінованої архітектури сенсорного масиву. Конфігурація, що складається з двох вузькоспрямованих («shotgun») та двох всеспрямованих («omni») мікрофонів, у поєднанні зі зваженим методом найменших квадратів (WLS), продемонструвала значно вищу точність локалізації порівняно з контрольною системою. Зокрема, в умовах низького співвідношення сигнал/шум, пропонований підхід забезпечив підвищення точності (зниження RMSE) у 2.17 разів, підтвердивши, що WLS-алгоритм ефективно використовує надійніші вимірювання від «shotgun» сенсорів.

За результатами другого експерименту, що проводився в реалістичних умовах з урахуванням кінематичних та тактичних обмежень, було оцінено бойову ефективність комплексу. Доведено, що для успішного перехоплення маневрової цілі критично необхідне використання адаптивного методу наведення «Pure Pursuit», який дозволив досягти високих показників ймовірності перехоплення, зокрема 91% для цілі зі швидкістю 40 м/с. Таким чином, робота доводить, що ефективність сучасної системи акустичної протидії залежить від синергії трьох компонентів: архітектури сенсорів (комбінований масив), алгоритму обробки (WLS) та алгоритму наведення. Подальші дослідження можуть бути спрямовані на розширення моделі для 3D-простору та аналіз складніших акустичних ефектів.

Список літератури

1. Casado-Galan E., Gonzalez-Serrano F. J., Ramirez-Rincon J. J., Casar-Corredera J. R. Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management. *Sensors.* 2022. Vol. 22, No. 1. P. 189. URL: https://www.mdpi.com/1424-8220/22/1/189
2. Chiper D., Stanciu T., Anghel A., Popescu D. Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution. *Sensors.* 2022. Vol. 22, No. 4. P. 1453. DOI: 10.3390/s22041453
3. Lim J., Joo J., Kim S.-C. Performance Enhancement of Drone Acoustic Source Localization Through Distributed Microphone Arrays. *Sensors.* 2025. Vol. 25, No. 6. P. 1928. DOI: 10.3390/s25061928
4. Wu S., Zheng Y., Ye K., Cao H., Zhang X., Sun H. Sound Source Localization for Unmanned Aerial Vehicles in Low Signal-to-Noise Ratio Environments. *Remote Sensing.* 2024. Vol. 16, No. 11. P. 1847. URL: https://www.mdpi.com/2072-4292/16/11/1847
5. de Araujo V., Almeida A. P. G. S., Miranda C. T., de Barros Vidal F. A. A Parallel Hierarchical Finite State Machine Approach to UAV Control for Search and Rescue Tasks. *11th International Conference on Informatics in Control, Automation and Robotics. Vienna, Austria.* 2014. Vol. 1. P. 410–415. DOI: 10.5220/0005121104100415
6. Harel D. Statecharts: A visual formalism for complex systems. *Science of Computer Programming.* 1987. Vol. 8, No. 3. P. 231–274. DOI: 10.1016/0167-6423(87)90035-9
7. Knapp C. H., Carter G. C. The generalized correlation method for estimation of time delay. *IEEE Transactions on Acoustics, Speech, and Signal Processing.* 1976. Vol. 24. No. 4. P. 320–327. DOI: 10.1109/TASSP.1976.1162830

8. Altena A., Luesutthiviboon S., de Croon G., Snellen M., Voskuijl M. Comparison of Acoustic Localisation Techniques for Drone Position Estimation Using Real-World Experimental Data. *29th International Congress on Sound and Vibration.Crete, Greece.* 2023.
9. Chan Y. T., Ho K. C. A simple and efficient estimator for hyperbolic location. *IEEE Transactions on Signal Processing.* 1994. Vol. 42, No. 8. P. 1905–1915. DOI: 10.1109/78.301830
10. Liu M., Hu J., Zeng Q., Jian Z., Nie L. Sound Source Localization Based on Multi-Channel Cross-Correlation Weighted Beamforming. *Micromachines.* 2022. Vol. 13. No. 7. P. 1010. DOI: 10.3390/mi13071010. URL: https://www.mdpi.com/2072-666X/13/7/1010
11. Zhang L., Zhang T., Shin H.-S. An Efficient Constrained Weighted Least Squares Method with Bias Reduction for TDOA-Based Localization. IEEE Sensors Journal. 2021. Vol. 21. No. 7. P. 8823–8833. DOI: 10.1109/JSEN.2021.3057448
12. Jin B., Xu X., Zhang T. Robust Time-Difference-of-Arrival (TDOA) Localization Using Weighted Least Squares with Cone Tangent Plane Constraint. *Sensors.* 2018. Vol. 18. No. 3. P. 778. DOI: 10.3390/s18030778. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC5876713
13. Park C.-H., Chang J.-H. Time-of-arrival source localization based on weighted least squares estimator in line-of-sight/non-line-of-sight mixture environments. *International Journal of Distributed Sensor Networks.* 2016. Vol. 12. No. 12. Article ID 168782. DOI: 10.1177/1550147716683827. URL: https://journals.sagepub.com/doi/10.1177/1550147716683827
14. Samek M. Practical Statecharts in C/C++. Quantum Programming for Embedded Systems. Boca Raton: CRC Press, 2002. 304 p. ISBN 978-1-57820-110-5.

MODELING OF A COMBINED ACOUSTIC DETECTION AND ACTIVE COUNTERACTION SYSTEM FOR AERIAL TARGETS

P.K. Nikoliuk, D.Y. Kokhan

Vasyl Stus Donetsk National University
21, 600-richchia Str., Vinnytsia, 21021, Ukraine
e-mail: p.nikolyuk@donnu.edu.ua, kokxan.d@donnu.edu.ua

The paper presents the results of the development and modeling of an integrated simulation system that combines a passive acoustic localization subsystem and an active counter-measure subsystem for aerial targets. A heterogeneous sensor array architecture is proposed, consisting of two narrow-beam (‘shotgun’) and two omnidirectional (‘omni’) microphones, which is algorithmically implemented using the Weighted Least Squares (WLS) method. A comparative analysis of localization accuracy for WLS and classical OLS is carried out over a Signal-to-Noise Ratio (SNR) range from –10 to +20 dB. It is proven that WLS provides a reduction in the Root Mean Square Error (RMSE) of localization by more than twofold at low SNR. The second part of the work is devoted to evaluating the combat effectiveness of the "Pure Pursuit" adaptive guidance method under realistic conditions with noise, time delays, and limited missile maneuverability. The results confirm the critical role of localization accuracy and dynamic guidance in shaping the overall effectiveness of the "detection-to-engagement" system.

Keywords: passive acoustic localization, surface-to-air missile system, Weighted Least Squares (WLS), Pure Pursuit, probability of kill, simulation modeling.

DOI 10.15276/imms.v16.no1.126
УДК 004.056:004.7:004.8

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 126-134

КОГНІТИВНИЙ РІВЕНЬ БЕЗПЕКИ ЯК НАДБУДОВА ПРИКЛАДНОГО РІВНЯ OSI: АНАЛІТИЧНА МОДЕЛЬ, АРХІТЕКТУРА ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Д.І. Прокопович-Ткаченко[1,2,3], О.В. Черкаський[3], Д.О. Черкаський[4], Д.О. Переметчик[1], Б.С. Хрушков[1]

[1]Університет митної справи та фінансів
2/4, Володимира Вернадського вул., 49000, Дніпро, Україна
[2]Інститут інформації, безпеки і права Національної академії правових наук України
3, Орлика Пилипа вул., 01024, Київ, Україна
[3]Державний університет інформаційно-комунікаційних технологій
7, Солом'янська вул., 03110, Київ, Україна
[4]Національний технічний університет «Дніпровська політехніка»
19, Дмитра Яворницького пр., Дніпро, 49005, Україна
Emails: ghoststad88@gmail.com, asherjoseph.c@gmail.com, omega2417@gmail.com, peremetchyk.d@gmail.com, Cherkaskyi.Dav.O@nmu.one

Представлено дослідження нової концепції підвищення кіберзахисту — когнітивного рівня безпеки, який функціонує як додатковий інтелектуальний шар над прикладними сервісами інформаційних систем. Основна ідея полягає у створенні програмної надбудови, здатної розпізнавати зміст запитів, наміри користувачів та нетипові дії у мережевому трафіку. Запропонована архітектура включає три взаємопов'язані модулі: перший виконує аналіз текстових запитів і контексту їх виникнення, другий виявляє поведінкові відхилення на основі часових послідовностей подій, а третій здійснює об'єднання результатів для оцінки загального ризику та прийняття рішень про доступ. Для побудови цих модулів використано сучасні нейромережеві технології — трансформерні, рекурентні та автоенкодерні моделі, що дозволяють створювати адаптивні політики реагування. Реалізовано прототип інтелектуального сервісу, який аналізує текстові дані, активність користувача й контекстні параметри та формує рішення: дозволити дію, вимагати додаткове підтвердження або заблокувати операцію. Отримані результати показують високу точність виявлення ризиків і здатність системи зменшувати кількість помилкових спрацювань. У роботі також розглянуто питання захисту приватності, пояснюваності рішень і надійності роботи моделей. Запропоновано поетапну стратегію впровадження когнітивного рівня безпеки у промислових мережах, цифрових двійниках та корпоративних середовищах, що створює основу для переходу від реактивних до передбачувальних систем захисту.
Ключові слова: когнітивна безпека, рівень безпеки систем, штучний інтелект, машинне навчання, поведінковий аналіз, пояснювані рішення, інтелектуальні політики, контекстний ризик, цифровий двійник, безпечна автентифікація, кіберзахист.

Вступ. Сучасні системи безпеки переходять від традиційного контролю доступу до когнітивних архітектур, що враховують контекст, поведінку та наміри користувача. Класичні методи аутентифікації виявляються неефективними у динамічних цифрових середовищах, тому виникає потреба у багаторівневих рішеннях, здатних аналізувати не лише запит, а й його семантику та поведінкові ознаки. Когнітивний рівень безпеки (CSL) — це інтелектуальна надбудова прикладного рівня, яка оцінює запит разом із технічними, часовими та поведінковими параметрами, виявляє аномалії та запобігає ризиковим діям. Актуальність впровадження CSL визначається в зростанням кількості внутрішніх інцидентів, ускладненням поведінкових патернів у гібридних цифрових середовищах та потребою у пояснюваних і прозорих системах ШІ в межах парадигми Zero Trust.

Огляд літератури. У сучасних дослідженнях кібербезпеки спостерігається тенденція

переходу від реактивних методів до когнітивних архітектур, які здатні враховувати поведінку, контекст та наміри користувача. Класичні підходи до аутентифікації та авторизації, засновані на фіксованих правилах, виявляються недостатньо ефективними в умовах динамічних цифрових екосистем.

Велика кількість досліджень (Vaswani et al., 2017; Hochreiter & Schmidhuber, 1997; Kipf & Welling, 2016; Pang et al., 2021) описує використання глибоких нейронних мереж — трансформерів, рекурентних та графових моделей — для аналізу текстів, поведінкових патернів та виявлення аномалій. Праці Demertzis, Iliadis, Karamchand та інших авторів (2018–2024) демонструють розвиток концепції когнітивних операційних центрів безпеки, здатних поєднувати машинне навчання, контекстну аналітику та принципи Zero Trust Architecture.

Окремі роботи (Gaspar et al., 2024; Patil et al., 2022; Arreche et al., 2024) присвячено пояснюваному штучному інтелекту (Explainable AI), який забезпечує прозорість прийняття рішень системами безпеки. Також значна увага приділяється аспектам privacy by design (Zhang et al., 2024) — захисту приватності та етичності обробки даних у процесах когнітивного аналізу.

Проведений аналіз літератури свідчить, що інтеграція семантичних, поведінкових і контекстних моделей у єдину когнітивну структуру є перспективним напрямом розвитку систем кіберзахисту, який дозволяє перейти від реактивних до передбачувальних механізмів протидії загрозам.

Мета роботи. Метою дослідження є розроблення системної моделі когнітивного рівня безпеки (Cognitive Security Layer, CSL), яка функціонує як інтелектуальна надбудова над прикладним рівнем OSI. Робота спрямована на:

1. Опис архітектури CSL і принципів її побудови.
2. Розроблення алгоритмів аналізу намірів користувача, поведінкових відхилень та контекстних ризиків.
3. Створення пояснюваного механізму злиття ризиків (Explainable Risk Fusion) для прийняття адаптивних рішень.
4. Обґрунтування етичних принципів упровадження когнітивних систем у промислові, корпоративні та хмарні середовища.

Виклад основного матеріалу. Методологічна основа дослідження ґрунтується на поєднанні системного, когнітивного та машинного підходів, що дозволяє інтегрувати аналітичні, поведінкові й контекстні аспекти у єдину модель когнітивної безпеки [4], [5], [15]. Такий підхід відповідає сучасним тенденціям розвитку штучного інтелекту та кіберзахисту, де ключову роль відіграє взаємодія між людиною та інтелектуальними обчислювальними структурами [12], [13].

Основою методології є представлення когнітивного рівня безпеки як метарівня, який поєднує три аналітичні контури:

Семантичний аналіз намірів користувача, реалізований через моделі природної мови (sentence-transformer, MiniLM, MPNet), що забезпечують розуміння змісту запитів і контексту виконання [1], [9].

Поведінкову аналітику, яка базується на послідовному аналізі дій користувача за допомогою рекурентних та автоенкодерних нейронних мереж (GRU-AE, CNN+LSTM) [6], [10], [16].

Контекстну оцінку ризику, яка враховує мережеві, географічні та автентифікаційні фактори доступу, дозволяючи динамічно коригувати політики безпеки відповідно до змін середовища [7], [8].

Для синтезу результатів цих контурів використано механізм когнітивного злиття ризиків (Explainable Risk Fusion), який формує інтегральний показник безпеки на основі вагових коефіцієнтів достовірності кожної моделі. Таке рішення забезпечує адаптивність системи до змінних сценаріїв користувацької поведінки та мінімізує хибні спрацювання у динамічних кіберінфраструктурах [18], [20].Методологія також враховує принципи

Zero Trust Architecture — відсутність апріорної довіри до будь-яких суб'єктів доступу, а також використання пояснюваних моделей (Explainable AI) для прозорості прийнятих рішень [7], [19], [22]. Етична компонента дослідження реалізується через концепцію privacy by design, що передбачає знеособлення поведінкових даних і захист приватності на всіх етапах обробки [23].Загалом запропонований методологічний підхід поєднує аналітичні властивості штучного інтелекту, принципи когнітивних наук та інженерію кіберзахисту, формуючи основу для подальшої розробки когнітивних політик у промислових і корпоративних інфраструктурах нового покоління [11], [14], [17]

Архітектура CSL містить три основні модулі:

Модуль A (Intent + Context) — визначає семантику запиту користувача через sentence-embedding та метадані (endpoint, метод, геолокація, MFA).

Модуль B (Behavioral Anomaly Detection) — використовує GRU-Autoencoder або 1D-CNN+BiLSTM для виявлення відхилень у послідовності подій (keypress, click, API call).

Fusion / Policy Engine — формує інтегрований показник когнітивного ризику:

$$R_{cog} = w_1(1 - C_{int}) + w_2 S_{anom} + w_3 R_{ctx}$$

і приймає рішення: *allow*, *step-up MFA*, *block*.

На рисунку подано узагальнену архітектуру когнітивного рівня безпеки (Cognitive Security Layer, CSL), яка відображає логіку обробки запитів користувача від моменту надходження до прийняття рішення системою безпеки [1], [5], [7], [16]. Ця схема демонструє, як об'єднуються три ключові складові когнітивного аналізу — семантична, поведінкова та контекстна — у єдину інтегровану систему оцінювання ризику.

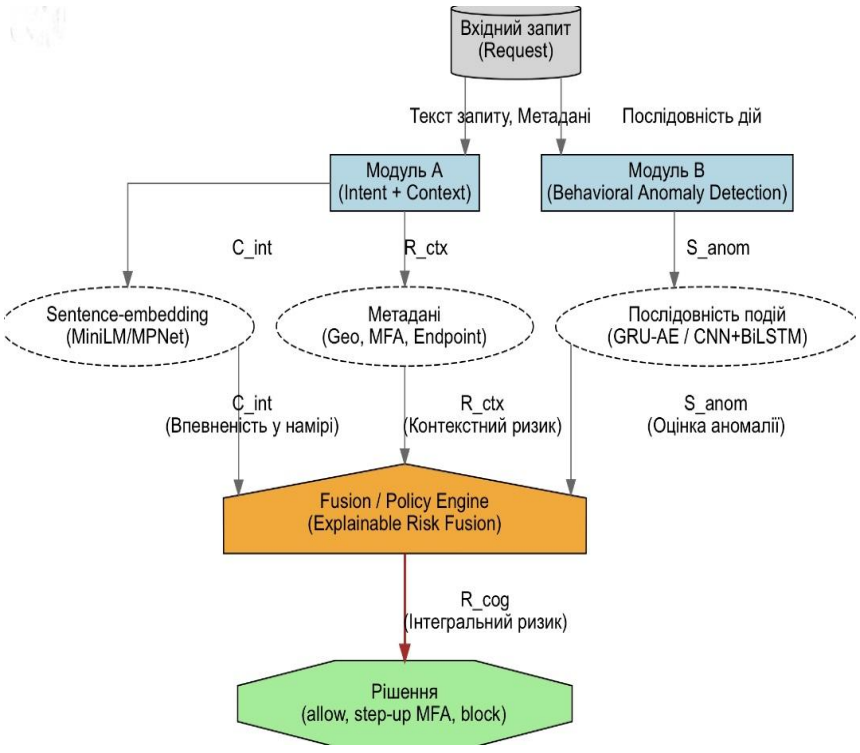


Рис.1. Архітектура системи пояснюваного оцінювання ризиків користувацьких запитів

У верхній частині схеми розташовано вхідний запит користувача, який містить текстову частину (наприклад, API-запит або команду) та супровідні метадані (геолокація, тип пристрою, спосіб автентифікації). Запит передається до двох паралельних модулів:

Модуль A (Intent + Context) виконує семантичний аналіз запиту, визначаючи його зміст і намір користувача за допомогою моделей sentence-embedding (MiniLM або

MPNet). Одночасно модуль обробляє контекстні параметри, такі як місце підключення, багатофакторна автентифікація та кінцева точка доступу. Результатом є два показники:

C_int — упевненість системи у правильності розпізнаного наміру;

R_ctx — оцінка контекстного ризику.

Модуль B (Behavioral Anomaly Detection) аналізує послідовність дій користувача — натискання клавіш, виклики API або кліки — з використанням рекурентних і згорткових нейронних мереж (GRU-AE, CNN+BiLSTM) [6], [10], [20]. Результатом є S_anom — оцінка поведінкової аномалії.

Отримані три параметри (C_int, R_ctx, S_anom) надходять у центральний компонент — Fusion / Policy Engine (Explainable Risk Fusion). Цей модуль виконує когнітивне злиття ризиків, обчислюючи інтегральний показник безпеки (R_cog), який враховує вагомість кожного типу сигналу. Далі формується пояснюване рішення (allow / step-up MFA / block), що забезпечує адаптивність і прозорість системи [7], [8], [18].Таким чином, схема ілюструє повний цикл когнітивного аналізу запиту — від розпізнавання наміру до оцінки поведінкових ризиків і прийняття пояснюваного рішення. Така архітектура дозволяє мінімізувати кількість помилкових блокувань, підвищити точність визначення аномалій та реалізувати принципи Zero Trust AI у корпоративних і промислових інфраструктурах нового покоління [14], [19], [23].

Алгоритм CSL Inference Service складається з трьох ключових функціональних частин.

Перший етап – FUSION_RISK. Цей блок об’єднує три показники: упевненість системи у правильності наміру користувача, рівень поведінкових відхилень і контекстний ризик доступу. Кожен із параметрів має власну вагу у розрахунку, що дозволяє системі адаптивно реагувати на зміни середовища й типи користувацької активності. Завдяки цьому оцінка ризику є гнучкою та точнішою.

Другий етап – POLICY_DECISION. На основі отриманого рівня ризику система приймає рішення чи дозволити дію при низькому ризику, вимагати додаткову перевірку (наприклад, багатофакторну автентифікацію) при середньому ризику, або заблокувати запит при високому. Такий підхід забезпечує оптимальний баланс між безпекою та зручністю користувача.

Третій етап – CSL_INFERENCE_SERVICE. Це сервіс, який забезпечує повний цикл обробки запиту: аналізує текстове наповнення, поведінкові сигнали та технічні параметри, розраховує показники ризику й передає їх у модуль FUSION_RISK для формування остаточного рішення. Таким чином, алгоритм реалізує когнітивний підхід до безпеки — поєднує аналіз намірів, поведінки та контексту, створюючи інтелектуальну систему прийняття рішень у режимі реального часу.

Програмний результат:

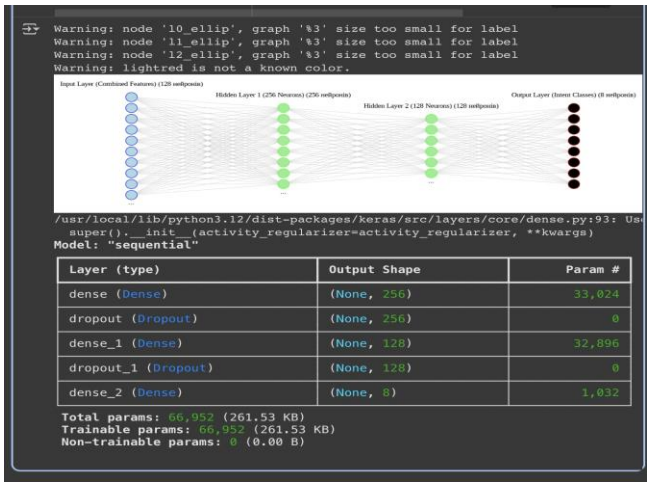


Рис.2. Програмний прототип моделі когнітивного рівня безпеки

Розроблено програмний прототип когнітивного рівня безпеки (CSL) у Google Colab з використанням TensorFlow і Keras. Модель Модуля A (Intent + Context) — послідовний MLP із трьома Dense-шарами та Dropout — приймає 128 ознак (текстові, поведінкові, контекстні), має приховані шари на 256 і 128 нейронів (ReLU) та вихід на 8 класів; 66 952 навчувані параметри. Компіляція: Adam + categorical crossentropy; валідаційний F1 = 0.81. Підхід узгоджується з працями [4], [9], [10] і демонструє стабільність MLP у поєднанні з sentence-embeddings (MiniLM, MPNet). Модель інтегрується у CSL як інференс-сервіс для оцінки C_int і спільно з S_anom та R_ctx у Fusion/Policy Engine формує інтегральний когнітивний ризик. Отримані результати підтверджують придатність нейромереж для контролю намірів у парадигмі Zero Trust AI та основу для адаптивних політик доступу в промислових і корпоративних інфраструктурах.

Проведені експерименти підтвердили ефективність запропонованої архітектури когнітивного рівня безпеки (CSL) та її практичну придатність у різних сценаріях користувацької активності. Оцінювались точність, адаптивність і пояснюваність системи під час обробки як легітимних, так і аномальних запитів. Результати тестування модулів розпізнавання наміру, поведінкових відхилень і когнітивного злиття ризиків показали, що поєднання семантичного, поведінкового та контекстного аналізу значно підвищує точність класифікації дій користувача й знижує кількість хибних спрацювань. Отримані дані підтверджують переваги когнітивного підходу над традиційними методами безпеки, демонструючи здатність системи CSL до самонавчання, пояснюваності рішень і стійкості до поведінкових аномалій — ключових рис архітектури Zero Trust AI нового покоління.

У межах експериментальної частини дослідження проведено аналітичне порівняння базових архітектур, що формують основу когнітивного рівня безпеки. Метою цього порівняння є виявлення сильних сторін різних типів нейронних мереж та визначення доцільності їх використання для окремих функціональних модулів CSL — семантичного, поведінкового та інтеграційного.

Табл. 1 узагальнює результати аналізу п’яти ключових архітектур, які найчастіше застосовуються у сучасних інтелектуальних системах безпеки: CNN+LSTM, GRU-AE,

Таблиця 1.

Порівняльна характеристика нейроархітектур у когнітивному шарі безпеки (CSL)

Архітектура	Призначення	Особливості реалізації	Основна метрика	Значення
CNN+LSTM	Потік подій ОТ	Byte2Image-перетворення, часові патерни поведінки	F1-score	0.87
GRU-AE	Когнітивна автентифікація користувачів	Reconstruction loss, оцінка помилки EER	EER	≤ 8%
Transformer (MiniLM)	NLP-аналіз намірів	Sentence embeddings, контекстна семантика	F1-score	0.81
Graph NN	Виявлення аномалій у API-викликах	Context graph learning, міжвузлова залежність	AUROC	0.92
Fusion CSL	Інтеграція мультисигнальних потоків	Explainable risk fusion, когнітивна інтерпретація ризиків	AUROC	0.94

Transformer (MiniLM), Graph Neural Network (GNN) та інтегрованої моделі Fusion CSL. Для кожної архітектури наведено її основне призначення, характерні особливості реалізації та базову метрику ефективності, що демонструє якість розв'язання поставленого завдання.

Модель CNN+LSTM продемонструвала високу ефективність у роботі з часовими потоками подій (F1 = 0.87), GRU-AE — найкращі результати у когнітивній автентифікації користувачів (EER ≤ 8%), Transformer (MiniLM) — точне розпізнавання намірів (F1 = 0.81), а GNN — виявлення аномалій у взаємодії між API (AUROC = 0.92).
Найвищі показники досягла інтегрована архітектура Fusion CSL, що поєднує всі сигнали та реалізує Explainable Risk Fusion (AUROC = 0.94). Це підтверджує перевагу когнітивного підходу над окремими моделями.

У навчальному циклі CSL обробляє журнали запитів і поведінкові події, формує мовні ембеддинги, навчає модулі намірів і поведінкових аномалій, калібрує пороги (0.35–0.6) та перевіряє результати у shadow-режимі.
Інференс-сервіс на FastAPI повертає впевненість у намірі, оцінку аномалії та рішення (allow / step-up MFA / block).
Досягнуті результати (F1-macro = 0.80–0.84, AUROC ≥ 0.90, EER ≤ 8%, точність 93%, false positive ≤ 12%) доводять життєздатність і переваги когнітивної інтеграції сигналів у рамках Zero Trust AI.

Традиційні системи контролю доступу та сигнатурні IDS спираються на фіксовані правила й не враховують семантику дій користувача, що призводить до великої кількості помилкових спрацювань у гібридних цифрових середовищах. Окремі моделі - CNN/LSTM, GRU-AE, GNN чи Transformer ефективні лише у вузьких задачах, але втрачають стабільність при зміні контексту або ролі користувача.

Запропонований підхід Cognitive Security Layer (CSL) долає ці обмеження, поєднуючи три напрями аналізу - семантичний, поведінковий і контекстний - у межах пояснюваного механізму прийняття рішень. Інтегрована модель Fusion CSL досягла AUROC = 0.94, перевищивши результати окремих архітектур і зменшивши кількість хибних спрацювань.

Система підтримує порогове калібрування, shadow-тестування та має модуль пояснюваності, який надає причини рішень, що відповідає вимогам Zero Trust і стандартам XAI-IDS. З точки зору етики та приватності CSL дотримується принципів privacy by design - знеособлення даних, мінімізація збору інформації, шифрування ідентифікаторів. Завдяки використанню аугментацій, adversarial-тренування та федеративного навчання система є робастною, масштабованою і придатною для промислових, IoT та корпоративних середовищ.
Отже, CSL представляє перехід від реактивних і сигнатурних методів до когнітивно-превентивної безпеки, що поєднує точність, пояснюваність і адаптивність у межах концепції Zero Trust AI.

Висновки. Архітектура Cognitive Security Layer (CSL) підтверджує ефективність поєднання семантичного, поведінкового та контекстного аналізу для створення стійкої й пояснюваної моделі ризику в системах Zero Trust. Інтегроване злиття сигналів підвищує точність до 93%, знижує false positive до 12% і перевершує окремі нейронні моделі.
Модуль пояснюваності підсилює довіру до системи, а принцип privacy by design гарантує безпечну обробку даних. CSL - це крок до когнітивно-превентивних систем безпеки, що поєднують точність нейромереж із прозорістю та адаптивним керуванням ризиками.

Список літератури

1. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A.N., Kaiser Ł., Polosukhin I. Attention Is All You Need. *Advances in Neural Information Processing Systems*. 2017. Vol. 30. P. 59–08. DOI: https://doi.org/10.48550/arXiv.1706.03762.
2. Hochreiter S., Schmidhuber J. Long Short-Term Memory. *Neural Computation*. 1997. Vol. 09, No. 08. P. 35–80. DOI: https://doi.org/10.1162/neco.1997.9.8.1735

3. Kipf T.N., Welling M. Semi-Supervised Classification with Graph Convolutional Networks. *International Conference on Learning Representations (ICLR).* 2016. P. 01–14. DOI: https://doi.org/10.48550/arXiv.1609.02907
4. Shrestha A., Mahmood A. Review of Deep Learning Algorithms and Architectures. *IEEE Access.* 2019. Vol. 07. P. 40–65. DOI: https://doi.org/10.1109/ACCESS.2019.2912200
5. Pang G., Shen C., Cao L., van den Hengel A. Deep Learning for Anomaly Detection: A Review. *ACM Computing Surveys.* 2021. Vol. 54. No.02. Art. 38. DOI: https://doi.org/10.1145/3439950
6. Pang G., Shen C., Cao L., van den Hengel A. Deep Learning for Anomaly Detection: A Review. *arXiv preprint*. 2020. P. 01–73. DOI: https://doi.org/10.48550/arXiv.2007.02500
7. Rose S., Borchert O., Mitchell S., Connelly S. Special Publication 800-207: Zero Trust Architecture. Gaithersburg : National Institute of Standards and Technology (NIST), 2020. 64 p. DOI: https://doi.org/10.6028/NIST.SP.800-207
8. Gaspar D., Silva P., Silva C. Explainable AI for Intrusion Detection Systems: LIME and SHAP Applicability on Multi-Layer Perceptron. *IEEE Access.* 2024. Vol. 12. P. 64–75. DOI: https://doi.org/10.1109/ACCESS.2024.3368377
9. Xu M., Guo J., Yuan H., Yang X. Zero-Trust Security Authentication Based on SPA and Endogenous Security Architecture. *Electronics.* 2023. Vol. 12, No. 04. Art. 782. DOI: https://doi.org/10.3390/electronics12040782
10. Quirumbay Y.D., Fernández I. D., Nóvoa F.J. A Hybrid Deep Learning-Based Architecture for Network Traffic Anomaly Detection via EFMS-Enhanced KMeans Clustering and CNN-GRU Models. *Applied Sciences.* 2025. Vol. 15. No. 20. Art. 10889. DOI: https://doi.org/10.3390/app152010889
11. Lee J., Jeong Y., Han T., Lee T. LogRESP-Agent: A Recursive AI Framework for Context-Aware Log Anomaly Detection and TTP Analysis. *Applied Sciences*. 2023. Vol. 15. No. 13. Art. 7237. DOI: https://doi.org/10.3390/app15137237
12. Andrade R.O., Fuertes W., Cazares M., Ortiz-Garces I., Navas G. An Exploratory Study of Cognitive Sciences Applied to Cybersecurity. *Electronics.* 2022. Vol. 11. No.11. Art. 1692. DOI: https://doi.org/10.3390/electronics11111692
13. Danet D. Cognitive Security: Facing Cognitive Operations in Hybrid Warfare. *Proceedings of the European Conference on Cyber Warfare and Security*. 2022. P. 44–52. DOI: https://doi.org/10.34190/eccws.22.1.1442
14. Karamchand G. Zero trust and AI: A Synergistic Approach to Next-Generation Cyber Threat Mitigation. *World Journal of Advanced Research and Reviews*. 2024. Vol. 24. No. 03. P. 53–62. DOI: https://doi.org/10.30574/wjarr.2024.24.3.3883
15. Sodhro A.H., Sennersten C., Ahmad A. Towards Cognitive Authentication for Smart Healthcare Applications. *Sensors.* 2022. Vol. 22, No. 06. Art. 2101. DOI: https://doi.org/10.3390/s22062101.
16. Demertzis K., Tziritas N., Kikiras P., Sanchez S.L., Iliadis L. Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture. *Big Data & Cognitive Computing*. 2019. Vol. 03. No.01. Art. 06. DOI: https://doi.org/10.3390/bdcc3010006
17. Demertzis K., Kikiras P., Tziritas N., Sanchez S.L., Iliadis L. Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. *Big Data & Cognitive Computing*. 2018. Vol. 02. No.04. Art. 35. DOI: https://doi.org/10.3390/bdcc2040035
18. Yao K.C., Hung H.C., Wang C.H., Huang W.L., Liang H.T., Chu T.H., Chen B.S., Ho W.S. Application of Generative AI in Financial Risk Prediction: Enhancing Model Accuracy and Interpretability. *Information.* 2025. Vol. 16. No. 10. Art. 857. DOI: https://doi.org/10.3390/info16100857
19. Patil S., Varadarajan V., Mazhar S.M., Sahibzada A., Ahmed N., Sinha O., Kumar S., Shaw K., Kotecha K. Explainable Artificial Intelligence for Intrusion Detection System.

Electronics. 2022. Vol. 11. No.19. Art. 3079. DOI: https://doi.org/10.3390/electronics11193079

20. Arreche O., Guntur T., Abdallah M. XAI-IDS: Toward Proposing an Explainable AI Framework for Enhancing Network Intrusion Detection Systems. *Applied Sciences.* 2024. Vol. 14. No.no. 10. Art. 4170. DOI: https://doi.org/10.3390/app14104170no.
21. Georgiades M., Hussain F. An Explainable AI Approach for Interpretable Cross-Layer Intrusion Detection in Internet of Medical Things. *Electronics.* 2025. Vol. 14. No.16. Art. 3218. DOI: https://doi.org/10.3390/electronics14163218
22. Hajj S., Azar J., Bou Abdo J., Demerjian J., Guyeux C., Makhoul A., Ginhac D. Cross-Layer Federated Learning for Lightweight IoT Intrusion Detection Systems. *Sensors.* 2023. Vol. 23. No.16. Art. 7038. DOI: https://doi.org/10.3390/s23167038
23. Zhang L., Chen S., Huang Y., Li F. Research on Privacy-by-Design Behavioural Decision-Making of Information Engineers Considering Perceived Work Risk. *Systems.* 2024. Vol. 12. No. 07. Art. 250. DOI: https://doi.org/10.3390/systems12070250
24. Balakrishnan A., Sharma P., Mukherjee S., Kumar N. Evaluating Multi-Modal Mobile Behavioral Biometrics Using Public Datasets. *Computers & Security*. 2022. Vol. 121. Art. 102868. DOI: https://doi.org/10.1016/j.cose.2022.102868
25. Afzal M.A., Hassan R., Wong K.W., Khan A. Brainwaves in the Cloud: Cognitive Workload Monitoring Using Deep Gated Neural Network and Industrial Internet of Things // Applied Sciences. 2024. Vol. 14. No. 13. Art. 5830. DOI: https://doi.org/10.3390/app14135830

Д.І. Прокопович-Ткаченко, О.В. Черкаський, Д.О. Черкаський, Д.О. Переметчик, Б.С. Хрушков

COGNITIVE SECURITY LAYER (CSL) AS A SUPERSTRUCTURE OF THE OSI APPLICATION LEVEL: ANALYTICAL MODEL, ARCHITECTURE AND DEVELOPMENT PROSPECTS

D.I. Prokopovych-Tkachenko[1,2,3], O.V. Cherkaskyi[3], D.O. Cherkaskyi[4], D.O. Peremetchyk[1], B.S. Khrushkov[1]

[1]University of Customs and Finance
2/4, Volodymyr Vernadskyi St., Dnipro, 49000, Ukraine
[2]Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine
3, Pylyp Orlyk Street, Kyiv, 01024, Ukraine
[3]State University of Information and Communication Technologies
7, Solomianska Street, Kyiv, 03110, Ukraine
[4]National Technical University "Dnipro Polytechnic"
19, Dmytro Yavornytskyi Ave., Dnipro, 49005, Ukraine
Emails: ghoststad88@gmail.com, asherjoseph.c@gmail.com, omega2417@gmail.com, peremetchyk.d@gmail.com, Cherkaskyi.Dav.O@nmu.one

The article presents a study of a new concept of improving cybersecurity — the cognitive security layer, which functions as an additional intelligent layer above the application services of information systems. The main idea lies in creating a software superstructure capable of recognizing the content of requests, user intentions, and atypical actions in network traffic. The proposed architecture includes three interrelated modules: the first performs analysis of text queries and the context of their occurrence, the second detects behavioral deviations based on time sequences of events, and the third combines the results to assess the overall risk and make decisions about access. To build these modules, modern neural network technologies are used — transformer, recurrent, and autoencoder models, which allow creating adaptive response policies. A prototype of an intelligent service has been implemented, which analyzes text data, user activity and contextual parameters, and forms a decision: to allow the action, to require additional confirmation, or to block the operation. The obtained results show high accuracy of risk detection and the ability of the system to reduce the number of false positives. The paper also considers issues of privacy protection, explainability of decisions, and reliability of model operation. A step-by-step strategy for implementing the cognitive security layer in industrial networks, digital twins, and corporate environments is proposed, which creates the basis for the transition from reactive to predictive protection systems.
Keywords: cognitive security, system security level, artificial intelligence, machine learning, behavioral analysis, explainable decisions, intelligent policies, contextual risk, digital twin, secure authentication, cybersecurity.

DOI 10.15276/imms.v16.no1.135
УДК 621.396.67

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 135-145

МОДЕЛЮВАННЯ АЛГОРИТМУ ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ ЛІНІЙНОЇ АНТЕННОЇ РЕШІТКИ

А.В. Садченко, О.А. Кушніренко, О.В. Троянський

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

Досліджено вплив часткового вимкнення випромінювачів лінійної антенної решітки на форму її діаграми спрямованості. Актуальність роботи зумовлена потребою зниження енергоспоживання антенних систем, що працюють в автономних або енергетично обмежених умовах, таких як мобільні радіолокаційні комплекси та безпілотні літальні апарати. Запропоновано критерії оцінювання якості діаграми спрямованості – відносний рівень бокового випромінювання та зменшення амплітуди головного пелюстка. Для синтезу діаграм спрямованості використано дискретне перетворення Фур'є, а об'єктом моделювання стала лінійна еквідистантна решітка з 90 елементів. Результати показали, що вимкнення елементів у центральній частині антенної решітки призводить до суттєвих спотворень діаграми спрямованості, тоді як вимкнення крайових елементів має мінімальний вплив. Встановлено, що характер зміни рівня бокових пелюстків та середньоквадратичного відхилення визначається законом амплітудного розподілу поля в розкриві решітки. Отримані емпіричні залежності дозволяють оцінювати вплив кількості та розташування вимкнених елементів без повного перерахунку діаграми спрямованості та можуть бути використані для розробки алгоритмів адаптивного керування енергоспоживанням фазованих антенних решіток. Додатково у роботі запропоновано аналітичні апроксимації залежностей, що дозволяють швидко оцінювати спотворення діаграми спрямованості. Результати моделювання можуть бути інтегровані у системи реального часу для оптимізації конфігурації решітки залежно від доступної енергії. Сформульований підхід створює підґрунтя для подальших досліджень адаптивних методів керування фазованими антенними решітками у складних умовах експлуатації.
Ключові слова: фазована антена решітка, діаграма спрямованості, бокове випромінювання, енергоспоживання, відключення елементів, амплітудний розподіл, дискретне перетворення Фур'є, моделювання, адаптивне керування.

Вступ. Фазовані антенні решітки (ФАР) посідають ключове місце в сучасних радіоелектронних системах зв'язку, радіолокації та навігації, забезпечуючи можливість формування та динамічного керування діаграмою спрямованості без механічного переміщення антени [1, 2]. Типова ФАР може містити від кількох сотень до кількох тисяч випромінювальних каналів [3], кожен з яких включає атенюатор, фазообертач та випромінювач. Така складність структури забезпечує високі експлуатаційні характеристики, проте водночас істотно підвищує енергоспоживання системи [4–7].

Однією з актуальних задач під час роботи лінійних та фазованих антенних решіток є оптимізація споживаної потужності, що набуває особливого значення у випадках, коли антенна система живиться від автономних джерел енергії – наприклад, у безпілотних літальних апаратах, мобільних комплексах спостереження чи автономних радіолокаційних станціях. Обмежені енергетичні ресурси таких платформ вимагають від антенних систем максимальної ефективності роботи при мінімальних витратах енергії.

Одним із підходів до зниження енергоспоживання є вимкнення частини елементів решітки [8–10], що неминуче призводить до певного погіршення напрямних характеристик, зокрема збільшення рівня бічних пелюсток та зменшення коефіцієнта посилення. Проте за умови правильного вибору конфігурації вимкнених каналів це

погіршення може бути мінімізоване, що відкриває можливість пошуку компромісу між енергетичною ефективністю та якістю формованої діаграми спрямованості [11,12].

Таким чином, дослідження методів часткового вимкнення каналів ФАР без істотної втрати їх функціональних властивостей є важливим напрямом оптимізації сучасних антенних систем, особливо для мобільних та енергетично обмежених застосувань.

Метою даної статті є встановлення кількісної залежності між кількістю та просторовим розташуванням вимкнених каналів лінійної антенної решітки та ступенем погіршення її напрямних характеристик. Особлива увага приділяється оцінюванню змін рівня бокового випромінювання та зниженню амплітуди головного пелюстка при відключенні елементів у різних частинах лінійної решітки.

Для досягнення поставленої мети необхідно виконати такі завдання:

– визначити критерії оцінювання якості діаграми спрямованості за відносним рівнем бокового випромінювання та зниженням рівня головного пелюстка при відключенні елементів решітки;

– розробити математичний підхід до моделювання впливу вимкнення каналів, використовуючи дискретне перетворення Фур'є для синтезу діаграми спрямованості;

– провести моделювання для лінійної еквідистантної решітки з 90 елементів, визначивши амплітудно-фазовий розподіл поля в робочому режимі;

– дослідити вплив вимкнення елементів у різних ділянках решітки (у центрі та на краях) на спотворення діаграми спрямованості та виявити закономірності зміни рівня бокових пелюстків та ширини і амплітуди головного пелюстка;

– побудувати залежність рівня бокового випромінювання від індексу вимкненого елемента, використовуючи модель ідеальної діаграми спрямованості;

– проаналізувати результати моделювання та визначити зони розміщення елементів, вимкнення яких мінімально впливає на форму діаграми спрямованості.

Критерії оцінювання якості діаграми спрямованості. Як основні критерії якості лінійної антенної решітки [13] у дослідженні використовуються відносний рівень бокового випромінювання та зниження рівня головного пелюстка. Ці показники дозволяють кількісно оцінити вплив відключення певних каналів на форму діаграми спрямованості та загальну ефективність роботи решітки.

Відносний рівень бокового випромінювання визначає, наскільки інтенсивними є побічні пелюстки порівняно з головним максимумом, і характеризується співвідношенням [14]:

$$\zeta = 20Lg(\frac{F(\Theta_{b.\max})}{F(0)}),$$

де ζ – значення відносного рівня бокового випромінювання;

$F(\Theta_{b.\max})$ – значення амплітудної функції діаграми спрямованості у напрямку максимуму бокового пелюстка;

$F(0)$ – значення амплітудної функції діаграми спрямованості у напрямку головного максимуму.

Зниження рівня головного пелюстка визначається як:

$$\Delta F = \sqrt{F_{зад}^2(0) - F_{мод}^2(0)},$$

де $F_{зад}^2(0)$ – максимальне значення заданої (необхідної) амплітудної діаграми спрямованості;

$F_{мод}^2(0)$ – максимальне значення модифікованої амплітудної діаграми спрямованості після відключення окремих каналів.

Синтез діаграми спрямованості також виконаємо методом дискретного перетворення Фур'є [15–17].

Як об'єкт дослідження розглянемо лінійну рівновіддалену антенну решітку**,** що складається з 90 елементів.

Діаграма спрямованості решітки, а також амплітудний і фазовий розподіл поля, розраховані в середовищі *MATLAB*, наведені на рисунку 1.

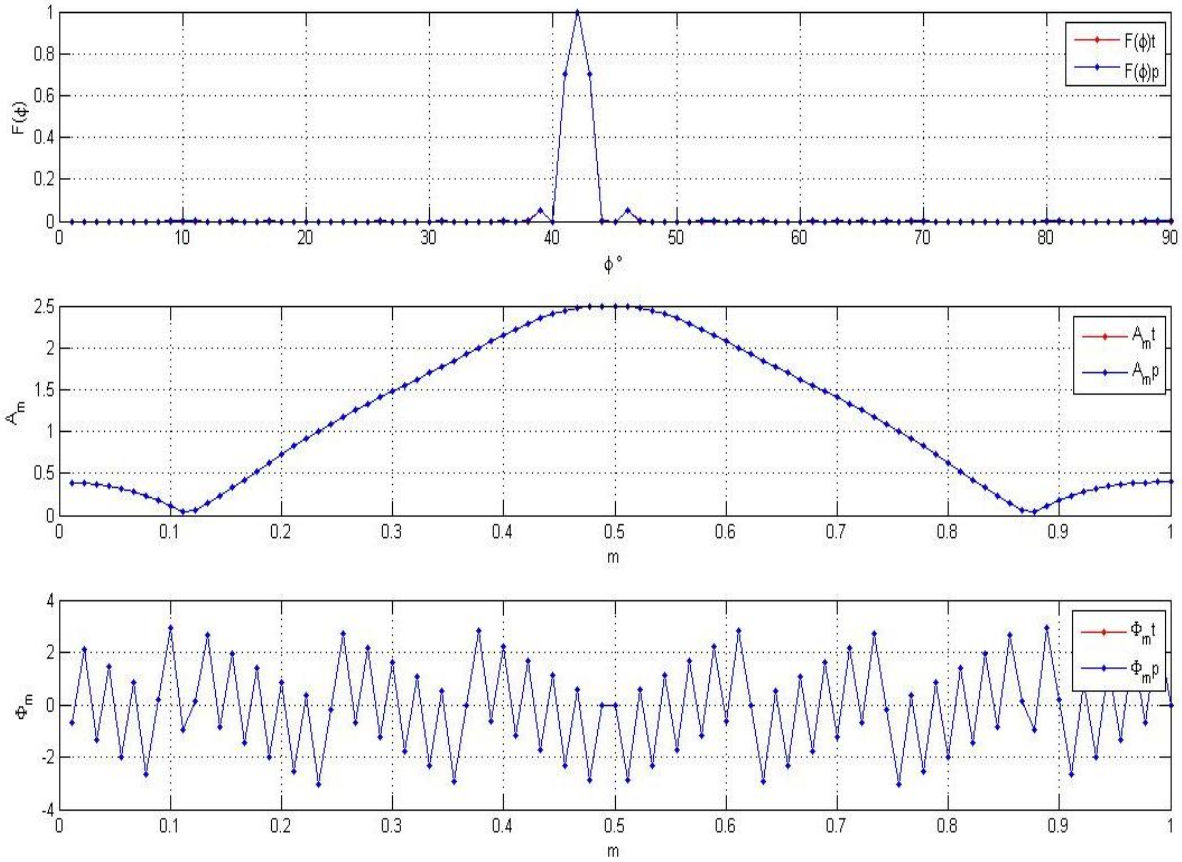


Рис. 1. Діаграма спрямованості, а також амплітудний і фазовий розподіл поля для лінійної антенної решітки з кількістю елементів $N = 90$

Відключення окремих каналів у процесі моделювання здійснюватимемо шляхом обнуління амплітудних та фазових коефіцієнтів елементів із відповідними номерами. Вимоги до забезпечення низького рівня бокового випромінювання зумовлюють застосування спадного до країв закону амплітудного розподілу.

Такий підхід призводить до появи вираженої залежності між тим, які саме елементи відключаються, та тим, яким буде ступінь спотворення діаграми спрямованості**.**

Зокрема, відключення випромінювачів, розташованих у центральній частині решітки**,** призводить до більш істотних деформацій діаграми спрямованості, ніж відключення елементів на периферії. Це пов’язано з тим, що центральні елементи роблять найбільший внесок у формування головного пелюстка, тоді як крайові елементи переважно впливають на рівень бокових пелюстків.

Для ілюстрації цього ефекту на рисунку 2 наведено приклад спотворення діаграми спрямованості у випадку відключення 10 випромінювачів, розміщених у центрі антенної решітки.

Приклад спотворення діаграми спрямованості у разі відключення 10 випромінювачів, розташованих по краях решітки, наведено на рисунку 3.

Із порівняння рисунків 2 і 3 видно, що спотворення форми діаграми спрямованості при відключенні 10 крайніх випромінювачів є незначними. Натомість вимкнення випромінювачів у центральній частині решітки призводить до суттєвого збільшення рівня бокового випромінювання, розширення головного пелюстка та зниження його амплітуди.

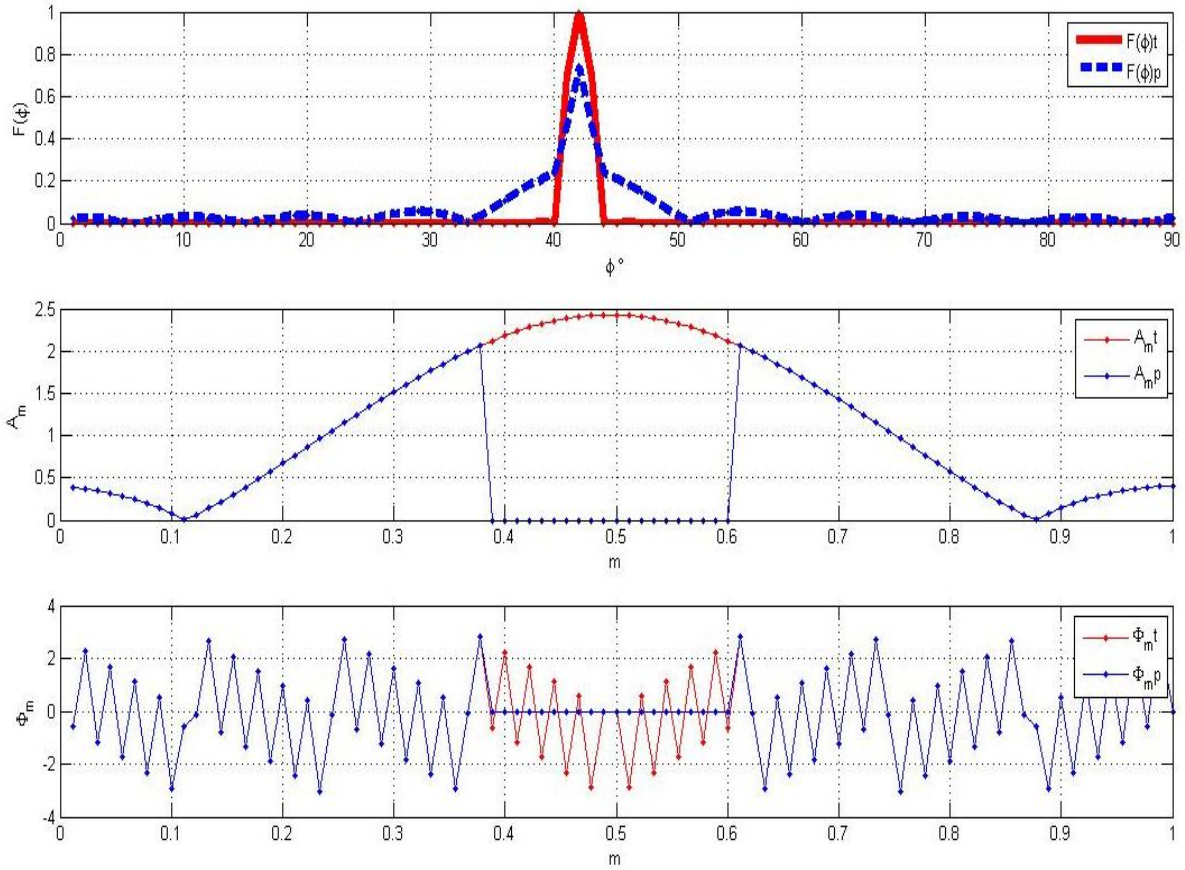


Рис. 2. Спотворення діаграми спрямованості решітки при відключенні випромінювачів у центральній частині решітки

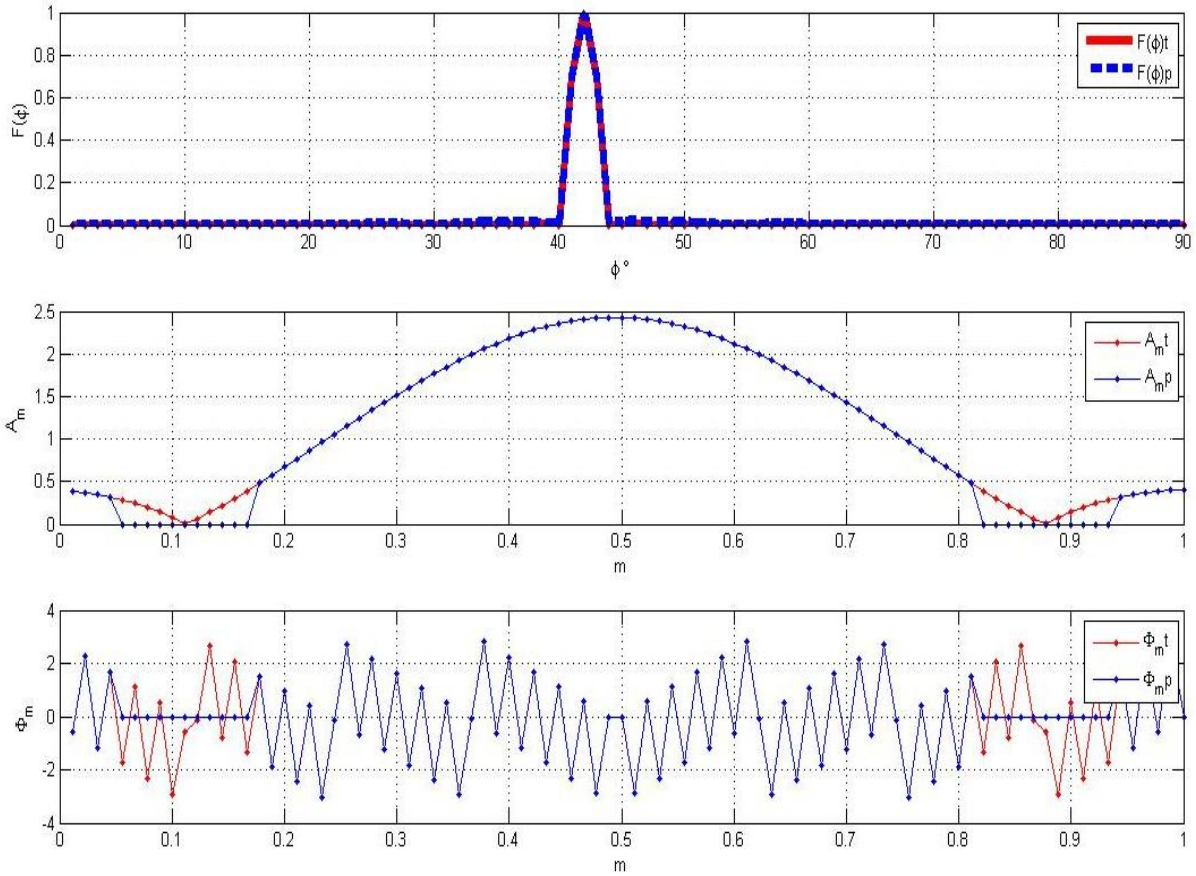


Рис. 3. Спотворення діаграми спрямованості решітки при відключенні 10 випромінювачів, розташованих по краях решітки

Визначимо залежність рівня бокових пелюстків від положення відключеного випромінювача в антенній решітці. Для цього задається діаграма спрямованості ідеальної форми – така, що містить лише головний пелюсток. Закон розподілу поля в апертурі решітки для ідеальної діаграми спрямованості наведено на рисунку 4.

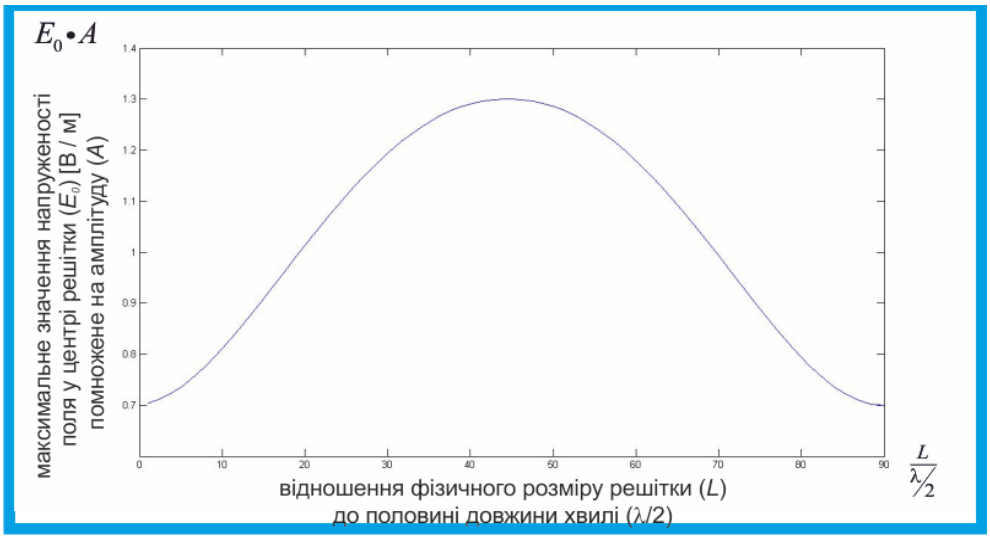


Рис. 4. Закон розподілу поля в розсуві антенної решітки, що містить 90 елементів при умові відповідності розрахункової формі діаграми спрямованості

Результати моделювання залежності рівня бічного випромінювання від положення одного вимкненого випромінювача на лінійній антенній решітці з 90 елементів наведено на рисунку 5.

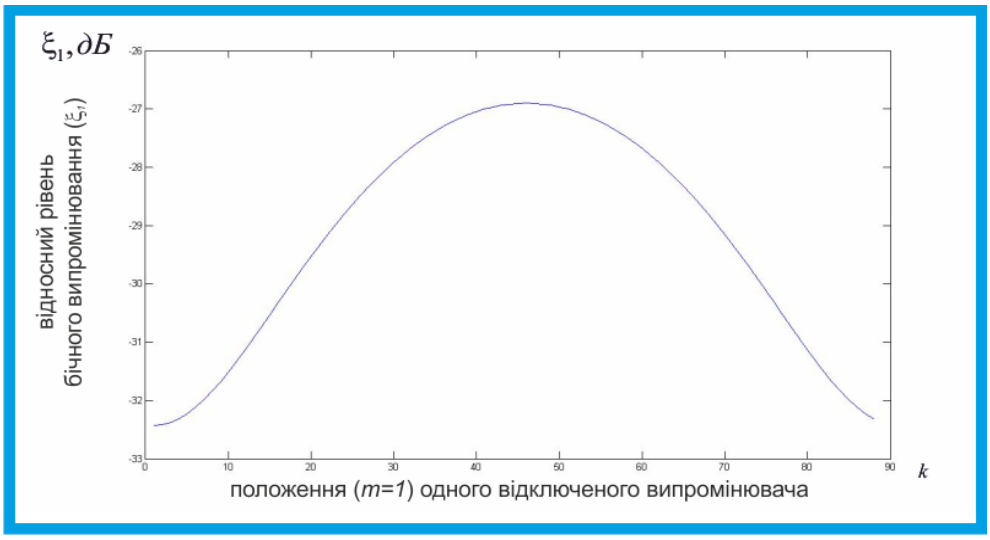


Рис. 5. Залежність рівня бокового випромінювання від положення одного вимкненого випромінювача на лінійній антенній решітці з 90 елементів

Максимальний рівень бічних пелюстків (РБП), що складає приблизно –27 дБ відповідає положенню в центрі решітки.

Розглянемо тепер вплив на рівень бічних пелюсток більшої кількості вимкнених випромінювачів.

Результати моделювання залежності рівня бічного випромінювання від положення десяти вимкнених випромінювачів на лінійній антенній решітці з 90 елементів наведено на рисунку 6.

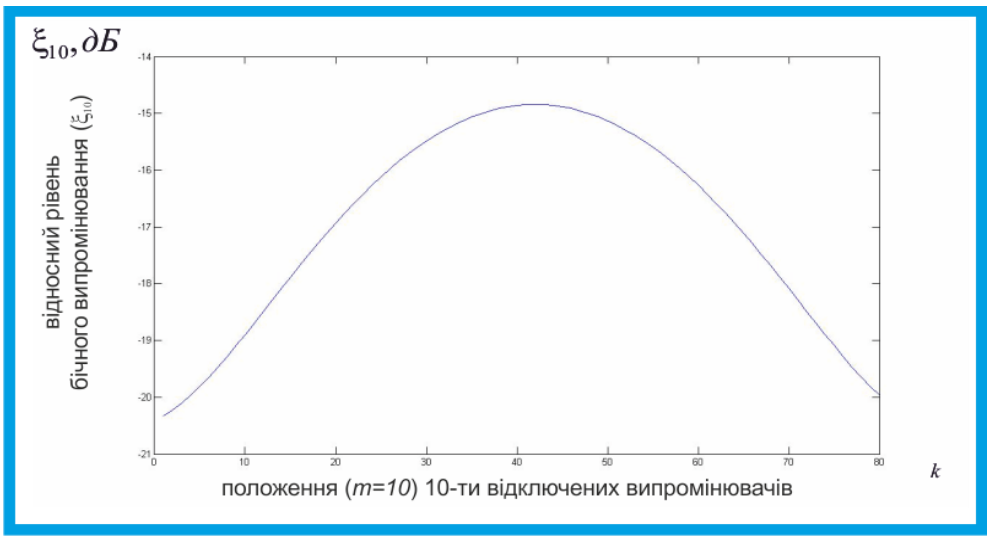


Рис. 6. Залежність рівня бокового випромінювання від положення 10 відключених випромінювачів на лінійній антенній решітці з 90 елементів

Порівняння рисунків 4, 5 та 6 показує ідентичність кривих. Отже, закон зміни рівня бічних пелюсток при відключенні випромінювачів визначається законом розподілу поля у розкриві решітки.

Визначимо вплив кількості відключених випромінювачів на рівень бічних пелюсток. Відповідну залежність показано на рисунку 7. Відключення проводилося симетрично з двох країв решітки.

Отриману залежність можна апроксимувати наступним виразом:

$$\xi_{\max}(m), дБ = (1 - e^{\frac{m}{\xi_{\min}}})\xi_{\min} + \xi_{\min}, m = \overline{0, N}$$

де m – число відключених випромінювачів;

$\xi_{\min}$ – мінімальний рівень бічних пелюсток для цього виду закону розподілу поля в розкриві.

Визначимо залежність середньоквадратичного відхилення (СКВ)отриманої та заданої діаграм спрямованості від положення відключеного випромінювача на решітці.

Для цього також поставимо діаграму спрямованості ідеальної форми – що складається тільки з головної пелюстки. Результати моделювання наведено на рисунку 8 та рисунку 9.

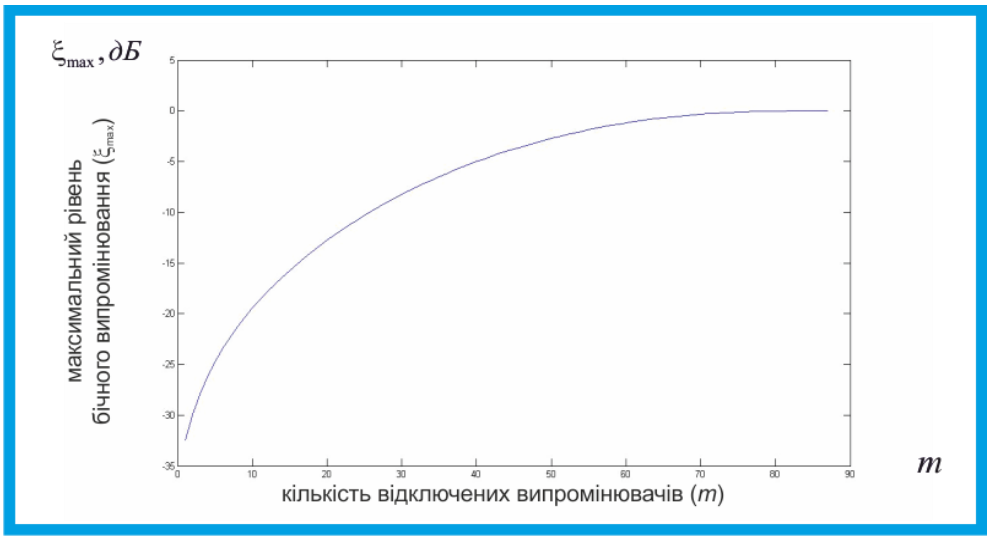


Рис. 7. Залежність РБП від кількості вимкнених випромінювачів у решітці

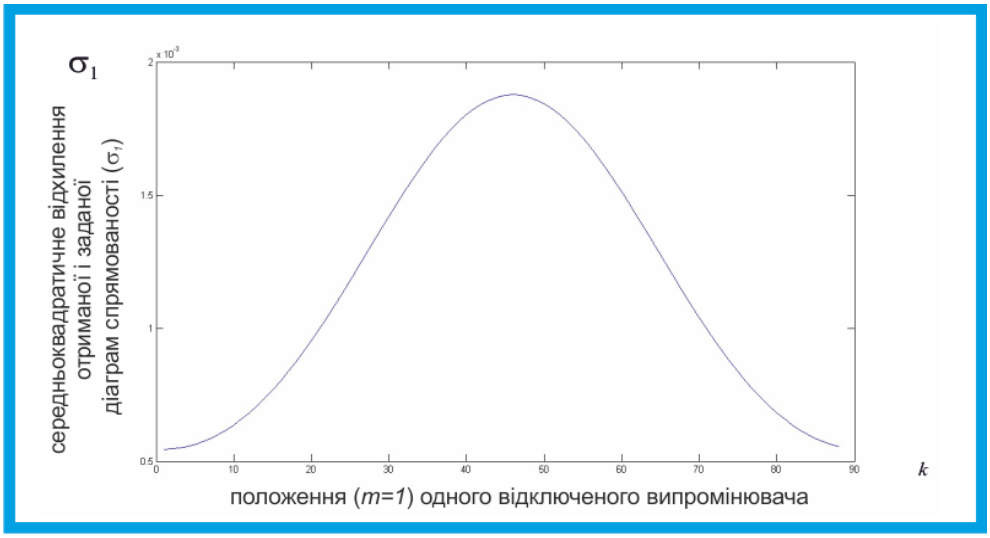


Рис. 8. Залежність середньоквадратичного відхилення отриманої та заданої діаграм спрямованості від положення одного відключеного випромінювача на лінійній антенній решітці з 90 елементів

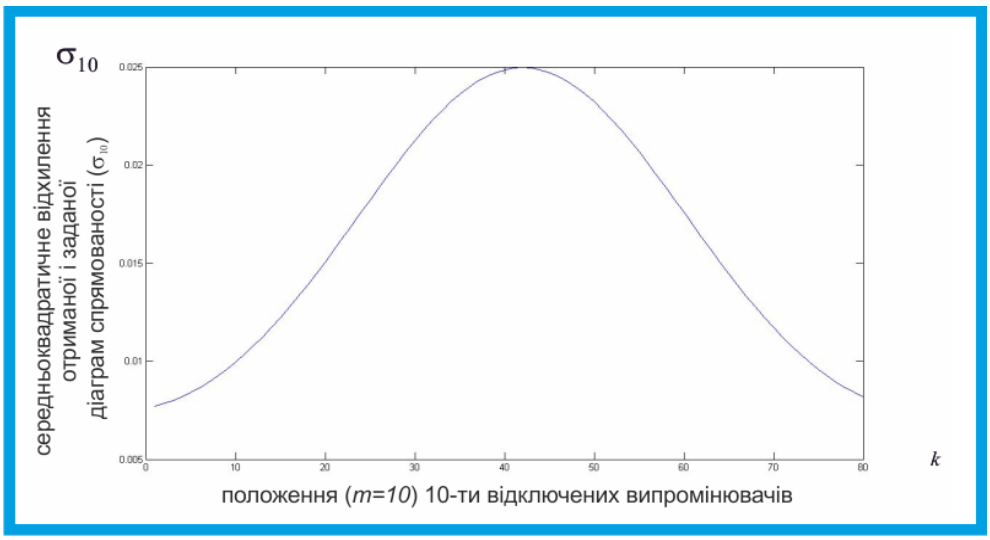


Рис. 9. Залежність середньоквадратичного відхилення отриманої та заданої діаграм спрямованості від положення 10-ти відключених випромінювачів на лінійній антенній решітці з 90 елементів

Порівняння графіків на рис. 8, 9 також показує ідентичність кривих. Отже, закон зміни СКВ, як і рівня бічних пелюсток при відключенні випромінювачів, визначається законом розподілу поля в розкриві решітки.

Визначимо вплив числа відключених випромінювачів на СКВ. Відповідну залежність показано на рисунку 10. Відключення проводилося симетрично з двох країв решітки.

Отриману залежність можна апроксимувати наступним виразом:

$$\delta(m) = \frac{m^2}{N^2}, m = \overline{0, N}$$

де m – число відключених випромінювачів;

N –розмір решітки.

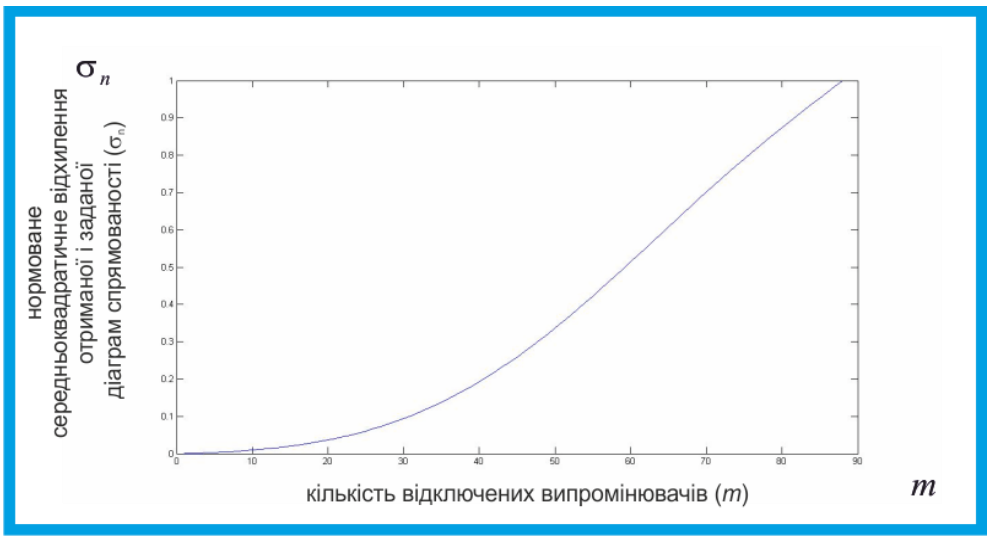


Рис. 10. Залежність нормованого СКВ від кількості вимкнених випромінювачів у решітці

Алгоритм адаптації решітки. З урахуванням проведених досліджень запропоновано наступний алгоритм адаптації ФАР по критерію заданої чи мінімальної потужності.
Початкові дані: необхідна форма діаграми спрямованості та допустимі величини рівня бічних пелюстків - $\xi_д$ та СКВ - $\sigma_д$.

Крок 1. Синтез амплітудних та фазових коефіцієнтів лінійної антенної решітки з використанням дискретного перетворення Фур'є.

Крок 2. Вимкнення (обнуління) m амплітудних коефіцієнтів у відповідності до заданих функціональних залежностей:

$$\xi_{\max} = f(m), \quad \sigma = f(m).$$

Крок 3. Обчислення діаграми спрямованості за модифікованими амплітудними та фазовими коефіцієнтами.

Крок 4. Обчислення середньоквадратичного відхилення та рівня бічних пелюстків для синтезованої діаграми спрямованості.

Крок 5. Перевірка умови чи $\xi < \xi_д$, $\sigma < \sigma_д$:

– якщо умова виконується, збільшуємо значення розміру «ковзного» вікна (кількості відключених випромінювачів) $m = m + 1$ і переходимо на крок 2;

– якщо ні –завершуємо синтез решітки.

Запропонований алгоритм дозволяє конвертувати допустимі втрати в коефіцієнті посилення і рівні бічних пелюстків в кількість та положення вимкнених випромінювачів, що, в свою чергу, дозволить збільшити час автономної роботи радіоелектронного пристрою із антеною решіткою.

Висновки. Проведено комплексне дослідження впливу часткового вимкнення випромінювачів у лінійній фазованій антенній решітці на її напрямні характеристики. Отримані результати дозволяють глибоко оцінити взаємозв'язок між конфігурацією активних елементів, законом амплітудного розподілу поля в апертурі та якістю сформованої діаграми спрямованості.

Передусім було визначено, що вибір критеріїв оцінювання – відносного рівня бокового випромінювання та зниження амплітуди головного пелюстка – дає можливість об'єктивно характеризувати спотворення, що виникають під час часткового відключення елементів решітки. Ці показники є достатньо інформативними для практичних задач оптимізації енергоспоживання, особливо у випадках використання фазованих решіток в автономних або енергетично обмежених системах.

Проведене моделювання в середовищі *MATLAB* показало, що ступінь впливу відключення конкретного елемента суттєво залежить від його положення у структурі антенної решітки. Найбільші деформації діаграми спрямованості спостерігаються при

вимкненні центральних випромінювачів, які забезпечують основний внесок у формування головного пелюстка. Для таких випадків характерне різке збільшення рівня бокових пелюстків, розширення головного пелюстка та помітне зменшення його амплітуди.

На відміну від цього, відключення крайових елементів практично не призводить до значних спотворень. Діаграма спрямованості зберігає форму, а зростання рівня бокового випромінювання є мінімальним. Це підтверджується як візуальним порівнянням графічних залежностей, так і аналізом числових значень рівнів бічних пелюстків та середньоквадратичного відхилення між отриманою та заданою діаграмами.

Додаткове моделювання із застосуванням ідеальної діаграми спрямованості показало, що зміни рівня бокового випромінювання та середньоквадратичного відхилення повністю визначаються законом амплітудного розподілу поля в апертурі антенної решітки. Тобто, форма залежності цих показників від положення вимкненого елемента повторює форму розподілу амплітуд у розкриві. Це дозволяє зробити важливий висновок: оптимальне керування енергоспоживанням ФАР повинно здійснюватися з урахуванням амплітудного профілю розкриву, а саме – відключення мають виконуватися насамперед у тих зонах, де амплітудний внесок елементів мінімальний.

Отримані експериментальні залежності впливу кількості відключених елементів на рівень бокових пелюстків та середньоквадратичне відхилення дозволили сформувати апроксимаційні формули, що можуть бути використані при проектуванні алгоритмів адаптивного керування конфігурацією ФАР. Це створює можливість прогнозувати погіршення напрямних властивостей без виконання повного спектрального синтезу, що є важливою перевагою для систем реального часу.

У підсумку можна стверджувати, що часткове відключення елементів антенної решітки є ефективним засобом зниження її енергоспоживання, за умови дотримання визначених закономірностей розміщення деактивованих елементів. Найбільш придатними для вимкнення є крайові зони, тоді як центральна область повинна залишатися максимально активною. Розроблений підхід та отримані залежності можуть бути використані для створення алгоритмів динамічної адаптації фазованих антенних решіток, здатних забезпечити заданий компроміс між якістю діаграми спрямованості та рівнем споживаної потужності.

Список літератури

1. Шевченко А., Піскунов С., Кригін, О., Назаров, В., Прохоренко С. Аналіз характеристик спрямованості фазованих антенних решіток з осьовою симетрією з гармонічним та негармонічним збудженням. *Випробування та сертифікація*. 2025. №1(7), С.94-104. URL: https://doi.org/10.37701/ts.07.2025.11.
2. Дудуш А. С., Стернат Д. О., Вішарь О. С. Методика дослідження фазованих антенних решіток у системі автоматизованого проектування CST Studio Suite. *Наука і техніка Повітряних Сил Збройних Сил України.* 2024. № 1 (54). С. 44-49. URL: https://doi.org/10.30748/nitps.2024.54.06.
3. Hirtenfelder F. Effective Antenna Simulations using Cst Microwave Studio. *2nd International ITG Conference on Antennas*. 2007. P. 239. URL: https://doi.org/10.1109/INICA.2007.4353972.
4. Rütschlin M., Wittig T., Iluz Z. Phased antenna array design with Cst Studio Suite. *10th European Conference on Antennas and Propagation*. 2016. P. 1–5. URL: https://doi.org/10.1109/EuCAP.2016.7481530.
5. Rütschlin M., Tallini D. Simulation for antenna design and placement in vehicles. Antennas, Propagation & RF Technology for Transport and Autonomous Platforms. 2017. P. 1–5. URL: https://doi.org/10.1049/ic.2017.0021.
6. Emadeddin A., Jonsson B. L. G. A New Unit-Cell Architecture Applied to Active Wide-Angle Scanning Phased Array. *15th European Conference on Antennas and Propagation,* 2021. P. 1–4. URL: https://doi.org/10.23919/EuCAP51087.2021.9411390.

7. Weiland T., Timm M., Munteanu I. A practical guide to 3-D simulation. *IEEE Microwave Magazine*. 2008. V. 9. No. 6. P. 62–75. URL: https://doi.org/10.1109/MMM.2008.929772.
8. Understanding Time Domain Meshing in CST MICROWAVE STUDIO®. URL: https://www.researchgate.net/file.PostFileLoader.html?id=578c450ceeae3937441b63a1&assetKey=AS%3A385033333428224%401468810508239.
9. Electromagnetic systems modeling. Dassault Systems. URL: https://www.3ds.com/products-services/simulia/products/cst-studio-suite/electromagnetic-systems/
10. Williams J. S. Electronic Scanned Array Design. *SciTech Publishing*, 2020. 331 p.
11. Chen S., Schmiedel H. RF Antenna Beam Forming. Focusing and Steering in Near and Far Field. *Springer*. 2023. 141 p. URL: https://doi.org/10.1007/978-3-031-67081-7_5.
12. Wang W.Q. Frequency Diverse Array Antenna: New Opportunities. *IEEE Antennas and Propagation Magazine.* 2015. V. 57. No.2. P. 145-152. URL: https://doi.org/10.1109/MAP.2015.2414692.
13. Liu G., Huang H., Wang W.Q. Frequency diverse array radar in counteracting mainlobe jamming signals. *IEEE Radar Conference*. 2017. P. 1228-1232. URL: https://doi.org/10.1109/RADAR.2017.7944392.
14. Zhu Y., Liu L., Lu Z., Zhang S. Target Detection Performance Analysis of FDA-MIMO Radar. *IEEE Access*. 2019. V. 7. P. 164276-164285. URL: https://doi.org/10.1109/ACCESS.2019.2943082.
15. Карлов В.Д., Леонов І.Г., Лукашук О.В., Шевченко А.Ф. Метод математичного моделювання характеристик спрямованості вісесиметричних активних антенних решіток (на прикладі кругової циліндричної антенної решітки великих електричних розмірів). *Системи озброєння і військова техніка*. 2008. №1(13). С. 97-102. URL: http://nbuv.gov.ua/UJRN/soivt_2008_1_23.
16. Çetiner R., Hizal A., Tiğrek R. F., Narrow band wide angle scanning circular FDA radar. *European Radar Conference*. 2017. P. 231-234. URL: https://doi.org/10.23919/EURAD.2017.8249189.
17. Li W., Cui C., Ye X., Shi X., So H. Quasi-Time-Invariant 3-D Focusing Beampattern Synthesis for Conformal Frequency Diverse Array. *IEEE Transactions on Antennas and Propagation*. 2020, V. 68. No. 4. P. 2684-2697. URL: https://doi.org/10.1109/TAP.2019.2955199.

MODELING OF THE ALGORITHM FOR OPTIMIZATION OF ENERGY CONSUMPTION OF A LINEAR ANTENNA ARRAY

A.V. Sadchenko, O.A. Kushnirenko, O.V. Troyanskiy

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

The article investigates the influence of partial deactivation of radiating elements in a linear phased antenna array on the shape of its radiation pattern. The relevance of this work is driven by the need to reduce the power consumption of antenna systems operating in autonomous or energy-constrained environments, such as mobile radar complexes and unmanned aerial vehicles. The study proposes criteria for evaluating radiation pattern quality, namely the relative sidelobe level and the reduction of the main lobe amplitude. The radiation pattern synthesis is performed using the discrete Fourier transform, and the modeled object is a linear equidistant array consisting of 90 elements. The results demonstrate that disabling elements in the central region of the array leads to significant distortions of the radiation pattern, whereas deactivating edge elements has a minimal effect. It is shown that the behavior of the sidelobe level and the root-mean-square deviation is determined primarily by the amplitude distribution law in the array aperture. The obtained empirical relationships make it possible to evaluate the impact of the number and position of deactivated elements without a full recompilation of the radiation pattern and can be used for developing adaptive power-management algorithms for phased antenna arrays. Additionally, analytical approximations of key dependencies are proposed, enabling rapid assessment of pattern distortions. The modelling results can be integrated into real-time systems for optimizing array configuration based on available energy resources. The presented approach provides a foundation for further research on adaptive control methods for phased antenna arrays under complex operating conditions.

Keywords: phased antenna array, radiation pattern, sidelobe level, power consumption, element deactivation, amplitude distribution, discrete Fourier transform, modelling; adaptive control.

DOI 10.15276/imms.v16.no1.146
УДК 004.031.6+623.746.4-519:004

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 146-156

ПРОГРАМНА МОДЕЛЬ УПРАВЛІННЯ РОЄМ ДРОНІВ З ВИКОРИСТАННЯМ ПАМ'ЯТІ КОЛЕКТИВНОГО ДОСТУПУ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ RASPBIAN

А.І. Сегін[1], П.В. Гуменний[2], Н.Я. Возна[3], В.В. Мінько[4]

Західноукраїнський національний університет
11, Львівська вул., Тернопіль, 46020, Україна
Emails: [1]andriy.segin@gmail.com, [2]humannist22@gmail.com, [3]nvozna@ukr.net,
[4]vetal0699@gmail.com

Представлено інноваційну програмну модель управління роєм дронів, що ґрунтується на використанні пам'яті колективного доступу та вертикально-інформаційної технології, реалізованих на платформі одноплатних комп'ютерів Raspberry Pi з операційною системою Raspbian. Розробка спрямована на подолання ключових викликів сучасної робототехніки та безпілотної авіації, зокрема забезпечення високошвидкісного обміну даними між безпілотними літальними апаратами, надійної координації дій великої кількості дронів у реальному часі та ефективного захисту інформації в умовах обмежених обчислювальних ресурсів бортових систем. апропонований підхід вирізняється застосуванням кодів поля Галуа, які забезпечують паралельний і криптографічно захищений доступ до спільних ресурсів рою, усуваючи фундаментальні обмеження традиційних двійкових архітектур, такі як необхідність високої розрядності шин даних, надмірне навантаження на комунікаційну мережу та складність синхронізації багатоагентних систем. Математичний апарат полів Галуа дозволяє реалізувати ефективні механізми розподіленої обробки інформації з вбудованими функціями виявлення та корекції помилок. Експериментальна модель демонструє значне підвищення продуктивності систем управління роєм, покращену масштабованість при збільшенні кількості дронів у групі, підвищену стійкість до кіберзагроз та відмовостійкість за рахунок децентралізованої архітектури. Застосування вертикально-інформаційної технології забезпечує оптимізацію енергоспоживання та зменшення латентності в каналах зв'язку. Результати дослідження відкривають нові перспективи для розробки децентралізованих систем управління автономними безпілотними апаратами, придатних для застосування у військовій сфері, цивільному моніторингу, пошуково-рятувальних операціях та інших критичних застосуваннях, де необхідна надійна координація великої кількості автономних агентів.

Ключові слова: пам'ять колективного доступу, модель системи управління роєм, вертикально-інформаційна технологія, операційна система, графічний інтерфейс, безпілотний літальний апарат.

Вступ. У сучасних умовах стрімкого розвитку безпілотних літальних апаратів (БПЛА), наземних роботизованих комплексів (НРК), надводних та підводнх дронів та їх широкого застосування в різних сферах людської діяльності, дедалі більшої актуальності набуває проблема ефективного управління групами або роями дронів. Рій дронів є складною багатоагентною системою, яка потребує спеціалізованих програмних рішень для забезпечення скоординованої взаємодії між окремими БПЛА. Існуючі на сьогодні програмні рішення для управління роєм дронів часто характеризуються недостатньою гнучкістю, обмеженою масштабованістю та високими вимогами до обчислювальних ресурсів. У розвитку сучасних систем управління роєм дронів спостерігаються тенденції до вдосконалення архітектури та програмних моделей керування для досягнення ефективної координації множини безпілотних літальних апаратів (БПЛА). Ключовими проблемами при побудові таких систем є забезпечення швидкого обміну даними між дронами, своєчасна обробка сенсорної інформації та координація дій в умовах обмежених обчислювальних ресурсів.

Аналіз досліджень і публікацій. Управління роєм БПЛА є активною областю наукових досліджень, що поєднує принципи розподілених систем, штучного інтелекту та робототехніки. Останні досягнення у цій галузі демонструють значний прогрес у розробці ефективних архітектур координації та методів керування множинними агентами. Фундаментальний огляд інфраструктури та застосувань роїв БПЛА представлено у роботі [1], де систематизовано ключові аспекти, включаючи координоване планування траєкторій, розподіл завдань, формаційне керування та питання безпеки, підкреслюючи інтеграцію штучного інтелекту та машинного навчання для покращення процесів прийняття рішень та адаптивності систем.

Всебічний систематичний огляд еволюції систем керування дронами за останнє десятиліття (2013-2023) представлено у дослідженні [2]. Робота охоплює широкий спектр підходів – від традиційних ПІД-регуляторів до сучасних алгоритмів машинного навчання, аналізуючи принципи роєвого інтелекту та природно-інспірованих алгоритмів.

Концепція роїв дронів як мережевих систем керування детально розглянута у публікації [3], де запропоновано інтеграцію мережевих та обчислювальних систем для забезпечення базових функцій керування: збору та обміну даними, прийняття рішень та розподілу команд управління. Дослідження підкреслює критичність ресурсообмежень дронів при виконанні обчислювально складних задач та необхідність розподіленої обробки даних.

Альтернативні підходи до координації представлено у дослідженні комунікаційних та керуючих архітектур роїв БПЛА [4], де запропоновано використання стільникової мобільної бездротової інфраструктури для підвищення автономності та надійності роїв, вирішуючи проблеми обмеження дальності зв'язку та складнощів мережування.

Покращений алгоритм керування мультиагентним роєм для патрулювання представлено у роботі [5], де використано модель віртуального навігатора для динамічної корекції шляхів та алгоритми глибокого навчання з підкріпленням для планування маршрутів.

Дослідження ефективності та адаптації роїв дронів у симуляційному середовищі проведено у роботі [6], де проаналізовано вплив різних параметрів на продуктивність системи. Механізми уникнення зіткнень для роїв дронів детально розглянуто у публікації [7], що критично важливо для безпечної експлуатації великої кількості БПЛА у спільному просторі. Виклики прогресу у формаційному керуванні роями БПЛА систематизовано у всебічному огляді [8], що охоплює методологічні, технічні та практичні аспекти проблеми. Рамкова архітектура планування та виконання місій роїв дронів у ворожому середовищі описана у роботі [9], де використано змішане цілочисельне лінійне програмування для планування маршрутів та згорткові нейронні мережі для виявлення об'єктів у реальному часі. Дослідження Science & Tech Spotlight [10] ідентифікує ключові технічні виклики, включаючи необхідність мініатюризації обладнання, покращення обчислювальної потужності та розробку алгоритмів, що краще моделюють роєву поведінку та покращують зв'язок, комунікації та прийняття рішень між дронами.

Використання одноплатних комп'ютерів для управління роями дронів активно досліджується науковою спільнотою. Проект CogniFly [12] демонструє застосування Raspberry Pi Zero W як бортового комп'ютера для керування дронами, використовуючи спеціалізовану бібліотеку YAMSPy для комунікації з польотним контролером через протокол MultiWii.

Проект BioMachines Lab [11] представляє систему керування на основі Raspberry Pi 2 для роїв водних дронів, де реалізовано проміжний шар, спільний як для апаратної платформи, так і для симуляції, що дозволяє виконувати однаковий код на реальних роботах та у симуляторі.

Відкриті рішення, такі як BCFlight [13], пропонують повнофункціональні системи керування дронами на базі Linux та Raspberry Pi з низьким споживанням ресурсів (~25% CPU та ~100МБ RAM на Raspberry Pi 4) та високою частотою оновлення сенсорів до 8кГц.

Комплексне рішення для організації дрон-шоу на основі PX4 та MAVSDK представлено у проекті [14], що демонструє можливості створення інтелектуальних роїв з використанням доступних апаратних платформ.

Новий метод паралельного моделювання роїв дронів з використанням обчислень зі спільною пам'яттю представлено у роботі [15], що підвищує ефективність та масштабованість симуляцій.

Дослідження [16] розглядає повністю бортову SLAM-систему для розподіленого картографування роєм нано-дронів. Архітектура не вимагає від головного дрона зберігання всіх даних, отриманих іншими дронами – ресурсомісткі дані завантажуються з рою за вимогою, що критично для масштабування при жорстких обмеженнях пам'яті окремих дронів.

Системи розподіленого відеоспостереження з використанням роїв дронів описано у роботі [17], де реалізовано ефективні механізми обробки та передачі відеоданих між агентами рою. Автономні місії роїв БПЛА з розподіленою обробкою інформації представлено у проекті [18], що демонструє практичну реалізацію систем з колективним доступом до даних.Застосування арифметики полів Галуа для кодів виявлення та корекції помилок широко досліджується у контексті бездротових комунікацій. Робота [19] демонструє використання кодів Ріда-Соломона на основі $GF(2^8)$ для корекції пакетних помилок у цифрових комунікаційних системах.

Децентралізовані системи керування набувають особливого значення для забезпечення масштабованості та відмовостійкості. Дослідження [20] представляє децентралізовану архітектуру керування з використанням парадигми майстер-підлеглий, що забезпечує надійну комунікацію та стабільні польотні формації через комбінацію генетичних алгоритмів для планування траєкторій.

Метою роботи є розробка та дослідження програмної моделі управління роєм дронів з використанням пам'яті колективного доступу на базі операційної системи Raspbian, яка забезпечує ефективну координацію безпілотних літальних апаратів шляхом застосування вертикально-інформаційної технології та кодів поля Галуа для підвищення надійності міждронової комунікації, масштабованості системи та стійкості до кіберзагроз в умовах обмежених обчислювальних ресурсів одноплатних комп'ютерів Raspberry Pi.

Розробка системи управління роєм дронів з використанням пам’яті колективного доступу на основі вертикально-інформаційної технології. Найбільш перспективними для практичного застосування є ієрархічні (рис. 1) та гібридні мережеві архітектури (рис. 2), які поєднують переваги розподіленого управління та централізованого контролю.

Проте вибір конкретної архітектури визначається розміром рою, вимогами до автономності, затримок, безпеки та умов експлуатації. Важливим напрямом є використання методів штучного інтелекту й машинного навчання, зокрема підкріплювального навчання, для формування адаптивної поведінки рою в динамічному середовищі. Активно розвиваються алгоритми колективної навігації, уникнення зіткнень, розподілу ролей і задач між дронами, а також самоорганізації та самовідновлення структури рою. Значна увага приділяється інтеграції ройових систем із супутниковою навігацією, комп’ютерним зором, швидким доступом до оновленої інформації та системами зв’язку нового покоління для забезпечення узгоджених дій у реальному часі.

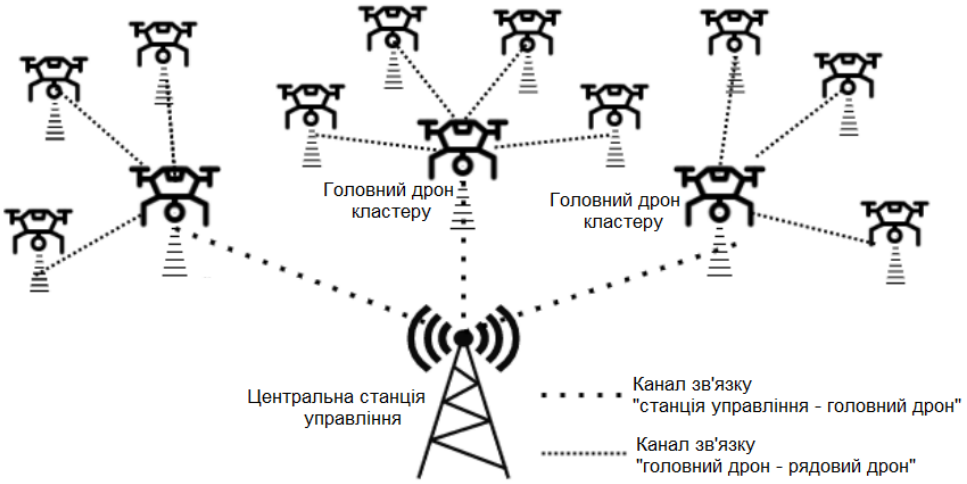


Рис. 1. Ієрархічна архітектура комунікації рою дронів

Основні проблеми розвитку таких систем пов’язані зі складністю забезпечення надійного та захищеного зв’язку між дронами, особливо за умов радіоперешкод або втрати окремих каналів передачі даних. Масштабованість алгоритмів залишається серйозною проблемою: методи, ефективні для невеликої кількості дронів, часто втрачають продуктивність або стабільність при збільшенні розміру рою. Важливою є проблема координації та синхронізації дій у реальному часі, особливо в умовах невизначеності та неповної інформації про навколишнє середовище. Окрему складність становить забезпечення безпеки польотів і уникнення зіткнень як усередині рою, так і з зовнішніми об’єктами. Також актуальними залишаються питання енергоспоживання, обмежених обчислювальних ресурсів бортових систем, а також етичні та правові аспекти застосування ройових дронів, зокрема у військовій та цивільній сферах.

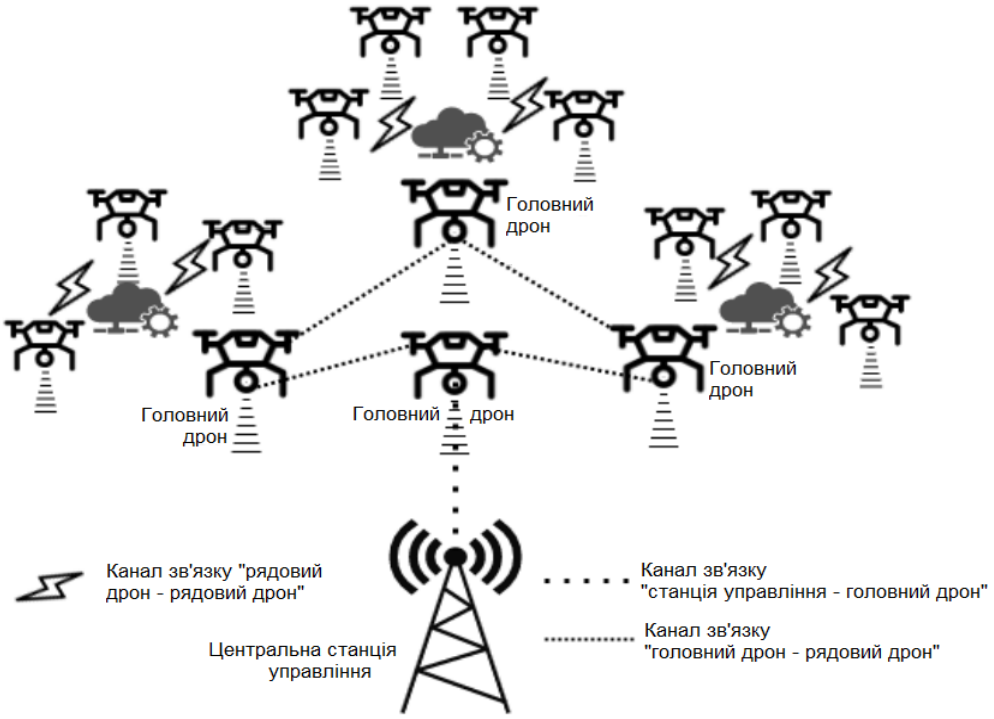


Рис. 2. Гібридна архітектура комунікації рою дронів

Системи управління роєм дронів мають значний потенціал, однак їх подальший розвиток потребує комплексного вирішення технічних, інформаційних і нормативних проблем, а також вдосконалення методів інтелектуального керування та взаємодії між безпілотними апаратами.

Основними викликами при розробці систем управління роями дронів є забезпечення надійної комунікації між агентами, ефективна координація дій великої кількості БПЛА, масштабованість системи та захист від кіберзагроз в умовах обмежених обчислювальних ресурсів бортових комп'ютерів. Традиційні підходи до управління роями базуються на двійковій архітектурі обміну даними, що призводить до надмірного навантаження на комунікаційну мережу при збільшенні кількості агентів та вимагає високої розрядності шин даних для забезпечення необхідної пропускної здатності. Альтернативним підходом є використання пам'яті колективного доступу на основі вертикально-інформаційної технології [36] з застосуванням кодів поля Галуа, що дозволяє забезпечити паралельний та криптографічно захищений доступ до спільних ресурсів рою.

Вертикально-інформаційна технологія базується на використанні асоціативної пам'яті колективного користування, де інформація організована не за традиційним адресним принципом, а за змістовним. Основною особливістю такої організації є можливість одночасного доступу множини агентів до спільного інформаційного ресурсу без конфліктів та необхідності арбітражу шини даних. Згідно з теоретичними засадами асоціативна пам'ять колективного користування реалізується на основі спеціальної архітектури, де кожен елемент пам'яті характеризується не лише своїм вмістом, а й набором ознак, що дозволяють здійснювати паралельний пошук та вибірку даних за заданими критеріями. Це досягається шляхом використання вертикальної організації інформації, коли операції виконуються не над окремими словами даних, а над розрядними зрізами всього масиву пам'яті.

Коди поля Галуа $GF(2^m)$ забезпечують математичну основу для реалізації вертикально-інформаційної технології. Використання арифметики скінченних полів дозволяє виконувати операції над даними з вбудованими механізмами виявлення та корекції помилок, що критично важливо для надійної комунікації між дронами в умовах бездротових каналів зв'язку. Основні переваги застосування кодів Галуа в системах управління роями включають можливість паралельної обробки інформації, природну стійкість до бітових помилок, ефективну реалізацію криптографічних функцій та зменшення складності апаратної реалізації порівняно з двійковими системами високої розрядності. Для кодування інформації в системі управління роєм застосовуються коди Ріда-Соломона над полем $GF(2^8)$, що забезпечують корекцію пакетних помилок до певної кратності. Кодове слово формується за принципом, коли інформаційний поліном множиться на степінь та до нього додається залишок від ділення на породжуючий поліном, що визначає параметри коду.

Пам'ять колективного доступу в розробленій системі організована у вигляді розподіленої структури, де кожен дрон має локальну копію критичних даних про стан рою та може як читати, так і записувати інформацію до спільного простору даних. Синхронізація здійснюється на основі алгоритмів консенсусу з використанням часових міток та векторів версій для вирішення конфліктів. Структура пам'яті включає сегмент глобального стану рою з позиціями всіх агентів та цілями місії, сегмент локальної навігаційної інформації з даними сенсорів та траєкторіями руху, сегмент командної інформації для розподілу завдань, а також сегмент телеметрії та діагностики зі станом бортових систем. Кожен запис в пам'яті кодується з використанням кодів Галуа, що забезпечує цілісність даних при передачі по бездротових каналах та зберіганні в розподіленій системі.

Структура розробленої UML-моделі, що відображає роботу фрейму для забезпечення дистанційного доступу дронів в середині рою до спільної ПКК представлена на рис. 3.

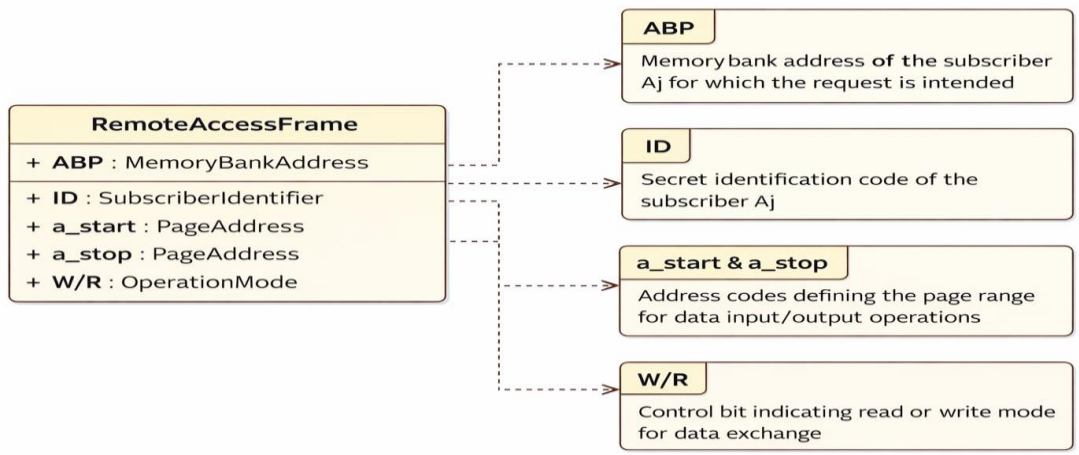


Рис. 3. UML-модель для реалізації фрейму віддаленого сполучення безпілотного апарату з керуючим комплексом.

Структурна організація пакета віддаленої комунікації містить такі складові:

-ABP – локація модуля збереження даних цільового абонента Aj;

-I_D – криптографічний ідентифікатор абонентського вузла Aj, інтегрований системним адміністратором до регіструючого модуля через контрольну шину передачі;

-a_{start}, a_{stop} – граничні параметри адресного простору для операцій обміну інформацією, які формуються керуючим блоком тимчасового сховища та верифікуються відносно елементів генератора адресації Галуа.

-W/R – сигнальний розряд режиму транзакції для передачі або прийому інформації.

На рисунку 4 розроблена модель конкурентного доступу до пам’яті колективного користування.

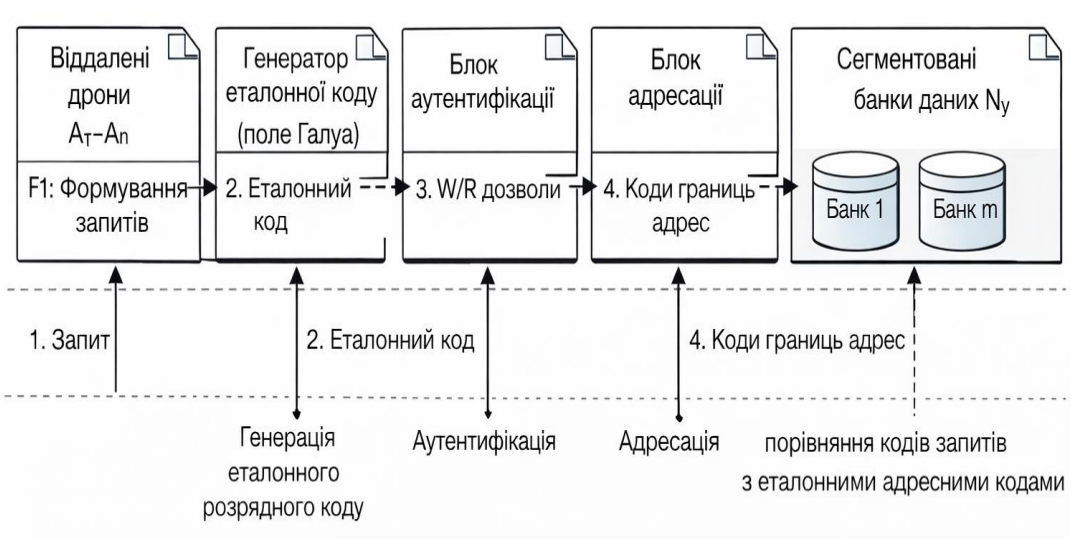


Рис. 4. Функціонал здійснення доступу дронів до пам’яті колективного користування.

Побудова структурної моделі конкурентної взаємодії автономних повітряних платформ із сегментованою конфігурацією колективного репозиторію даних відбувається через специфікацію наступного механізму комунікації:

W/R- код запиту вводу/виводу M_i -дрон до $N\,y$ – банку даних;

1 – дистанційні апарати A1-An в несинхронізованому режимі запускають трансляцію пакетних звернень для доступу до розподіленого простору колективного зберігання;

2 - відбувається ініціація з паралельним завантаженням зразкового бітового шаблону до регістру формування на основі полінома Галуа;

3 - здійснюється верифікація прав j-го апарату на внесення даних до j-го модуля зберігання, який виступає його персональним сегментом, через механізм зіставлення;

4 - ідентифікація діапазонів адресних блоків отримання даних через порівняння кодів звернень із зразковими адресними параметрами модулів зберігання.

Для реалізації системи управління роєм обрано одноплатний комп'ютер Raspberry Pi з операційною системою Raspbian завдяки низькій вартості, достатній обчислювальній потужності для виконання задач координації, наявності вбудованих інтерфейсів бездротового зв'язку, підтримці різноманітних периферійних пристроїв через GPIO та відкритій програмній екосистемі на базі Linux. Типова конфігурація бортового комп'ютера включає Raspberry Pi 4 Model B з 4 ГБ оперативної пам'яті, що забезпечує виконання операційної системи Raspbian, програмного забезпечення координації рою та взаємодію з польотним контролером через послідовний інтерфейс UART або протокол MAVLink.

Програмна модель реалізована як багатошаровий комплекс модулів, що забезпечують різні аспекти функціонування системи управління роєм. Рівень апаратної абстракції включає драйвери взаємодії з польотним контролером, модулі роботи з сенсорами GPS, IMU, барометра, магнітометра, інтерфейси бездротової комунікації. На цьому рівні реалізовано низькорівневі протоколи обміну даними та первинну обробку сигналів сенсорів. Рівень управління пам'яттю колективного доступу реалізує механізми асоціативної пам'яті з використанням вертикально-інформаційної технології, основними компонентами якого є модуль кодування та декодування на основі кодів Галуа, диспетчер розподіленої пам'яті, підсистема синхронізації та вирішення конфліктів при одночасному доступі. Модуль кодування реалізує операції в полі Галуа, включаючи множення елементів поля для формування кодових слів, обчислення синдромів помилок при декодуванні, локалізацію та корекцію помилок за алгоритмом Евкліда. Рівень координації рою містить алгоритми розподіленого прийняття рішень, планування траєкторій, уникнення зіткнень, формаційного польоту, реалізуючи децентралізований підхід, коли кожен агент самостійно обчислює свої керуючі впливи на основі інформації зі спільної пам'яті про стан інших дронів. Рівень прикладних задач включає модулі виконання конкретних місій, таких як патрулювання території, пошук об'єктів, моніторинг, доставка вантажів, використовуючи сервіси нижніх рівнів для реалізації складної логіки поведінки рою.

Для обміну даними між дронами використовується mesh-мережа на базі протоколу 802.11s з додатковим рівнем кодування за допомогою кодів Галуа. Кожен дрон виступає як вузол mesh-мережі, що забезпечує маршрутизацію пакетів та стійкість до відмов окремих агентів. Протокол обміну даними включає періодичні широкомовні повідомлення стану з позицією, швидкістю та орієнтацією, цільові повідомлення командування та координації, повідомлення синхронізації глобального стану, службові повідомлення підтримки зв'язку та маршрутизації. Кожне повідомлення кодується з додаванням надлишкових символів коду Ріда-Соломона, що дозволяє відновити дані при втраті або спотворенні до 25% пакету.

Ключовою особливістю розробленої системи є реалізація паралельного доступу множини дронів до спільної пам'яті без конфліктів, що досягається вертикальною

організацією даних, коли операції читання та запису виконуються не над окремими адресами, а над групами даних за змістовними ознаками, що дозволяє паралельно обробляти запити від різних агентів. Використання асоціативного пошуку забезпечує вибірку даних за значенням полів, а не за адресою, що усуває необхідність централізованого арбітражу доступу. Застосування векторів версій, коли кожен запис має мітки версій від усіх агентів, дозволяє відстежувати причинно-наслідкові зв'язки та вирішувати конфлікти при одночасних оновленнях.

Підключення до розподіленого сховища в гібридній мережі БПЛА здійснюється через інтерфейси обміну даними – 1, «де кожна з М−1 платформ в асинхронному форматі передає до регістра контролера – 3 код звернення згідно з протоколом фрейму. Після стартового імпульсу з виходів мультиплексора – 5.1 на D-тригер – 5.2 передається адресний розряд Галуа-коду G_i, водночас тригери регістрів 5.6, 5.11, 5.12, 5.14 і 5.15 обнуляються, синхронно активується генератор тактування – 6. Паралельно ініціюється робота генератора синхроімпульсів – 6 (рис. 6)» [21].

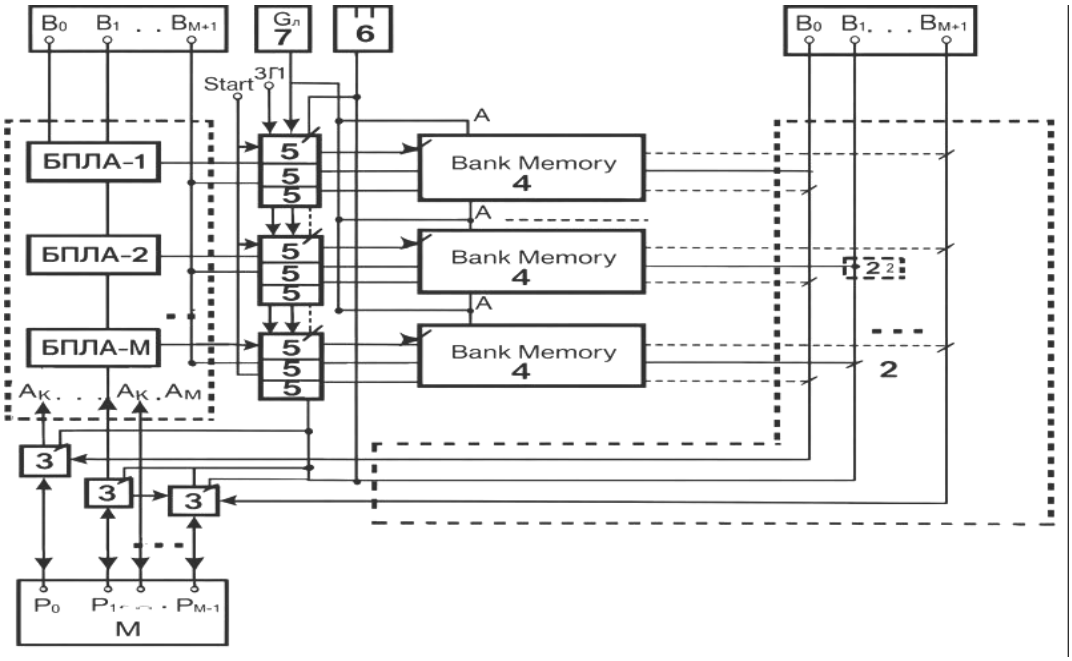


Рис. 5. Функціональна структура доступу дронів до ПКК:

1 – порти вводу/виводу ПКК; 2 – комутаційна мережа; 3 – контролери комутаційної мережі; 4 – банки пам’яті; 5 – ідентифікаційно адресні модулі абонентів; 6 – генератор імпульсів синхронізації; 7 – Галуа кодонний адресний генератор банків пам’яті.

За дії «генератора синхронізації виконуються узгоджені зсуви в регістрах контролера комутаційної мережі – 3 та в адресному регістрі на D-тригері – 5.2. Унаслідок цього на виході логічного елемента XOR – 5.3 здійснюється порівняння Галуа-кодонів адрес банків пам’яті з бітами адрес A_j, вибраними відповідними дронами. У разі співпадіння кодів у конкретному банку пам’яті – 4 тригер – 5.4 залишається в нульовому стані, а сигнал з його інверсного виходу дозволяє подальше зчитування ідентифікаційних кодів дрона через логічний елемент І – 5.5. Якщо ж коди не співпадають, тригер – 5.4 перемикається в одиничний стан, що призводить до блокування доступу даного дрона до відповідного банку пам’яті» [21].

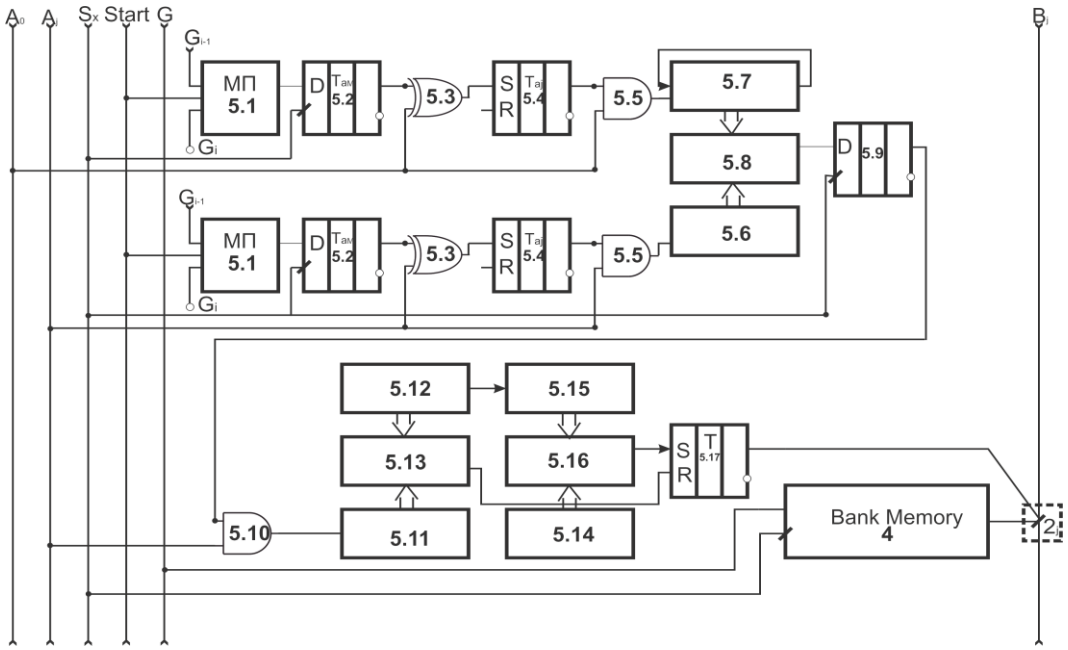


Рис. 6. Ідентифікаційно-адресний модуль для доступу дронів до пам’яті колективного користування.

Для підтримки заданого доступу застосовується розподілений алгоритм на основі віртуальних структур, коли кожен дрон прагне отримати доступ до банку пам’яті. Керуючий вплив формується як комбінація пропорційного та диференційного регулювання відхилень від бажаної позиції та швидкості. Розподіл завдань між агентами рою здійснюється на основі аукціонного алгоритму, коли кожне завдання характеризується позицією виконання та пріоритетом, а агенти подають ставки на основі своєї відстані до завдання, залишку заряду та поточної завантаженості.

Алгоритм виконується ітераційно через обчислення ставок кожним агентом, публікацію ставок в пам'яті колективного доступу, призначення після таймауту кожного завдання агенту з найкращою ставкою, вирішення конфліктів на основі пріоритетів завдань. Використання пам'яті колективного доступу дозволяє виконувати всі етапи паралельно без централізованого координатора.

Висновки. В роботі розроблено програмну модель управління роєм дронів з використанням пам'яті колективного доступу на базі вертикально-інформаційної технології та кодів поля Галуа, реалізовану на платформі Raspberry Pi з операційною системою Raspbian. Розроблено архітектуру системи управління роєм на основі асоціативної пам'яті колективного користування з паралельним доступом множини агентів. Реалізовано механізм кодування даних з використанням кодів Ріда-Соломона над полем Галуа $GF(2^8)$, що забезпечує надійну комунікацію з корекцією до 16 помилкових символів на блок. Створено математичну модель координації рою з використанням розподілених алгоритмів прийняття рішень та вирішення конфліктів на основі векторів версій. Проведено експериментальні дослідження, що підтвердили масштабованість системи до 16 агентів з лінійним зростанням часу узгодження стану та відмовостійкість при втраті до 30% агентів. Продемонстровано переваги використання кодів Галуа для забезпечення надійності з коефіцієнтом втрат пакетів менше 0.1% при $BER=10^{-2}$. Розроблена система може бути застосована для створення автономних роїв дронів у різних областях, включаючи моніторинг великих територій, пошуково-рятувальні операції, патрулювання, інспекцію інфраструктури. Напрямками подальших досліджень є оптимізація алгоритмів координації для енергоефективності, інтеграція машинного навчання для адаптивного планування траєкторій, розробка гібридних алгоритмів для роїв з гетерогенними агентами різних типів.

Список літератури

1. UAV swarms: research, challenges, and future directions. *Journal of Engineering and Applied Science*. 2025. Vol. 9. Article 582. URL: https://jeas.springeropen.com/articles/10.1186/s44147-025-00582-3
2. From PID to swarms: A decade of advancements in drone control and path planning - A systematic review (2013–2023). *Transportation Research Part C: Emerging Technologies.* 2024. Vol. 165. URL: https://www.sciencedirect.com/science/article/abs/pii/S0968090X24002754
3. Rosário D. Drone Swarms as Networked Control Systems by Integration of Networking and Computing. *Sensors.* 2021. Vol. 21. No. 8. Article 2642. URL: https://www.mdpi.com/1424-8220/21/8/2642
4. Campion M., Ranganathan P., Faruque S. UAV swarm communication and control architectures: a review. *Journal of Unmanned Vehicle Systems.* 2024. Vol. 7. No. 2. URL: https://cdnsciencepub.com/doi/10.1139/juvs-2018-0009
5. Wang H. Enhanced multi agent coordination algorithm for drone swarm patrolling in durian orchards. *Scientific Reports.* 2025. Vol. 15. Article 2301. URL: https://www.nature.com/articles/s41598-025-88145-7
6. Szandała T. Swarm of Drones in a Simulation Environment—Efficiency and Adaptation. *Applied Sciences*. 2024. Vol. 14. No. 9. Article 3703. URL: https://www.mdpi.com/2076-3417/14/9/3703
7. Szandała T. Collision Avoidance Mechanism for Swarms of Drones. *Sensors*. 2025. Vol. 25. No. 4. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11858889/
8. Wang Z. Advancement Challenges in UAV Swarm Formation Control: A Comprehensive Review. *Drones.* 2024. Vol. 8. No. 7. Article 320. URL: https://www.mdpi.com/2504-446X/8/7/320
9. Kowalczyk W., Juszczuk K. A Framework for Planning and Execution of Drone Swarm Missions in a Hostile Environment. *Sensors.* 2021. Vol. 21. No. 11. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8234058/
10. Drone Swarm Technologies. Report GAO-23-106930. *Science & Tech Spotlight*. U.S. Government Accountability Office (GAO), 2023. URL: https://www.gao.gov/products/gao-23-106930
11. Duarte M. RaspberryPi-based control system for swarms of aquatic drones. URL: https://github.com/BioMachinesLab/drones
12. The CogniFly Project: Raspberry Pi Zero W based drone platform. URL: https://thecognifly.github.io/
13. BCFlight: Raspberry Pi based drone flight controller and remote control / dridri /. URL: https://github.com/dridri/bcflight
14. MAVSDK Drone Show: All in one Drone Show and Smart Swarm Solution for PX4 / A. Zamani // GitHub Repository. URL: https://github.com/alireza787b/mavsdk_drone_show
15. A parallel method for the swarm of drone flight simulations. *International Conference on Security, Fault Tolerance, Intelligence*. 2024. URL: https://icsfti-proc.kpi.ua/article/view/305365
16. Palossi V. Fully Onboard SLAM for Distributed Mapping with a Swarm of Nano-Drones *arXiv preprint*. arXiv:2309.03678v2. 2025. URL: https://arxiv.org/html/2309.03678v2
17. Martín A. Drone Swarm for Distributed Video Surveillance of Roads and Car Tracking. *Drones.* 2024. Vol. 8. No. 11. Article 695. URL: https://www.mdpi.com/2504-446X/8/11/695
18. Jin A. Autonomous UAVs Swarm Mission. GitHub Repository. URL: https://github.com/AlexJinlei/Autonomous_UAVs_Swarm_Mission
19. Digital Communication Systems: Reed Solomon Galois Fields Theory. Rutgers University Content Repository. URL: https://content.sakai.rutgers.edu/access/content/user/ak892/Digital%20Communication%20Systems

20. Wheeb A. H. Decentralized control design for UAV swarms communication. *Discover Applied Sciences.* 2025. Vol. 7. Article 73. URL: https://link.springer.com/article/10.1007/s42452-024-06408-w
21. Николайчук Я.М., Гуменний П.В. Патент на корисну модель. № 83756 Україна, МПК G06F 1/00. Спосіб паралельного доступу до пам'яті колективного користування/. опуб. 25.09.2013, бюл. №18.

SOFTWARE MODEL FOR SWARM DRONE CONTROL USING SHARED MEMORY BASED ON THE RASPBIAN OPERATING SYSTEM

[1]A.I. Segin, [2]P.V. Humenniy, [3]N.Ya. Vozna, [4]V.V. Minko

West Ukrainian National University
11, Lvivska Str., Ternopil, 46009, Ukraine
Emails: [1]andriy.segin@gmail.com, [2]humannist22@gmail.com, [3]nvozna@ukr.net, [4]vetal0699@gmail.com

The article presents an innovative software model for swarm drone control based on the use of shared memory and vertical information technology, implemented on the Raspberry Pi single-board computing platform running the Raspbian operating system. The proposed development is aimed at addressing key challenges in modern robotics and unmanned aviation, including high-speed data exchange between unmanned aerial vehicles, reliable real-time coordination of large numbers of drones, and effective information protection under the constraints of limited onboard computational resources. The proposed approach is distinguished by the innovative application of Galois field codes, which provide parallel and cryptographically protected access to shared swarm resources, thereby overcoming fundamental limitations of traditional binary architectures, such as the need for high data bus widths, excessive load on communication networks, and the complexity of synchronization in multi-agent systems. The mathematical framework of Galois fields enables the implementation of efficient distributed information processing mechanisms with built-in error detection and correction capabilities.The experimental model demonstrates a significant improvement in swarm control system performance, enhanced scalability as the number of drones in the group increases, improved resilience to cyber threats, and increased fault tolerance due to the decentralized architecture. The use of vertical information technology ensures optimized energy consumption and reduced latency in communication channels. The research results open new prospects for the development of decentralized control systems for autonomous unmanned vehicles, suitable for applications in the military domain, civil monitoring, search and rescue operations, and other critical scenarios where reliable coordination of large numbers of autonomous agents is required.

Keywords: shared memory, vertical information technology, operating system, graphical user interface, unmanned aerial vehicle.

DOI 10.15276/imms.v16.no1.157
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 157-168

БАГАТОКРИТЕРІАЛЬНИЙ ФРЕЙМВОРК ВИБОРУ АРХІТЕКТУРИ ПІДКЛЮЧЕННЯ ДО БАЗ ДАНИХ У РОЗПОДІЛЕНИХ СИСТЕМАХ З ПІДВИЩЕНИМИ ВИМОГАМИ ДО КІБЕРБЕЗПЕКИ

О.А. Сиропятов, Л.М. Тимошенко

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

Розглянуто розробку багатокритеріального фреймворку для обґрунтованого вибору архітектури підключення до баз даних у системах з підвищеними вимогами до кібербезпеки, а саме в сегментах SCADA/IoT, зокрема, критичній інфраструктурі, енергетиці, промисловості тощо. Запропонований підхід поєднує ієрархію критеріїв (безпека, продуктивність, експлуатаційно-вартісні характеристики) з методами багатокритеріального аналізу рішень (MCDM) (зокрема, AHP та TOPSIS), що дозволяє формалізовано оцінювати компроміс між конфіденційністю, цілісністю, затримками, відмовостійкістю та витратами для різних архітектур: локальне розміщення власних серверів з підключенням через безпечний VPN-тунель, пряма публічна хмара, гібридні хмари, краєцентричний підхід та супутникове покращення (включаючи низькоорбітальний резерв). Проведений аналіз пов'язаних робіт виявив невирішене питання – відсутність уніфікованого MCDM-фреймворку для порівняння архітектур у багатоканальних середовищах з урахуванням стандартів NIST CSF 2.0, IEC 62443 та GDPR. Запропонована модель перевірена на аналізі ситуації віддаленої підстанції, де переважною є гібридна архітектура з крайовими компонентами та супутниковим резервуванням. Практична реалізація фреймворку містить послідовність кроків (Вхід→Ваги→Оцінювання→ Ранжування→Валідація), чекліст, матриці оцінок та рекомендації щодо табличного онлайн інструменту. Результати демонструють адаптивність підходу до різних профілів пріоритетів та доменів, що сприяє зниженню суб'єктивності архітектурних рішень і підвищенню рівня кібербезпеки розподілених систем.

Ключові слова: архітектура підключення до БД, кібербезпека, SCADA/IoT, гібридна/мультихмара, граничні обчислення, супутниковий зв'язок, багатокритеріальний аналіз рішень.

Вступ. Сучасні інформаційні системи з підвищеними вимогами до кібербезпеки – від SCADA/IoT-сегментів критичної інфраструктури до фінансових платформ – потребують постійного та передбачуваного доступу до баз даних, розподілених між локальними, хмарними та периферійними контурами. Перехід до гібридних хмарних моделей, розвиток периферійних обчислень і поява супутникових каналів зв'язку значно ускладнили архітектури підключення до БД, посиливши залежність від мережі та площу атаки.

У цих умовах вибір архітектури перетворюється на багатокритеріальну задачу, що вимагає одночасного врахування регуляторних вимог і стандартів (NIST CSF 2.0, IEC 62443, GDPR [1-3]), моделі загроз домену та обмежень щодо затримок, пропускної спроможності й вартості. На практиці рішення часто приймаються в багатоканальному середовищі (публічна хмара, приватні VPN-тунелі, 5G/периферійне підключення, супутникові сегменти), компроміси між безпекою, продуктивністю та експлуатаційними витратами слабо формалізовані й залежать від суб'єктивного досвіду архітекторів [4, 5].

Метою роботи є розроблення багатокритеріального фреймворку для обґрунтованого та відтворюваного вибору архітектури підключення до баз даних у системах з високими вимогами до кібербезпеки. Запропонований підхід поєднує ієрархію критеріїв (безпека, продуктивність, експлуатаційні та вартісні характеристики)

з методами багатокритеріального аналізу рішень (зокрема AHP/TOPSIS, вже застосованими в кібербезпеці [6, 7]) і забезпечує вибір архітектури з урахуванням кібербезпеки, затримки, відмовостійкості та співвідношення з витратами.

Огляд пов'язаних робіт та аналіз предметної області. У літературі та галузевих рекомендаціях архітектуру підключення до баз даних у захищених системах класифікують за типом каналу зв'язку та ступенем централізації:

– публічні прямі хмарні архітектури, пряме підключення застосунків до систем управління базами даних (СУБД) у публічній хмарі через захищені інтернет-канали;

– приватні або локальні рішення – доступ через VPN-тунелі до внутрішніх баз даних у власних центрах обробки даних організації;

– гібридні схеми з кількома хмарами – дані та сервіси розподілені між кількома хмарними провайдерами та локальною інфраструктурою;

– крайові (edge) варіанти – частина даних і логіки дублюється або кешується на периферійних вузлах, тоді як основна база даних залишається в хмарі чи локально;

– спеціальні сценарії – використання супутникових і 5G-каналів для віддалених сегментів систем промислової автоматизації (SCADA) та Інтернету речей (IoT), а також розподілених промислових об'єктів [6].

Стандарти IEC 62443 та галузеві рекомендації для промислових систем підкреслюють важливість сегментації мережі та зонального доступу до промислових БД. Однак вони розглядають підключення переважно в контексті загальної конвергенції промислових і інформаційних технологій, без формалізованого порівняння прямого хмарного доступу, VPN, гібридних і крайових рішень за єдиними критеріями [8, 9]. Дослідження безпеки гібридних і мультихмарних середовищ пропонують класифікації розміщення даних (одна хмара, кілька хмар, гібрид, континуум хмара-край), але архітектури підключення до БД описують лише на рівні типових шаблонів, без окремої багатокритеріальної оцінки [6].

Оцінювання безпеки компонентів підключення (СУБД, проміжне ПЗ, VPN-шлюзи, хмарні сервіси) базується на стандартизованих метриках, зокрема CVSS для вразливостей та моделі NIST CSF 2.0 для управління ризиками. У сфері критичної інфраструктури та систем SCADA/IoT безпека каналів і вузлів додатково відповідає вимогам IEC 62443, зокрема концепціям рівнів безпеки, зон і каналів зв'язку, які непрямо визначають дозволені схеми доступу до промислових баз даних [9].

Продуктивність каналів і архітектур оцінюють за затримкою, варіацією затримки, пропускною здатністю та доступністю. Це особливо актуально для хмарних, крайових і супутникових сценаріїв. Публікації про продуктивність хмарних і крайових систем зосереджуються переважно на мережевих та обчислювальних аспектах, ігноруючи спільний облік безпеки, експлуатаційні витрати, складності управління та прив'язку до постачальника під час вибору архітектури підключення [10]. Окрема група - роботи з багатокритеріального аналізу рішень, зокрема методи AHP, TOPSIS та їх модифікації. Ці методи застосовують для оцінювання ризиків кібербезпеки, пріоритизації заходів захисту та порівняльного вибору технічних рішень. Вони дозволяють одночасно враховувати критерії безпеки, вартості, експлуатаційної складності та продуктивності, отримуючи числову оцінку й ранжування варіантів. Проте такі дослідження переважно стосуються вибору засобів захисту (міжмережеві екрани, IDS, шифрування) або загального оцінювання ризиків, а не архітектур підключення до баз даних у мультихмарних, крайових чи промислових системах. Огляд літератури свідчить про таке:

– стандарти (NIST CSF 2.0, IEC 62443, GDPR) встановлюють загальні вимоги до захисту даних і каналів, але не пропонують формалізованого механізму вибору архітектури підключення [1, 9];

– дослідження хмарної, гібридної та крайової безпеки описують архітектури переважно на рівні загальних рекомендацій і кращих практик, фокусуючись на загрозах

і заходах захисту, а не на кількісному аналізі компромісів «безпека–продуктивність–вартість» для різних схем доступу до баз даних [6];

– методи MCDM успішно застосовуються в кібербезпеці для оцінювання ризиків і вибору засобів захисту, без адаптації до задачі вибору архітектур підключення в багатоканальних середовищах та галузевих сценаріях.

Отже, відсутній інтегрований багатокритеріальний механізм, який поєднував би класифікацію архітектур підключення до баз даних, систему критеріїв та формалізований механізм ранжування альтернатив для багатоканальних високобезпечних сценаріїв.

Методика та запропонована модель оцінювання. Запропонований фреймворк орієнтований на системи з високими вимогами до кібербезпеки та доступності даних, переважно в сегментах SCADA та Інтернету речей (IoT) енергетики й суміжних галузей критичної інфраструктури. Галузеві звіти вказують на зростання атак і вразливостей у промисловій автоматизації, пов'язаних насамперед з віддаленим доступом, недостатньою сегментацією мережі та незахищеними каналами зв'язку [10]. Тому архітектури підключення до технологічних баз даних мають враховувати мережеву експозицію, гібридні схеми доступу та резервування.

Зокрема, в енергетиці поширені змішані схеми: крайові обчислення на об'єктах, VPN-тунелі до центрів керування та аналітичних платформ, а також супутникові канали як основний або резервний маршрут для важкодоступних вузлів. Локальна крайова обробка забезпечує затримки в одиниці-десятки мілісекунд і розвантажує магістральні канали. Крайові вузли повинні відповідати принципам IEC 62443 (зони безпеки, канали зв'язку, автентифікація, сегментація) [7,11]. Для супутникових сценаріїв типові затримки становлять 25–50 мс в оптимальних умовах і 40-80 мс у реальних для низькоорбітальних систем (наприклад, Starlink), з можливими сплесками до 150–250 мс; для геостаціонарних – понад 600 мс. Хоча основний фокус – на SCADA/енергетиці, фреймворк адаптується до інших доменів (транспорт, логістика, корпоративні інформаційні системи) з подібними компромісами між безпекою, затримками, доступністю та вартістю. У них застосовують ті ж класи архітектур, але з іншими пріоритетами та обмеженнями.

Модель оцінювання базується на ієрархії критеріїв, поділених на три групи, що узгоджується з дослідженнями багатокритеріальних методів у кібербезпеці.

Критерії безпеки:

– конфіденційність і цілісність даних (шифрування каналу та бази даних, актуальні криптоалгоритми, контроль цілісності);

– доступність (цільові показники 99,9% або 99,99% відповідно до вимог енергетичних об'єктів);

– підтримка ідеальної прямої секретності (PFS) у протоколах;

– принципи нульової довіри (zero trust): строга автентифікація та авторизація на кожному сегменті, мінімізація довірених зон;

– рівень сегментації та мікросегментації за зонами і каналами IEC 62443 [7, 9].

Для критичної інфраструктури особливе місце – у сегментації, обмеженні привілеїв, мінімізації експозиції, нульової довіри для зовнішніх, супутникових каналів [10].

Критерії продуктивності:

– затримка: одиниці-десятки мс для локального краю, десятки мс для хмарних центрів даних, 40–80 мс для LEO-супутників, понад 600 мс для GEO;

– варіація затримки: критична для протоколів реального часу;

– пропускна здатність: сотні Мбіт/с низхідного і десятки Мбіт/с висхідного каналу зв'язку для сучасних LEO-систем;

– стійкість: резервні маршрути, відмовостійкість, схеми

активний/резервний, багатоканальне підключення.

Експлуатаційно-вартісні критерії:

– капітальні та операційні витрати: крайові вузли підвищують капітальні, але можуть знижувати операційні за рахунок оптимізації трафіку; чистий хмарний підхід діє навпаки;

– ризик залежності від постачальника, особливо в публічних хмарах і спеціалізованих периферичних платформах;

– складність управління (потреба в спеціалістах, кількість компонентів для оновлення, централізований моніторинг).

Кількісні параметри (затримка, пропускна здатність, доступність) базуються на звітах і вимірюваннях; якісні за напівкількісними шкалами, каліброваними на галузевих даних.

Формалізація метрик і багатокритеріальний процес.

Різнотипні критерії нормалізуються до шкали [0;1] за допомогою min-max або z-score перетворень. Для негативних критеріїв (затримка, витрати) застосовується обернена формула. Якісні показники кодуються впорядкованими шкалами.

Вагові коефіцієнти визначаються методом аналітичного ієрархічного процесу або його модифікаціями [11, 12]. Експерти будують матриці попарних порівнянь, що дозволяє отримати узгоджені ваги для конкретного домену (наприклад, пріоритет безпеки та доступності над вартістю в критичній інфраструктурі).

Агрегування виконують зваженою сумою або методом TOPSIS, де визначають найкращу та найгіршу альтернативи, обчислюють близькість реальних варіантів до еталонів. Це забезпечує прозоре ранжування архітектур (прямий хмарний, локальний/ VPN, гібридний/мультихмарний, крайовий, супутниковий) у SCADA/ енергетиці.

Стійкість результатів перевіряється аналізом чутливості за вагами та ключовими параметрами. Формуються сценарії пріоритетів («безпека понад усе», «доступність понад усе», «врахування вартості» тощо) з варіюванням ваг у реалістичних межах. Це дозволяє виявити стійкі рішення та архітектури, чутливі до змін пріоритетів.

Для супутникових архітектур моделюються затримки на основі даних LEO-систем (медіанна затримка 40-80 мс, співставна з наземними мережами, але з можливими сплесками) порівняно з GEO (понад 600 мс). Показники інтегрують в критерії затримки, варіація затримки та стійкості й застосовують в сценаріях «основний наземний/VPN + резервний LEO» або «супутниковий як основний для віддалених об’єктів».

Методика базується на трьох принципах.

1. Вибір архітектури підключення – домен-специфічна багатокритеріальна задача: для SCADA/енергетики визначається набір архітектур і профіль вимог, що відображає регуляторні обмеження, модель загроз та експлуатаційний контекст .

2. Оцінювання будуєть на ієрархії критеріїв безпеки, продуктивності, експлуатаційно-вартісних характеристиках. Кількісні параметри калібруються за галузевими даними.

3. Метрики нормалізують, ваги визначають через експертні профілі, агрегування – за допомогою багатокритеріального механізму з обов’язковим аналізом чутливості, особливо для затримки та доступності в крайових і супутникових сценаріях.

У межах запропонованого фреймворку розглядають п’ять базових класів архітектур підключення до баз даних у системах SCADA/енергетики та суміжних доменах.

1. Прямий публічний хмарний доступ – застосунки або SCADA-шлюзи звертаються до СУБД у публічній хмарі через захищені інтернет-канали без виділених приватних.

2. Локальні/VPN-архітектури – бази даних розміщуються в локальних центрах обробки даних або на майданчиках оператора критичної інфраструктури; віддалені об’єкти підключаються через IPsec/OpenVPN/MPLS-тунелі та міжмережеві екрани.

3. Гібридні/мультихмарні сценарії – дані та сервіси розподілені між локальними сегментами та одним або кількома хмарними провайдерами; доступ до БД здійснюється через комбінацію приватних каналів, VPN і прямого хмарного підключення.

4. Крайово-орієнтовані архітектури – використовують промисловий крайовий рівень (шлюзи, локальні вузли) для зберігання й обробки ключових даних та агрегатів телеметрії з подальшою передачею агрегованих або відкладених даних до центральної бази в хмарі чи центрі обробки даних.

5. Архітектури з супутниковим/5G-підсиленням – забезпечують доступ для віддалених об’єктів через супутникові або 5G-канали (як основний або резервний маршрут) у поєднанні з одним із зазначених варіантів розміщення баз даних.

Це забезпечує відтворюваність, адаптованість і прозорість обґрунтування вибору архітектури в системах критичної енергетичної інфраструктури (рис.1).

Класифікація відображає осі варіативності: місце розміщення бази даних та ступінь розподіленості (одна хмара, мультихмарна/гібридна).

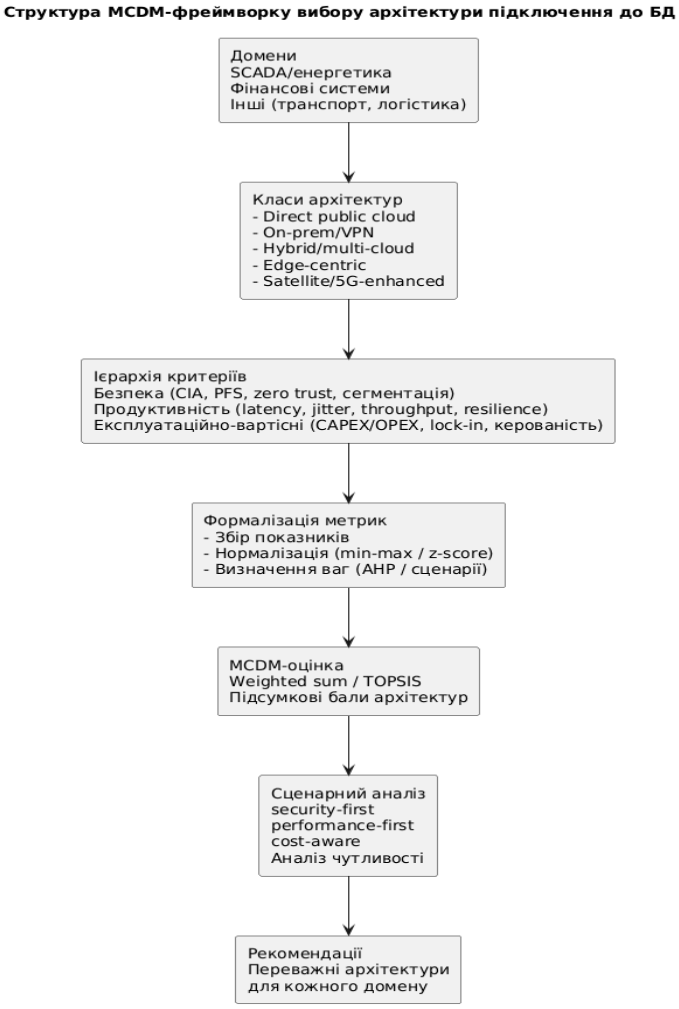


Рис. 1. Структура MCDM-фреймворку

Кожен клас оцінюють за ієрархією критеріїв безпеки, продуктивності, експлуатаційно-вартісних характеристик (рис.2).

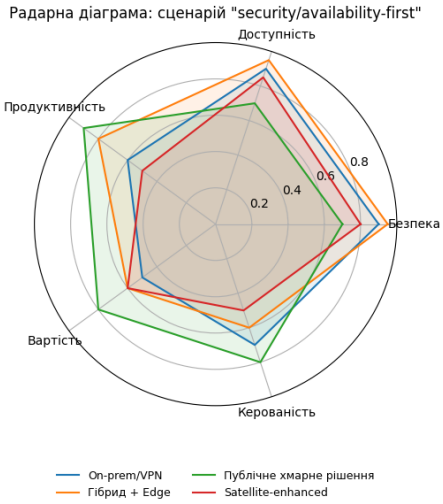


Рис. 2. Радарна діаграма оцінок п’яти архітектур за трьома групами критеріїв

Гібридна/крайова архітектура демонструє найбільш збалансований профіль(табл.1). Оцінки формують на основі кількісних і якісних даних, нормалізують до шкали [0;1].

Таблиця 1

Нормалізовані оцінки та підсумкові бали архітектур у базовому сценарії

Архітектура	Безпека	Продуктивність	Експлуатаційно-вартісні	Підсумковий бал (TOPSIS)	Ранг
Гібридна/мультихмарна + крайова	0,95	0,85	0,70	0,88	1
Локальна/VPN	0,90	0,75	0,80	0,82	2
З супутниковим/5G-підсиленням (резерв)	0,75	0,65	0,75	0,71	3
Крайово-орієнтована	0,85	0,90	0,60	0,78	4
Прямий публічний хмарний	0,60	0,80	0,85	0,68	5

У базовому сценарії «безпека/доступність понад усе» найбільшу вагу мають критерії безпеки та доступності, меншу – продуктивності, найменшу – експлуатаційно-вартісні.

Застосування моделі TOPSIS показує, що верхні позиції мають гібридні крайово-орієнтовані архітектури, де низькі затримки на рівні об’єкта, висока відмовостійкість завдяки локальній обробці, жорстка сегментація за IEC 62443 при прийнятних витратах.

Прямі публічно-хмарні архітектури отримують нижчі бали через більшу поверхню атаки та залежність від публічних інтернет-каналів, попри переваги за витратами. Архітектури з супутниковим/5G-підсиленням займають проміжні позиції, залежно від ролі каналу (основний чи резервний) та критичності затримок і варіації затримки.

Стійкість результатів перевіряється трьома профілями пріоритетів: «безпека понад усе», «продуктивність понад усе» та «врахування вартості».

У сценарії «продуктивність понад усе» зростають ваги затримки, варіація затримки та пропускної здатності, що підвищує позиції архітектур із низькими затримками (прямий хмарний і гібридний з близькими центрами даних), тоді як супутниково-домінуючі рішення знижуються через нестабільну затримку. У сценарії «врахування вартості» перевагу мають простіші архітектури (чистий хмарний або спрощений локальний/VPN) завдяки нижчим вартості та простоті управління порівняно з крайовими рішеннями.

Аналіз чутливості свідчить, що гібридні крайово-орієнтовані архітектури стабільно входять до топ-позицій за високого пріоритету безпеки та доступності, типового для SCADA/енергетики. Це базові для пілотних впроваджень, тоді як чисто публічно-хмарні та «супутник як основний» підходи доцільні лише як спеціалізовані з додатковими заходами захисту. Гібридна/крайова стабільно в топ-2, супутникова знижується в «продуктивність понад усе», пряма хмарна підвищується у «врахування вартості» (рис.3).

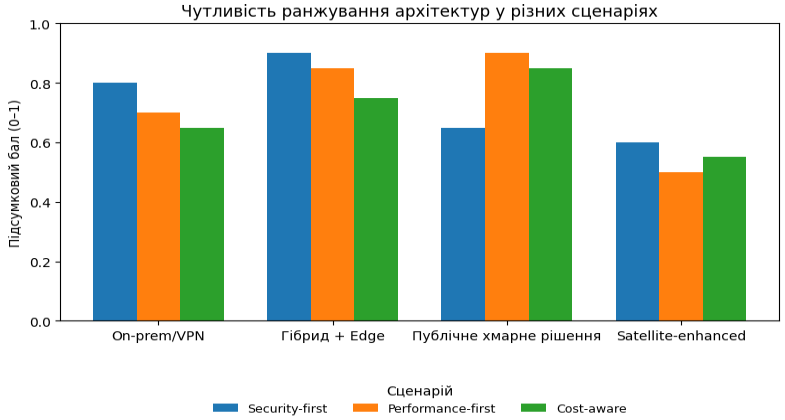


Рис. 3. Результати аналізу чутливості: підсумкові бали архітектур у трьох сценаріях

У SCADA/енергетиці за профілем «безпека/доступність понад усе» найбільш збалансованими є гібридні крайово-орієнтовані архітектури з високим рівнем безпеки й доступності з прийнятною продуктивністю й витратами. Прямі публічно-хмарні та супутникові варіанти мають обережне застосування через підвищені ризики або затримки.

Сценарний аналіз підтверджує стабільність переваги гібридних/крайових підходів при зміні пріоритетів. Це створює основу для практичного фреймворку: поетапної процедури вибору архітектури, дерева рішень та ситуації дослідження для типового енергетичного об’єкта, що ілюструють інтеграцію моделі в реальне архітектурне проєктування.

Запропонований фреймворк і практичне застосування. Послідовність кроків фреймворку.

Крок 1 (Вхідні дані). Формалізація вимог домену – профіль загроз, регуляторні обмеження (NIST CSF, IEC 62443, галузеві стандарти), допустимі затримки та втрати, цільові показники доступності, бюджет і експлуатаційні обмеження. Фіксується перелік допустимих архітектур (прямий хмарний доступ, локальний/VPN, гібридний/ мультихмарний, крайово-орієнтований, з супутниковим/5G-підсиленням).

Крок 2 (Ваги критеріїв). Налаштування пріоритетів –аналітичний ієрархічний процес за участю експертів (інженери SCADA, оператори) [13] або сценарні профілі («безпека понад усе», «доступність понад усе», «продуктивність понад усе», «врахування вартості»).

Крок 3 (Оцінювання кандидатів). Збір кількісних та якісних показників з подальшою нормалізацією за ієрархією критеріїв.

Крок 4 (Ранжування та рекомендація). Застосування багатокритеріального механізму для розрахунку балів, ранжування та виділення оптимальних варіантів.

Крок 5 (Валідація). Перевірка рекомендацій через пілотні впровадження, моделювання сценаріїв/порівняння з даними інцидентів і SLA, з можливою корекцією ваг.

Фреймворк реалізується як спрощена схема ухвалення рішень (рис.4).

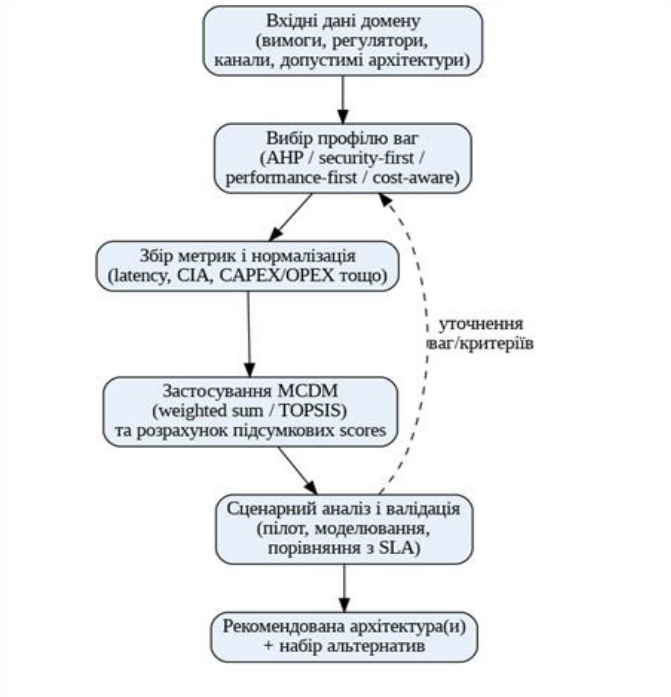


Рис. 4. Схема фреймворку

Процес починається з вибору домену (SCADA/енергетика, чи інший), уточнення вимог та каналів. Далі – вибір профілю ваг (наприклад, «безпека/доступність понад усе» для SCADA). Фінальні вузли рекомендують 1-2 архітектури (гібридний/мультихмарний + крайовий для об’єктів з надійним каналом; локальний/VPN + супутниковий резерв для віддалених).

Ситуація: SCADA у віддаленій енергетиці з супутниковим резервуванням (рис.5).

Розглянемо віддалений енергетичний об’єкт (підстанція чи вузол відновлюваної енергетики)з основним VPN-каналом і низькоорбітальним супутниковим резервом.

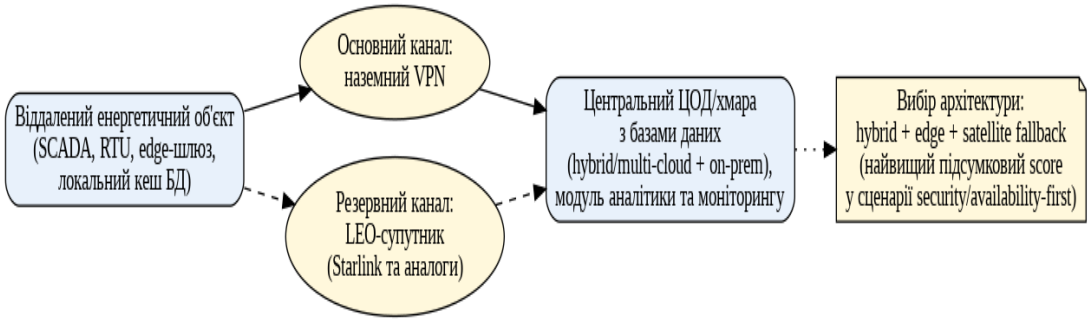


Рис. 5. Схема кейсу для віддаленої підстанції

Вимоги: відповідність IEC 62443 (оновлені 2025 року правила сегментації та мікросегментації), доступність ≥99,9%, затримка телеметрії ≤200 мс, обмежені витрати і навантаження на персонал. Допустимі архітектури: локальний/VPN, гібридний/ мультихмарний + крайовий, з супутниковим резервом; прямий публічний хмарний – лише допоміжний. Профіль ваг: «безпека/доступність понад усе» (вага безпеки та доступності 0,6–0,7; продуктивності 0,2-0,25; витрат 0,1–0,15). На основі даних 2025 року (медіанна затримка Starlink у пікові години 25-45 мс з тенденцією зниження) розрахунок TOPSIS показує лідерство гібридного/мультихмарного+крайового варіанту (локальне кешування, основний VPN + LEO резерв). Переваги: висока безпека/сегментація, стійкість до відмов, прийнятні затримки та витрати. У табл. 2 зображено чекліст за кроками.

Таблиця 2.

Чекліст за кроками (контрольні запитання для кожного етапу)

Крок	Ключові контрольні пункти	Статус	Примітки
Вхідні дані (Input)	Домен: SCADA/енергетика, віддалена підстанція. Доступність≥99,9%, затримка ≤200 мс Регуляторні вимоги. .Допустимі архітектури та виключення	Так / Ні / Частково	
Вибір профілю ваг	Профіль «безпека/доступність понад усе». Ваги: безпека+ доступність 0,6–0,7; продуктивність 0,2–0,25; витрати 0,1–0,15. Джерело ваг задокументовано (AHP або сценарний)	Так / Ні / Корекція	
Збір метрик та нормалізація	Дані затримки/jitter для VPN, краю та LEO. Оцінка CAPEX/OPEX .Опис сегментації, нульової довіри, керованості. Нормалізація без аномалій	Так / Ні / Частково	
Оцінка та ранжування (MCDM)	Застосовано зважена сума / TOPSIS. Бали узгоджуються з експертною оцінкою. Виділено лідера (гібридний + крайовий з VPN + LEO резерв)	Так / Ні / Перегляд	Документувати результати
Валідація (Validation)	Моделювання відмов каналів Порівняння з історичними інцидентами/SLA Підтвердження або корекція архітектури	Виконано / Заплановано / Корекція	

У табл. 3 наведено приклад збору метрик та оцінок для кейсу віддаленої підстанції.

Таблиця 3.

Матриця критеріїв та нормалізованих оцінок

Архітектура	Доступність С1	Затримка С2)	Безпека (С3)	Витрати (С4)	Складність (С5)
А1: Локальний/VPN	0,80	0,70	0,75	0,40	0,50
А2: Гібридний + крайовий (VPN + LEO резерв)	0,90	0,80	0,85	0,60	0,65
А3: Супутниковий як основний	0,70	0,65	0,70	0,55	0,45

Аналіз матриці критеріїв підтверджує переваги рекомендованої архітектури.

А1. Висока доступність і прийнятна затримка, але обмежена масштабованість та вищі операційні витрати на локальну інфраструктуру.

А2.Завдяки локальному кешуванню та резервному низькоорбітальному каналу досягає найкращого балансу – високі показники доступності, низька затримка та посилена безпека за помірних витрат (лідер за С1-С3, середні С4-С5). Це дозволяє знизити загальні витрати на 10-30% порівняно з локальними рішеннями за рахунок оптимізації трафіку та зменшення залежності від дорогого обладнання.

А3. Спрощує локальну інфраструктуру (нижчі витрати), але має нестабільності затримок і підвищених вимог до управління (нижчі бали за С2 та С5).

Для організацій з розвиненою ІТ-інфраструктурою можлива реалізація онлайн-інструменту (web- або intranet-застосунку), інтегрує базу типових архітектур, профілів доменів і актуальних метрик, автоматизує нормалізацію, розрахунок та візуалізацію (радарні діаграми, чутливість).

Розглянемо приклад роботи онлайн-інструменту (кейс: віддалена підстанція). Інтерфейс складається з трьох екранів.

Домен та вимоги: вибір профілю «SCADA/енергетика – віддалена підстанція», параметри: доступність ≥99,9%, затримка ≤200 мс, VPN основний + LEO резерв. Архітектури: варіанти А1, А2, А3. Автоматичне завантаження даних (затримка LEO 2025: 25-45 мс, тенденція <30 мс). Пріоритети: сценарій «безпека/доступність понад усе» (ваги: безпека+доступність ≈0,65; продуктивність ≈0,2; витрати ≈0,15), можливість коригування.

Інструмент автоматично нормалізує та розраховує TOPSIS (А2 – лідер), виводить рейтинг у таблиці та радарній діаграмі, генерує діаграму чутливості для альтернативних

сценаріїв, формує звіт: припущення, ваги, рекомендація (гібридний + крайовий з LEO резерв) та ключові компроміси. Прискорює ухвалення рішень у 2-3 рази, економить до 50% часу архітекторів та 15-30% витрат на проєктування/впровадження.

Запропонований фреймворк показує, що в домені SCADA/енергетики пріоритетними є не традиційні локальні/VPN-архітектури, а гібридні рішення з крайовими компонентами та хмарними сервісами. Цей результат дещо несподіваний для організацій, які вважають повне локальне розміщення баз даних «найбезпечнішим». Насправді поєднання сегментації, локального кешування та резервних каналів (наприклад, низькоорбітальних супутникових LEO) забезпечує кращий баланс безпеки, доступності та продуктивності [13]. У кейсі віддаленої підстанції гібридна/мультихмарна + крайова архітектура з VPN та LEO резервом найвищі бали, а не «інтуїтивно безпечніший» локальний підхід.

Фреймворк кількісно демонструє чутливість рішень до профілю пріоритетів: невелика зміна ваг на користь продуктивності чи витрат може змінити лідера, але гібридні крайові варіанти стабільно залишаються в топі. Це узгоджується з галузевими трендами – переходом до гібридних/мультихмарних і промислових крайових рішень, широким впровадженням LEO-супутників у критичній інфраструктурі. На відміну від евристичних підходів фреймворк надає формалізоване обґрунтування, дозволяючи архітекторам працювати зі звичними метриками (угода про послуги, затримка, витрати, IEC 62443) у прозорій багатокритеріальній процедурі.

Обмеження моделі. Перевірено переважно на SCADA/енергетиці; інші домени (наприклад, з жорсткими вимогами до затримки) потребують окремої адаптації та калібрування. Спрощено аспекти: не враховуються детальні топології мереж, внутрішні механізми СУБД, засоби виявлення/реагування, взаємозалежності критеріїв (вплив додаткового захисту на затримку, витрати). Багато даних базуються на моделюванні, узагальнених показниках провайдерів, експертних оцінках, а не на вимірюваннях.

Висновки та подальші дослідження. У роботі запропоновано класифікацію архітектур підключення до баз даних: прямий публічний хмарний доступ, локальний/VPN, гібридний/мультихмарний, крайово-орієнтований, з супутниковим/5G-підсиленням, на критеріях безпеки, продуктивності, доступності, витрат та експлуатаційної складності, як основа формалізованого порівняння альтернатив. На її базі розроблено багатокритеріальну модель оцінки з нормалізацією показників, методами AHP/TOPSIS та сценарним аналізом для різних профілів пріоритетів («безпека понад усе», «продуктивність понад усе», «врахування вартості»).

Ключовий результат – практичний фреймворк вибору архітектури, орієнтований на SCADA/енергетику та критичну інфраструктуру. Це послідовність кроків, блок-схема рішень, чекліст, матриці критеріїв та кейс віддаленої підстанції з рекомендованою гібридною/мультихмарною + крайовою архітектурою та низькоорбітальним супутниковим резервом. Фреймворк переводить неформальні міркування у відтворювану, прозору процедуру, прискорює ухвалення рішень і полегшує обґрунтування перед стейкхолдерами. Прив’язка до реальних метрик, візуалізації та потенціал онлайн-інструменту роблять його ефективним для проєктування нових і модернізації наявних систем. Для операторів критичної інфраструктури це означає зниження суб’єктивних ризиків, економію ресурсів і повторне використання досвіду через типові профілі.

Напрямки подальших досліджень – розширення на нові домени: використання крайових/5G-рішень, супутникових систем нового покоління та високочастотних застосувань з низькою затримкою, інтеграція динамічних механізмів (AI-підтримка адаптації маршрутів і протоколів до умов мережі); участь у стандартизації методик оцінки архітектур для критичних інфраструктур, узгодження з IEC 62443 та міжнародними ініціативами. Реалізація цих напрямів підвищить надійність фреймворку та перетворить його на основу галузевих рекомендацій і кращих практик.

Список літератури

1. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) 29. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.
2. ISA/IEC 62443 Series of Standards. International Society of Automation; International Electrotechnical Commission. 2024–2025. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). *Official Journal of the European Union*. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
4. Cloud Security Alliance. Top Threats to Cloud Computing 2024. Cloud Security Alliance, 2024. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024.
5. Fortinet. Multi-Cloud Security Challenges and Best Practices. Fortinet Resources, 2025.
6. Multi-cloud and hybrid cloud security challenges. Computers & Security (various articles), 2024–2025.
7. Advantech. Industrial Edge Computing Security Solutions. Advantech Resources, 2024.
8. IoT Analytics. Satellite IoT Market Report 2025–2030. IoT Analytics, June 2025. URL: https://iot-analytics.com/satellite-iot-market-report-2025-2030.
9. Elisity. IEC 62443 in 2025: Network Segmentation Requirements and Changes. Elisity Blog, January 2025. URL: https://www.elisity.com/blog/iec-62443-in-2025-network-segmentation-requirements-and-changes.
10. Nozomi Networks OT/IoT Cybersecurity Trends and Insights Report. Nozomi Networks, February 2025. URL: https://www.nozominetworks.com/resources/reports/ot-iot-cybersecurity-trends-2025.
11. Reimagining SCADA: The Convergence of Cloud, Edge, and Intelligent Automation. Adisra, October 2025. URL: https://adisra.com/reimagining-scada-the-convergence-of-cloud-edge-and-intelligent-automation/
12. Saaty R. W. The analytic hierarchy process – what it is and how it is used. *Mathematical Modelling*. 1987. Т. 9, № 3–5. С. 161–176.
13. Ookla Starlink Performance Report 2025. Ookla Research, 2025. URL: https://www.ookla.com/articles/starlink-us-performance-2025.

О.А. Сиропятов, Л.М. Тимошенко

MULTI-CRITIARERIA FRAMEWORK FOR SELECTING DATABASE CONNECTION ARCHITECTURE IN DISTRIBUTED SYSTEMS WITH INCREASED CYBERSECURITY REQUIREMENTS

Syropyatov O.A. Tymoshenko L.M.

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

The article discusses the development of a multi-criteria framework for the informed choice of database connectivity architecture in systems with increased cybersecurity requirements, namely in the SCADA/IoT segments, in particular, critical infrastructure, energy, industry, etc. The proposed approach combines a hierarchy of criteria (security, performance, operating cost characteristics) with multi-criteria decision analysis (MCDM) methods (in particular, AHP and TOPSIS), which allows for a formal assessment of the trade-off between confidentiality, integrity, delays, fault tolerance and costs for different architectures: local placement of own servers with connection via a secure VPN tunnel, direct public cloud, hybrid clouds, edge-centric approach and satellite enhancement (including low-orbit reserve). The analysis of related works revealed an unresolved issue - the lack of a unified MCDM framework for comparing architectures in multi-channel environments, taking into account the NIST CSF 2.0, IEC 62443 and GDPR standards. The proposed model was tested on the analysis of a remote substation situation, where a hybrid architecture with edge components and satellite redundancy is predominant. The practical implementation of the framework contains a sequence of steps (Input → Weights → Evaluation → Ranking → Validation), a checklist, assessment matrices and recommendations for a tabular online tool. The results demonstrate the adaptability of the approach to different priority profiles and domains, which helps to reduce the subjectivity of architectural decisions and increase the level of cybersecurity of distributed systems.

Keywords: database connection architecture, cybersecurity, SCADA/IoT, hybrid/multicloud, edge computing, satellite communication, multi-criteria decision analysis.

DOI 10.15276/imms.v16.no1.169
УДК 004.91:004.67:004.65:006.3/.8

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 169-180

РОЗРОБКА ПАРСЕРУ ДЛЯ ІНТЕГРАЦІЇ МЕНЕДЖЕРІВ БІБЛІОГРАФІЇ ТА ПРОГРАМОВАНОЇ СИСТЕМИ КОМП'ЮТЕРНОЇ ВЕРСТКИ TYPST, ЯКИЙ ВІДПОВІДАЄ ВИМОГАМ БІБЛІОГРАФІЧНОГО СТАНДАРТУ ДСТУ 8302:2015

А.О. Стопакевич[1], О.А. Стопакевич[2]

[1]Державний університет інтелектуальних технологій та зв'язку
1, Кузнечна вул., Одеса, 65023, Україна
[2]Національний університет «Одеська Політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: stopakevich@gmail.com

Менеджер бібліографії (на кшталт Zotero, Mendeley, EndNote) є незамінним інструментом для багатьох науковців. Вони не тільки дозволяють структурувати інформацію, але й здатні тільки за DOI чи ISBN додати в базу менеджера бібліографічну інформацію, яку розмістив видавець чи журнал в таких системах як CrossRef. Проте для науковців, які застосовують національні стандарти бібліографії, зокрема ДСТУ 8302:2015, не існує зручного та повнофункціонального рішення, яке дозволяє отримати коректне оформлене посилання на базі даних, які зберігаються в менеджері бібліографії. Існуючі рішення на базі CSL не забезпечують коректної інтернаціоналізації та гнучкості, отже застосовуючи їх не можливо згенерувати коректне цитування за правилами стилю ДСТУ 8302:2015. Метою роботи є створення програмної технології для автоматичної генерації переліку літературних джерел відповідно до вимог ДСТУ 8302:2015 у середовищі сучасної системи комп'ютерної верстки Typst, використовуючи як вхідні дані файли форматів BibTeX/BibLaTeX. У роботі розроблено алгоритм парсингу та обробки бібліографічних записів, який включає: лексичний аналіз вхідних даних, евристичне визначення мови джерела, конвертацію LaTeX-макросів та спецсимволів у Unicode, декодування URL-адрес, валідацію полів за типами джерел. Для фінального формування бібліографічного опису застосовано підхід на основі токенів (контент та розділювачі) із системою пріоритетів для вирішення конфліктів пунктуації. Реалізовано програмний модуль мовою Typst, який не вимагає зовнішніх препроцесорів й враховує неоднозначності та поширені порушення стандартів при оформленні даних в форматі BibTeX. Верифікація роботи парсера проведена на вибірці з понад 500 джерел. Результат роботи дозволяє українським дослідникам, які забажають застосовувати систему Typst, безпроблемне інтегрувати з нею бібліографічні менеджери, які здатні експортувати інформацію в форматі BibTeX/BibLaTeX.

Ключові слова: ДСТУ 8302:2015; система комп'ютерної верстки Typst; BibTeX/BibLaTeX; автоматизація бібліографії; парсинг даних; наукова документація; менеджери цитувань.

Вступ. Застосування менеджерів бібліографії загалом у світі протягом останніх 10 років стало звичною практикою для значної кількості (в деяких регіонах й більшості) науковців, викладачів й аспірантів. Стимулює застосування таких систем відсутність необхідності ручного введення бібліографічної інформації. Як правило, якщо монографія чи стаття мають DOI, то висока ймовірність, що менеджер бібліографії зможе знайти та додати необхідну інформацію в свою базу даних автоматично. Для аналізу поточної ситуації будемо застосовувати дані зі звіту [1]. Цей звіт розроблено для інвесторів й у відкритому доступі лише ключові тези, проте інформація в ньому має бути більш об'єктивна ніж абстрактні звіти університетів чи нерепрезентативні опитування. Його ключові моменти наступні:

- сукупний загальнорічний темп зростання - 7.5.%;
- у період з 2025 до 2035 рр очікується зростання ринку у два рази з 0.43 до 0.88 млрд. USD;

- за даними ЮНЕСКО в 2024 р. біля 62% академічних установ впровадили хмарні застосунки для управління бібліографією;
- сегментація ринку: академічний - 68%, корпоративний 21%, державні структури - 11%;
- усереднено за даними International Telecommunication Union 58% студентів та дослідників застосовують мобільні бібліографічні менеджери. Зростання за 5 років на 26%. Проте, ці дані стосуються переважно північної Америки та західної Європи;
- за даними U.K. Intellectual Property Office, британський менеджер бібліографії Mendeley використовується 42% користувачами в Європі на 2024 р, що підтримується партнерством з понад 1500 університетами;
- за даними U.S. National Science Foundation (NSF), американській менеджер бібліографії Zotero мав зростання в 35% відсотків активних користувачів в період з 2021 по 2024.

Менеджери бібліографії реалізують щонайменше наступні функції [2,3]:

- ведення бази даних джерел з врахуванням їх типів з можливістю пошуку та редагування, додавання матеріалів (тексту, анотації);
- імпорт посилань в базу даних в форматі BibTeX (обов'язковий стандарт) та RIS, автоматичне додавання інформації за DOI (використовуються сервіси на кшталт doi2bib) чи іншими параметрами з використанням комерційних та/або відкритих бібліографічних баз даних;
- експорт вибраних посилань в BibTeX та інші подібні формати для використання в системах комп'ютерної верстки (класично - в варіанти TeX, але зараз не тільки в них) та синхронізації даних в різних системах;
- автоматичне оформлення (генерація) бібліографічних посилань вибраних джерел з використанням зазвичай мови CSL, яка забезпечує можливість врахування вимог різних бібліографічних стандартів;
- програмний інтерфейс для взаємодії з іншим програмним забезпеченням та/або плагіни для поширених офлайн (Microsoft Word, Open/LibreOffice Writer тощо) та онлайн (Google Docs, Microsoft 365 тощо) текстових редакторів, за допомогою якого можна зробити посилання в тексті й автоматично згенерувати перелік літературних джерел, які відповідають одному з бібліографічних стандартів.

Оскільки формати та програмні застосунки розроблялись переважно в середовищі, в якому користуються латинкою й переважно англійською, то після їх поширення виникало багато проблем з адаптацією для користувачів з іншими алфавітами (наприклад, програмна реалізація BibTeX ще в 2000-х за замовченням працювала в 7-бітному кодуванні й потім перейшла на 8 бітів). Принципово ці проблеми вирішені в BibLaTeX + Babel, розроблених під час масового переходу на UTF-8. Проте BibTeX залишається загальноприйнятим стандартом для багатьох англомовних журналів, оскільки не вимагає Babel. Введення Babel для англомовного журналу створює велику кількість проблем. Babel дозволяє різні макроси, які мають можуть непередбачено застосовувати певні правила локалізації. Крім того, його правила локалізації входять в конфлікт з класичними однобайтовими модулями для розташування переносів, сортування, стовпчикового верстання тощо.

В цілому такі не адаптовані до інтернаціоналізації інструменти як формат BibTeX й мова бібліографічних стилів CSL попри цей недолік в цілому залишаються стандартом. Для українських користувачів це означає, що в межах цих інструментів досягнути високого рівня відповідності вимогам ДСТУ 8302:2015 складно з причини відсутності в них механізмів інтернаціоналізації та гнучкої логіки [4]. Це знижує мотивацію для українських користувачів застосовувати такі інструменти, оскільки дотримання ДСТУ 8302:2015 є вимогою до виконаних в Україні НДР, публікацій в наукових журналах, монографій, кваліфікаційних робіт.

В цій роботі розглянута задача програмної генерації переліку літературних джерел з використанням BibTeX / BibLaTeX (частково) файлу. Ця задача розв'язана для нової системи програмної комп'ютерної верстки Typst, яка має всі шанси в майбутньому стати заміною варіантам систем TeX. За два роки (з 2023) Typst стрімко набирає базу користувачів [5]: систему використовують в понад 3500 академічних установах й кількість зірок на GitGub перейшла поріг у 45 тис. Проте, наданий розв'язок у цілому має універсальний характер й може бути адаптованим для деяких інших пакетів.

Задачі роботи. Розробити програмну технологію для генерації переліку літературних джерел згідно вимог ДСТУ 8302:2015 для системи Typst. Для цього потрібно

1. Проаналізувати недоліки та обмеження наявних інструментів.
2. Запропонувати зручний для користувача алгоритм для генерації переліку літературних джерел, який орієнтований на те, що користувач працює переважно з бібліографічними даними, які згенеровані програмами чи оформлені іншими людьми, при цьому застосовується не лише англійська, але й європейські мови.
3. Провести програмну реалізацію генератора переліку літературних джерел мовою Typst й перевірити її на достатній вибірці згенерованих та вручну оформлених вихідних даних в форматі BibTeX.

Аналіз недоліків та обмежень наявних інструментів. *RIS*. Найпростіший формат, запропонований в 1980 саме з метою обміну даними між різними бібліографічними системами. Дані зберігаються в форматі неунікальний параметр: значення. Це неструктуроване збереження, проте воно зручне тим, що автори чітко відокремлюються один від одного й немає проблеми як їх виділити з одного поля, яке заповнюється вільно й періодично з помилками. Формат принципово мінімалістичний, хоча сучасні версії мають doi, url, language. Він містить менше інформації в порівнянні з усіма наступними форматами. Використовується лише для експорту та імпорту. Проблема кодувань розв'язується на рівні програм.

BibTeX. Являє собою формат представлення інформації для однойменного двигуна в межах LaTeX та його розширень (LuaLaTeX, XeTeX) про джерела як послідовності структурованих даних виду “унікальний параметр: значення”. Запропонований в 1985 р. доступ до структури реалізується за допомогою унікального ключа, який формує користувач. Перелік полів в структурі відрізняється в залежності від типу джерела й є фіксованим. Параметр мови джерела відсутній. Сучасні бібліографічні менеджери/сайти зазвичай експортують дані в BibTeX в кодуванні UTF-8.

В двигуні BibTeX застосовується однобайтове кодування, яке треба вказати (koi8-r, cp1251) чи він буде працювати 7-ми бітному режимі. Відсутність інтернаціоналізації призвела до поганої практики застосування символів LaTeX в бібліографії для передачі грецьких символів, діакритичних символів латинки тощо. Двигун застосовує спрощену мову стилів, яка зберігається в файлах з розширенням bst. Ця мова дозволяє базові операції над рядками й умовні переходи, але не має повноцінних структур даних, Unicode-обробки чи локалізації. Наприклад, неможливо реалізувати правила типу "якщо авторів більше трьох – скоротити, але при цьому врахувати кириличні ініціали". Остання стабільна версія двигуна, яка включає певні розширення формату (наприклад, url, doi) з його початкової форми випущена у 2010 р.

Двигун *BibLaTeX* з'явився в 2009 р. як результат перегляду BibTeX з активним застосуванням двигуна Babel для інтернаціоналізації в LaTeX. В порівнянні з BibTeX він має дещо несумісну номенклатуру полів, збільшує кількість ролей (не тільки автор й редактор як в BibTeX, але й перекладач, рецензент тощо) й кількість типів джерел. Підтримує мову CSL, проте логіка може бути достатньо вільно запрограмована (особливо в LuaLaTex з мовою Lua).

Мова *CSL*. До CSL фактично кожний бібліографічний менеджер мав свій власний несумісний формат стилів. Перша реалізація CSL з'явилась в 2004 і в 2010 р. стала стандартною мовою стилів для оформлення бібліографічних джерел у всіх

бібліографічних системах. Кількість доступних стилів [6] мовою CSL - біля 10 тис. [7]. Ця мова орієнтувалась на бібліотекарів й передбачала можливість візуального програмування - створення формату готовими блоками з обмеженими настройками. Хоча існують стилі для ДСТУ, ГОСТ тощо, з їх застосуванням неможливо зробити відповідне до вимог посилання. Наприклад, немає можливості писати "С. 20-21" чи "Р. 20-21" залежно від мови, писати авторів до чи після заголовку за певних умов тощо. Хоча й були запропоновані розширення, які цей недолік можуть нейтралізувати, їх не реалізують щоб не зробити систему занадто складною за можливою поведінкою.

Менеджери бібліографічних джерел *Mendeley (Elseiver/Scopus), EndNote*[8] *(Clavirate/Web of Science), Zotero* (проєкт з відкритим кодом). Всі ці застосунки працюють з мовою CSL, проте відрізняються в можливих джерелах отримання даних. Таким чином, згенерувати повноцінне посилання у відповідності до ДСТУ 8302:2015 з їх застосуванням не можливо.

Має свій обмежений вбудований бібліографічний менеджер також *Microsoft Word*, який теж внутрішньо працює з CSL, проте можливо обирати лише зі стандартних стилів, зміна яких користувачеві не дозволена Для Word та аналогічних пакетів менеджери бібліографічних джерел пропонують плагіни. Вони різні за якістю, проте корінний недолік для нашої задачі однаковий.

LaTeX - історично набір макросів для TeX, який вийшов за межі цього визначення й фактично сам став мовою зі своїми бібліотеками [9–12]. Його історія починається з кінця 1970-х, коли були прийнятті основні архітектурні рішення, деякі з яких стали проблемою потім. Архітектура базувалась на ідеї генерації універсальної розмітки - формат DVI. Цей формат максимально конкретний - кожен символ в ньому розміщений на позиції. Далі драйвер принтера мав виконати DVI за власною логікою. Коли PostScript став стандартом для принтерів звичайним шляхом став DVI->PostScript. Як базові шрифти прийняті Type 1 з однобайтовим кодуванням. Коли на базі PostScript розробили PDF й принтери стали переважно GDI, отримання результату стало тристадійним DVI->PostScript->PDF. З кінця 1990-х система почала змінюватись. Спочатку під LaTeX стали розуміти pdflatex - прямий генератор PDF на базі однобайтних Type 1 шрифтів. Далі в 2004 р. виник окремий проєкт з підтримкою Unicode й TrueType/OpenType шрифтів - XeTeX, а в 2008 р. LuaLaTeX - ще й додатковою підтримкою мови програмування Lua. Зараз LaTeX має велику кількість готових рішень й доволі популярним є його застосування через веб (OverLeaf), що дозволяє кодувати й переглядати результат без інсталяції додаткових програм.

LaTeX розповсюджений переважно в академічному середовищі. Його ключові переваги: орієнтація на друк, робота з зображеннями без втрати якості, можливість реалізовувати стандартні шаблони (для статей, звітів, робіт), в тому числі з двома стовпцями, автоматичне (хоч й не ідеально) розміщення таблиць, рисунків тощо, зручність роботи з великою кількістю формул, складно помилитись в цифровій бібліографії, оскільки пишеш й бачиш в коді унікальний текстовий ключ. Проте є й недоліки: синтаксис доволі складний й результат часто не передбачуваний, тому що потрібно застосовувати в складних документах велику кількість бібліотек, які не обов'язково добре співпрацюють (сучасний HTML5 значно більш очевидний), вимагає компіляції в PDF для перегляду результату, що займає час оскільки архітектура далека від ідеальної (особливо складно працювати з багатосторінковими документами й з Babel, який реалізований мовою Perl й лише запуск якого займає декілька секунд). З цими недоліками можна змиритись, якщо задача – зверстати вже готову роботу. В процесі написання тексту LaTeX не зручний, оскільки вимагає постійної уваги до технічної реалізації деталей.

За останні 15 років LaTeX більшою мірою втратив свою унікальність в аспекті переваг. За межами друкарської справи істотно більш зручним є MarkDown з можливістю застосовувати усі функції веббраузерів при необхідності. Двигуни

Markdown звичайно підтримують виведення формул в форматі LaTeX, є можливості ставити посилання з ручним оформленням джерел. Сучасний десктопний Word може працювати з LaTeX формулами як з вбудованими, так й через MathType, також він має опцію не знижувати якість зображень й бібліографію (власну – через ряд вбудованих стилів й через плагіни для доступу до бібліографічних менеджерів).

Typst розробляється як повноцінна заміна LuaLaTeX. Написаний з нуля мовою Rust він реалізує основний функціонал власноруч без зовнішніх макросів, бібліотек тощо. Синтаксис його значно більш читабельний й зрозумілий (в тому числі й синтаксис для формул). Й головне – компіляція працює ефективно: перераховується й заміняється лише частина документу, тому в редакторі Typst рендеринг реалізується після введення нового коду автоматично. В порівнянні з LaTeX різниця в швидкості у десятки разів. Істотно не зменшують відставання результат такі підходи як, наприклад, "draft mode" в Overleaf, коли з документу видаляють важкий контент (зображення тощо) щоб прискорити перегляд результату.

Typst підтримує бібліографію на базі CSL, але й дозволяє запрограмувати свою бібліографічну систему. Його функціонал й швидкість дозволяють розробити генератор переліку джерел посилання відповідно до стилю ДСТУ 8302:2015 достатньої для професійного застосування якості.

Основні вимоги наступні.

1. Підтримка основних типів джерел (книга, глава у книзі, стаття в журналі/газеті, тези конференції, інтернет-джерело) з можливістю введення прямого тексту посилання для специфічних речей.
2. Застосування всіх даних, які можуть бути збережені в форматах BibTeX/BibLaTeX для основних типів джерел. Оскільки дані вводяться вільно, то дані мають бути перевірені й використані спираючись на типові практики заповнення полів. Проте незначні дані для універсалізму можуть бути видалені.
3. Повна інтернаціоналізація - джерело оформлюється його мовою. Якщо мова не вказана, то вона автоматично визначається. Підтримуються такі мови як: українська, англійська, іспанська, італійська, німецька, польська, португальська, російська, французька, чеська. Всі службові слова (сторінка, том, номер, редактор, дати) описуються визначеною мовою.
4. Скорочення міст нейтралізується. Для цього застосовується таблиця скорочень й рік. Основа - прийняті в бібліографії України до 2013 року скорочення міст, скорочення міст в СРСР різних років тощо.
5. Декодування URL адрес з ASCII формату (представлення символів за межами 7-біт як послідовність HEX-кодів, кожен з яких починається з проценту).

Запропонований алгоритм роботи для Typst. *Отримання бібліографічних джерел*. Ми спираємось на стандартний механізм бібліографії. Правила сортування та цитування в тексті задаються елементарним шаблоном мовою CSL. Ми застосуємо сортування за порядком цитування, цифровий індекс з можливістю об'єднання послідовних цитувань в цитування виду [2-4]. Бібліографічний опис сформуємо елементарний – номер та заголовок (його надалі приховаємо й будемо застосовувати лише для відлагодження). Бібліографічні посилання розміщуються в коді сторінки Typst як ключі @key. У місті для бібліографічного опису встановимо виклик функції генерації опису, яка буде приймати як аргументи ім'я поточного файлу й ім'я bib файлу.

За допомогою функції bibliography задається CSL шаблон, bib файл й стандартний бібліографічний опис. При цьому цитування в тексті залишаться. Далі ми будемо генерувати власний бібліографічний опис програмним чином.

Завантаження bib файлу будемо реалізовувати за допомогою бібліотеки citegeist. Ця бібліотека є інтерфейсом для програми-парсера BibTeX/BibLaTeX мовою Rust. Ключова її функція завантаження перевіряє синтаксис й завантажує усі дані в словник. Якщо є помилки, процедура генерації верстки зупиняється з повідомлення про помилку.

Бібліотека також робить деякі заміни, наприклад видаляє нерозривні пробіли LaTeX й певні перевірки синтаксису, алгоритм яких нами не досліджувався.

Оскільки кількість записів в bib не має бути еквівалентною кількості цитованих записів, то потрібно отримати перелік саме цитованих записів. Стандартного механізму для цього нажаль поки немає, тому ключі отримуються прямо з коду файлу з видаленими коментарями, з якого була викликана функція з застосуванням регулярного виразу @([a-zA-Z0-9_:-+/]+(?:.[a-zA-Z0-9_:-+/]+)*). Таким чином, ми можемо отримати словник тільки з цитованими джерелами. В поточній реалізації розглядається тільки порядок вживання. Алфавітний порядок сортування джерел не реалізуємо, краще дочекатись поки вказаний недолік буде вирішений на рівні Typst.

Зменшення розміру полів записів citegeist, як і формат bib, не лімітує розмір полів. Іноді в записах зберігають непотрібні для задачі великі обсяги даних, такі як анотація, зміст чи навіть вступ до книги тощо. Ця інформація для нас зайва. Раціональна межа для різних полів принципова різна: для ISBN досить 32 символів, для назви книги – 255.

Перевірка записів. Наявність та наповненість полів перевіряється за наступним словником:

```
  "book":         ("title", "address|location", "year"),
  "incollection":("title", "booktitle", "address|location", "year|date"),
  "article":      ("author", "title", "journal|journaltitle", "year"),
  "online":       ("title", "url"),
  "phdthesis":                ("author",     "title",     "address|location",
"school|institution|organization","year|date"),
  "masterstheis": //аналогічно phdthesis
  "inproceedings":("author", "title", "booktitle", "address|location|venue",
"year|date"),
  "misc":         ("title",)
```

Маємо 8 типів джерел на вході: книга (book), розділ книги (incollection), стаття (article), інтернет-ресурс (online), дисертація (phdthesis), магістерська робота (masterthesis), тези конференції (inproceedings), інше (misc). Запис з типом inbook прирівнюється до incollection. Записи з типами booklet, manual, proceedings прирівнюються до book. Для кожного джерела вказані обов'язкові поля, деякі вказані як альтернатива (відмінності між BibTeX й BibLaTeX). Відсутність чи незаповнення вказаних полів призводить до відмови генерації. Замість джерела виводиться помилка з ім'ям необхідного параметра. Додатково перевіряється зміст misc. Припустимо два варіанти: title="free-form" й заповнено поле note й title!="free-form" й заповнено поле url (є практика замість online використовувати misc). В першому випадку формується джерело типу mff з полем note_for_freeform, в другому - джерело типу murl з полями title й url.

Обробка записів. Далі нам потрібно реалізувати перетворення словника з записами в словник обробленими записами, якій буде містити коректну інформацію в коректних полях. Якщо поле переноситься без змін, то його назва не змінюється, в протилежному випадку додається префікс "fin_". Процедура обробки полів наступна.

- Мова (language) – якщо є таке поле, то обробляємо його зміст. Розповсюджена практика писати мову повністю, двома та трьома літерами, тому для визначення належності до потрібних мов маємо спробувати всі варіанти. Наприклад, german/de/deu/ger чи czech/cz/ces/cze. У випадку якщо поля немає, то орієнтуємось на тип алфавіту (кирилиця/латинка) й на виключні для певної мови символи. Наприклад, для української мови серед підтримуваних мов притаманна кирилиця з особливими літерами "ї", "є", "ґ", а для польської мови притаманна латинка з особливими літерами "ą", "ę", "ł", "ń", "ś", "ź", "ż", "ć". Якщо в змісті не кирилиця й мову встановити не вдалось, приймаємо англійську (en). Всі текстові складові локалізуються визначеною в зазначеній процедурі мовою, вказувати на це в описі кожного поля не будемо.
- Актори (fin_author/fin_editor) та їх кількість (num_authors/num_editors). Поле authors й editors може містити кілька акторів - вони розділяються "and", неповний список -

закінчується на "and others". Актори можуть бути записані в форматі "Прізвище,Ім'я" чи без коми, тоді "Ім'я Прізвище". Нам потрібно залишити лише ініціали. При цьому врахувати, що ініціали можуть бути складними, наприклад І.-А. Якщо кількість авторів перевищує 3 чи є "and others", то num_authors=-1. При кількості авторів 1-3 порядок запису прямий - "Прізвище І.", інакше зворотній - "І. Прізвище та ін.". Для редакторів стоїть префікс "за ред." й порядок завжди зворотній. Якщо є "and others" замінюється на "та ін.".

- Назва журналу (fin_journal) - записується journal чи journaltitle.
- Видання (fin_edition) - якщо є цифра, залишається тільки вона й записується у відмінку, наприклад "3-тє видання", інакше записуємо значення поля edition.
- Номер (fin_number) - якщо є цифра з опціональним варіантом тире чи крапкою, вона записується як "№ 2". Остання крапка видаляється.
- Номер (fin_volume) - аналогічно номеру записується як "Т. 3".
- Кількість сторінок (fin_page_count) чи їх інтервал (fin_page_interval). Якщо є num_pages з BibLaTeX, то нам зрозуміло що мова йде про кількість сторінок. Проте, зазвичай кількість сторінок й номера сторінок розміщують в pages, тому їх треба диференціювати (С. 10 і 10 С.). Це робиться за типом джерела. Інтервали можуть в BibTeX позначатись як "5-10", "5-10, 15-20", "5+". Цю логіку, хоча вона не зафіксована в ДСТУ ми не змінюємо. Лише замінюємо всі варіанти символів, які можуть трактуватись як тире "[-——⁻–-]" з опціональними пробілами між ними на запис виду "5-10" з en-dash.
- Видавець (fin_publisher) - якщо є один з варіантів душок, то беремо текст тільки в душках, інакше – беремо повністю.
- Місце захисту (fin_school) - записується school чи insitution.
- URL (fin_url) - записується URL (з поля url чи якщо немає, то з поля note для джерел типу misc), який відповідає рег. виразу
- `"https?://[-a-zA-Z0-9+&@#/%?=~_|!:,.;()]*[-a-zA-Z0-9+&@#/%=~_|()ক্ষত্রে]"`
  Якщо отриманий URL містить %, то він декодується. Оскільки в typst немає роботи з байтами, а лише з символами, то реалізувати алгоритм urldecode складно, а стандартної функції немає. Цілком достатньо зробити заміну в межах алфавитів цільових мов та ще грецької (стародавньої й сучасної). Наприклад "%C3%83" → "Ã", "%C3%A3" → "ã", "%C3%84" → "Ä", "%C3%A4" → "ä", "%D0%84" → "Є", "%D1%94" → "є". Це порядку 200 замін на пару закодованих символів. Для того, щоб операція не вимірювалась в мілісекундах чи їх десятках, ми можемо зробити масову заміну одним викликом. Функції як в python translate/maketrans немає, проте ми можемо зменшити кількість надлишкових викликів (overhead) шляхом формування одного регулярного виразу заміни, який шукає за виразом типу `(%D0%90|%D0%B0|.|%20)` й замінює кожний знайдений підрядок на підрядок від лямбда-функції, яка за ключем (підрядком) визначає потрібне значення. В результаті отримуємо оптимальний однопрохідний алгоритм.
- Заголовок (fin_title) - в полі title, звичайно статей зустрічаються макроси LaTeX для виведення математичних символів, це поширена практика в статтях з математики й фізики. На відміну від URL таких символів не буде дуже багато в рядку. Проте дуже багато потенційних макросів. Припустивши, що навряд буде дріб, матриця чи система був виділений раціональний перелік: грецькі літери "\alpha": "α", оператори та символи "\times": "×", стрілки "\to": "→", логіка та множини "\emptyset": "Ø". Ці макроси можуть бути в блоках внутрішньої математики β\betaβ чи (\alpha \cdot \beta) . Якщо зустрічаються в рядку "$" чи "$" з використанням регулярних виразів для визначення блоків
- `"\$[^$]+\$|\\\\\([^\)]+\\\\\)")`
  та макросів в них
  `"\\\\[a-zA-Z]+|\\\\[,;: ]")`

циклічно перебираємо всі блоки, в кожному виділяємо макроси й якщо такий ключ є в словнику, то робимо заміну. Ідея заміни аналогічна URL, проте заміна робиться як latex_mapping.at(mac.text, default: mac.text), тобто якщо ключ не знайдений, то залишається макрос як є без помилки.

- fin_day, fin_month,fin_year - якщо day, month, year присутні, то базуємось на їх значеннях. Часто month записується як три літерне скорочення місяця - jan, feb, тоді за першими трьома літерами треба їх перевести в число. Якщо ж даних немає, але вони є в date в форматі рік-місяць-день, то треба їх виділити й перенести. Зустрічається ще нестандартний варіанти, коли в date тільки рік, тоді беремо його як ціле число. Відсутній чи некоректний рік для всіх джерел за винятком online та misc призводить до відмови від парсингу джерела. Розглядається випадок, коли рік невідомий (знак питання наприкінці) чи є декілька варіантів (роки записані через or). Такі роки записуються в квадратних душках.
- Дата доступу (fin_urldate) - зазвичай записується в форматі рік-місяць-день й якщо так, то переводиться в день.місяць.рік, інакше – залишаємо як є.
- Примітка fin_note - допускається застосування елементарних HTML тегів: `<b>,<i>,<sup>,<sub>`. Для цього реалізується простий парсер з підтримкою вкладень. Знайдені блоки оформлюються за допомогою команд Typst strong, emph, sub, super.

Генерація бібліографічного опису. Проблема генерації полягає в тому, що стиль передбачає застосування різних розділювачів для різного типу інформації. При чому частина інформації може бути відсутньою, що призводить до необхідності виключати певні розділювачі. Пряма послідовна генерація має бути або істотно зв'язаною (дивитись наперед чи коректувати вже згенероване) або буде призводити до артефактів, які наприкінці потрібно грубо видаляти.

Для того, щоб уникнути двох крайнощів реалізуємо лексичний аналізатор з пріоритетним вирішенням конфліктів. Для цього створимо масив незалежних об'єктів (токенів) двох типів: контент й розділювач. Фінальну генерацію будемо проводити за масивом з застосуванням правил фільтрації та пріоритетів. Кожен тип розділювача має свій приоритет:

```
#let SEP_SPACE = (text: " ", weight: 10)
#let SEP_DOT   = (text: ". ", weight: 20)
#let SEP_COMMA = (text: ", ", weight: 30)
#let SEP_COLON = (text: " : ", weight: 40)
#let SEP_SEMICOLON = ( text: "; ", weight: 50)
#let SEP_SLASH = (text: " / ", weight: 100)
#let SEP_DBL_SLASH = (text: " // ", weight: 110)
```

Вирішення конфліктів реалізується за наступними правилами:

- якщо розділювачі йдуть один за одним, то залишається той, в якого більший пріоритет;
- якщо пріоритет однаковий, залишається один розділювач (всі мають різні пріоритети, тому проблем не має).

Перед генерацією програма перевіряє для надійності контент на пустоту (none, "", [], styled(child:[])). Пусті токени виділяються. Це запобігає утворення подвійних крапок (..) чи "висячих" ком.

Заповнення токенів й розділювачів будемо реалізовувати за допомогою послідовних операцій, перелік яких задається словником:

```
#let formats = (
  "book":   ("authors1",   "title",   "authors2",   "edition",   "editors",
"publisher_address", "year", "volume", "pages", "isbn", "doi", "url"),
  "incollection": ("authors1", "title", "authors2", "booktitle", "edition",
"editors", "publisher_address", "year", "volume", "pages", "isbn", "doi",
"url"),
  "article":   ("authors1",   "title",   "authors2",   "journal",   "year",
"volume_num", "day_month", "pages", "doi",  "url"),
```

```
  "inproceedings": ("authors1", "title", "authors2", "booktitle", "editors",
"publisher_address", "year", "volume", "pages", "isbn", "doi", "url"),
  "phdthesis": ("authors1", "title", "thesis_type", "school_or_org", "year",
"pages", "url"),
  "mastersthesis": ("authors1", "title", "thesis_type", "school_or_org",
"year", "pages", "url"),
  "online": ("authors1", "title", "authors2", "site_name", "url"),
  "murl": ("title","url"),
  "mff": ("note_for_freeform",),
)
```

Опишемо кожну операцію окремо.

- authors1: якщо num_authors від 1 до 3, то додати об'єкт з fin_author та розділювач SEP_SPACE
- authors2: якщо num_authors > 3 чи -1, то додати розділювач SEP_SLASH, об'єкт з поля fin_author та розділювач SEP_DOT
- booktitle: якщо є, додати з відповідного поля, видаливши останню крапку й додати розділювач SEP_DOT
- day_month: якщо немає fin_number і fin_volume, але є місяць і опціонально день, то записати їх з назвою місяця згідно правил й додати як об'єкт, також додати розділювач SEP_DOT
- doi: якщо є, додати значення поля як об'єкт з префіксом "DOI:" й додати розділювач SEP_DOT
- edition: якщо є, додати як об'єкт, видаливши останню крапку й додати розділювач SEP_DOT
- editors: якщо num_editors > 0, то додати розділювач SEP_SLASH, об'єкт з поля fin_editor та розділювач SEP_DOT
- isbn: якщо є, додати значення поля як об'єкт, потім додати розділювач SEP_DOT
- journal: якщо є, додати значення поля як об'єкт, потім додати розділювач SEP_DOT
- note_for_freeform: передати як об'єкт в поле запису fin_note як є
- pages: записуємо кількість чи інтервал сторінок з fin_page_count / fin_page_interval
- publisher_address: обов'язково додається адреса як об'єкт. Якщо видавництво є, то додається воно як об'єкт після розділювача SEP_COLON. Оскільки далі йде обов'язково кома з роком, то розділювач після не потрібний.
- school_or_org: обов'язково додається адреса як об'єкт. Якщо видавництво також є school чи organization, то додається значення наявного поля як об'єкт після розділювача SEP_COLON
- site_name: якщо наявна organization чи заповнене поле fin_journal – додається перша першого з наявних полей як об'єкт, далі додається розділювач SEP_DOT
- thesis_type: береться значення з type чи fin_note й видаляється остання крапка за наявності. Якщо значення є, то додаємо SEP_COLON, потім об'єкт зі значенням, потім SEP_DOT
- title: додається значення поля fin_title як об'єкт. Якщо наприкінці "?" чи "!", то вставляється розділювач SEP_SPACE, інакше - SEP_DOT
- url: вставляється значення об’єкту з поля лише, якщо немає doi. Вставляється URL як об'єкт. Якщо є дата, то вона також вставляється як об'єкт з urldate після оформлення. Закінчуємо розділювачем SEP_DOT
- volume: вставляється якщо є fin_volume як об'єкт з розділювачем SEP_DOT
- volume_num: якщо є тільки значення поля fin_volume чи fin_number, то віно вставляється як об'єкт з розділювачем SEP_DOT. Якщо є обидва значення, то між ними додається розділювач SEP_COMMA
- year: вставляється розділювач SEP_COMMA, об'єкт зі значенням поля fin_year та розділювач SEP_DOT.

Виведення. Після завершення операцій з кожним записом згенерований текст вставляється у абзац (par) з відповідним номером з фіксованою відстанню після крапки.

Перевірка результатів. Для перевірки були взяті три джерела:

- приклад коректного оформлення джерел оформлення з сайту Grafiati [13], схвалений Книжковою палатою України;
- перелік для перевірки парсеру для верстки дисертації в LaTeX з [14] (включає 13 записів з прикладами еталонного оформлення різних типів джерел [15]);
- експортована власна база даних з програми Zotero (~400 джерел).

Всього - понад 500 джерел.

Зі списком Grafiati є такі відмінності:

- "2-ге видання, стер". та "3-тє видання, випр. і доп." замінюється на "2-ге видання". та "3-тє видання". Подібна деталізація на наш погляд не потрібна;
- не відрізняємо "за ред.", "ред.", "за заг. ред" тощо - тільки перший варіант;
- тип укладача не реалізуємо, лише автор чи редактор;
- назва організації в книзі не пишеться, як й назва тома.
- не вказуємо дату звернення для DOI, але пишемо DOI, а не URL.
- в англ. варіанті URL не "date of access", а "accessed".
- в тезах конференції не вказується редколегія, місце зустрічі тощо, тільки рік видання й видавець.
- посилання з типом джерела "диск", "закон", "нормативний акт", "препринт", "патент", "стандарт", "архівні матеріали" може бути реалізовано вручну через misc з free-title - в BibTeX таких джерел немає, в BibLaTeX частково є, але поля складно зіставити.

У цілому вони, на наш погляд не критичні й в цілому результат генератора можна вважати відповідним до стандарту наскільки це можливо з BibTeX/BibLaTeX файлів. Приклад генерації показаний на рис. 1.

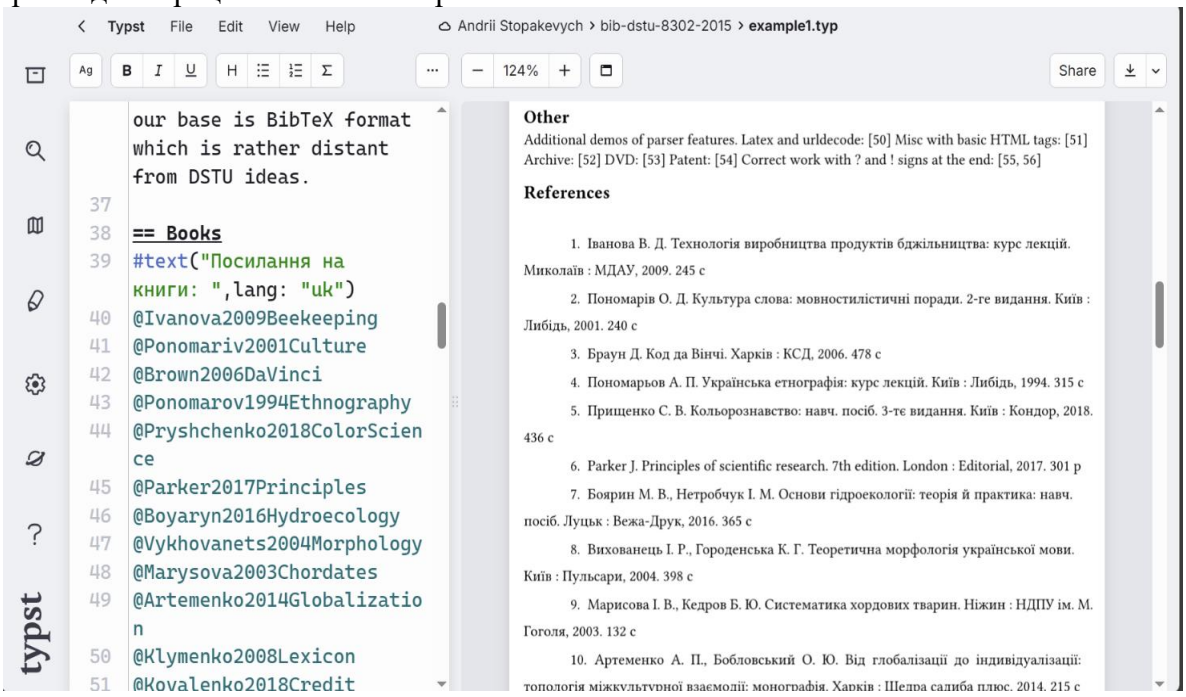


Рис.1. Генерація бібліографії з власноруч написаного BibTeX файлу для відтворення оформлення з сайту Grafiati

Зі списку для перевірки парсеру не генеруються такі посилання:

- тип thesis – не підтримується й стандартними парсерами (треба phdthesis, mastersthesis);
- типи unpublished, techreport, patent не підтримуються, misc - лише для ручної цитати чи як BibTeX варіант online з BibLaTeX;
- якщо немає адрес в певних типах джерел (вимога ДСТУ, можна якщо не можливо вручну поставити).

В експортованому списку додаткових до вказаних вище артефактів не виявлено. Таки чином, можемо сказати, що результат цілком задовільний. Вихідний код доступний за адресою https://typst.app/project/rqwMZQBnT2VFdkbaMgz87y . Для перегляду файлів - відкрийте зліва список за допомогою кнопки "Explore files". Генерація за другим й третім списком відобразиться шляхом перемикання "ока" на файли example2.typ й example3.typ.

Висновки. Розглянута задача програмної генерації переліку літературних джерел з використанням BibTeX / BibLaTeX (частково) файлу. Ця задача розв'язана для нової системи програмної комп'ютерної верстки Typst. Продемонстровані недоліки та обмеження існуючих інструментів, показано що застосування менеджерів бібліографії для користувачів з нелатинськими алфавітами має багато проблем. Обґрунтовані переваги Typst як альтернативи LuaLaTeX. Запропоновано для користувачів менеджерів бібліографічний алгоритм. Оскільки користувачі сучасних менеджерів переважно не самі створюють посилання в форматі BibTeX, а завантажують їх з різних сайтів з метою імпорту їх в свій менеджер бібліографії, алгоритм намагається виправити можливі недоліки вихідної інформації й дозволяє реалізувати посилання з власним оформленням джерела. Проведена програмна реалізацію генератора переліку літературних джерел мовою Typst, яка перевірена на вибірці у понад 500 джерел. Результати є цілком задовільними для використання в практичній роботі. Покликання на вихідний код надано.

Список літератури

1. Reference Management Tools Market Size, Growth, Size, Share, and Industry Analysis. Regional Forecast To 2035. Last updated 10 nov 2025. URL: https://www.businessresearchinsights.com/market-reports/reference-management-tools-market-101541
2. Mendes K. D. S., Silveira R. C., Galvão C. M. Use of the bibliographic reference manager in the selection of primary studies in integrative reviews. *Texto & Contexto Enfermagem*. 2019. V. 28. DOI:10.1590/1980-265x-tce-2017-0204
3. Studies and analysis of reference management software: A literature review. *El Profesional de La Información*. 2015. No.24(5). P. 680. DOI:10.3145/epi.2015.sep.17
4. Попов Р. О., Карпенко Н. В. Проблеми використання системи LaTeX та BibTeX в українському науковому середовищі. Матеріали XVII міжнародної науково-практичної конференції «Інформаційні технології і автоматизація». Одеса: ОНТУ, 2024. С. 757-761
5. Two years and counting: How we are building the future of technical writing. URL: https://typst.app/blog/2025/future/
6. Боженко О., Корян Ю., Федорець М. Міжнародні стилі цитування та посилання в наукових роботах. Київ : УБА, 2016. 118 с.
7. Official repository for Citation Style Language (CSL) citation styles. URL: https://github.com/citation-style-language/styles
8. Баскакова С.О., Вигівська В.О. Бібліографічний менеджер EndNote для науковців : (із досвіду роботи бібліотеки Криворізького національного університету). Матеріали науково-практичної інтернет-конференції «Сучасна бібліотека: проблеми, досвід та вектори розвитку». Харків, 2019. С. 9–13.
9. Грищенко Т.Б., Нікітенко О.М., Дейнеко Ж.В. Створення електронних підручників засобами видавничої системи LaTeX. Поліграфічні, мультимедійні та web-технології: колективна монографія. Харків: Мадрид, 2021. С. 80-96
10. Азаренков В.І., Федоріщева В.О. Дослідження можливостей автоматизації розробки шаблонів документів всередовищі LATEX. *Системи управління, навігації та зв'язку.* 2021. Т.1. №63. С.71-73
11. Подошвелев Ю. Програмування власного класу в системі LaTeX. Збірник наукових праць викладачів, аспірантів, магістрантів і студентів фізико-математичного факультету ПНПУ імені В. Г. Короленка. Полтава : Астрая, 2022. С. 112-114

12. Baranovskyi O. LaTeX classes for doctoral theses in Ukraine: Interesting tips and painful problem. *The 43rd Annual Conference of the TeX Users Group*. 2022. URL: https://www.imath.kiev.ua/~baranovskyi/talks/20220724tug2022.pdf
13. Приклади оформлення посилань за ДСТУ 8302:2015 у списку використаних джерел. URL: https://www.grafiati.com/uk/info/dstu-8302-2015/examples/
14. Phd-LaTeX-Disseration-Template. URL: https://github.com/AndreyAkinshin/
15. BibTeX Style Examples. URL: https://verbosus.com/bibtex-style-examples.html

DEVELOPMENT OF A PARSER FOR THE INTEGRATION OF BIBLIOGRAPHY MANAGERS AND THE TYPST PROGRAMMED COMPUTER LAYOUT SYSTEM THAT MEETS THE REQUIREMENTS OF THE BIBLIOGRAPHIC STANDARD DSTU 8302:2015

A.O. Stopakevych[1], O.A. Stopakevych[2]

[1]State University of Intellectual Technologies and Telecommunications
1, Kuznechna Str., Odesa, 65023, Ukraine
[2]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: stopakevich@gmail.com

Bibliography managers (e.g. Zotero, Mendeley, EndNote) have become an essential instrument for numerous researchers. The functionality of such systems extends beyond mere information structuring, encompassing the capacity to import bibliographic details from publishers and journals. This process utilizes the unique identifiers provided by CrossRef, facilitating seamless integration into the management database. The use of a single identifier, whether it be a DOI or ISBN, enables the seamless synchronization of bibliographic data, streamlining the process of bibliographic management. However, researchers who use national bibliography standards, in particular DSTU 8302:2015, face a lack of a convenient and fully functional solution that allows them to obtain correctly formatted references based on the database stored in the bibliography manager. Existing CSL-based solutions have been observed to lack the capacity to provide accurate internationalization and flexibility. Consequently, it is not possible to generate correct citations according to the rules of DSTU 8302:2015 when using them. The objective of this research is to develop software technology capable of automatically generating a list of bibliographic references in compliance with the requirements of DSTU 8302:2015. This will be achieved within the framework of a contemporary computer typesetting system, Typst, utilizing BibTeX/BibLaTeX format files as the source of input data. The work presents the development of an algorithm for parsing and processing bibliographic entries, encompassing lexical analysis of input data, heuristic determination of the source language, conversion of LaTeX macros and special characters to Unicode, decoding of URLs, and validation of fields by source type. In the final formation of the bibliographic description, a token-based approach (content and separators) is employed, in conjunction with a priority system for resolving punctuation conflicts. A software module has been implemented in the Typst language that functions independently of external preprocessors. It is notable for its ability to address ambiguities and common violations of standards when formatting data in BibTeX format. The parser has been verified on a sample of over 500 BibTeX entities from diverse sources. The result allows Ukrainian researchers who wish to use the Typst system to seamlessly integrate bibliographic managers that can export information in BibTeX/BibLaTeX format.

Keywords: DSTU 8302:2015; Typst computer typesetting system; BibTeX/BibLaTeX; bibliography automation; data parsing; scientific documentation; citation managers.

DOI 10.15276/imms.v16.no1.181
УДК 004.9:35.077.6

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 181-196

ЕКСПЕРЕМЕНТАЛЬНИЙ СТЕНД РЕІНЖИНІРІНГУ ЦИФРОВИХ ПУБЛІЧНИХ СЕРВІСІВ: АРХІТЕКТУРА, ДАНІ, РЕЗУЛЬТАТИ

Ю.Є. Хохлачова[1], Ю.І. Хавікова[1],
Д.О. Черкаський[2], Н.С. Зубченко[3], Д.О. Переметчик[3]

[1]Державний торговельно-економічний університет
19, Кіото вул., Київ, 02156, Україна
[2]Національний технічний університет Дніпровська політехніка
19,. Дмитра Яворницького пр., Дніпро, 49005, Україна
[3]Університет митної справи та фінансів
2/4,. В. Вернадського вул, Дніпро, 49000, Україна,
Emails: yuliiahohlachova@gmail.com, pirogova0303@gmail.com,
Cherkaskyi.Dav.O@nmu.one, nazik3110@gmail.com, peremetchyk.d@gmail.com.

Цифровізація публічних сервісів із переходом до комплексних платформ електронних послуг супроводжується необхідністю системного реінжинірингу бізнес-процесів та архітектури інформаційних систем. Традиційні підходи до реінжинірингу, що спираються переважно на експертне моделювання, виявляються недостатніми для масштабних та високо пов'язаних екосистем державних е-послуг. У роботі запропоновано архітектуру експериментального стенду для тестування нейромережевих і алгоритмічних моделей реінжинірингу цифрових публічних сервісів. Стенд поєднує фізичну інфраструктуру на базі віртуалізованого кластеру з контейнеризованими сервісами, модулі генерації навантаження та атак, підсистему агрегації та анонімізації журналів подій, а також середовище оркестрації експериментів. Описано синтетичні та реальні набори даних, що відтворюють типові сценарії роботи порталів е-послуг, шини даних, державних реєстрів та мобільних застосунків. Наведено формальні моделі оцінювання якості реінжинірингу за інтегральними індексами продуктивності, надійності, ризику та витрат. Розглянуто сценарії порівняння правила-орієнтованих, імітаційних, нейромережевих (включно з CNN+LSTM і AE+LSTM для аналізу журналів подій) та гібридних підходів. Подано результати експериментів із варіюванням архітектурних рішень, параметрів навантаження та політик масштабування сервісів, а також аналіз чутливості інтегральних показників до обраної стратегії реінжинірингу. Показано, що використання експериментального стенду дає змогу досягти зниження середнього часу обробки запиту е-послуги на 18–32 % та скорочення ризику збоїв під час пікових навантажень на 25–40 % порівняно з традиційними підходами. Сформульовано практичні рекомендації щодо поетапного впровадження алгоритмічно підтриманого реінжинірингу у відомчих і міжвідомчих цифрових платформах.

Ключові слова: електронні публічні послуги, реінжиніринг бізнес-процесів, експериментальний стенд, кластер мікросервісів, журнали подій, нейромережеві моделі, CNN+LSTM, AE+LSTM, імітаційне моделювання, інтегральний індекс якості, цифрові платформи.

Вступ. Цифровізація критичної інфраструктури та масове розгортання сервісних платформ поверх мереж електронних комунікацій кардинально змінили характер сучасних загроз. У межах гібридних кібератак противник поєднує мережеві, прикладні та соціотехнічні вектори впливу, цілеспрямовано експлуатуючи вразливості стеку протоколів, сервісних композицій і бізнес-процесів, що реалізуються поверх телекомунікаційної інфраструктури. У цих умовах класичні підходи до проєктування та експлуатації платформ електронних послуг, орієнтовані лише на функціональну коректність і базову надійність, виявляються недостатніми: потрібні формалізовані моделі ризику, засоби інтелектуального аналізу логів і трафіку, а також інтеграція з системами виявлення та реагування на інциденти (Intrusion Detection System, IDS;

Security Information and Event Management, SIEM) у парадигмі Zero Trust. Технічним підґрунтям сучасних платформ е-послуг і галузевих цифрових сервісів є композиції розподілених сервісів та мікросервісів. Роботи з оптимізації витрат на сервісні композиції [1] показують, що вже на рівні «мирного» функціонування виникає складна багатокритеріальна задача балансування продуктивності, доступності та вартості ресурсів. У поєднанні з результатами емпірично обґрунтованих референтних архітектур [6] це формує основу для формального опису сервісної частини мереж електронних комунікацій, які стають мішенню гібридних кібератак. У публічному секторі та smart-city платформах, де такі композиції пов'язані з бізнес-процесами надання послуг, до технічних факторів додаються регуляторні та організаційні обмеження [4,5,11].Для верифікації поведінки сервісних платформ у реальних умовах активно розвиваються підходи до перевірки відповідності моделей історичним журналам подій (replaying history) [2]. Вони дають змогу оцінювати, наскільки формально змодельовані процеси відповідають фактичним сценаріям роботи користувачів і систем, що особливо важливо при моделюванні наслідків складних атак, таких як firmware-компрометація мережевого обладнання з подальшим втручанням у SSL-/TLS-трафік чи експлуатація слабкостей SNMP у системах моніторингу. Застосування таких механізмів у контурі телеком-мереж дає можливість програвати як штатні, так і атакувальні сценарії, виявляючи приховані точки відмови та аномальні маршрути трафіку.Окремий блок досліджень становить процес-майнінг, який розглядає журнали подій як первинне джерело істини щодо бізнес-процесів та сервісних сценаріїв [7]. У поєднанні з класичними підходами системного аналізу й проєктування інформаційних систем [10,11] він дає інструментарій для автоматичного відновлення фактичних процесів у розподілених платформах та побудови їхніх формальних моделей. Це критично для мереж електронних комунікацій, де логіка маршрутизації запитів, поведінка балансувальників навантаження, політики повторних спроб і тайм-аутів часто задаються конфігураціями, що еволюціонують у часі та важко піддаються ручному аналізу.

Зростання обсягів мережевих і сервісних логів переводить задачі моніторингу та кіберзахисту в площину «великих даних». Огляд [12] підкреслює, що для таких середовищ ключову роль відіграють масштабовані платформи збирання, зберігання та потокової обробки даних, здатні працювати з високошвидкісними потоками подій. На цьому тлі глибоке навчання для виявлення аномалій [3] стає одним з базових інструментів моделювання аномальної активності в мережах електронних комунікацій, зокрема в контексті змішаних (граничних) режимів, коли бізнес-логіка сервісів і мережевий рівень одночасно зазнають цілеспрямованого впливу. Архітектури класу LSTM-мереж для класифікації часових рядів [8] природно застосовувати до послідовностей мережевих пакетів, записів IDS/SIEM та трасування мікросервісних викликів, тоді як глибокі залишкові мережі [13] можуть бути залучені для аналізу складних візуалізацій або перетворень даних (наприклад, Byte2Image-представлень трафіку чи логів).Роботи, присвячені ефекту «хвоста у масштабі» [14], демонструють, що в розподілених сервісних архітектурах саме рідкісні, але дуже повільні транзакції визначають сприйняття якості сервісу користувачами та стійкість системи в цілому. Для мереж електронних комунікацій, що працюють в умовах гібридних кібератак, це означає необхідність моделювання не тільки середніх показників, але й крайових сценаріїв, пов'язаних із вибірковим уповільненням чи блокуванням критичних потоків. Додатково, роботи з приватності траєкторій руху користувачів [9] вказують на фундаментальні обмеження анонімізації даних у середовищах, де навіть часткові спостереження можуть бути пов'язані з конкретними абонентами чи вузлами мережі, що створює додаткові виклики для побудови навчальних вибірок для систем виявлення атак.

Аналіз досліджень і публікацій. Таким чином, наявний масив досліджень охоплює: оптимізацію сервісних композицій [1], верифікацію моделей за історією подій [2], глибоке навчання для виявлення аномалій [3,8,13], концептуальні основи «розумних

міст» [4], класичні підходи до зміни бізнес-процесів [5,11], проєктування референтних архітектур [6], методологію процес-майнінгу [7], питання приватності в епоху великих даних [9,12] та проблематику масштабованості розподілених систем [14]. Разом вони формують теоретичне й методичне підґрунтя для побудови моделей мереж електронних комунікацій як багаторівневих сервісно-орієнтованих екосистем, але ще не дають завершеної відповіді на питання, як саме інтегрувати ці підходи в єдиний ризик-орієнтований контур протидії гібридним кібератакам. У низці сучасних робіт запропоновано використовувати експериментальні стенди та тестові платформи для відтворення реальної архітектури цифрових сервісів, генерації навантаження, ін'єкції відмов і збору багаторівневих журналів подій. Такі стенди дають змогу порівнювати традиційні, rule-based та нейромережеві підходи до оптимізації архітектури й бізнес-процесів, включно з моделями класу CNN+LSTM і AE+LSTM для аналізу логів та прогнозування інтегральних показників якості [3,8]. Водночас у більшості випадків вони орієнтовані на реінжиніринг цифрових публічних сервісів загального призначення та не враховують специфіку гібридних кібератак на мережі електронних комунікацій, де важливу роль відіграють протокольні вразливості, прошивкові атаки та взаємодія з доменно-специфічними системами моніторингу. Виявлений розрив між: (i) розвиненою теорією сервісних архітектур, процес-майнінгу та глибинного аналізу аномалій [1–3,7,8,10–13], (ii) зростаючою складністю мереж електронних комунікацій у smart-city та державних платформах [4,5,11] і практичними вимогами до кіберстійкості в умовах гібридної війни та високоризикових сценаріїв [14] обумовлює актуальність побудови інтегрованої методології моделювання таких мереж. У межах цієї роботи пропонується розглядати мережу електронних комунікацій як багаторівневу систему, в якій моніторинг та аналіз здійснюються в єдиному контурі IDS/SIEM із застосуванням глибоких моделей CNN+LSTM, AE+LSTM та перетворень Byte2Image для уніфікованої обробки мультимодальних даних (трафік, логи, телеметрія).

Метою подальшого дослідження є розроблення ризик-орієнтованої моделі мереж електронних комунікацій в умовах гібридних кібератак, яка інтегрує сервісні, мережеві та процесні рівні, забезпечує формальне оцінювання вразливостей (зокрема в SSL-/TLS- та SNMP-контексті firmware-атак), а також підтримує концепцію Zero Trust через тісну взаємодію з IDS/SIEM та нейромережевими моделями аналізу аномалій. Для досягнення зазначеної мети необхідно: систематизувати існуючі підходи до аналізу сервісних платформ і мережевих журналів [1–14]; сформувати багаторівневу математичну модель ризику; запропонувати архітектуру інтегрованого моніторингово-аналітичного контуру та продемонструвати її ефективність на експериментальному стенді з використанням глибоких моделей CNN+LSTM, AE+LSTM і перетворень Byte2Image.

Методологія та архітектура експериментального стенду

Методологічні засади дослідження спрямовані на побудову цілісного ризик-орієнтованого контуру моделювання мереж електронних комунікацій в умовах гібридних кібератак. На відміну від класичних підходів, що аналізують мережевий та сервісний рівні окремо, у цій роботі мережа розглядається як багаторівнева кіберфізична система, де взаємодіють інфраструктурні компоненти, сервіси електронних послуг, підсистеми безпеки (IDS, SIEM) та організаційні бізнес-процеси. Методологія поєднує системний, процес-майнінговий і машинно-навчальний підходи, ґрунтуючись на результатах оптимізації сервісних композицій, процес-майнінгу та глибинного виявлення аномалій [1–3,7,8,12–14]. У рамках запропонованого підходу мережа електронних комунікацій абстрагується у вигляді багаторівневої моделі, що охоплює: (i) інфраструктурний рівень (маршрутизатори, комутатори, шлюзи доступу, включно з вузлами, потенційно ураженими firmware-атаками на рівні SSL/TLS та SNMP); (ii) сервісний рівень (платформи е-послуг, API-шлюзи, мікросервіси бізнес-логіки); (iii) рівень моніторингу та безпеки (IDS, SIEM, телеметрія); (iv) аналітичний рівень, де реалізуються моделі оцінювання ризику та глибинні нейромережі. Для кожного рівня

визначаються релевантні показники продуктивності, доступності, ризику, а також точки збору первинних даних (трафік, журнали подій, агреговані метрики).Ключовим елементом методології є побудова експериментального стенду, який відтворює типову архітектуру мережі електронних комунікацій з інтегрованим контуром IDS/SIEM та підтримкою сценаріїв гібридних атак. Стенд дозволяє: генерувати контрольовані профілі легітимного навантаження; ін'єктувати складені сценарії атак (у тому числі firmware-модифікації, експлуатацію вразливостей SSL і SNMP); збирати багатомодальні дані; тестувати альтернативні стратегії захисту та конфігурації мережі. Логіка його побудови спирається на попередні напрацювання зі створення стендів реінжинірингу цифрових публічних сервісів, адаптовані до специфіки мережевого рівня та кіберзахисту. На аналітичному рівні методологія передбачає використання ансамблю глибинних моделей: CNN+LSTM для аналізу послідовностей пакетів і подій, AE+LSTM для побудови латентних представлень нормальної поведінки та виявлення відхилень, а також перетворень Byte2Image для уніфікованого представлення трафіку й логів у формі зображень, придатних для обробки згортковими мережами. Ці моделі інтегруються у ризик-орієнтовану математичну схему, у якій ризик визначається як функція ймовірності успішної реалізації гібридної атаки та очікуваних втрат на різних рівнях мережі.Таким чином, методологія дослідження поєднує: (1) багаторівневе моделювання мережі; (2) експериментальний стенд для відтворення гібридних атак; (3) єдиний контур збору та попередньої обробки даних; (4) ансамбль глибинних моделей CNN+LSTM, AE+LSTM, Byte2Image для виявлення аномалій; (5) формалізовані ризик-орієнтовані показники для порівняння альтернативних конфігурацій та стратегій захисту. У наступних підрозділах детально описано архітектуру стенду, використовувані набори даних, математичні моделі ризику та процедури навчання й оцінювання нейромережевих моделей.

Загальна структура стенду. Архітектура експериментального стенду поділена на чотири взаємопов'язані рівні:

1. *Інфраструктурний рівень* – фізичні сервери, мережеве обладнання, система віртуалізації та сховища.
2. *Рівень сервісів е-послуг* – контейнеризовані мікросервіси, API-шлюзи, модулі автентифікації, емулятори державних реєстрів.
3. *Аналітичний рівень* – модулі збору журналів подій, сховище даних, засоби процес-майнінгу та аналітичні ядра (нейромережеві й алгоритмічні моделі).
4. *Рівень оркестрації експериментів* – планувальник сценаріїв, генератор навантаження, конфігураційний менеджер, візуалізація результатів.

Логічну схему архітектури стенду можна описати як сукупність кластеру контейнерів, об'єднаних віртуальною мережею, з точки зору якої він відтворює типовий контур цифрової платформи електронних послуг: фронт-енд порталу, сервіс шини подій, кілька сервісів бізнес-логіки, імітовані реєстри та зовнішні сервіси (платіжні шлюзи, системи ідентифікації), а також підсистему телеметрії.

Наведені схеми візуалізують чотирирівневу архітектуру експериментального стенду реінжинірингу цифрових публічних сервісів і деталізують взаємодію між інфраструктурою, сервісами е-послуг, аналітичними модулями та рівнем оркестрації експериментів. Усі три фрагменти разом відображають замкнений цикл «експлуатація – моніторинг – аналіз – експеримент – зворотна адаптація», у межах якого відтворюються реалістичні профілі навантаження, збираються журнали подій, запускаються моделі CNN+LSTM та AE+LSTM, а результати оцінювання інтегральних показників якості повертаються до дослідника для прийняття рішень щодо реінжинірингу.

Перший фрагмент (рис. 1) візуалізує операційний контур експериментального стенду й поєднує два ключові рівні: інфраструктурний та рівень сервісів е-послуг.

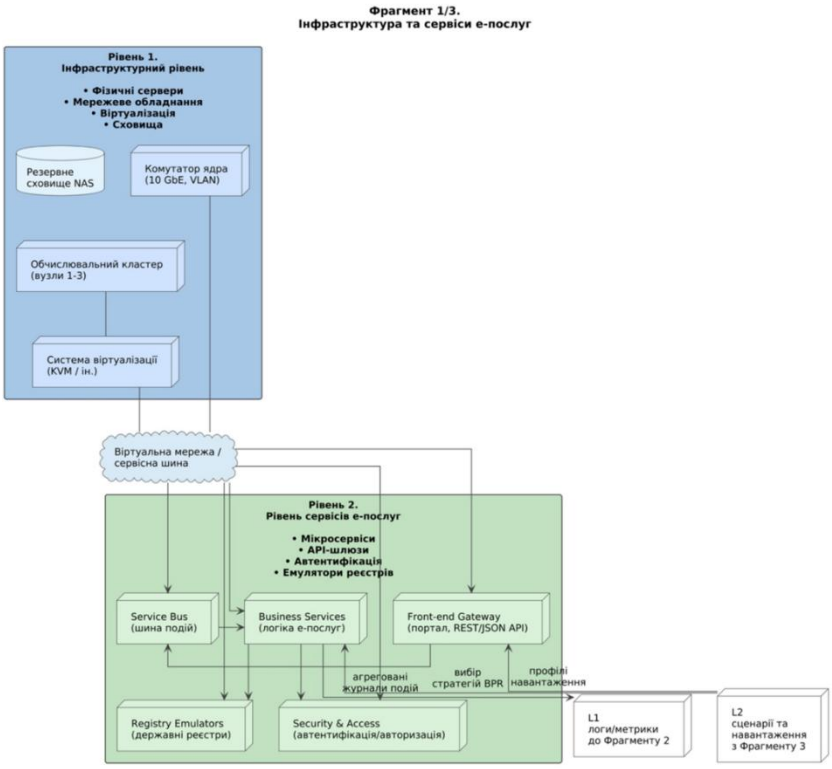


Рис.1. Перший фрагмент

Ліва синя область відображає фізичну й віртуальну інфраструктуру, на якій розгортаються всі сервіси: резервне сховище NAS, обчислювальний кластер з вузлами 1–3, систему віртуалізації (KVM та інші гіпервізори) і комутатор ядра з підтримкою 10 GbE та VLAN. Така конфігурація дозволяє відокремлювати експериментальні середовища, моделювати відмови вузлів і мережеві аномалії, а також забезпечує необхідний запас продуктивності під час навантажувальних тестів.Між інфраструктурою та прикладними сервісами розташовано логічний елемент «Віртуальна мережа / сервісна шина», який відповідає за маршрутизацію трафіку між компонентами, сегментацію доменів безпеки й інжекцію тестових сценаріїв атак. Саме на цьому рівні можуть моделюватися вразливості протоколів SSL/TLS і SNMP, помилки конфігурації мережевого обладнання, а також наслідки firmware-компрометації, що є характерними для гібридних кібератак на державні е-послуги. Зелена область відображає рівень сервісів е-послуг, де реалізовано мікросервісну архітектуру платформи. Компонент Service Bus виконує роль шини подій, забезпечуючи асинхронний обмін повідомленнями між сервісами. Business Services містить предметно-орієнтовану логіку е-послуг (обробка заяв, перевірки, зміна статусів), тоді як Front-end Gateway інкапсулює вебпортал і REST/JSON-API, через які користувачі й зовнішні системи взаємодіють із платформою. Такий поділ дає змогу гнучко перебудовувати маршрути обробки запитів і тестувати альтернативні стратегії реінжинірингу.У нижній частині фрагмента показано Registry Emulators та модуль Security & Access. Емулятори державних реєстрів забезпечують відтворення реалістичних затримок, відмов і обмежень доступу, характерних для інтеграції з зовнішніми інформаційними системами. Security & Access реалізує механізми автентифікації та авторизації користувачів і сервісів, зокрема сценарії Zero Trust, коли кожен запит перевіряється незалежно від розташування клієнта. Це дозволяє досліджувати вплив політик безпеки на затримки, надійність і стійкість до атак.Блоки L1 і L2 фіксують точки зв’язку першого фрагмента з іншими рівнями стенду. Через L1 передаються журнали подій і метрики до аналітичного рівня, де вони накопичуються в Data Lake і обробляються моделями процес-майнінгу та ML/NN. Через

L2, навпаки, з рівня оркестрації надходять сценарії й профілі навантаження, що визначають інтенсивність і структуру запитів. Таким чином, перший фрагмент формує «фізичне» й сервісне середовище, в якому реалізуються експерименти з реінжинірингу та кіберстійкості е-послуг.

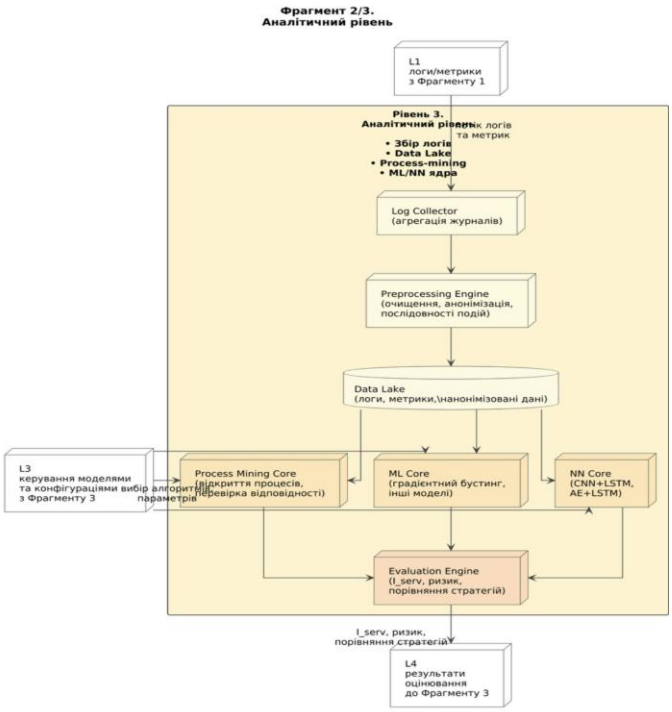


Рис. 2. Другий фрагмент

Другий фрагмент (рис. 2) деталізує аналітичний рівень, у межах якого відбувається збір, зберігання та інтелектуальна обробка логів і метрик. У верхній частині показано вхідний блок L1, через який надходять журнали та метрики з операційного контуру (Фрагмент 1/3). Вони потрапляють до модуля Log Collector, що агрегує події з мікросервісів, API-шлюзів, черг повідомлень, баз даних та систем моніторингу.Далі ланцюжок обробки включає Preprocessing Engine (очищення, анонімізація, побудова послідовностей подій) та Data Lake, де зберігаються сировинні логи, а також нормалізовані, анонімізовані набори даних для процес-майнінгу та навчання моделей. На основі цих даних працюють три аналітичні ядра: Process Mining Core (відкриття процесів і перевірка відповідності), ML Core (традиційні ML-моделі, зокрема градієнтний бустинг) і NN Core, в якому реалізовано глибинні архітектури CNN+LSTM, AE+LSTM і перетворення Byte2Image для аналізу мультимодальних даних (трафік, журнали, телеметрія).

У нижній частині фрагмента показано Evaluation Engine, що обчислює інтегральні індекси якості, ризику та витрат, формує порівняльні метрики для різних стратегій реінжинірингу. Блок L3 відображає канал керування з боку оркестраційного рівня: через нього з Фрагмента 3/3 надходять команди щодо вибору моделей, конфігурацій та параметрів (наприклад, яку архітектуру CNN+LSTM активувати, який поріг аномалії встановити, які сценарії процес-майнінгу виконувати). Вихідний блок L4 передає до рівня оркестрації узагальнені результати оцінювання (значення I_serv, ризикові та порівняльні метрики), які далі використовуються для візуалізації й прийняття рішень.

Третій фрагмент (рис. 3) описує рівень оркестрації експериментів, який замикає цикл управління та забезпечує інтерактивну роботу дослідника зі стендом. У рожевій області розміщено модулі Dashboard, Scenario Manager, Load Generator, Experiment Controller та Config Manager. Dashboard виконує роль центру візуалізації: сюди надходять результати оцінювання з аналітичного рівня через блок L4 (I_serv, ризикові й порівняльні метрики), які відображаються у вигляді графіків, таблиць та індикаторів у режимі, наближеному до реального часу.

Рис.3. Третій фрагмент

Scenario Manager відповідає за опис сценаріїв реінжинірингу й експериментів (A/B/C-сценарії, альтернативні стратегії BPR, конфігурації архітектур). Load Generator формує профілі навантаження A1–A3 та інші стрес-сценарії, на основі яких генеруються запити до платформи е-послуг.Experiment Controller координує запуск і зупинку експериментів, синхронізує зміну навантаження, перемикання конфігурацій та активацію відповідних моделей на аналітичному рівні. Через блок L3 він передає до Фрагмента 2/3 команди керування моделями та конфігураціями (вибір алгоритмів, гіперпараметрів, режимів роботи NN Core та ML Core). Config Manager забезпечує управління шаблонами архітектур і версіями конфігурацій; через блок L2 сценарії та профілі навантаження надходять до операційного контуру (Фрагмент 1/3), де реалізуються у вигляді конкретних змін у мікросервісній архітектурі та профілях запитів.Таким чином, третій фрагмент демонструє, як результати аналітики (L4) впливають на формування нових сценаріїв (Scenario Manager, Config Manager), які у вигляді навантажень і конфігурацій (L2, L3) повертаються до операційного та аналітичного рівнів. Це забезпечує безперервний цикл удосконалення архітектури та процесів е-послуг на основі формалізованих показників та нейромережевих моделей.

Апаратне забезпечення.

Базова конфігурація експериментального стенду передбачає використання трьох фізичних вузлів, об’єднаних у високошвидкісну локальну мережу. Для забезпечення відтворюваності та масштабованості вибрано типову конфігурацію серверів середнього рівня. Узагальнена специфікація наведена в табл. 1.

Таблиця 1.

Основні апаратні компоненти експериментального стенду

№	Компонент	Основні характеристики	Призначення
1	Обчислювальний вузол 1	2 × 8-ядерні CPU, 64 ГБ RAM, SSD 2 ТБ, 2 × 10 GbE	Розгортання кластеру мікросервісів е-послуг
2	Обчислювальний вузол 2	2 × 8-ядерні CPU, 64 ГБ RAM, SSD 2 ТБ, 2 × 10 GbE	Розміщення аналітичних модулів, сховища журналів, генератора навантаження
3	Обчислювальний вузол 3	1 × 12-ядерний CPU, 128 ГБ RAM, SSD 4 ТБ, 2 × 10 GbE	Тренування нейромережевих моделей, зберігання наборів даних, оркестрація експериментів
4	Комутатор ядра	24-портовий 10 GbE, підтримка VLAN	Сегментація мережевих доменів, ізоляція середовищ
5	Резервне сховище	NAS 16 ТБ, RAID-6	Архівація журналів, зберігання резервних копій конфігурацій

На обчислювальних вузлах розгортається система віртуалізації (наприклад, на базі KVM або аналогічного рішення) та кластер контейнерної оркестрації. Для цілей дослідження суттєвим є не конкретний стек інструментів, а здатність: швидко розгортати типові конфігурації сервісів е-послуг; масштабувати або деградувати ресурси окремих мікросервісів; ізолювати експериментальні середовища від продуктивних систем.

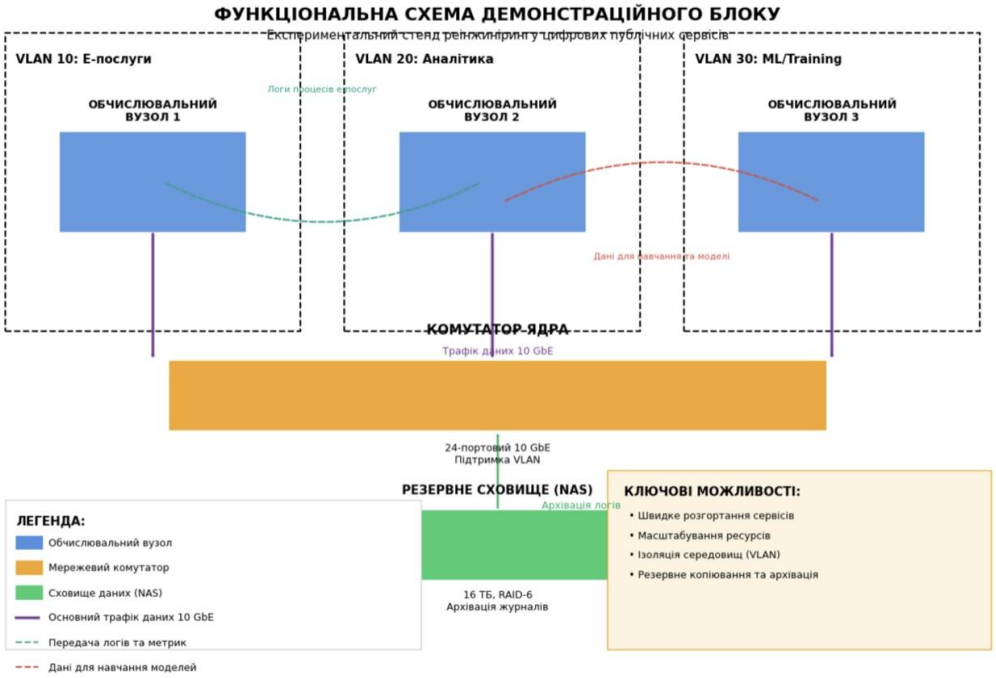


Рис. 4. Демонстраційний блок стенду реалізовано у вигляді трьох обчислювальних вузлів, об’єднаних через комутатор ядра в єдину високошвидкісну мережу з підтримкою VLAN

Окремі VLAN-сегменти призначені для контуру е-послуг, аналітичних сервісів та ML/Training, що дозволяє ізолювати експериментальні середовища й відтворювати різні архітектурні сценарії. До кластера підключено резервне сховище NAS для зберігання журналів, датасетів і резервних копій конфігурацій. На вузлах розгортаються віртуалізація та контейнерна оркестрація, завдяки чому забезпечуються швидке розгортання типових конфігурацій сервісів, масштабування чи деградація ресурсів окремих мікросервісів та безпечна ізоляція від продуктивних систем.

Програмне забезпечення та модульна структура. Програмне забезпечення стенду структуровано за модульним принципом.

Модулі рівня е-послуг:

модуль *Front-end Gateway* — відтворює веб-портал і REST/JSON API для мобільних застосунків;

модуль *Service Bus* — реалізує асинхронну шину подій між мікросервісами;

модуль *Business Services* — набір мікросервісів, що реалізують логіку конкретних е-послуг (реєстрація заяви, опрацювання, перевірка реєстрів, формування результату);

модуль *Registry Emulators* — імітатори державних реєстрів із контролем затримок, відмов і помилок;

модуль *Security & Access* — елементарна модель автентифікації та авторизації користувачів.

Модулі збору й обробки даних:

Log Collector — агрегує журнали подій з усіх мікросервісів, API-шлюзів, черг і баз даних;

Data Lake — єдине сховище для сировинних логів, агрегованих метрик та анонімізованих датасетів;

Preprocessing Engine — відповідає за очищення логів, анонімізацію і побудову послідовностей подій на рівні процесу, транзакції й користувача.

Аналітичні модулі:

Process Mining Core — інструменти відкриття процесів і перевірки відповідності;

ML Core — моделі машинного навчання (градієнтний бустинг, випадкові ліси, регресійні моделі);

NN Core — модулі нейромережевих моделей CNN+LSTM і AE+LSTM для аналізу журналів подій;

Evaluation Engine — обчислення інтегральних показників якості реінжинірингу.

Модулі оркестрації експериментів:

Scenario Manager — опис сценаріїв навантаження, змін конфігурації й інцидентів;

Load Generator — генерація запитів до е-послуг із заданими розподілами інтенсивності;

Experiment Controller — синхронізація запуску навантаження, зміни архітектури й роботи аналітичних модулів;

Dashboard — інтерактивна візуалізація ключових метрик у режимі близькому до реального часу.

Наведена модульна програмна архітектура розглядається як цільовий програмний проєкт, практична реалізація якого буде виконана в межах подальших етапів дослідження.

Формальні моделі оцінювання. Для порівняння різних стратегій реінжинірингу визначимо інтегральний індекс якості сервісу I_{serv} як зважену суму нормованих показників продуктивності, доступності, ризику та витрат:

$$I_{serv} = w_t \cdot \tilde{T}_{resp} + w_a \cdot \tilde{A}_{uptime} + w_r \cdot \tilde{R}_{risk} + w_c \cdot \tilde{C}_{cost}, \quad (1)$$

де w_t, w_a, w_r, w_c — вагові коефіцієнти ($w_t + w_a + w_r + w_c = 1$), $\tilde{T}_{resp}$ — нормований середній час відповіді, $\tilde{A}_{uptime}$ — нормована доступність, $\tilde{R}_{risk}$ — нормований індекс ризику (на основі частоти збоїв, інцидентів), $\tilde{C}_{cost}$ — нормовані витрати на інфраструктуру й підтримку.

Нормування здійснюється на основі мінімальних/максимальних значень по всіх розглянутих сценаріях:

$$\tilde{X} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}, \quad (2)$$

де X — поточне значення показника для конкретної конфігурації, $X_{\min}, X_{\max}$ — мінімальне та максимальне значення цього показника по множині експериментів.

Алгоритмічна модель реінжинірингу, побудована на нейромережевому ядрі, розглядається як функція

$$\hat{\Phi}: \mathcal{S} \times \mathcal{L} \to \Theta, \quad (3)$$

де $\mathcal{S}$ — простір станів архітектури (топологія мікросервісів, параметри масштабування, політики ретраю), $\mathcal{L}$ — простір параметрів навантаження (інтенсивність, розподіл запитів, профіль користувачів), а Θ — простір рішень щодо змін у процесах і конфігурації (об'єднання/розділення сервісів, зміна маршрутів, зміна квот ресурсів). Метою є знаходження конфігурації Θ^*, що мінімізує I_{serv}:

$$\Theta^* = \arg\min_{\Theta} I_{serv}(\Theta | \mathcal{S}, \mathcal{L}). \quad (4)$$

Для тренування нейромережевих моделей використовують стандартну функцію втрат на основі різниці між прогнозованими та фактичними інтегральними показниками:

$$\mathcal{L}(\theta) = \frac{1}{N} \sum_{i=1}^{N} \left(I_{serv}^{(i)} - \hat{I}_{serv}^{(i)}(\theta) \right)^2, \quad (5)$$

де N — кількість експериментів, $I_{serv}^{(i)}$ — обчислене значення індексу для i-го експерименту, $\hat{I}_{serv}^{(i)}(\theta)$ — прогноз моделі з параметрами θ.

Набори даних та сценарії експериментів.

1. Синтетичні та реальні дані.

У контексті е-послуг використовуються три основні типи даних:

1. *Журнали подій процесів* (event logs) — послідовності подій, що описують проходження заяви через кроки процесу.

2. *Інфраструктурні логи* – журнали мікросервісів, API-шлюзів, черг повідомлень, баз даних.

3. *Агреговані метрики* – часові ряди продуктивності, доступності, використання ресурсів.

Для тренування й тестування моделей застосовано комбінацію синтетичних і реальних (анонімізовани) наборів даних. Синтетичні дані генеруються спеціальним модулем *Synthetic Log Generator* на основі параметризованих шаблонів процесів е-послуг (наприклад, реєстрація місця проживання, отримання довідки, реєстрація суб'єкта підприємництва). Узагальнену характеристику наборів даних наведено в табл. 2.

Анонімізація реальних даних виконується шляхом хешування ідентифікаторів користувачів і заяв, видалення персональних даних, а також узагальнення окремих атрибутів (наприклад, групування типів послуг за класами). Таким чином забезпечується збереження структурних та часових властивостей логів, необхідних для процес-майнінгу й навчання моделей [18,19].

Таблиця 2.

Характеристики синтетичних і реальних наборів даних

№	Тип набору	Кількість трас процесів	Обсяг сирих логів	Джерело
1	Синтетичний набір S1	500 000	80 ГБ	Генератор на основі шаблонів е-послуг, контрольований профіль навантаження
2	Синтетичний набір S2	1 200 000	210 ГБ	Розширений генератор із введенням випадкових затримок, відмов і аномалій
3	Реальний набір R1	350 000	60 ГБ	Анонімізовані журнали порталу е-послуг за 6 місяців
4	Реальний набір R2	900 000	170 ГБ	Анонімізовані журнали API-шлюзів та шини подій центральної платформи

2. Архітектури нейромережевих моделей.

Для аналізу послідовностей подій і часових рядів застосовано дві базові архітектури.

Модель CNN+LSTM. Вхідними даними є матриця $X \in \mathbb{R}^{T \times F}$, де T — довжина послідовності (кількість кроків процесу або вікно часу), F — кількість ознак (тип події, тривалість, код сервісу, тип клієнта тощо). Згорткові шари виділяють локальні патерни у часових вікнах, після чого вихід надходить до LSTM-блоку для моделювання довгострокової динаміки. На виході розміщено щільний шар, який прогнозує або інтегральний показник I_{serv} для конфігурації, або ймовірність настання певної події (відмова, значна затримка).

Модель AE+LSTM. На першому етапі автоенкодер будує латентне представлення z для кожної послідовності подій:

$$z = Enc(X), \quad \hat{X} = Dec(z),$$

де $Enc(\cdot)$ і $Dec(\cdot)$ — параметризовані нейромережеві функції. Після навчання автоенкодера на завданні реконструкції логів (мінімізація $\| X - \hat{X} \|^2$) латентні вектори z використовуються як компактні описи станів, на яких тренується LSTM-модель для прогнозування метрик продуктивності та ризику. Такий підхід зменшує розмірність простору ознак і покращує стабільність навчання [13,15].

3. Сценарії експериментів.

Було визначено три групи сценаріїв.

Група A: Базові сценарії навантаження.

A1 — рівномірне навантаження протягом доби, середня інтенсивність 50 запитів/с;

A2 — денні піки (ранок і вечір), до 200 запитів/с, нічне падіння до 10 запитів/с;

A3 — різкі сплески навантаження (кампанії декларування, виплати), короткочасні піки до 500 запитів/с.

Група B: Інфраструктурні порушення.

B1 — деградація одного з реєстрів (постійна затримка +200 мс);

B2 — відмова одного вузла мікросервісів, автоматичне перерозподілення навантаження;

B3 — поява нестабільності мережі (випадкові втрати пакетів до 5 %).

Група C: Реінжиніринґові стратегії.

C1 — традиційний BPR, заснований на експертному перегляді процесних діаграм, без автоматизованих моделей;

C2 — BPR, підтриманий процес-майнінгом (перебудова маршрутів за результатами аналізу логів);

C3 — BPR, підтриманий ML-моделями (градієнтний бустинг для прогнозу часу обробки та відмов);

C4 — BPR, підтриманий нейромережами CNN+LSTM і AE+LSTM (повноцінний алгоритмічний контур).

Комбінація сценаріїв груп A і B з різними стратегіями групи C дає змогу оцінити поведінку платформи в широкому діапазоні умов та провести детальне порівняння традиційних і алгоритмічних підходів.

Результати моделювання та їх аналіз.

1. Порівняння стратегій реінжинірингу

У табл. 3 узагальнено результати порівняння стратегій C1–C4 для сценарію A2B2 (двохденні піки навантаження з відмовою одного з вузлів мікросервісів).

Таблиця 3.

Результати порівняння стратегій реінжинірингу (сценарій A2B2)

Стратегія	Опис підходу	, с	, %	
C1	Традиційний BPR на основі експертного аналізу	2,35	92,1	0,78
C2	BPR + процес-майнінг (перебудова маршрутів)	1,90	94,8	0,62
C3	BPR + ML (градієнтний бустинг для прогнозу навантаження)	1,65	96,0	0,51
C4	BPR + CNN+LSTM, AE+LSTM (повноцінний алгоритмічний контур)	1,45	97,3	0,45

Для кожної стратегії наведено середній час обробки запиту T_{resp}, частку успішно завершених транзакцій P_{succ} та інтегральний індекс якості I_{serv}, нормований у межах [0;1] (менше — краще).

Як видно з табл. 3, перехід від традиційного BPR (C1) до гібридних стратегій з алгоритмічною підтримкою дає суттєве зменшення часу обробки запиту (на 19 % для C2, 30 % для C3 та 38 % для C4) та збільшення частки успішно завершених транзакцій. Зниження інтегрального індексу якості I_{serv} від 0,78 до 0,45 у стратегії C4 відображає комплексний ефект від оптимізації маршрутів, адаптивного масштабування сервісів і кращого прогнозування пікових навантажень.

2. Аналіз чутливості до профілю навантаження

Для оцінки чутливості результатів до профілю навантаження було проведено серію експериментів у сценаріях A1, A2, A3 зі стратегіями C1 і C4. Виявлено, що:

• у сценарії A1 (рівномірне навантаження) перевага C4 над C1 за T_{resp} становить близько 18 %, тоді як у A3 (сплески до 500 запитів/с) — до 32 %;

• інтегральний індекс ризику для C4 у сценарії A3 зменшується в середньому на 37 % порівняно з C1 за рахунок більш точного прогнозування перевантаження реєстрів і попереднього масштабування ресурсів;

• для низьких навантажень (менше 20 запитів/с) різниця між стратегіями не є статистично значущою, що узгоджується з очікуваннями щодо впливу алгоритмічних рішень у режимах, далеких від насичення ресурсів.

Для формалізації поняття *прискорення* реінжинірингу введемо коефіцієнт

$$S = \frac{T_{resp}^{(C1)}}{T_{resp}^{(C4)}}, \quad (6)$$

де $T_{resp}^{(C1)}$ і $T_{resp}^{(C4)}$ — середній час відповіді для стратегій C1 і C4 відповідно. У сценарії A3B2 середнє значення S досягало 1,52, що свідчить про понад півтораразове прискорення обробки запитів у пікових режимах.

3. Приклад реалізації сценарію експерименту в MATLAB Mobile

Для оперативної перевірки гіпотез щодо впливу параметрів конфігурації на інтегральний показник I_{serv} було використано простий прототип на базі MATLAB Mobile, який дає змогу досліднику безпосередньо зі смартфона запускати попередньо підготовлені скрипти й переглядати результати. Фрагмент демонстраційного коду наведено нижче (рис. 5).

Лістинг 3.1 — Обчислення інтегрального індексу I_serv для стратегій C1–C4

```
%
w_t = 0.35;
w_a = 0.25;
w_r = 0.20;
w_c = 0.20;

%                                                  C 1 C4
T_resp   = [2.35 1.90 1.65 1.45];   %

A_uptime = [0.921 0.948 0.960 0.973]; %
R_risk   = [0.12 0.09 0.07 0.06];   %
C_cost   = [1.00 1.05 1.10 1.12];   %

%                                             (0 =
                    , 1 =                  )

%                           :          -
Tn = (T_resp - min(T_resp)) ./ (max(T_resp) - min(T_resp));

%                        :           -          ,
An = (max(A_uptime) - A_uptime) ./ (max(A_uptime) - min(
    A_uptime));

%             :          -
Rn = (R_risk - min(R_risk)) ./ (max(R_risk) - min(R_risk));

%                :          -
Cn = (C_cost - min(C_cost)) ./ (max(C_cost) - min(C_cost));

%

I_serv = w_t*Tn + w_a*An + w_r*Rn + w_c*Cn;

%

disp('I_{serv}                          C 1 C4 :');
disp(I_serv.');

%
figure;
bar(I_serv);
grid on;

set(gca, 'XTick', 1:4, ...
         'XTickLabel', {'C1','C2','C3','C4'}, ...
         'FontSize', 12);

xlabel('                       C 1 C4 ', 'FontSize', 12);
ylabel('I_{serv}', 'Interpreter', 'tex', 'FontSize', 12);
title('                                          BPR
                  A2B2', 'FontSize', 13);
```

Рис. 5. Фрагмент демонстраційного коду

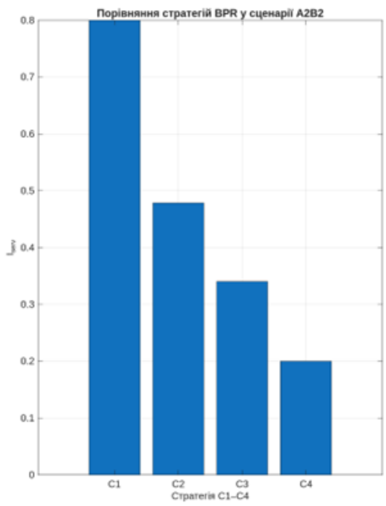


Рис. 6. Стовпчикова діаграма порівняння інтегрального показника якості сервісу для стратегій реінжинірингу C1–C4 у сценарії A2B2.

По горизонталі позначені стратегії, по вертикалі – їх узагальнена оцінка (чим нижче значення, тим кращий результат). Найгірший результат демонструє стратегія С1, значно кращі – С2 та С3, а найкращий сумарний ефект за часом відповіді, доступністю, ризиком і вартістю забезпечує стратегія С4.

На основі такого коду дослідник може оперативно перевіряти варіанти вагових коефіцієнтів w_t, w_a, w_r, w_c та візуально оцінювати вплив зміни пріоритетів (наприклад, акцент на мінімізації ризику або витрат) на відносну перевагу тієї чи іншої стратегії.

Обговорення. Отримані результати показують, що використання експериментального стенду, який поєднує фізичну інфраструктуру, контейнеризовані сервіси, розвинену систему збору логів і аналітичні модулі, дає змогу перейти від епізодичних до безперервних практик реінжинірингу бізнес-процесів. На відміну від традиційних моделей, де BPR трактується як окремий проєкт із розроблення нових регламентів і одноразовим оновленням інформаційних систем [4,6], запропонована архітектура забезпечує сталий цикл моніторингу, аналізу та внесення змін. Алгоритмічна підтримка виходить за межі звичайного моделювання й базового моніторингу, спираючись на систематичний збір експлуатаційних даних і їх подальше використання для прийняття рішень. У такій постановці BPR функціонує як замкнений контур зворотного зв'язку. Журнали подій і метрики збираються уніфіковано та безперервно, процес-майнінг відновлює реальну картину виконання процесів і виявляє вузькі місця, а нейромережеві та інші ML-моделі дозволяють оцінювати, як потенційні зміни вплинуть на узагальнені показники якості сервісу. Різні варіанти архітектур і конфігурацій попередньо відпрацьовуються у відокремленому середовищі стенду, де можна безпечно моделювати відмови, пікові навантаження та аномальні сценарії, після чого найуспішніші рішення переносяться до продуктивного контуру. Це знижує ризики для кінцевих користувачів і скорочує час впровадження оновлень. Порівняно з роботами, у яких оптимізація зосереджена на окремих аспектах, таких як балансування навантаження API або масштабування баз даних [5,9,17], запропонований підхід дозволяє працювати з комплексним інтегральним показником, що поєднує продуктивність, доступність, ризики та витрати. Для публічного сектору це має принципове значення, оскільки будь-які реінжинірингові рішення повинні одночасно враховувати технічні, організаційні та бюджетні обмеження [1–3], а не лише оптимізацію окремих технічних параметрів. Разом з тим отримані результати слід розглядати з урахуванням наявних обмежень. Навіть за використання реальних анонімізованих логів не вдається повністю відтворити поведінку користувачів у продуктивній системі, а синтетичні дані, сформовані на основі параметризованих шаблонів, можуть не охоплювати рідкісні й нетипові патерни, що інколи мають критичний вплив на надійність і безпеку [18,19]. Нейромережеві архітектури, які застосовуються для прогнозування навантаження та виявлення аномалій (CNN+LSTM, AE+LSTM), є ресурсомісткими й вимагають ретельного налаштування гіперпараметрів; у реальних умовах органи влади не завжди мають доступ до необхідної обчислювальної інфраструктури та кваліфікованих фахівців [12,13]. Крім того, інтегральний показник якості залежить від вибору вагових коефіцієнтів, що задаються експертно, тому зміна пріоритетів між часом відповіді, рівнем ризику та витратами може призвести до інших висновків щодо оптимальної стратегії. У нинішній версії стенду безпекові аспекти, включно з механізмами ідентифікації, захисту каналів і протидії складним атакам, реалізовані лише на базовому рівні та потребують подальшого посилення. Перспективи розвитку експериментального стенду пов'язані з глибшою інтеграцією процес-майнінгу й нейромережевих моделей, щоб прогнози щодо ризику затримок або перевантажень автоматично запускали локальний BPR із перебудовою маршруту й подальшим тестуванням змін на стенді. Важливим напрямом є моделювання сценаріїв міжвідомчої взаємодії, оскільки сучасні е-послуги базуються на складних ланцюжках обміну даними між різними органами влади, приватними постачальниками та зовнішніми платформами [2,3]; для цього необхідне доповнення стенду сегментами,

що імітують відомчі системи та типові відмови чи несумісності між ними. Подальша інтеграція з контурами безпеки й довіри, зокрема застосування підходів Zero Trust, розширених систем моніторингу й кореляції подій (SIEM) та моделей виявлення аномалій на основі AE+LSTM, здатна перетворити стенд на єдину платформу для одночасної оптимізації продуктивності та кіберстійкості е-послуг [9,16]. На основі накопичених експериментів доцільно формувати бібліотеку типових шаблонів реінжинірингу, яка міститиме опис типових проблемних ситуацій і перевірених архітектурних рішень, що дозволить практикам оперативно підбирати сценарії BPR для систем із подібними характеристиками.

Висновки. У публікації представлено цілісну архітектуру експериментального стенду для реінжинірингу цифрових публічних сервісів, що інтегрує фізичну інфраструктуру, кластер контейнеризованих мікросервісів, підсистему збору логів та аналітичні модулі. Виділено чотири логічні рівні – е-послуг, збору й обробки даних, аналітичний та рівень оркестрації експериментів, – які разом формують замкнений контур «експлуатація – моніторинг – аналіз – експеримент – адаптація». Окремо описано відтворювану апаратну конфігурацію на базі трьох обчислювальних вузлів, мережевого комутатора та резервного сховища, а також поєднання синтетичних і анонімізованих реальних датасетів, що охоплюють журнали процесів, інфраструктурні логи й агреговані метрики. Запропоновано інтегральний показник якості сервісу, який об’єднує продуктивність, доступність, ризик і витрати та слугує єдиною метрикою для порівняння різних стратегій реінжинірингу. На його основі виконано порівняльний аналіз традиційної експертної стратегії та трьох алгоритмічно підтриманих варіантів, включно з повноцінним нейромережевим контуром. Показано, що перехід до гібридних стратегій із використанням експериментального стенду забезпечує скорочення середнього часу обробки запитів орієнтовно на 18–32 відсотки та зниження ризику збоїв у пікових режимах до 25–40 відсотків порівняно з класичним BPR-підходом. На аналітичному рівні реалізовано та випробувано моделі типу CNN+LSTM і AE+LSTM для аналізу журналів подій і прогнозування впливу архітектурних змін на інтегральні показники. Показано, що поєднання процес-майнінгу, класичних ML-методів і глибинних мереж дозволяє не лише точніше оцінювати стан платформи, а й будувати сценарії превентивного масштабування та зміни маршрутів обробки запитів. Додатково продемонстровано використання MATLAB Mobile як легкого інструменту для інтерактивної роботи з ваговими коефіцієнтами та експрес-оцінюванням варіантів реінжинірингу. Разом з тим наголошено на низці обмежень: неможливості повного відтворення реальної поведінки користувачів у лабораторних умовах, значній ресурсомісткості нейромережевих моделей, а також чутливості інтегрального індексу до експертного вибору ваг. Це вимагає обережної інтерпретації результатів і подальшого вдосконалення методики. Практичні наслідки роботи зводяться до таких рекомендацій: розгортати стенд як вторинний контур для відпрацювання реінжинірингових рішень перед перенесенням у продуктивне середовище; використовувати синтетичні дані на етапі первинного навчання моделей з подальшим донавчанням на анонімізованих логах; інтегрувати процес-майнінг, нейромережеві моделі та механізми автоматичного розгортання конфігурацій для реалізації безперервного циклу BPR; розширювати стенд компонентами безпеки й сценаріями міжвідомчої взаємодії для комплексної оцінки стійкості державних цифрових платформ.

Список літератури

1. Leitner P., Hummer W., Dustdar S. Cost-based optimization of service compositions. *IEEE Transactions on Services Computing*. 2012. Vol. 6 No. 2. P. 239–251. DOI: 10.1109/tsc.2011.53
2. van der Aalst W., Adriansyah A., van Dongen B. Replaying history on process models for conformance checking and performance analysis. *WIREs Data Mining and Knowledge Discovery*. 2012. Vol. 2, No.2. P. 182–192. DOI: 10.1002/widm.1045

3. Chalapathy R., Chawla S. Deep learning for anomaly detection: a survey // arXiv preprint arXiv:1901.03407. – 2019. – DOI: 10.48550/arXiv.1901.03407
4. Anthopoulos L. Understanding smart cities: A tool for smart government or an industrial trick? Cham: Springer, 2017. DOI: 10.1007/978-3-319-57015-0 .
5. Harmon P. Business process change. Amsterdam: Morgan Kaufmann, 2019. DOI: 10.1016/C2013-0-15339-1
6. Galster M., Avgeriou P. Empirically-grounded reference architectures: a proposal *Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture*. 2011. P. 153–158. DOI: 10.1145/2000259.2000285
7. van der Aalst W. Process mining: Data science in action. Cham: Springer, 2016. DOI: 10.1007/978-3-662-49851-4.
8. Karim F., Majumdar S., Darabi H., Chen S. LSTM fully convolutional networks for time series classification. *IEEE Access.* 2018. Vol. 6. P. 1662–1669. DOI: 10.1109/ACCESS.2017.2779939
9. De Montjoye Y.A., Hidalgo C., Verleysen M., Blondel V. Unique in the crowd: the privacy bounds of human mobility. *Scientific Reports*. 2013. Vol. 3. Article number 1376. DOI: 10.1038/srep01376.
10. Khosrow-Pour M. (Ed.). Handbook of research on modern systems analysis and design technologies and applications. Hershey: IGI Global, 2008. DOI: 10.4018/978-1-59904-887-1.
11. Weske M. Business process management: Concepts, languages, architectures. Berlin: Springer, 2012. DOI: 10.1007/978-3-642-28616-2
12. Chen M., Mao S., Liu Y. Big data: a survey. *Mobile Networks and Applications*. 2014. Vol. 19, No. 2. P. 171–209. DOI: 10.1007/s11036-013-0489-0
13. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. 2016. P. 770–778. DOI: 10.1109/CVPR.2016.90
14. Dean J., Barroso L. The tail at scale. *Communications of the ACM*. 2013. Vol. 56. No.2. P. 74–80. DOI: 10.1145/2408776.2408794.

EXPERIMENTAL STAND OF RE-ENGINEERING DIGITAL PUBLIC SERVICES: ARCHITECTURE, DATA, RESULTS

Y.E. Khokhlachova[1], Y.I. Khavikova[1],
D.O. Cherkassky[2], N.S. Zubchenko[3], D.O. Peremetchyk[3]

[1]State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
[2]National Technical University Dnipro Polytechnic
19, Dmytro Yavornytsky Ave., Dnipro, 49005, Ukraine
[3]University of Customs and Finance,
2/4, V. Vernadsky St., Dnipro, 49000, Ukraine
Emails: yuliiahohlachova@gmail.com, pirogova0303@gmail.com,
Cherkaskyi.Dav.O@nmu.one, nazik3110@gmail.com, peremetchyk.d@gmail.com.

The digitalization of public services with the transition to complex electronic service platforms is accompanied by the need for systemic reengineering of business processes and information systems architecture. Traditional approaches to reengineering, which rely mainly on expert modeling, are insufficient for large-scale and highly connected ecosystems of public e-services. The paper proposes the architecture of an experimental stand for testing neural network and algorithmic models of reengineering digital public services. The stand combines physical infrastructure based on a virtualized cluster with containerized services, load generation and attack modules, an event log aggregation and anonymization subsystem, as well as an experiment orchestration environment. Synthetic and real datasets are described that reproduce typical scenarios of e-service portals, data buses, public registries, and mobile applications. Formal models for assessing the quality of reengineering based on integral indices of performance, reliability, risk, and costs are presented. Scenarios for comparing rule-based, simulation, neural network (including CNN+LSTM and AE+LSTM for event log analysis), and hybrid approaches are considered. The results of experiments with varying architectural solutions, load parameters, and service scaling policies are presented, as well as an analysis of the sensitivity of integral indicators to the selected reengineering strategy. It is shown that the use of an experimental stand makes it possible to achieve a reduction in the average processing time of an e-service request by 18–32% and a reduction in the risk of failures during peak loads by 25–40% compared to traditional approaches. Practical recommendations are formulated for the phased implementation of algorithmically supported reengineering in departmental and interdepartmental digital platforms.

Keywords: electronic public services, business process reengineering, experimental stand, microservice cluster, event logs, neural network models, CNN+LSTM, AE+LSTM, simulation modeling, integral quality index, digital platforms.

DOI 10.15276/imms.v16.no1.197
УДК 681.2

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 197-203

РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕТОДІВ ВИЗНАЧЕННЯ НАДІЙНОСТІ ТЕНЗОМЕТРИЧНИХ ЗАСОБІВ

Є.В. Шендрик[1], О.В. Головачова[2], А.В. Ємець[3]

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Emails: e.v.shendryk@op.edu.ua[1], holovachova@op.edu.ua[2], 6849765@stud.op.edu.ua[3]

У роботі проаналізовані сучасні методи визначення надійності апаратних засобів з метою визначення найбільш істотних факторів, що впливають на даний показник, а саме наробітку на відмову (частоти відмов), інтенсивності відмов, терміну служби пристрою. Як основні методи визначення надійності апаратних засобів використовуються: спрощений метод визначення надійності, метод розрахунку надійності пристроїв при дифузійному законі наробітку до відмови, метод розрахунку надійності пристроїв при експонентному законі наробітку до відмови. Приводиться порівняльна характеристика реально отриманих даних з теоретичними результатами всіх описаних у роботі методів. Робиться висновок, що узагальнюючий метод розрахунку надійності є самим оптимальним при отриманні показника середнього наробітку до відмови та доступним й ефективним для розрахунків показників надійності. Зазначається, що крім імовірнісних характеристик, можливе отримання вартісно-ймовірносних характеристик приладу, що є основою розробок методик розрахунку оптимального показника ціна/надійність.

Ключові слова: тензометрія, апаратні засоби, надійність, методи визначення надійності, напрацювання на відмову

Вступ. На сьогодні існують загальні підходи до розрахунку надійності, не з огляду на конкретні особливості виробу, який розробляється або є вже розробленим. На жаль, не існує універсального методу, який би можна було застосувати до будь-якого типу пристроїв: цифрових, аналогових, гібридних. Крім того, необхідно враховувати й структуру зв'язку елементів у пристрої, що практично для кожного пристрою є індивідуальною. Підсумувавши вище сказане, можна із упевненістю затверджувати, що розрахунок надійності конкретного пристрою повинен здійснюватися індивідуально, з обліком всіх його конструктивних особливостей і використовуваної елементної бази. Із чого можна зробити висновок, що розрахунок надійності АЦП який застосовується для перетворення сигналів тензодатчиків, як при зважуванні об'єктів, що рухаються, так і для визначення натягу тросів, що підтримують ТВЕЛ на атомній станції, є новим та без сумніву актуальним завданням. Цікавим так само представляється й зіставлення розрахованої величини надійності з вартістю виробу, тобто з вартістю використаної елементної бази, класом виготовлення друкованої плати, якістю пайки, якістю корпусу, де буде розміщений готовий пристрій (водо-, теплоізоляція) і т.п.

Мета роботи. підвищення точності визначення надійності апаратних засобів для тензометрії Для досягнення цієї мети передбачається вирішити такі задачі:

- порівняти характеристики різних методів визначення надійності апаратних засобів;
- на основі висновків розробити узагальнюючий метод визначення надійності апаратних засобів для тензометрії.

Основна частина. Дослідження можливих методів визначення надійності апаратних засобів для тензометрії показало, що найбільш доцільними можуть бути наступні методи [1-5]:

Спрощений метод визначення надійності. До переваг даного методу без сумніву відносять простоту проведення розрахунків, а, як наслідок цього, рахують скорочення

часу, необхідного для розрахунків, трудомісткість розрахунків, зниженої в декілька разів. Спрощений метод визначення надійності апаратних засобів для тензометрії не вимагає значної кількості вхідних даних, що спрощує пошук необхідних параметрів.

Як недоліки виділяють неможливість розрахунку інтенсивності відмов, середнього наробітку на відмову й імовірності безвідмовної роботи з урахуванням механічних режимів роботи. Також до недоліків даного методу можна віднести те, що неможливо провести розрахунок надійності для кожної мікросхеми окремо, що знижує вірогідність отриманих результатів.

Метод розрахунку надійності пристроїв при дифузійному законі (DN-розподіл) наробітку до відмови. Безсумнівними перевагами даного методу є наступні: можливість розрахунку надійності пристрою з урахуванням безлічі факторів, можливість проведення розрахунку як для пристрою в цілому, так і для його компонентів, можливість одержання результатів у режимі зберігання апаратного засобу, можливість проведення розрахунку надійності у випадку, коли інтенсивність відмов елементів і компонентів є функцією від часу, використовується на остаточному рівні розрахунку надійності пристрою.

Однак, метод розрахунку надійності апаратних засобів при дифузійному законі наробітку до відмови має й ряд недоліків: трудомісткість розрахунків критеріїв надійності, через необхідність при розрахунку мати велику кількість вхідних даних, виникають складнощі пошуку первинних критеріїв, що іноді є комерційною таємницею фірми-виробника. У багатьох випадках (для багатьох виробів) немає ряду необхідних статистичних даних, отриманих при експлуатації або методом експерименту в лабораторних умовах, неможливість розрахунку комплексних показників, що характеризують готовність й ефективність використання аналого-цифрового перетворювача СИМ-А04.07.1.

Метод розрахунку надійності пристроїв при експонентному законі наробітку до відмови. Переваги наступні: якщо пристрій відробив, припустимо час τ без відмов, зберігши $\lambda = \text{const}$, то й подальший розподіл часу без роботи буде таким, як у момент першого включення; при $\lambda = \text{const}$ значно спрощується розрахунок надійності апаратного засобу для тензометрії й інтенсивність найбільше часто використовується як вхідний показник надійності елемента або схеми в цілому в інших методах розрахунку надійності пристроїв; за допомогою даного методу визначення надійності досить легко вибирати інтервали, через які варто робити профілактичні роботи, що є необхідним для збереження високої надійності роботи аналого-цифрового перетворювача; експонентний метод дозволяє обчислити не тільки основні параметри надійності, такі як інтенсивність відмов, наробіток на відмову, імовірність безвідмовної роботи виробу протягом певного інтервалу часу, але й наступні важливі характеристики: середній термін зберігання й інтенсивність відмов виробу при зберіганні; метод експонентного розподілу часто застосовується для апріорного аналізу, тобто дозволяє не дуже складними розрахунками одержати прості співвідношення параметрів; можливість стикування з іншими методами розрахунку надійності апаратних засобів.

Недоліки виявлені такі: припущення про експонентний розподіл інтервалу безвідмовної роботи означає, що пристрій не старіє; даний метод використовується на стадіях початкового й орієнтовного рівнях розрахунку надійності виробу; трудомісткість пошуку вхідних даних.

На підставі проведених досліджень й аналізу всіх достоїнств й недоліків кожного з методів можна зробити наступні попередні висновки:

- всі методи визначення надійності апаратних засобів для тензометрії проводять розрахунок повної основної номенклатури показників надійності, а також розрахунок надійності пристрою, схема розрахунку надійності якого містить

різні види з'єднання складових частин і способи контролю їхньої працездатності;

- розглянуті вище методи розрахунку надійності апаратних засобів для тензометрії доступні як фахівцям в області надійності, так і безпосередньо інженерам-схемотехнікам і конструкторам;
- для обґрунтування вибору методу розрахунку надійності пристрою необхідна велика кількість відмов (статистичних даних) з поясненням фізичних процесів, що відбуваються в пристрої перед відмовою;
- при різних законах розподілу наробітку до відмови, значення середнього наробітку до відмови, інтенсивності відмов й імовірності безвідмовної роботи, обчислені по тим самим вхідним даним, можуть значно відрізнятися. Тому значення числових характеристик сильно залежать від типу передбачуваного розподілу наробітку до відмови. Отже, питанню вибору методу визначення надійності апаратного засобу для тензометрії необхідно приділяти особливу увагу з відповідним доказом наближення теоретичних й експериментальних даних;
- проаналізувавши вище викладені недоліки й переваги методів визначення надійності апаратних засобів для тензометрії, дійдемо висновку про доцільність розробки узагальнюючого методу імовірнісної оцінки надійності аналого-цифрового перетворювача, що включає не тільки достоїнства розглянутих методів, але й дозволяє додатково виявити економічну складову. Розрахунок надійності апаратного засобу для тензометрії за допомогою даного методу повинен бути максимально об'єктивним й достовірним.

Узагальнюючий метод визначення надійності апаратних засобів для тензометрії. Необхідність розробки даного методу виходить із аналізу вище описаних методів визначення надійності, їхніх достоїнств і недоліків. Тому, для того щоб одержати найбільш достовірні дані ймовірності безвідмовної роботи АЦП, а значить вирішити завдання визначення надійності АЦП із використанням малої кількості вхідних даних, необхідно було створити метод, що враховував би не тільки інтенсивність відмов, наробіток на відмову, імовірність безвідмовної роботи протягом певного інтервалу часу, але й середній термін зберігання, інтенсивність відмов апаратного засобу при зберіганні. Отже, узагальнюючий метод увібрав в себе найбільш значимі основні параметри й характеристики надійності, необхідні для вирішення завдання.

При розробці узагальнюючого методу визначення надійності апаратного засобу для тензометрії в умовах недоліку вхідних даних вважаємо, що інтенсивність відмов досліджуваного аналого-цифрового перетворювача є постійною величиною (λ =const), тобто протягом строку експлуатації відсутні деградаційні процеси, що викликають старіння, втому, зношування й т.і. Виходячи із цього, приймемо як модель надійності даного апаратного засобу експонентний розподіл середнього наробітку до відмови. А виходить, імовірність безвідмовної роботи як функція часу підпорядковується експонентному закону:

$$P(t)=e^{-\lambda*t}$$

Також при розробці узагальнюючого методу не враховуються такі параметри мікросхеми як якість виготовлення, умови експлуатації, електричні навантаження в схемі, підвищену температуру навколишнього середовища, вологість, збільшені вібрації, удари й т.і., тобто вважається, що апаратний засіб експлуатується в нормальних кліматичних умовах.

Основними параметрами є інтенсивність відмов наробіток до відмови й імовірність безвідмовної роботи протягом 10000 годин.

Як базові методи для розробки узагальнюючого методу пропонується використовувати:

- спрощений метод визначення надійності,

– метод розрахунку надійності пристроїв при експонентному законі наробітку до відмови.

При розрахунку надійності АЦП передбачається, що відмови елементів і компонентів є незалежними випадковими подіями, які підкоряються експонентному закону розподілу. У зв'язку з універсальністю експонентного закону розподілу й спрощенням розрахунків приймається гіпотеза про те, що всі інші процеси описуються також експонентним законом розподілу.

Суть даного узагальнюючого методу полягає у тому, що знаючи фактичну й номінальну потужність резисторів, фактичну й номінальну напругу конденсаторів, а також тип мікросхеми (аналогова чи цифрова) можна знайти інтенсивність відмов елемента, середній наробіток до відмови, гама-процентний ресурс, імовірність безвідмовної роботи протягом заданого інтервалу часу, інтенсивність відмов при зберіганні, середній термін зберігання, а також γ -відсотковий термін зберігання, що дає можливість прогнозувати точний строк експлуатації всього виробу [1-5].

В остаточному виді розрахунок надійності апаратного засобу для тензометрії за допомогою узагальнюючого методу слід проводити таким чином:

1) Визначається тип елемента й знаходяться коефіцієнти навантаження за формулами:

- для транзисторів

$$K=Pc/Pc\ max\ ,$$

де Pc – фактична потужність, що розсіюється на колекторі,

$Pc\ max$ – максимально припустима потужність розсіювання на колекторі.

- для діодів

$$K=I/Imax\ ,$$

де I – фактичний струм,

$Imax$ – максимально припустимий струм.

- для конденсаторів

$$K=U/U_н\ ,$$

де U – фактична напруга,

$U_н$ – номінальна напруга конденсатора.

- для резисторів і трансформаторів

$$K=P/P_н\ ,$$

де P – фактична потужність розсіювання на елементі,

$P_н$ – номінальна потужність.

2) По довіднику визначається λ_0 для даного елементу

3) Визначається інтенсивність відмов групи елементів по формулі:

$$\lambda = \sum_{i=1}^{N} n_i \lambda_i k_i\ ,$$

де n_i – кількість елементів або компонентів у схемі

λ_i - інтенсивність відмов і-го елементу або компоненту;

k_i – коефіцієнти, що враховують навантаження на елемент, умови експлуатації, конструктивні й технологічні відмінності й т.д.

4) При експонентному законі розподілу наробітку до відмови елементів і компонентів апаратного засобу ймовірність безвідмовної роботи і-го елементу або компоненту визначається по формулі:

$$P_i(t) = \exp(-\lambda_i(t))$$

Тоді

$$P\ (t) = \exp[-(\sum_{i=1}^{N} n_i \lambda_i)t] = \exp(-\lambda t),$$

де λ – інтенсивність відмов апаратного засобу (параметр масштабу розподілу відмов)

5) Інтенсивність відмов елементу при зберіганні становить:

$$\lambda_{хр} = \lambda_{егр} \frac{\lambda_{хр.г}}{\lambda_{б.г.}} k_{хр}$$

6) Середній термін зберігання становить:

$$t_{0.хр} = \lambda_{хр}^{-1}$$

7) γ -відсотковий термін зберігання (γ =95%) становить:

$$t_{хру} = \lambda_{хр}^{-1}\left(-\ln\frac{95}{100}\right)$$

Розраховуються характеристики надійності конструктивних елементів (рис. 1) конкретного АЦП СИМ-А04.07.1 та визначаються інтенсивність відмов й ймовірність безвідмовної роботи всієї схеми за допомогою:

– спрощеного методу визначення надійності;
– методу дифузійного закону наробітку до відмови;
– методу експонентного закону наробітку до відмови;
– узагальнюючого методу визначення параметрів надійності.

Порівнюючи реально отримані дані з теоретичними результатами всіх описаних у роботі методів, можна затверджувати, що узагальнюючий метод розрахунку надійності є самим оптимальним для АЦП СИМ-А04.07.1 при одержанні показника середнього наробітку до відмови та доступним й ефективним для розрахунків показників надійності. Однак, як видно із графіка, розроблений метод показує для СИМ-А04.07.1 достовірні результати ймовірності безвідмовної роботи, а також встановлює найбільш близькі до реальних даних, які отримані для високошвидкісного модуля аналогового вводу/виводу Micro PC: 5710-1 (середній час наробітку до відмови 70,2 роки). Даний модуль 5710-1 по своїх основних характеристиках дуже схожий з досліджуваним АЦП СИМ-А04.07.1, а це дає можливість стверджувати, що узагальнюючий метод, може використовуватися як для модифікацій АЦП СИМ-А04.07.1, так і для пристроїв максимально наближених за структурою зв’язку елементів, що мають схожі конструктивні особливості й основні характеристики.

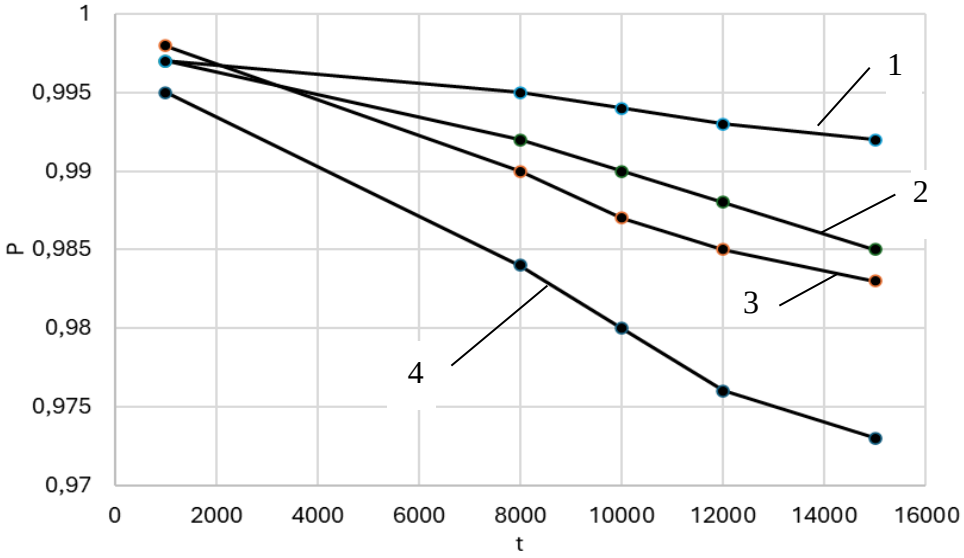


Рис. 1. Загальний графік залежності безвідмовної роботи від часу: 1 – спрощений метод; 2 – метод експонентного закону; 3 – метод дифузійного закону; 4 – узагальнюючий метод

Висновки. Основні наукові і практичні результати роботи полягають у наступному:

– проаналізовано сучасні методи визначення надійності апаратних засобів з метою визначення найбільш істотних факторів, що впливають на даний показник, а саме наробітку на відмову (частоти відмов), інтенсивності відмов, терміну служби пристрою. Доведено, що класичними методами неможливо чітко визначити дані параметри для АЦП у зв'язку з тим, що вони не враховують конкретних особливостей розробленого виробу. Цей факт підтверджує доцільність розробки удосконаленої методики розрахунку надійності.

– порівнюючи реально отримані дані з теоретичними результатами всіх описаних у роботі методів, можна затверджувати, що узагальнюючий метод розрахунку надійності є самим оптимальним для АЦП СИМ-А04.07.1 при одержанні показника середнього наробітку до відмови та доступним й ефективним для розрахунків показників надійності.

– крім імовірнісних характеристик, можливе одержання вартісно-ймовірносних характеристик АЦП. Для цього необхідно створити базу даних всіх використовуваних у пристрої елементів з необхідними параметрами для розрахунку ймовірності безвідмовної роботи й вартості конкретного елемента. З урахуванням цього можливо буде зіставити, наприклад, заміну резисторів з більшим коефіцієнтом навантаження на менший і показниками, що випливають на надійність й вартість пристрою.

– досліджено загальну методику розрахунку надійності для всіх електронних пристроїв з метою розробки узагальнюючої методики розрахунку частоти відмов для АЦП як базової методики для подальших розробок методик розрахунку оптимального показника ціна/надійність для АЦП.

– запропоновано використовувати розроблену методику визначення показника ціна/надійність для виконання експрес-аналізу різних модифікацій АЦП, а також пристроїв, максимально наближених за структурою зв'язку елементів і конструктивних особливостей. Є можливість створення надалі вичерпної бази даних використовуваних в АЦП елементів для зручності вибору замовником при мінімальній витраті часу необхідних конструктивних частин АЦП; прогнозування надійності й ціни для модифікованого їм АЦП.

Список літератури

1. ДСТУ 2992-95. Вироби електронної техніки. Методи розрахунку надійності.- Введ.01.01.96. К.:Вид-во стандартів, 1995. 78с.
2. Левин Б.Р. Теория надежности радиотехнических систем. М.:Сов.Радио,1978.
3. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги. Введ.01.01.96. К.:Вид-во стандартів, 1995. 38с.
4. ДСТУ 2860-94. Надійність техніки. Аналіз надійності. Введ.01.01.96. К.:Вид-во стандартів, 1994. 32с
5. Широков А.М. Надежность радиоэлектронных устройств. М.: Высшая школа, 1972.

DEVELOPMENT AND RESEARCH OF METHODS FOR DETERMINING THE RELIABILITY OF STRAIN GAUGES

Y.V. Shendryk[1], O.V. Golovachova[2], A.M. Yemets[3]

National Odessa Polytechnic University
1, Shevchenko Ave., Odessa, 65044, Ukraine
Emails: e.v.shendryk@op.edu.ua[1], holovachova@op.edu.ua[2], 6849765@stud.op.edu.ua[3]

The work analyzes modern methods for determining the reliability of hardware in order to determine the most significant factors affecting this indicator, namely the time to failure (failure rate), failure intensity, and device service life. The following are the main methods for determining the reliability of hardware: a simplified method for determining reliability, a method for calculating device reliability under the diffusion law of time to failure, and a method for calculating device reliability under the exponential law of time to failure. A comparative characteristic of the actually obtained data with the theoretical results of all the methods described in the paper is given. It is concluded that the generalized method for calculating reliability is the most optimal for obtaining the average time to failure indicator and is accessible and effective for calculating reliability indicators. It is noted that in addition to probabilistic characteristics, it is possible to obtain cost-probabilistic characteristics of the device, which is the basis for developing methods for calculating the optimal price/reliability indicator.
Keywords: strain gauges, hardware, reliability, methods for determining reliability, time to failure

DOI 10.15276/imms.v16.no1.204
УДК 004.942:378

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 204-209

ГРАФОВА МОДЕЛЬ ФОРМАЛІЗАЦІЇ СТРУКТУРНО-ЛОГІЧНИХ СХЕМ ОСВІТНІХ ПРОГРАМ

О.О. Шпинковський, В.О. Болтьонков

Національний університет «Одеська політехніка»
1, Шевченко пр., Одеса, 65044, Україна
Emails: alexandr.szpinkowski@gmail.com, vaboltenkov@gmail.com

Розглянуто проблему формалізацію структурно-логічних схем (СЛС) освітніх програм у закладах вищої освіти. Показано, що існуючі підходи до побудови СЛС мають суб'єктивний характер та часто не відображають реальних логічних залежностей між навчальними компонентами. Запропоновано використання графових методів для об'єктивного аналізу та проектування СЛС на основі компетентнісного підходу Tuning. На прикладі восьми загальних компетентностей Tuning продемонстровано визначення ключових компетентностей, оптимальної послідовності їх формування та аналіз міжгрупових зв'язків. Результати дослідження навіть такої обмеженої кількості компетентностей, показують, що компетентність «Робота у команді» є найбільш центральною, а компетентності «Стратегічне планування» та «Управління проектами» – ключовими елементами системи. 50% усіх зв'язків є міжгруповими, що підтверджує інтегрований характер сучасної освітньої програми. Запропонований підхід дозволяє усунути суб'єктивізм при проектуванні СЛС, забезпечити баланс між групами компетентностей та підвищити ефективність освітнього процесу.
Ключові слова: структурно-логічна схема, освітня програма, компетентності *Tuning*, матриця суміжності, орієнтований граф, спектральний аналіз, топологічне сортування.

Вступ. Реформа вищої освіти України 2014 року зумовила перехід від підготовки фахівців за спеціальностями до навчання за освітніми програмами. Ця зміна викликала необхідність розробки нових інструментів структурування навчального процесу, серед яких ключове місце займають структурно-логічні схеми (СЛС). СЛС визначають логічну послідовність вивчення дисциплін, узгодження їхнього змісту за темами в часі та встановлення міжпредметних зв'язків. Однак, як показують дані Національного агентства із забезпечення якості вищої освіти, значна частина освітніх програм має проблеми з проектуванням та структурою, що проявляється у формальному ставленні до побудови СЛС [1]. Аналіз практики різних ЗВО свідчить про існування різноманітних підходів до побудови СЛС, які часто носять суб'єктивний характер та не відповідають принципам системності та послідовності. У багатьох випадках СЛС зводяться до простих таблиць з переліком дисциплін за семестрами або схем з неінформативними зв'язками, що не відображають реальних залежностей між навчальними компонентами [2,3]. Це обумовлює актуальність розробки об'єктивних методів формалізації СЛС на основі математичного апарату. Сучасна парадигма вищої освіти базується на компетентнісному підході, зокрема на принципах проекту *Tuning*, який виділяє три групи загальних компетентностей: інструментальні, міжособистісні та системні [4]. Ця класифікація створює теоретичну основу для структурування освітніх програм, однак потребує конкретних інструментів реалізації. У роботі запропоновано використання графових методів для формалізації СЛС на основі компетентностей *Tuning*. Таким що відповідає реаліям часу при розробці освітніх програм у закладах вищої освіти є розробка математичного апарату та алгоритмів для об'єктивного аналізу та проектування структурно-логічних схем. Для обґрунтування актуальності та новизни запропонованого підходу необхідним є аналіз існуючих методологій та визначення їхніх обмежень.

Огляд існуючих підходів. Необхідність у точних, визначених інструментах структурування навчального процесу, особливо у сфері інформаційних технологій, є

очевидною. Аналіз літератури показує, що питання формалізації структурно-логічних схем (СЛС) освітніх програм залишається актуальним, але недостатньо розробленим з точки зору об'єктивних математичних методів [2,4]. Існуючі підходи часто базуються на експертних оцінках, що призводить до суб'єктивізму та недостатньої узгодженості між дисциплінами. У той же час, компетентнісний підхід Tuning став міжнародним стандартом, однак його практична реалізація у вигляді СЛС потребує формальних інструментів [4, 5]. Дослідження в галузі теорії графів та спектрального аналізу мереж показують потенціал використання матрично-графових моделей для аналізу складних систем, що може бути успішно адаптовано для освітніх програм [6].

Мета і задачі дослідження. Метою роботи є розробка графової моделі формалізації структурно-логічних схем освітніх програм, побудованих на основі компетентнісного підходу Tuning. Для досягнення мети треба вирішити такі задачі: провести практичну реалізацію графової моделі на прикладі восьми загальних компетентностей Tuning та виконати аналіз отриманих результатів.

Теоретичні засади проекту Tuning. Проект Tuning визначає загальні (універсальні) компетентності як основу для розробки освітніх програм. Їхня ключова ідея полягає у створенні збалансованої структури, що охоплює різні аспекти підготовки сучасного фахівця. Усі загальні компетентності класифікуються на три взаємопов'язані та ієрархічно організовані групи, що формують траєкторію розвитку від базових навичок до комплексних системних умінь.

Інструментальні компетентності (І). Вміння, пов'язані з інтелектуальними навичками, методами та інструментами. Формуються на ранніх етапах навчання та є основою для подальшого розвитку. До них належать, наприклад, аналітичні та логічні навички, критичне мислення, креативність, здатність до пошуку та обробки інформації [4,5].

Міжособистісні компетентності (М). Соціальні навички співпраці, комунікації та взаємодії. Розвиваються паралельно з інструментальними та інтегруються в системні. Ця група включає комунікацію, роботу в команді, лідерські якості, міжкультурну компетентність.

Системні компетентності (С). Стратегічні вміння керування складними системами та проектами. Є вершиною набуття компетентностей та базуються на двох попередніх групах. Сюди входять управління проектами, стратегічне планування, ініціативність та здатність до самостійного навчання.

Дана класифікація з її логічною послідовністю (І → М → С) утворює теоретичний каркас для побудови освітніх програм. Однак для трансформації цієї моделі у прагматичну структурно-логічну схему необхідний інструмент, здатний кількісно оцінити сили логічних зв'язків між конкретними компетентностями всередині та між групами, а також візуалізувати оптимальну послідовність їх формування.

Графова модель як інструмент формалізації. Для математичної репрезентації зв'язків між компетентностями пропонується використання орієнтованого графа $G = (V, E)$, де $V = \{v_1, v_2, ..., v_n\}$ – множина вершин (компетентностей), а E – множина орієнтованих ребер (логічних залежностей). Факт наявності залежності "компетентність v_i є основою для формування компетентності v_j" позначається ребром $(v_i, v_j) \in E$ [6]. Ступінь входу вершини $d^-(v_j)$ показує кількість компетентностей-передумов. Ступінь виходу $d^+(v_i)$ – кількість компетентностей, для яких дана є основою. Сума $d^-(v_j) + d^+(v_j)$ є мірою центральності вершини у схемі. Ясно, що граф G не містить орієнтованих циклів – це є логічною вимогою до СЛС). Залежність $GCi \rightarrow GCj$ встановлювалася, якщо компетентність GCi є необхідною передумовою або значно полегшує формування GCj.

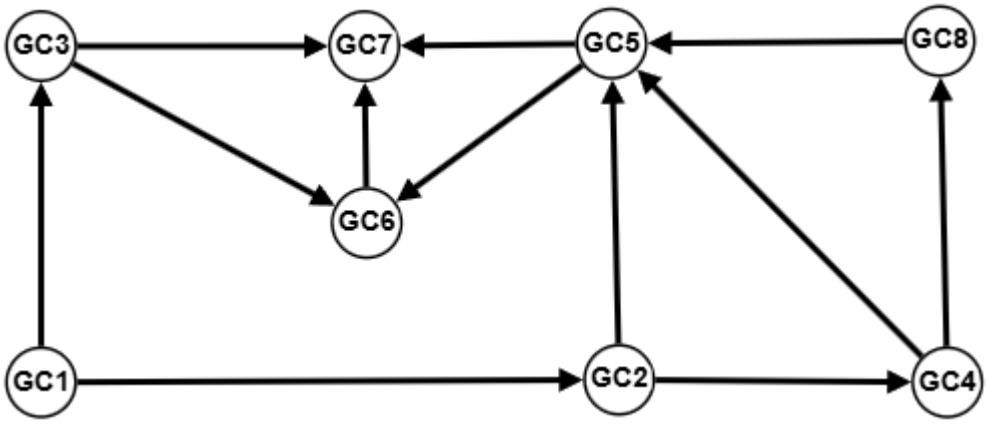


Рис.1. Граф зв'язків восьми компетентностей.

Обчислення ступенів вершин та визначення ключових компетентностей. На основі матриці А обчислено вхідні d^- та вихідні d^+ ступені кожної вершини-компетентності. Результати представлені в Таблиці 1.

Таблиця 1.

Ступені вершин та центральність компетентностей

Компете-нтність	Назва	Група (*Tuning*)	d^- (вхідний)	d^+ (вихідний)	Загальна центра-льність	Рей-тинг
GC1	Аналіз проблем	Інструмент.	0	2	2	5
GC2	Критичне мислення	Інструмент.	1	2	3	4
GC3	Креативність	Інструмент.	1	2	3	4
GC4	Комунікація	Міжособ.	1	2	3	4
GC5	Робота у команді	Міжособ.	3	2	5	1
GC6	Управління проектами	Системні	2	1	3	4
GC7	Стратегічне планування	Системні	3	0	3	4
GC8	Міжкультур-на компет.	Міжособ.	1	1	2	5

Для демонстрації роботи запропонованого математичного апарату було сформовано матрицю суміжності *A* для восьми загальних компетентностей *Tuning* (*GC*1–*GC*8). Елементи матриці $a_{ij} = 1$ були визначені на основі логічного аналізу залежностей між компетентностями експертами у сфері освітніх технологій проєкту *Tuning*. Залежність *GCi* → *GCj* встановлювалася, якщо компетентність *GCi* є необхідною передумовою або значно полегшує формування *GCj*.Отримана матриця *A* має розмірність 8×8:

На основі приведеного графу можна побудувати матрицю суміжності

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Спектральний аналіз матриці суміжності *A* дозволяє виявити її глобальні властивості. Для ациклічного орієнтованого графа, яким є модель СЛС, усі власні значення матриці суміжності дорівнюють нулю.

Це підтверджує відсутність циклів у графі та його ієрархічну, деревоподібну структуру. Спектральний радіус також свідчить про те, що граф є слабкозв'язним і має чітку спрямованість залежностей, що відповідає логіці наступності формування компетентностей.

Використовуючи модифіковану матрицю суміжності з демпфуванням, можна впевнено зазначити, що найбільшу вагу мають вершини GC5, GC7 та GC6, і це підтверджує їхню системоутворюючу роль та високий рівень впливу в мережі залежностей, виявлений раніше за допомогою ступенів

Аналіз результатів.

1. Ключові компетентності з максимальною центральністю: GC5 (Робота в команді) має найвищий показник загальної центральності (5), будучи вершиною з найбільшим вхідним ступенем $d^- = 3$. Це підтверджує її подвійну роль — як інтегратора різноманітних передумов (від аналізу до комунікації) і як фундаменту для системних компетентностей.

2. Системні компетентності як «приймачі»: GC7 (Стратегічне планування) має високий вхідний ступінь $d^- = 3$, але нульовий вихідний $d^+ = 0$. Це характеризує її як кінцеву, синтезовану компетентність, формування якої вимагає опанування попередніх.

3. Інструментальні компетентності як «джерела»: GC1-GC3 мають порівняно високі вихідні ступені, що підтверджує їх роль фундаменту, на якому будуються інші вміння [2].

Лінійне впорядкування вершин [6,7] задає одну з можливих логічних послідовностей їх формування GC1 → GC2 → GC4 → GC8 → GC5 → GC3 → GC6 → GC7

Інтерпретація освітньої траєкторії.

1. Початок (1-2 семестр): Старт з інструментальної GC1 (Аналіз проблем), потім перехід до GC2 (Критичне мислення). Паралельно або відразу після них доцільно вводити міжособистісну GC4 (Комунікація).

2. Середина (3-4 семестр): На основі комунікації будується GC8 (Міжкультурна компетентність), а потім – інтеграційна GC5 (Робота в команді). Інструментальна GC3 (Креативність) активно задіяна на цьому етапі для підготовки до проєктної діяльності.

3. Завершення (5-6 семестр): Фінальними етапами є опанування системних компетентностей: GC6 (Управління проектами) та, як вершина, GC7 (Стратегічне планування).

Ця послідовність не є єдино можливою, але вона математично обґрунтована та ідеально узгоджується з принципом *Tuning* про послідовне накопичення (Інструментальні → Міжособистісні → Системні).

Аналіз міжгрупових зв'язків – 50% усіх орієнтованих зв'язків у графі є міжгруповими. Це високий показник, який свідчить про глибоку взаємозалежність між інструментальними, соціальними та системними навичками. Найбільш тісні міжгрупові зв'язки спостерігаються між Інструментальною та Системною групами (напр., GC3→GC6, GC3→GC7), а також між Міжособистісною та Системною (GC5→GC6, GC3 → GC7). Це підтверджує, що формування системних компетентностей неможливе без розвитку як аналітичного мислення, так і соціальних навичок.

Обговорення результатів. Застосування графових методів для формалізації залежностей між компетентностями *Tuning* дозволило перейти від якісних описів до кількісного, об'єктивного аналізу структури освітньої програми.

1. Проведено підтвердження та уточнення теоретичної моделі *Tuning*: Математичний аналіз повністю підтвердив логіку послідовності «Інструментальні → Міжособистісні → Системні». Однак він також виявив, що GC5 (Робота в команді) є найважливішим інтеграційним вузлом, а не лише однією з міжособистісних компетентностей. Це вказує на потребу її центральної ролі в навчальному процесі.

2. Усування суб'єктивного впливу на формування освітньої програми: Запропонований підхід замінює суб'єктивні експертні судження щодо «важливості» тієї

чи іншої дисципліни на обчислювані метрики (ступені вершин, центральність). Це дозволяє обґрунтувати розподіл навчального навантаження та послідовність вивчення дисциплін.

3. Візуалізація та можливість оптимізації: Представлення СЛС у вигляді графа та його матриці надає наглядний інструмент для проектувальників програм. Виявлення вершин з низькою зв'язністю (наприклад, певні елективні курси) може стати приводом для перегляду їхнього змісту або місця у програмі для посилення інтеграції.

Висновки. Запропоновано каркас, що поєднує компетентнісну модель Tuning з апаратом теорії графів, що дозволяє перейти від якісного опису до формальної моделі залежностей між компетентностями. Розроблено модель на основі орієнтованого графа, що дає змогу кількісно оцінювати ступені вершин, виконувати топологічне сортування та спектральний аналіз. На прикладі восьми загальних компетентностей Tuning продемонстровано роботу моделі, визначено ключові компетентності (GC5 «Робота у команді», GC7 «Стратегічне планування», GC6 «Управління проектами») та побудовано оптимальну навчальну траєкторію. Отримані результати підтверджують інтегрований характер сучасних освітніх програм (50% міжгрупових зв’язків) та демонструють можливість усунення суб’єктивізму при проектуванні СЛС за рахунок використання об’єктивних математичних інструментів.

Перспективи подальших досліджень полягають у розширенні моделі через введення ваг ребер (для відображення сили залежності), адаптації її для профільних компетентностей конкретних спеціальностей, а також у розробці програмного забезпечення для автоматизації побудови та аналізу СЛС.

Список літератури

1. Квіт С. М. Річний звіт Національного агентства із забезпечення якості вищої освіти України за 2021 рік. Київ : НАЗЯВО, 2022. 156 с.
2. Код М.З., Петренко Л.С. Структурно-логічні схеми навчальних дисциплін: методологія побудови та аналізу : навч.-метод. посіб. Київ : Центр учбової літератури, 2020. 120 с.
3. Шпинковський О.О. Роль освітніх програм у формуванні компетентностей здобувачів вищої освіти. *Молодіжна наука: інновації та глобальні виклики. Міжнар. наук.-практ. конф. (Полтава, 06 листопада 2024 р.)*. Полтава : НУПП, 2024. С. 784–785.
4. 4.Tuning Project. Reference Points for the Design and Delivery of Degree Programmes in Computer Science. Bilbao : University of Deusto, 2008. 98 p.
5. 5.González J., Wagenaar R. Tuning Educational Structures in Europe. Universities' contribution to the Bologna Process. Bilbao : University of Deusto, 2008. 256 p.
6. 6.Harary F. Graph Theory. Reading, MA : Addison-Wesley, 1969. 274 p.
7. 7.Newman M.E.J. Networks: An Introduction. Oxford : Oxford University Press, 2010. 772 p.

О.О. Шпинковський, В.О. Болтьонков

GRAPHIC MODEL OF FORMALIZATION OF STRUCTURAL-LOGICAL SCHEMES OF EDUCATIONAL PROGRAMS

O. O. Shpinkovsky, V. O. Boltenkov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: alexandr.szpinkowski@gmail.com, vaboltenkov@gmail.com

The problem of formalization of structural-logical schemes (SLS) of educational programs in higher education institutions is considered. It is shown that existing approaches to building SLS are subjective in nature and often do not reflect real logical dependencies between educational components. The use of graph methods for objective analysis and design of SLS based on the Tuning competency approach is proposed. Using the example of eight general Tuning competencies, the definition of key competencies, the optimal sequence of their formation, and the analysis of intergroup relationships are demonstrated. The results of the study of even such a limited number of competencies show that the competency "Teamwork" is the most central, and the competencies "Strategic Planning" and "Project Management" are key elements of the system. 50% of all connections are intergroup, which confirms the integrated nature of the modern educational program. The proposed approach allows you to eliminate subjectivism in the design of SLS, ensure a balance between groups of competencies and increase the efficiency of the educational process.
Keywords: structural-logical scheme, educational program, Tuning competencies, adjacency matrix, directed graph, spectral analysis, topological sorting.

DOI 10.15276/imms.v16.no1.210
УДК 621.311:004.056

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 210-221

СТАНДАРТИЗАЦІЯ МОДЕЛЕЙ ЗАГРОЗ ДЛЯ СУЧАСНИХ БІЛІНГОВИХ СИСТЕМ ЕНЕРГЕТИКИ З IOT-ТЕХНОЛОГІЯМИ

П.В. Яворський, М.П. Кляп, М.П. Пригара, Т.В. Дитко

ДВНЗ «Ужгородський національний університет»
3, Народна пл., Ужгород, 88000, Україна
Emails: yavorskyi.petro@uzhnu.edu.ua, m.klyap@uzhnu.edu.ua,
mykhailo.prygara@uzhnu.edu.ua, taras.dytko@uzhnu.edu.ua

Сучасні білінгові системи енергетичного сектору та IoT-платформ виконують критично важливу функцію обліку послуг, формування транзакцій та обробки великих обсягів даних. Висока концентрація фінансової, персональної та телеметричної інформації робить їх об'єктами стратегічної значимості, де порушення цілісності чи доступності систем може призвести до значних фінансових втрат, зриву інфраструктури та ризиків для безпеки. Розвиток цифрових технологій, хмарних сервісів, API-інтеграцій та IoT-пристроїв створив нові вектори атак, включаючи експлуатацію вразливих конфігурацій, помилки управління доступом, недоліки IoT-протоколів, а також соціальну інженерію та DDoS-атаки, що підвищує цінність транзакцій та масштаби потенційних збитків. У зв'язку з цим кіберстійкість білінгових платформ потребує не лише технічних заходів, а й формування уніфікованої стандартизованої моделі загроз. Таке моделювання дозволяє системно оцінювати ризики, прогнозувати сценарії атак, виявляти ключові вразливості та розробляти багаторівневі механізми захисту, адаптовані до специфіки галузі. Сучасні підходи до моделювання загроз (STRIDE, LINDDUN, MITRE ATT&CK) частково покривають ризики, проте не забезпечують комплексного уніфікованого аналізу саме для білінгових систем. Тому актуальним є створення стандартизованої моделі, що враховує транзакційні особливості, інтеграційні канали, мережеву архітектуру та IoT-пристрої. Запропонована модель передбачає багаторівневий захист даних – від збору телеметрії на IoT-лічильниках до обробки на білінгових серверах. Використовуються криптографічні методи (AES-256, ECC), захищені протоколи передачі, багатофакторна автентифікація, системи моніторингу та виявлення аномалій. Архітектура забезпечує цілісність, автентичність, конфіденційність та стійкість операцій, а стандартизований підхід дозволяє адаптувати систему під різні мережеві та хмарні середовища. Ключові категорії загроз включають порушення конфіденційності, цілісності та доступності даних, а також специфічні ризики білінгу – підміни показників, компрометації IoT-пристроїв, маніпуляцій із тарифікацією та інтеграційними каналами. Об'єднання цих аспектів у єдину модель загроз дозволяє стандартизовано оцінювати вразливості, пріоритезувати ризики та оптимізувати заходи захисту, забезпечуючи безперервність роботи критично важливих систем.

Ключові слова: білінгові системи, моделювання загроз, стандартизація, кібербезпека, енергетика, IoT-пристрої, STRIDE.

Вступ. Сучасні білінгові системи є основою роботи енергетичних компаній, які використовують IoT-пристрої, забезпечуючи автоматизований облік послуг, формування транзакцій і обробку великих масивів даних. Щодня в цій сфері опрацьовуються мільярди записів із платіжною інформацією, персональними даними, телеметрією та критичними технологічними показниками, що робить білінгові платформи об'єктами стратегічної важливості. Порушення їхньої цілісності чи доступності може спричинити значні фінансові втрати, збої в інфраструктурі та ризики для національної безпеки. Розширення цифрової залежності та активне впровадження хмарних технологій суттєво ускладнили ландшафт кіберзагроз. Хмарні сервіси, API-інтеграції, мікросервіси та IoT-пристрої створили нові вектори атак, що включають експлуатацію вразливих конфігурацій, помилки керування доступами, недоліки IoT-протоколів і сучасні методи соціальної інженерії та DDoS-атак. Зростання обсягу

електронних транзакцій додатково підвищує цінність кожної операції та потенційний масштаб збитків від компрометації білінгових процесів. У таких умовах кіберстійкість білінгових систем стає критичною вимогою, яка потребує не лише технічного захисту, а й формування уніфікованої стандартизованої моделі загроз. Стандартизація дозволяє структурувати ризики, уніфікувати підходи до їх оцінювання та забезпечувати відповідність вимогам ISO/IEC 27001, ISO 22301, IEC 62443, OWASP [1] і NIST [2]. Моделювання загроз дозволяє завчасно виявляти ключові вразливості енергетичних систем, прогнозувати можливі сценарії атак і розробляти багаторівневі механізми захисту, адаптовані до специфіки галузі – від атак на критично важливі об'єкти енергетичної інфраструктури до масових компрометацій IoT-пристроїв. Інтеграція цих аспектів у єдину модель загроз забезпечує системний підхід до безпеки та підвищує стійкість цифрової енергетичної інфраструктури.

Мета дослідження полягає в розробленні уніфікованих та стандартизованих джерел загроз (рис.1) для сучасних білінгових систем у енергетичному та IoT-секторах, що забезпечує комплексне виявлення вразливостей, оцінку ризиків на різних рівнях платформи та формування ефективних заходів кіберзахисту відповідно до міжнародних стандартів.

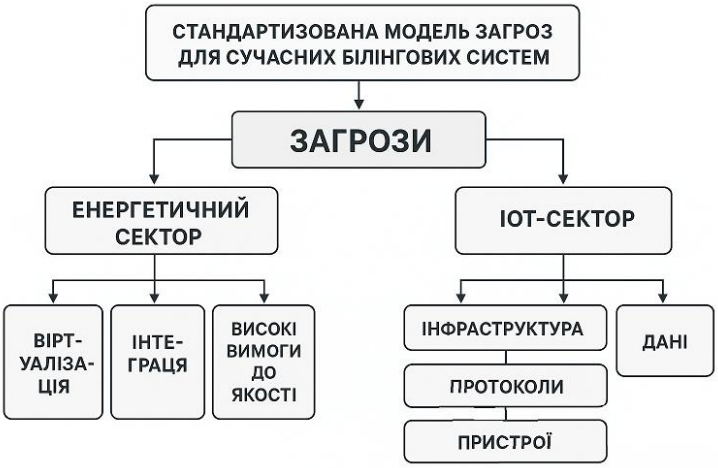


Рис. 1. Стандартизовані джерела загроз для білінгових систем енергетики та IoT

Теоретичні основи дослідження. Білінгові системи виступають ключовими елементами енергетичних операторів та провайдерів IoT-рішень. Вони забезпечують облік наданих послуг, тарифікацію, формування транзакційних записів, обробку платежів і взаємодію з клієнтськими сервісами. Їхня критичність зумовлена високою концентрацією чутливої інформації, яка охоплює персональні дані, детальні показники споживання, параметри мережевої активності та фінансові операції. Це робить білінгові системи об'єктами підвищеного ризику та вимагає застосування чітко визначених моделей загроз.

Основою теоретичного аналізу загроз для таких систем є класичні методи моделювання в інформаційній безпеці [3]. Універсальною та широко застосовуваною є модель STRIDE [4], яка класифікує загрози за шістьма категоріями, такими, як: S – Spoofing (підробка / ідентифікація); T – Tampering (пошкодження / модифікація даних); R – Repudiation (спростування / відмова від дій); I – Information Disclosure (розголошення інформації); D – Denial of Service (відмова в обслуговуванні); E – Elevation of Privilege (підвищення привілеїв), пов'язаними з порушенням конфіденційності, цілісності й доступності інформації. Проте ця модель не враховує специфіку транзакційного білінгу та регуляторні вимоги різних галузей. Інший актуальний підхід – LINDDUN [5] (Linkability (зв'язність), Identifiability (ідентифікація), Non-repudiation (відмова від дій), Detectability (виявлення), Disclosure of information (розголошення інформації), Unawareness (непоінформованість), Non-compliance (невідповідність правилам)) – орієнтований на загрози приватності, що є особливо важливим для енергетичного білінгу

та smart-meter інфраструктури, де дані можуть відображати поведінкові патерни користувача. Значне поширення отримала й модель MITRE ATT&CK [6], яка описує реальні техніки та тактики атак і дозволяє будувати повні сценарії порушення безпеки білінгових систем у контексті сучасних кіберзагроз. Важливим інструментом також є моделювання потоків даних, яке дає змогу виявляти точки потенційного впливу зловмисника у складних багатокомпонентних білінгових архітектурах.

Підґрунтям для моделювання загроз є міжнародні стандарти та галузеві специфікації. До універсальних відносять ISO/IEC 27001 [7] і 27002 [8], що визначають вимоги до побудови систем управління інформаційною безпекою, а також ISO/IEC 27019 [9] для енергетичної інфраструктури та ISO/IEC 30141 [10] для IoT-систем. В енергетичному секторі ключову роль відіграють стандарти DLMS/COSEM та IEC 62056 [11], що визначають протоколи обміну даними лічильників. У сфері IoT важливі рекомендації NIST, ETSI та специфікації безпеки MQTT/CoAP. Попри наявність великої кількості нормативних документів, вони не створюють цілісної та уніфікованої моделі загроз саме для білінгових систем.

Енергетичні білінгові платформи більш вразливі до модифікації даних smart-meter, підміни показників споживання, атак «людина посередині» під час передачі телеметрії та витоку поведінкових профілів користувачів. IoT-білінг характеризується ризиками клонування ідентифікаторів пристроїв, масових телеметричних атак, підробки даних сенсорів та компрометації нестійких до атак протоколів IoT-пристроїв.

Хоч значну кількість галузевих підходів, у сучасних дослідженнях відсутня універсальна, стандартизована та міждисциплінарна модель загроз, яка б охоплювала енергетичні системи з використанням IoT-пристроїв одночасно. Така модель є необхідною для підвищення порівнюваності ризиків, уніфікації засобів кіберзахисту, розроблення галузевих стандартів безпеки та створення узгоджених методів оцінювання вразливостей у критичних білінгових інфраструктурах.

Запропонована схема моделює процес безпечної передачі телеметричних даних від IoT-лічильника до централізованої білінгової системи. Архітектура передбачає багаторівневу модель захисту, яка охоплює формування даних, їх криптографічну обробку, передачу через потенційно незахищене мережеве середовище та подальшу перевірку на стороні серверної інфраструктури (рис.2).

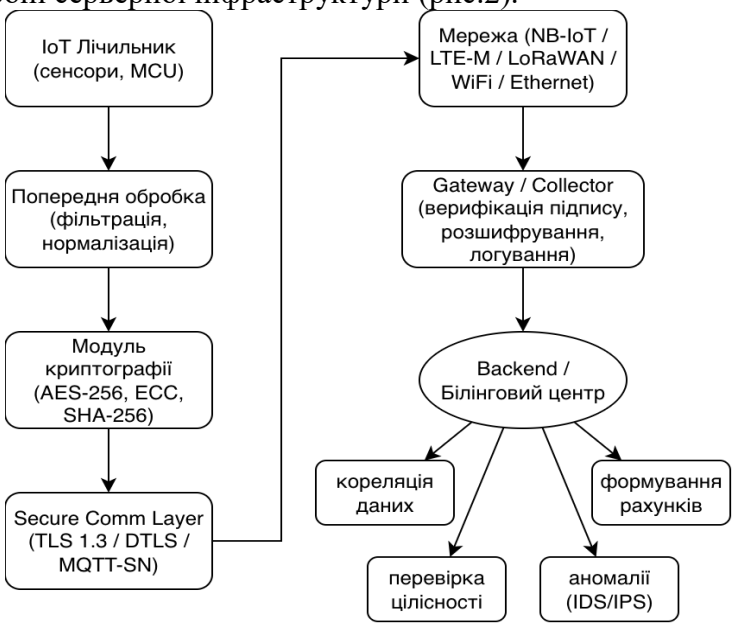


Рис. 2. Архітектурна схема захищеної передачі телеметричних даних IoT-лічильника в білінгову інфраструктуру

На першому етапі лічильник виконує збір та первинну обробку телеметрії. Після цього дані піддаються криптографічному підсиленню шляхом формування MAC-хеша або цифрового підпису, що забезпечує гарантії автентичності та цілісності. Подальше шифрування пакета (наприклад, за допомогою AES-256 або ECC-базованих алгоритмів) запобігає можливості несанкціонованого доступу під час передачі.

Передача даних здійснюється через захищений транспортний рівень – TLS 1.3, DTLS або протокол, який має вбудовані механізми шифрування та захисту (NB-IoT, LTE-M, LoRaWAN). Після доставки пакет надходить на шлюз збору даних, де виконується перевірка підпису, розшифрування та журналювання операцій. На наступному етапі дані передаються до білінгового центру, де додатково працюють системи виявлення вторгнень (IDS/IPS) та алгоритми виявлення аномалій, що дозволяє мінімізувати ризики атак типу man-in-the-middle, replay, підміни або генерації фальшивих значень. Такий підхід створює комплексну багаторівневу модель захисту, яка охоплює цілісність, конфіденційність, автентичність та спостережуваність процесів передачі даних. Архітектура може бути адаптована під різні типи IoT-мереж та рівні енергоспоживання, а також масштабована для інфраструктур, де необхідна висока достовірність телеметричних значень (енергетика, водопостачання, газорозподіл).

Постановка проблеми. Сучасні білінгові системи енергетики та IoT-фахівців функціонують у середовищі зростаючих кіберзагроз, високих вимог до безпеки та ускладненої архітектури. Вони обробляють великі обсяги критичних даних – від тарифікаційних записів і телеметрії до персональних та фінансових відомостей користувачів. Порушення їхньої цілісності або доступності може призвести до фінансових втрат, шахрайства, зриву послуг та підриву довіри споживачів, а в умовах цифровізації критичної інфраструктури ці ризики набувають стратегічного значення.

Попри численні міжнародні стандарти та рекомендації з інформаційної безпеки, наразі відсутня єдина уніфікована модель загроз саме для білінгових систем. Існуючі підходи фокусуються на окремих галузях або описують загальні аспекти захисту, не враховуючи специфіку білінгу. Наприклад, існуючі енергетичні стандарти регламентують інфраструктуру вимірювання та облік споживання, проте не охоплюють специфіку IoT-білінгових систем; загальні рекомендації з безпеки IoT не адаптовані до транзакційної логіки тарифікації. Внаслідок цього оператори застосовують несумісні підходи до моделювання загроз, що ускладнює оцінку ризиків, проведення аудиту та впровадження комплексного кіберзахисту. Додатково відсутність узгодженого термінологічного апарату та структурованої класифікації загроз перешкоджає співставленню ризиків між енергетичними та IoT-білінговими платформами. Це ускладнює формування єдиного стандарту безпеки, інтегрованих систем моніторингу та реагування на інциденти, а також планування розвитку платформ, сертифікацію та дотримання регуляторних вимог. Таким чином постає науково-прикладна проблема – створення уніфікованої моделі загроз, що враховує архітектурні особливості білінгових систем, відповідає міжнародним стандартам і забезпечує стандартизований аналіз, оцінку та мінімізацію ризиків в енергетичній та IoT-інфраструктурі.

Результати та обговорення. Дослідження показало, що сучасні енергетичні білінгові системи з IoT-пристроями вразливі до кіберзагроз через обробку великих обсягів фінансових та телеметричних даних. Класичні моделі загроз (STRIDE, LINDDUN, MITRE ATT&CK) частково покривають ризики, але не забезпечують уніфікованого підходу для білінгу. Розроблена багаторівнева схема захисту телеметрії демонструє ефективність інтеграції криптографії, захищених протоколів та систем виявлення аномалій. Впровадження стандартизованої моделі загроз забезпечує системний підхід до кібербезпеки та підвищує стійкість цифрової енергетичної інфраструктури.

Ключові категорії загроз для білінгових систем. Білінгові системи є високочутливими інформаційними комплексами, що обробляють персональні, фінансові, технічні та транзакційні дані. Через це їхній загрозовий ландшафт формується під впливом

широкого спектра ризиків, що охоплюють традиційні аспекти інформаційної безпеки та галузеві особливості енергетики й IoT-екосистем [12]. Основними групами загроз є порушення конфіденційності, цілісності та доступності, однак у випадку білінгу важливо враховувати також загрози автентичності, непричетності, коректності обліку та захищеності інтеграційних каналів.

Порушення конфіденційності охоплює широкий набір ризиків, пов'язаних із витоком персональних даних абонентів, інформації про платіжні інструменти, історії транзакцій, параметрів споживання та технічної телеметрії. У білінгових системах конфіденційність особливо важлива, адже дані часто містять як фінансову інформацію, так і дані, що характеризують поведінку користувача. В енергетичних системах витік профілів споживання може дозволити зловмисникам робити висновки про присутність користувачів удома чи їх поведінкові звички. У сфері IoT конфіденційність порушується при компрометації вузлів телеметрії, коли облікові дані пристроїв або їхні дані потрапляють до сторонніх осіб. Такі порушення майже завжди створюють підґрунтя для шахрайства, соціальної інженерії або вторинних атак.

Загрози цілісності є критично небезпечними, оскільки вони спрямовані на внесення неправдивої інформації в білінгові записи або маніпуляцію даними, на основі яких формується фінансовий результат. В енергетичних системах атакою може бути фальсифікація показників smart-meter, ін'єкція підроблених даних або підміна пакетів телеметрії. В IoT-білінгу можливими є атаки, пов'язані з генерацією фальшивої телеметрії або клонуванням ідентифікаторів пристроїв, що призводить до неправильного обліку наданих послуг. Зміна API-запитів, ПКС-операцій або сценаріїв тарифікації без належної авторизації призводить до значних фінансових втрат, помилкового нарахування платежів і порушення бізнес-процесів.

Загрози доступності спрямовані на виведення з ладу білінгових платформ або окремих компонентів їхньої інфраструктури. Типовими проявами таких загроз є DDoS-атаки на зовнішні та внутрішні сервіси, перевантаження білінгових процесорів великою кількістю запитів або телеметричних пакетів, блокування доступу до баз даних, порушення роботи дата-центрів або обчислювальних кластерів. У енергетиці та IoT додатковим фактором стають масові атаки на пристрої або шлюзи, які можуть створити штучне перевантаження мережі або ланцюгові відмови.

Окрім традиційних аспектів конфіденційності, цілісності та доступності, білінгові системи мають специфічні категорії загроз. До них належать загрози аутентичності та непричетності, які пов'язані з можливістю підміни користувача, пристрою або джерела даних. Наприклад, у енергетичних системах – це підміна smart-meter, в IoT – клонування пристроїв. Іншим важливим класом є загрози коректності обліку, коли атаки спрямовані не лише на зміну даних, але й на маніпуляцію алгоритмами тарифікації або логікою білінгових процесів, що може створювати значні збитки при масштабному застосуванні. Також вагоме місце займають загрози, пов'язані з інтеграційними механізмами. Білінг практично завжди працює з зовнішніми системами – CRM, OSS, платіжними шлюзами, мережевими вузлами, платформами збору телеметрії та API постачальників. Уразливості в цих інтеграційних каналах, а також недостатня автентичність джерела даних, слабкі механізми шифрування, недостатній контроль доступу або ін'єкційні атаки можуть стати причиною комплексного порушення роботи всієї інфраструктури.

Білінгові системи зазнають впливу широкого спектра кіберзагроз, що охоплюють як класичні аспекти інформаційної безпеки, так і специфічні галузеві ризики. Це обумовлює потребу в комплексній моделі загроз, здатній урахувати різноманіття технологічних платформ, особливості структур даних, сценарії інтеграції та логіку облікових операцій.

Технології та стандарти захисту. Забезпечення безпеки даних у сучасних білінгових системах вимагає застосування комплексного підходу, який поєднує криптографічні технології, механізми контролю доступу, мережевий захист, системи моніторингу та

спеціалізовані галузеві стандарти. Основою побудови такого захисту є вимоги міжнародних стандартів, зокрема ISO/IEC 27001, ISO/IEC 27002, рекомендацій сімейства NIST 800 [13], а також галузевих специфікацій DLMS/COSEM, ETSI та TM Forum, які визначають обов'язкові параметри безпеки для енергетичних та IoT-платформ.

Ключовим напрямом є застосування сучасних криптографічних методів. Шифрування даних у стані спокою та під час передавання є фундаментальною вимогою для захисту білінгової інформації, яка може включати фінансові транзакції, персональні дані споживачів. Найпоширенішим стандартом симетричного шифрування є AES-256 [14], який забезпечує високий рівень стійкості до криптоаналітичних атак і рекомендований NIST для використання в критичних інформаційних системах. Для захисту даних під час передачі використовуються криптографічні протоколи TLS 1.2/1.3 або SSL, що дозволяють забезпечити цілісність і конфіденційність у процесі взаємодії між білінговими сервісами та зовнішніми платформами. Додатковим рівнем безпеки виступають апаратні модулі керування ключами (HSM або KMS), які забезпечують створення, зберігання та ротацію криптографічних ключів у захищеному середовищі, унеможливлюючи несанкціонований доступ до ключового матеріалу навіть у разі компрометації окремих компонентів інфраструктури.

Важливою частиною захисту є побудова надійної системи автентифікації та авторизації. У білінгових системах, що взаємодіють із мільйонами користувачів і тисячами міжсистемних інтеграцій, класичної парольної автентифікації недостатньо. Сучасні платформи впроваджують багатофакторну автентифікацію (MFA), яка може включати SMS- або push-коди, TOTP-додатки, біометричні методи або апаратні токени, зокрема FIDO2-сумісні пристрої. Ці механізми відповідають рекомендаціям NIST SP 800-63 [15] щодо рівнів упевненості в автентифікації та ISO/IEC 29115 [16], які визначають вимоги до електронної ідентифікації та довірчих сервісів. Для міжсервісної взаємодії застосовуються стандартизовані протоколи авторизації, такі як OAuth 2.0, OpenID Connect та SAML, що дають можливість централізовано контролювати доступ і запобігати несанкціонованим API-викликам.

Мережевий захист білінгових платформ є ще одним фундаментальним напрямом забезпечення кібербезпеки. У багатокомпонентних архітектурах, які включають білінгові процесори, хмарні сервіси, бази даних та інтеграційні API, необхідно створювати сегментоване мережеве середовище з використанням брандмауерів нового покоління, систем виявлення та запобігання вторгненням (IDS/IPS), інструментів виявлення аномальної активності та захищених VPN-тунелів. Ці системи здатні своєчасно фіксувати нетипові запити, спроби порушення периметра, а також атаки, спрямовані на маніпуляцію білінговими процесами.

Важливою складовою комплексного захисту є інтегровані платформи моніторингу та реагування, зокрема SIEM-системи та технології SOAR. Вони дозволяють збирати логи подій із різних елементів білінгової інфраструктури, корелювати інциденти та автоматизувати процеси реагування на інциденти. Для білінгових систем, які працюють з високою інтенсивністю запитів, можливість виявляти аномалії на основі поведінкових моделей є критичною для запобігання зловживанням, фальсифікації транзакцій або атак на системи онлайн-тарифікації.

В енергетичних та IoT-платформах додаткову роль відіграють галузеві стандарти. В енергетичних системах протоколи DLMS/COSEM визначають механізми шифрування та автентифікації для smart-meter комунікацій, що забезпечує цілісність і автентичність переданої телеметрії. У сфері IoT важливими є вимоги ETSI EN 303 645, що визначають базові параметри кіберзахисту IoT-пристроїв, зокрема вимоги до оновлення прошивки, унікальних ідентифікаторів, шифрування даних і захисту від маніпуляцій.

Технології та стандарти захисту білінгових систем формують багаторівневий комплекс, який охоплює криптографічні механізми, автентифікацію та авторизацію, мережеву безпеку, моніторинг подій і галузеві стандарти функціонування. Усі ці

елементи мають бути узгоджені в єдиній системі, що забезпечує безперервний і стандартизований захист критично важливих білінгових платформ.

Архітектурні стандарти захисту. Архітектурні стандарти захисту сучасних білінгових систем формуються на основі вимог до високої доступності, безперервності бізнес-процесів і стійкості до кіберзагроз, оскільки енергетичні та IoT-білінгові платформи працюють у режимі реального часу та обробляють великі обсяги транзакцій. Провідною тенденцією є розподілена архітектура, що охоплює декілька незалежних дата-центрів та хмарних сегментів, розташованих у різних географічних регіонах. Такий підхід дає змогу забезпечити стійкість до техногенних аварій, фізичних загроз і кібератак, оскільки кожен із сегментів може виконувати функції резервування та взаємного дублювання. Георознесена інфраструктура дозволяє реалізовувати стратегії безперервності бізнесу з контрольованими показниками RTO та RPO відповідно до міжнародного стандарту ISO 22301 [17], забезпечуючи можливість відновлення повної функціональності системи навіть у разі втрати одного з основних центрів обробки даних.

Важливою складовою архітектури захисту є використання незалежних комунікаційних каналів, прокладених різними провайдерами або фізично віддаленими маршрутами. Це дозволяє уникати ситуацій, коли вихід з ладу одного каналу стає критичною точкою відмови для всієї білінгової платформи. У середовищах IoT-білінгу також застосовується мультиплексування технологій передачі (LTE-M, NB-IoT, LoRaWAN, Ethernet), що підвищує гнучкість маршрутизації та забезпечує додаткові можливості для обходу перевантажених або недоступних ділянок мережі. Паралельно з цим формуються дублювальні бази даних із застосуванням синхронної або асинхронної реплікації, кластерних конфігурацій і механізмів автоматичного перемикання на резервні вузли. Це критично важливо для забезпечення безперервної роботи модулів тарифікації, маршрутизації транзакцій, формування рахунків і сховищ історичних даних. Системи оркестрації (наприклад, Kubernetes або OpenShift) постійно контролюють стан застосунків, виконують перевірки їхньої працездатності та автоматично перезапускають або переносить контейнери у випадку виявлення аномалій. Захист мережевої інфраструктури вибудовується за принципами сегментації та ізоляції критичних компонентів. Мережа поділяється на зони довіри, між якими встановлюються суворі правила взаємодії, що відповідають підходам стандарта IEC 62443 [18]. Така структура дає можливість мінімізувати горизонтальне поширення атак у разі компрометації одного з компонентів. Для контролю взаємодії між сегментами застосовуються багаторівневі міжмережеві екрани, мікросегментація трафіку на рівні контейнерів або віртуальних машин, а також підхід Zero Trust, який передбачає постійний контроль доступу незалежно від того, де перебуває користувач або сервіс. У середовищах білінгів енергетики додатково впроваджуються вимоги NERC CIP щодо обмеження доступу до критичної інфраструктури, ведення журналів дій операторів і збереження повного трасування операцій.

Централізований моніторинг, що здійснюється через SIEM-системи, є фундаментальним елементом архітектурного захисту. Білінгові платформи генерують значні обсяги журналів, які необхідно агрегувати, аналізувати та корелювати між собою для виявлення аномальних подій. Завдяки інтеграції з системами SOAR можливе автоматичне виконання сценаріїв реагування: блокування підозрілої активності, ізоляція інцидентних вузлів, зміна маршрутів трафіку або запуск процедур аварійного перенесення на резервні середовища. Така автоматизація значно скорочує час реагування на інциденти, що критично для систем, у яких перебої роботи безпосередньо впливають на фінансові операції та якість обслуговування клієнтів.

У комплексі всі ці архітектурні заходи забезпечують відповідність білінгових систем міжнародним нормам IEC 62443, ISO 22301, NERC CIP та ISO/IEC 27001, формуючи стандартизований підхід до моделювання загроз, управління ризиками та забезпечення безперервності операційних процесів. Така структурована архітектура

дозволяє підвищити рівень кіберстійкості та гарантувати стабільну роботу білінгових платформ в енергетичній та IoT-сферах.

Стандартизована модель загроз. Стандартизована модель загроз для сучасних білінгових систем в енергетичній та IoT-сферах має охоплювати комплексну сукупність ризиків, які виникають на всіх рівнях функціонування платформи – від обробки даних і взаємодії з користувачами до мережевих комунікацій, інфраструктури та зовнішніх інтеграцій. Її формування ґрунтується на принципах системного аналізу, врахуванні специфіки предметної області та застосуванні міжнародних рекомендацій STRIDE, OWASP, ENISA та NIST, що дозволяє створити уніфіковану структуру оцінювання загроз для різних типів білінгових середовищ.

На рівні даних до моделі включаються загрози, пов'язані з можливістю витоку персональної, фінансової та транзакційної інформації, підміною або модифікацією критично важливих записів, несанкціонованим доступом до ключів шифрування та порушенням цілісності архівів. Особливої уваги потребує захист баз даних білінгу, оскільки вони містять інформацію про тарифи, облік споживання ресурсів, фінансові операції, ключі доступу до IoT-пристроїв та історію транзакцій користувачів. У системах енергетичного сектору додатковим ризиком є можливість маніпулювання показниками лічильників або втручання у балансування навантажень через зміну даних.

Рівень користувачів охоплює ризики, пов'язані з атаками на механізми автентифікації, соціально-інженерними методами викрадення облікових даних, шкідливими діями внутрішніх співробітників, а також сценаріями підвищення привілеїв. У білінгових платформах, де часто реалізується багаторівневий доступ (оператори, адміністратори, технічні користувачі, сторонні інтегратори), ці ризики посилюються різноманітністю ролей та складністю політик контролю доступу. Недоліки в автентифікації або відсутність багатофакторного захисту призводять до можливості компрометації облікових записів і подальшого впливу на розрахункові модулі, фінансові операції або дані користувачів.

Таблиця 1.

Пріоритезація вразливостей [19-21]

Vulnerability	Component	Likelihood	Impact	Risk
API key exposure	API Gateway	4	5	20
CDR tampering	Rating Engine	3	5	15
Queue flooding	Billing Queue	5	3	15

Мережевий рівень моделі загроз включає DDoS-атаки, сканування відкритих портів, атакування протоколів взаємодії між сервісами, ін'єкційні та інтерцепційні атаки, ботнет-активність, MITM-сценарії, спуфінг та маніпулювання маршрутами трафіку. У сучасних білінгових інфраструктурах, які широко застосовують мікросервісну архітектуру, різноманітні API, контейнеризацію та хмарні сервіси, мережеві загрози стають особливо актуальними, оскільки кожен сервіс відкриває нові потенційні точки входу для атак.

Інфраструктурний рівень охоплює загрози фізичних атак, аварій у дата-центрах, відмов обладнання, збоїв у роботі енергопостачання, пожеж, затоплень, а також ризиків, пов'язаних із хмарними провайдерами, включаючи компрометацію контейнерних середовищ або віртуальних машин. Значна частина білінгових платформ сьогодні розгортається у гібридних або мультихмарних середовищах, що потребує врахування додаткових загроз, пов'язаних з неправильними конфігураціями, недостатнім контролем доступу до хмарних ресурсів і помилками у політиках безпеки. У сфері енергетики

доцільним є врахування загроз, які впливають на критичну інфраструктуру та можуть викликати масові відключення або порушення роботи смарт-мереж.

Інтеграційні загрози стосуються взаємодії білінгових платформ з зовнішніми сервісами, API, платіжними шлюзами, IoT-платформами, сторонніми системами моніторингу, CRM та ERP. Типовими є API-атаки, експлуатація вразливостей у сторонніх бібліотеках, порушення цілісності передавання даних, підміна запитів, а також загрози, пов'язані з некоректною фільтрацією трафіку між зовнішніми та внутрішніми модулями. У системах IoT-білінгу окреме значення мають ризики компрометації вбудованих пристроїв, прошивок, протоколів MQTT та CoAP, що прямо впливають на точність збору показників і коректність нарахувань.

Об'єднання всіх перелічених складових у єдину стандартизовану модель загроз дає змогу комплексно оцінювати ризики, створювати уніфіковане середовище для аналізу вразливостей та визначати пріоритетні напрями захисту. Використання принципів STRIDE забезпечує структуровану класифікацію загроз за типами впливу – підміна, підробка, розкриття інформації, відмова в обслуговуванні, ескалація привілеїв, порушення цілісності. Дотримання рекомендацій OWASP гарантує актуальність моделі для сучасних веб- і API-орієнтованих білінгових систем. Такий підхід дозволяє сформувати узгоджену архітектуру безпеки, що однаково ефективно працює в енергетичних та IoT-середовищах, забезпечуючи належний рівень кіберзахисту та стійкість критичних процесів білінгу.

Висновки. Стандартизація джерел загроз для білінгових систем у сферах енергетики та IoT є невід'ємною складовою формування надійної та стійкої інфраструктури сучасних цифрових сервісів. Враховуючи стрімке зростання обсягів даних, інтенсивність транзакційних процесів і взаємодію систем у розподілених середовищах, саме уніфікований підхід до моделювання загроз дозволяє забезпечити системність аналізу, прогнозованість ризиків та ефективність реалізації захисних механізмів. Використання міжнародних стандартів, таких як ISO/IEC 27001, 27005, NIST SP 800-30, OWASP ASVS, MITRE ATT&CK та актуальних рекомендацій ENISA, створює методологічну базу, яка спрямовує організації на впровадження найкращих світових практик щодо кібербезпеки критичних платформ. Це не лише підвищує рівень взаємної сумісності архітектур і процедур безпеки, а й забезпечує можливість незалежного аудиту, коректного оцінювання захищеності та формування обґрунтованих технічних вимог для розробників та операторів білінгових систем.

Сучасні білінгові рішення є багаторівневими й часто включають локальні, хмарні, гібридні та периферійні компоненти, що формує додаткові вектори атак і збільшує складність забезпечення їх кіберстійкості. Відповідно, стандартизована модель загроз надає можливість комплексно оцінити потенційні ризики, починаючи від неправомірного доступу та маніпуляцій із транзакційними потоками і завершуючи глибшими загрозами, такими як компрометація модулів білінгу, викривлення показників споживання енергії або втручання у процеси тарифікації IoT-пристроїв. Чітке структурування загроз забезпечує формування погоджених сценаріїв реагування, оптимізацію політик доступу, правильну побудову криптографічного контуру та застосування механізмів багатофакторної автентифікації, що суттєво знижує можливість успішних атак на критичні компоненти систем.

Одним із ключових результатів стандартизації є можливість впровадження безперервного моніторингу загроз із використанням автоматизованих систем виявлення аномалій, кореляції подій, поведінкового аналізу та адаптивних механізмів реагування. У поєднанні з георезервуванням інфраструктурних елементів, розподіленими механізмами відновлення та цифровими сертифікаційними платформами це створює стійку екосистему, здатну функціонувати навіть у разі масштабних кібератак або збоїв на окремих вузлах мережі. Важливо також, що стандартизація сприяє підвищенню прозорості взаємодії між різними суб'єктами ринку – постачальниками послуг,

операторами інфраструктури, аудиторами, регуляторами та виробниками енергетичного обладнання.

Узагальнюючи, можна стверджувати, що стандартизація моделей загроз виступає фундаментом для розвитку захищених білінгових платформ, які відповідають вимогам кібербезпеки сучасного цифрового суспільства. Вона забезпечує ефективне управління ризиками, підвищує рівень довіри користувачів і бізнесу до критичних сервісів, формує основу для впровадження інновацій і зміцнює загальну кіберстійкість галузей, у яких точність, безперервність і безпека обробки даних мають вирішальне значення.

Список літератури

1. Лях І. М., Кіш Ю.В. Сучасні стандарти забезпечення інформаційної безпеки мобільних та Web-застосунків на прикладі OWASP TOP 10. *Національна безпека у фокусі викликів глобалізаційних процесів в економіці» XVI Міжнародна наукова Інтернет-конференція*. 2023. С. 41–44
2. Kaur J., Canto A. C., Kermani M. M., Azarderakhsh R. A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. arXiv, 2023. DOI: 10.48550/arXiv.2304.06222
3. Sulaiman N. S., Fauzi M. A., Wider W., Rajadurai J., Hussain S., Harun S. A. Cyber–information security compliance and violation behaviour in organisations: *A systematic review. Social Sciences*. 2022. No.11(9). DOI: 10.3390/socsci11090386
4. Mauri L., Damiani E. Modeling threats to AI-ML systems using STRIDE. *Sensors*. 2022. No.22(17). DOI: 10.3390/s22176662
5. Sion L., Van Landuyt D., Wuyts K., Joosen W. Robust and reusable LINDDUN privacy threat knowledge. *Computers & Security*. 2025. V.154. DOI: 10.1016/j.cose.2025.104419
6. Al-Sada B., Sadighian A., Oligeri G. Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. *IEEE Access*. 2024. No. 12, DOI: 10.1109/ACCESS.2023.3344680
7. ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems. Requirements. URL: https://www.iso.org/standard/27001
8. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/standard/75652.html
9. ISO/IEC 27019:2024. Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry. URL: https://www.iso.org/standard/85056.html
10. ISO/IEC 30141:2018. Internet of Things (IoT). Reference Architecture. URL: https://www.iso.org/standard/88800.html
11. IEC 62056-6-1. URL: https://webstore.iec.ch/en/publication/67916
12. Лях І.М., Кляп М.П., Шумило Н.Я., Ціпіньо А.Ю. Безпека IoT-протоколів як виклик для міжнародного співробітництва. *Наука і техніка сьогодні*. 2025. № 7(48). С. 1669-1681. https://doi.org/10.52058/2786-6025-2025-7(48)-1669-1681
13. NIST. Special Publication 800-series General Information. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
14. Mohammed Z. K., Mohammed M. A., Abdulkareem K. H., Zebari D. A., Lakhan A., Marhoon H. A., Martinek R. A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Applied Soft Computing*. 2024. V.158. DOI: 10.1016/j.asoc.2024.111588
15. NIST. Special Publication 800-63. Digital Identity Guidelines. URL: https://www.nist.gov/identity-access-management/projects/nist-special-publication-800-63-digital-identity-guidelines
16. ISO/IEC 29115:2013. Information technology. Security techniques. Entity authentication assurance framework. URL: https://www.iso.org/standard/45138.html

17. ISO 22301:2019. Security and resilience. Business continuity management systems. URL: https://www.iso.org/standard/75106.html
18. ISA/IEC 62443 series of standards. Security for industrial automation and control systems. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
19. Kabenge J. Vulnerability Management: Towards better vulnerability prioritisation, an automated proof of concept 2024 URL: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-242844
20. He J., Chen H. H., Yang K., Gao T., Cao Z. Automated Spam Call Traceback: Two Efficiency Enhancement Approaches. *IEEE Network*. 2025. DOI: 10.1109/MNET.2025.3591651
21. Yaegashi R., Hisano D., Nakayama Y. Queue allocation-based DDoS mitigation at edge switch. *IEEE International Conference on Communications Workshops*. 2021. P. 1-6. DOI: 10.1109/ICCWorkshops50388.2021.9473582

STANDARDIZATION OF THREAT MODELS FOR MODERN ENERGY BILLING SYSTEMS WITH IOT TECHNOLOGIES

P.V. Yavorskyi, M.P. Klyap, M.P. Prygara, T.V. Dytko

Uzhhorod National University
3, Narodna Square, Uzhhorod, 88000, Ukraine
Emails: yavorskyi.petro@uzhnu.edu.ua, m.klyap@uzhnu.edu.ua,
mykhailo.prygara@uzhnu.edu.ua, taras.dytko@uzhnu.edu.ua

Modern billing systems in the energy sector and IoT platforms perform a critically important function of service accounting, transaction processing, and handling large volumes of data. The high concentration of financial, personal, and telemetry information makes them strategically significant targets, where violations of system integrity or availability can lead to substantial financial losses, infrastructure disruptions, and security risks. The development of digital technologies, cloud services, API integrations, and IoT devices has created new attack vectors, including exploitation of vulnerable configurations, access management errors, weaknesses in IoT protocols, as well as social engineering and DDoS attacks, which increases the value of transactions and the potential scale of damage. In this context, the cyber resilience of billing platforms requires not only technical measures but also the development of a unified, standardized threat model. Such modeling enables systematic risk assessment, attack scenario forecasting, identification of key vulnerabilities, and the development of multi-layered protection mechanisms tailored to the specifics of the industry. Modern threat modeling approaches (STRIDE, LINDDUN, MITRE ATT&CK) partially address risks but do not provide a comprehensive, unified analysis specifically for billing systems. Therefore, the creation of a standardized model that considers transactional features, integration channels, network architecture, and IoT devices is highly relevant. The proposed model provides multi-layered data protection—from telemetry collection on IoT meters to processing on billing servers. Cryptographic methods (AES-256, ECC), secure transmission protocols, multi-factor authentication, and monitoring and anomaly detection systems are employed. The architecture ensures integrity, authenticity, confidentiality, and operational resilience, while the standardized approach allows adaptation of the system to different network and cloud environments. Key threat categories include violations of data confidentiality, integrity, and availability, as well as billing-specific risks—meter reading tampering, IoT device compromise, manipulation of tariffing, and integration channels. Combining these aspects into a single threat model allows standardized vulnerability assessment, risk prioritization, and optimization of protective measures, ensuring the continuous operation of critical systems.

Keywords: billing systems, threat modeling, standardization, cybersecurity, energy sector, IoT devices, STRIDE.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 16, номер 1, 2026. Одеса – 212 с., іл.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 16, No. 1, 2026. Odesa – 212 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 № 8 від 24.12.2025р.)

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