

**ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ
ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

Виходить 4 рази на рік

№ 83

Згідно Наказу МОН №1188 від 24.09.2020, п. №156 Додатку 5 «Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка» включено до категорії «Б» за спеціальностями:

- 124 – «Системний аналіз»;
- 126 – «Інформаційні системи та технології»
- 254 – «Забезпечення військ (сил)»
- 255 – «Озброєння та військова техніка»

КИЇВ – 2024

ISSN 2524-0056 (Print)

ISSN 2519-481X (Online)

**MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

**COLLECTION OF SCIENTIFIC WORKS
OF THE MILITARY INSTITUTE OF TARAS SHEVCHENKO
NATIONAL UNIVERSITY OF KYIV**

It comes out 4 times a year

№ 83

According to the Order of the Ministry of Education and Science No. 1188 from 09/24/2020, item No. 156 of Appendix 5 «Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv» is included in category «B» by specialties:

- 124 – «System analysis»;
- 126 – «Information systems and technologies»
- 254 – «Supply of troops (forces)»
- 255 – «Armament and military equipment»

KYIV – 2024

УДК621.43

ББК 32-26.8-68.49

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2024. № 83. 144 с.

Голова редакційної колегії:

Ленков С.В.

доктор технічних наук, професор, ВІКНУ;

Члени редакційної колегії:

Анісімов А.В.

доктор фізико-математичних наук, професор, член-кор. НАНУ, КНУ;

Барабаш О.В.

доктор технічних наук, професор, НТУУ «КПІ»;

Гунченко Ю.О.

доктор технічних наук, професор, ОНУ;

Жиров Г.Б.

кандидат технічних наук, старший науковий співробітник, КНУ;

Заславський В.А.

доктор технічних наук, професор, КНУ;

Карпінський М.П.

доктор технічних наук, професор, Університет у Бельсько-Бялій (Польща)

Лепіх Я.І.

доктор фізико-математичних наук, професор, ОНУ;

Петров О.С.

доктор технічних наук, професор, УНТ, Краків (Польща);

Погорілий С.Д.

доктор технічних наук, професор, КНУ;

Толок І.В.

кандидат педагогічних наук, доцент, НУЦЗУ;

Хайрова Н.Ф.

доктор технічних наук, професор, НТУ «ХП»;

Хлапонін Ю.І.

доктор технічних наук, професор, КНУБіА;

Шаронова Н.В.

доктор технічних наук, професор, НТУ «ХП».

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень і побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації – серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до Наказу МОН України від 24.09.2020 № 1188 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до категорії «Б» (технічні науки).

Затверджено на засіданні Вченої ради ВІКНУ від 19.09.24 р., протокол № 1.

Відповідальний за макет:

Сотніков Є.О.

Відповідальність за новизну і достовірність наведених результатів, тактико-технічних та економічних показників і коректність висловлювань несуть автори. Точка зору редколегії не завжди збігається з позицією авторів. Усі матеріали надруковані в авторській редакції.

Усі статті, що публікуються у збірнику, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів. Незважаючи на перевірку статей на антиплагіат остаточною відповідальністю за плагіат несуть автори.

Видання безкоштовне.

Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, у науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та в наукових бібліотеках України згідно списку МОН. Електронна версія збірника розміщена на відповідних сайтах.

Видання індексується Google Scholar.

Адреса редакції: 03189, м. Київ, вул. Ю. Здановської, 81, тел./факс +38 (044) 521 – 33 – 82

Наклад 50 прим. Ел.адреса редактора: lenkov_s@ukr.net

Офіційний сайт журналу: <http://miljournals.knu.ua>

UDC621.43

LBC 32-26.8-68.49

Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv.
K.: VIKNU, 2024. № 83. 144 p.

Chairman of the editorial board:

Lienkov S.V. doctor of technical sciences, professor, VIKNU;

Members of the editorial board:

Anisimov A.V.	doctor of physics and mathematics, professor, corresponding member of. NASU, KNU;
Barabash O.V.	doctor of technical sciences, professor, NTUU «KPI»;
Gunchenko Yu.O.	doctor of technical sciences, professor, ONU;
Zhyrov G.B.	candidate of technical sciences, senior researcher, KNU;
Zaslavsky V.A.	doctor of technical sciences, professor, KNU;
Karpins'kyj M.P.	doctor of technical sciences, professor, University of Bielsko-Biala (Poland)
Lepikh Ya.I.	doctor of physics and mathematics, professor, ONU;
Petrov O.S.	doctor of technical sciences, professor, UNT, Krakow (Poland);
Pogorilyy S.D.	doctor of technical sciences, professor, KNU;
Tolok I.V.	candidate of pedagogical sciences, docent, NUCP
Khairova N.F.	doctor of technical sciences, profecor, NTU «KhPI»;
Khlaponin Yu.I.	doctor of technical sciences, professor, KNUBiA;
Sharonova N.V.	doctor of technical sciences, professor, NTU «KhPI».

The editorial board strives to improve the content and quality of the publication and will be grateful to the authors and readers for their comments and wishes.

Registered by the Ministry of Justice of Ukraine, certificate of state registration of printed mass media – KV series No. 11541 – 413P from 07/21/2006.

In accordance with the Order of the Ministry of Education and Science of Ukraine from September 24, 2020 No. 1188, «Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv « is included in category «B» (technical sciences).

Approved at the meeting of the Scientific Council of VIKNU from 19.09.2024, protocol No1.

Responsible for the layout:
Sotnikov Y

The authors are responsible for the novelty and reliability of the given results, tactical-technical and economic indicators and the correctness of statements. The point of view of the editorial board does not always coincide with the position of the authors. All the materials are printed in the author's edition.

All articles published in the collection undergo a mandatory review, which is carried out anonymously for both authors and reviewers. Despite checking the articles for anti-plagiarism, the final responsibility for plagiarism lies with the authors.
The publication is free.

Copies of the collections are in the National Library of Ukraine named after V.I. Vernadsky, in the scientific library named after M. Maksymovych, in the library of the Military Institute and in the scientific libraries of Ukraine according to the list of the Ministry of Education and Science. The electronic version of the collection is posted on the relevant websites.

The publication is indexed by Google Scholar.

Address of the editorial office: 03189, Kyiv, str. Y. Zdanovska, 81, phone/fax +38 (044) 521 – 33 – 82

Edition of 50 copies. E-mail address of the editor: lenkov_s@ukr.net

Official website of the journal: <http://miljournals.knu.ua>

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Banzak O.V., Lienkov S.V., Sieliukov O.V., Gaber A.A. Methods and means of control of nuclear materials and status of protective barriers at npp in wartime conditions	7
Адамов Ю.І., Завальнюк В.В. Методика визначення віддаленого десантування парашутно-реактивної системи	17
Гайша О.О., Онищенко О.А., Гайша О.О. Аналіз якості функціонування системи нечіткого управління заспокоювачем хитавиці реактивної дії	27
Кривцун В.І., Голушко С.Л. Методика розрахунку основних параметрів осколкових вибухових пристроїв направленої дії для ураження повітряних цілей типу БПЛА	35

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Братченко Г.Д., Гончарук А.А., Абрамов С.В., Дуйловський А.О. Розв'язання мультимодальної транспортної задачі з урахуванням обмежень логістичних показників	47
Власенко В.В., Міночкін Д.А. Огляд механізмів root cause аналізу телекомунікаційних мереж	58
Джулій В.М., Філюк Є.В. Метод багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation	65
Ленков С.В., Гришак О.М., Охромович М.М., Сотніков Є.О. Аналіз сучасних та традиційних методів проектування і виробництва військової техніки з використанням автоматизованих інформаційних систем	82
Максименко Ю.А., Маміч В.В., Дідик В.О., Шаршаткін Д. Ю., Король Д. А. Дослідження можливостей структурованих аналітичних методів у розвідувальній інформаційній роботі	100
Субач І.Ю., Власенко О.В. Методика виявлення кіберінцидентів сітєм-системою в базах даних інформаційно-комунікаційних систем військового призначення	107

ЗАГАЛЬНІ ПИТАННЯ

Германенко Л.М., Шинкаренко О.М. Соціокультурний аналіз трансформацій гендерної структури військової сфери: вітчизняний та зарубіжний досвід	122
Дані про авторів	134
Алфавітний покажчик	135
Редакційна політика та етичні норми	136
Порядок подання і оформлення статей до «Збірника наукових праць Військового інституту Київського національного університету імені Тараса Шевченка»	138

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

Banzak O.V., Lienkov S.V., Sieliukov O.V., Gaber A.A. Methods and means of control of nuclear materials and status of protective barriers at npp in wartime conditions	7
Yu. Adamov, V. Zavalniuk Methodology for determining the remote landing of a parachute-jet system	17
Haisha O.O., Onishchenko O.A., Haisha O.O. Functioning quality analysis of the fuzzy control system of a reactive ship stabilizer	27
Kryvtsun V.I., Holushko S.L. Methodology for calculating the main parameters of fragmentation explosive devices for destruction of air targets of the bpl type	35

INFORMATION TECHNOLOGIES

Bratchenko H.D., . Honcharuk A.A., Abramov S.V., Duilovskyi A.O. Solving of the multimodal transportation problem taking into account limitations of logistics indicators	47
Vlasenko V.V., Ph.D. Minochkin D.A. Overview of root cause analysis mechanisms for telecommunication networks	58
Dzhuliy V.M., Filyuk E. Method of multi-party computation management of cryptoassets based on multi-party computation technology	65
Maksimenko Yu.A. Mamich V.V. Didyk V.O. Sharshatkin D.Y. Korol D. A. Research of the possibilities of structured analytical methods in intelligence information work	82
Lienkov S.V., Grishchak O.M., Okhramovych M.M., Sotnikov Y.O. Analysis of Modern and Traditional Methods of Designing and Manufacturing Military Equipment Using Automated Information Systems	100
Subach I., Vlasenko O. Methodology for Detecting Cyber Incidents by SIEM System in Databases of Military Information and Communication Systems	107

GENERAL QUESTIONS

Hermanenko L.M., PhD. Shynkarenko O.M. Socio-cultural analysis of transformations of the gender structure of the military sphere: domestic and foreign experience	122
Data on Authors	134
Alphabetical Index	135
Editorial policy and ethical standard	136
The order of submission and registration of articles to the "Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv "	138

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

UDC 531:535

Dr. Tech. Sci., prof. **Banzak O.V.** (SUITC)
Dr. Tech. Sci., prof. **Lienkov S.V.** (VIKNU)
Dr. Tech. Sci., prof. **Sieliukov O.V.** (SNU China)
Ph.D **Gaber A.A.** (SUITC)

DOI: <http://doi.org/10.17721/2519-481X/2024/83-01>

METHODS AND MEANS OF CONTROL OF NUCLEAR MATERIALS AND STATUS OF PROTECTIVE BARRIERS AT NPP IN WARTIME CONDITIONS

The level of development and application radiations technologies is largely determined by the state of nuclear instrumentation. In a relatively short period of time, this industry went through several stages of development, and each them was marked by the appearance of various devices that register and measure the parameters of ionizing radiation nuclear materials: gas discharge counters, scintillators, semiconductor detectors, and others.

The appearance of modern semiconductor radiation sensors for the first time connected nuclear instrumentation and electronics into a single complex - a semiconductor detector. It combines a semiconductor primary converter of ionizing radiation (sensor), a secondary converter of information from the sensor (electronics) and software for processing this information, which are interconnected by the problem to be solved and parameters. However, the development of atomic energy, spread of nuclear technologies in various industries has put forward new requirements for the control and metrology of ionizing radiation, which cannot be fully satisfied by modern level of nuclear instrumentation and applied nuclear physics research. The new generation radiation sensors and measurement systems based on them created in this work open up previously unknown opportunities in solving the problems of nuclear fuel analysis, increasing the accuracy and efficiency of monitoring technological parameters and the state of protective barriers in nuclear power plants, and creating means for MASATE inspections.

In the work, the use of algebraic reconstructive passive tomography (APT) methods for the reconstruction of the image of the internal structure of heat-emitting assemblies is proposed for the first time. For this purpose, a new algorithm for passive tomography of nuclear fuel was developed using the example of VVER-1000, which uses the method of angular projections own radiation of heat-emitting assemblies (HEA). Computer tomography experiments of this object showed that radiation intensity measurements at 360 points of the detector location relative to HEA axis are optimal for two or more values of the gamma radiation energy of the reference isotope ^{134}Cs . In this case, the proposed APT method makes it possible to identify defective tvels cells with a leakage level of more than 30% on restored tomograms, as well as the absence of tvels cells in HEA.

Key words: radiation sensors, ionizing radiation of nuclear materials, passive tomography, tvels

Introduction. The key problem of nuclear power engineering – radiation safety – is solved by ensuring the reliability of protective barriers of the main objects of the technological process of AES operation: tvels, fuel assemblies (FA), coolant transfer circuits, etc.

To implement the algorithm of computed tomography of WCPR-1000 nuclear fuel, a modern CdZnTe-detector with high resolution or a set of spatially distributed detectors, a digital gamma-spectrometric path and a medium-performance computer for processing and interpreting the tomography results are required. There are several possible ways to form spatial projections of FA self-radiation field: discrete angular movement of the controlled FA around its own axis, placement of a sufficiently large number of detectors around the controlled FA, placement of gamma-detector matrices at several angular positions around the FA. Regardless of the method of implementing computed tomography, radial movement of the gamma detector or the controlled FA seems to be very complex from a design point of view. Therefore, further computer tomography of nuclear fuel is studied only for angular projections of the fuel assembly's own radiation [1-3].

Analysis of previous studies. Methods of tomographic analysis of objects of various physical nature, i.e. reconstruction of the physical structure of an object by physical fields measured outside the object, as a rule, on a closed surface, originated in the 1970s in connection with the construction of X-ray tomographic images of human organs [1,2]. In the 1980s, tomographic methods were already widely used in industry for flaw detection [3-5]. Most of the methods developed to date, as a rule, use active tomography, which assumes the presence of a radiation source passing through the object being examined, and a receiver (or group of receivers) recording the radiation passed through the object. To analyze the state of nuclear fuel (NF), in particular, fuel assemblies, it is advisable to use passive emission tomography based on recording the intrinsic gamma radiation of fission products (FP) of NF with subsequent determination of their activity inside the studied FA.

Formation of the problem. In recent years, some attention has been paid to the use of high-energy microparticles in solid-state electronics: fast electrons and neutrons, protons, gamma-quanta. The diversity of nature of such microparticles in itself indicates a wide range of possibilities for controlling (modifying) the parameters of solid-state electronics products with their help. However, the prejudice caused by the destructive effect of such microparticles under nuclear explosion conditions, the danger of their flows for operators and the associated problems of using generators - all these are factors that hinder the development of this scientific and technical direction.

Results. To implement the developed algorithm for computed tomography of WCPR -1000 nuclear fuel (NF), a modern high-resolution CdZnTe-detector or a set of spatially distributed detectors, a digital gamma-spectrometric path, and a medium-performance computer for processing and interpreting the tomography results are required. Several methods are possible for forming spatial projections of FA self-radiation field: discrete angular movement of the monitored FA around its own axis, placement of a sufficiently large number of detectors around the monitored FA, placement of gamma-ray detector matrices at several angular positions around the FA. Regardless of the method for implementing computed tomography, radial movement of the gamma detector or the monitored FA seems to be very complex from a design point of view. Therefore, further computed tomography of NF is studied only for angular projections of FA self-radiation [7, 9].

When the detector is located at n -th observation point at a distance R_n from FA axis, the measured gamma-radiation intensity of i -th isotope with energy E_{γ_j} at the detector location point is equal to:

$$I_n^i = \sum_m A_{mi} k_{ij} w_{mn} \varepsilon(E_{\gamma_j}), \quad (1)$$

where A_{mi} – activity of i -th isotope for m -th fuel element taking into account its actual state; k_{ij} – yield of the gamma line with number j for i -th isotope; w_{mn} – contribution coefficient of m -th fuel element to the radiation intensity of i -th isotope with energy E_{γ_j} , taking into account the attenuation effects during propagation of the gamma radiation beam from m -th fuel element to n -th observation point; $\varepsilon(E_{\gamma_j})$ – detection efficiency of the detector for energy E_{γ_j} , $m=1, \dots, M$, where M – is the total number of fuel elements in the fuel assembly.

When measuring in the selected peak of total absorption of a specific reference isotope, the constants can be omitted k_{ij} , $\varepsilon(E_{\gamma_j})$ and expression (1) can be written in a simplified form:

$$I_n = \sum_m A_m w_{mn}. \quad (2)$$

The principle of tomographic study of fuel assemblies consists of performing n measurements

of γ -radiation intensity for different mutual arrangements of the detector and fuel assemblies, in particular, for different angular positions of the detector. This makes it possible to form a system of n equations of the form (2), which is usually called a projection system in algebraic reconstructive tomography, in this case - angular.

The task of algebraic reconstructive tomography is to reconstruct m values of the activity of fuel elements A_m inside the fuel assembly for the selected reference isotope by solving the resulting system of equations. In this formulation, in this paper (in contrast to [7, 8]), we formulate tomography problem according to the principle of "one fuel element - one pixel of the reconstructed tomogram". More detailed tomography is possible - by dividing the cross-sectional area of fuel element into several pixels in accordance with the specific geometry of the fuel assembly. However, the modeling results presented below show that this is not practically necessary.

When solving the problem of reconstructing the fuel assembly tomogram and modeling field formation at the detector location, a number of assumptions were used:

- problem is considered in a flat section of the fuel assembly and fuel rods, i.e. vertical non-uniformity of the fission product activity distribution over fuel rods is not taken into account;
- fuel rod is considered as a homogeneous cylinder with gamma-activity A_m ;
- effects of radiation scattering on the fuel assembly structural elements are not taken into account;
- of practical interest are sufficiently large distances of the detector from the fuel assembly axis (about 25 cm), therefore the geometric effects of the collimator are not taken into account; at the specified distances, the assembly is visible from the detector location at a sufficiently small angle (less than 300), therefore it can be assumed that the radiation passes through the collimator without geometric losses.

To solve the problem, a rectangular coordinate system XOY with the origin in the geometric center of the fuel assembly was introduced (fig. 1). All fuel elements and rod guides are numbered in horizontal rows, starting from the upper left. The coordinates of each fuel element or rod hole (x_m, y_m) are found based on the correct triangular symmetry of the structure, with a period of 12.75 mm.

The detector coordinates are initially specified in polar coordinates (ρ, θ) (the pole θ coincides with the origin 0, the angle is measured counterclockwise), and then converted to rectangular (x_0, y_0) . The further steps of the algorithm are as follows.

Step 1. For each n -th detector (x_{0n}, y_{0n}) position and each m -th fuel element with the coordinate of the center, the equation of the straight line passing through the detector location point and the center of m -th fuel element is found:

$$Ax + By + C = 0. \quad (3)$$

The coefficients of this line are determined by relations:

$$A = -(y_{0n} - y_m), \quad (4)$$

$$B = x_{0n} - x_m, \quad (5)$$

$$C = -y_m(x_{0n} + x_m) + x_m(y_{0n} + y_m). \quad (6)$$

Step 2. For each i -th fuel element with coordinates of the center (x_i, y_i) , through which gamma radiation from fuel element m passes, the distances along the normal from its center to the line $Ax+By+C=0$ are calculated:

$$d_i = \frac{Ax_i + By_i + C}{\sqrt{A^2 + B^2}}. \quad (7)$$

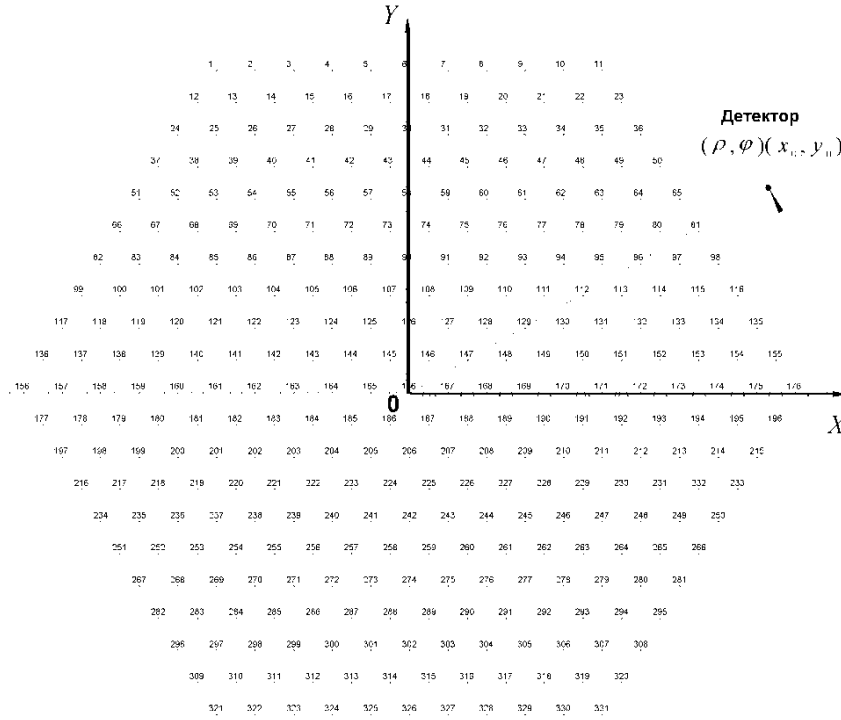


Figure 1 – Cartogram FA. Geometry of tomogram reconstruction problem

Step 3. The fuel elements through which the radiation from a given fuel element passes on its way to the detector are determined. These fuel elements must satisfy two conditions:

- fall within the “corridor” equal to the radius of the fuel element (0.455 cm);
- be located at a distance from the detector no greater than the emitting fuel element.

Step 4. For each of the fuel elements located in the radiation path, the free path in material of the zirconium cladding of the fuel element is found:

$$L_{Zr i} = 2\sqrt{R_H^2 - d_i^2} - 2\sqrt{R_{\theta H}^2 - d_i^2}, \quad (8)$$

where R_H and $R_{\theta H}$ – are outer and inner radii of the fuel element, respectively; d_i – distance along the normal from the center of the fuel element to the line $Ax+By+C=0$.

And in uranium dioxide:

$$L_{UO_2 i} = 2\sqrt{R_{\theta H}^2 - d_i^2}. \quad (9)$$

Step 5. If there are core holes among the fuel elements found according to condition of point 3, then values of the mean free paths in them are excluded from array $\{L_{Zri}, L_{UO_2i}\}$.

Step 6. For all fuel elements, the sums L_{Zri} and L_{UO_2i} are found, which are the total values of the mean free path of radiation in Zr and UO₂. The total attenuation of radiation from m -th fuel element on the way to the detector in the fuel element materials will be:

$$P_{\Sigma}^{(m)} = \exp(-(\mu_{Zr} \sum_i L_{Zri} + \mu_{UO_2} \sum_i L_{UO_2i})). \quad (10)$$

Step 7. The total mean free path of gamma beam from emitting fuel element to the detector is:

$$\sqrt{(x_m^2 - x_{0n}^2)^2 + (y_m^2 - y_{0n}^2)^2}. \quad (11)$$

Step 8. The mean free path in water (both inside the assembly and outside it) will be:

$$\sqrt{(x_m^2 - x_{0n}^2)^2 + (y_m^2 - y_{0n}^2)^2} - \sum_i L_{Zri} - \sum_i L_{UO_2i}, \quad (12)$$

and the total attenuation of radiation of a single m -th fuel element in water, respectively, is:

$$P_{H_2O}^{(m)} = \exp(-\mu_{H_2O} (\sqrt{(x_m^2 - x_{0n}^2)^2 + (y_m^2 - y_{0n}^2)^2} - \sum_i L_{Zri} - \sum_i L_{UO_2i})). \quad (13)$$

Step 9. The contribution coefficient of each m -th fuel element is calculated as:

$$w_{mn} = \frac{S_{det} P_{\Sigma}^{(m)} P_{H_2O}^{(m)}}{4\pi R_{mn}^2}. \quad (14)$$

When modeling the tomography algorithm, the modeled activity distribution over the fuel elements inside fuel assembly is specified A_m , $m=1, \dots, 312$, and the radiation intensity at n -th point of the detector location is calculated:

$$I_n = \sum_m w_{mn} A_m. \quad (15)$$

Algorithm for calculating the Moore-Penrose pseudoinverse matrix.

A matrix X of dimensions $n \times m$ is called the Moore-Penrose pseudoinverse matrix for the matrix A ($m \times n$), if it satisfies the following four conditions:

1. $AXA = A$.
2. $XAX = X$.
3. AX is symmetric.
4. XA is symmetric.

It can be shown that such a matrix always exists and is unique [10]. The pseudoinverse matrix is denoted by $A^\#$. The pseudoinverse matrix is calculated using the singular value decomposition

algorithm (SVD-decomposition, SVD-algorithm) [10,11].

The singular value decomposition of a real matrix A ($m \times n$) is any factorization of the form:

$$A = U \Sigma V^T, \quad (16)$$

where U – is an orthogonal ($m \times m$) matrix; V is an orthogonal ($n \times n$) matrix; Σ – is a diagonal ($m \times n$) matrix, whose singular values $\sigma_{ij} = 0$ at $i \neq j$ and $\sigma_{ii} = \sigma_i \geq 0$.

Taking into account the above definitions, the pseudoinverse matrix can be calculated using the SVD-decomposition algorithm by the relation:

$$A^\# = V \Sigma^\# U^T. \quad (17)$$

The pseudoinverse matrix is related to the problem of least squares method (LSM) by the fact that vector x of the smallest length, minimizing form $\|Ax - b\|$, can be expressed as $x = A^\# b$ in the sense of minimum residual LSM. Such a calculation is a regularizing procedure, which is convenient for solving ill-posed problems that are very sensitive to measurement noise. The problem of reconstructive emission tomography of fuel assemblies is one of such problems. Thus, by using Moore-Penrose pseudoinverse matrix to solve a system of projection equations, we not only organize an effective computational procedure, but also apply a regularization algorithm that smooths out measurement noise to a certain extent.

If the last relation $A^\# = V \Sigma^\# U^T$ is written out element by element for $i=1, \dots, n$ and $j=1, \dots, m$, we obtain a direct algorithm for calculating the elements of pseudoinverse matrix [14,15]:

$$a_{ij} = \sum_{\sigma_k \neq 0} \frac{v_{ik} u_{jk}}{\sigma_k}. \quad (18)$$

To study the process of restoring the fuel element activities, a series of experiments were conducted in which the initial data contained a defective fuel element. The decrease in the activity of such a fuel element was set within the range from 10 to 50% of the nominal value.

During the experiments, systems of equations of the form (3) were formed for different energies, noise levels and the number of measurements. Then these systems were solved using the SVD decomposition method.

A preliminary analysis of the obtained tomograms showed that there are no generally accepted criteria for assessing the quality of determining the fuel element activity. Therefore, it was decided to study the reconstructed tomograms in terms of the relative dispersion δ_i^* of the deviation of fuel element activities within the entire tomogram, relative dispersion of deviation fuel element activities within one row A_i^{max} , maximum deviation of the activity within one row and the histogram of the deviation of the fuel element activities. To calculate δ^* and δ_i^* dispersion of the fuel element activity original model and the dispersion of fuel element activity within the corresponding row were taken as reference point, respectively.

The analysis of reconstructed tomograms allowed us to draw an important conclusion: with an increase in the number of measurements, the quality of reconstructed tomograms improves insignificantly. An idea of determining the activity fuel elements by several energy values was proposed. From a computational point of view, there is no particular difference whether to reconstruct a tomogram by 720 detector readings or by 360 for two energy values. Therefore, a new series of tomograms was formed, reconstructed by (2...4) energy values.

Further analysis confirmed the feasibility of proposed idea. Figure 2 shows the dependences

of relative dispersion δ^* on the noise level for a different number of energy values used in reconstructing tomograms. The analysis of dependences allows us to draw following conclusions.

Firstly, with an increase in the noise level, for the case of one energy, the value of δ^* acquires a significant spread. In practice, this means that it is impossible to predict in advance the possibility of obtaining useful information from the reconstructed tomograms.

Secondly, the use of several energy values in the reconstruction process allows us to reduce the parameter δ^* by 2...3 orders of magnitude! This is clearly seen in figure 2. Although from a computational point of view these two cases are absolutely identical, using two energy values provides a significant gain in reducing the error.

Thirdly, increasing the number of measurements to $n > 360$ does not seem appropriate. However, additional studies have also shown that reducing the number of measurements leads to a sharp decrease in quality. Thus, the number of measurements $n = 360$ seems preferable.

Fourthly, from a computational point of view it is inappropriate to use more than three energy values in restoration, since in this case the ratio "gain in quality" / "expended resources" tends to zero.

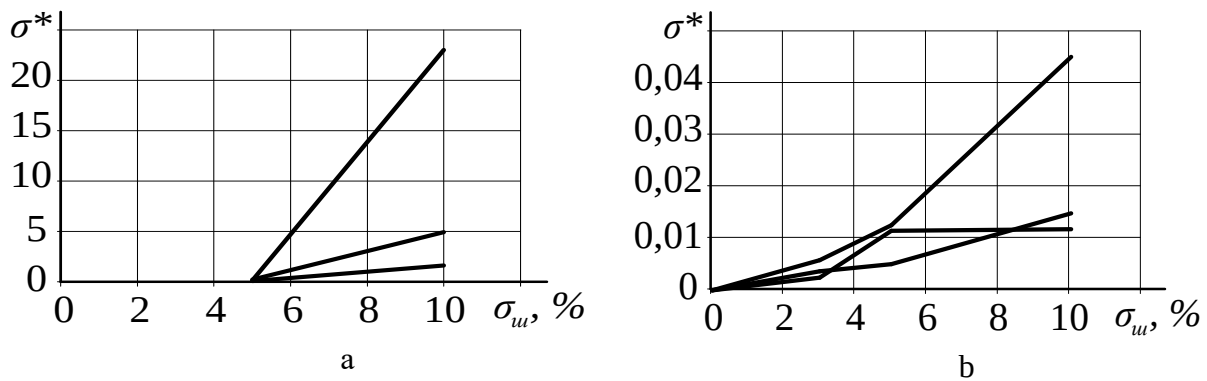


Figure 2 – Dependences of the relative dispersion σ^* on the noise level $\sigma_{\text{ш}}$ for different numbers of energy values N_E and measurements n : a – $N_E = 1$, $n = 720$; b – $N_E = 2$, $n = 360$.

1 – first, second rows of fuel elements; 2 – third row of fuel elements;

3 – center of the fuel assembly behind the guide channels

The results of the analysis of the relative dispersion δ^* also allowed us to draw a conclusion about the accuracy of SVD- method as a whole. However, they do not allow us to answer the question of how to find a defective fuel element.

In the course of further research, the histograms presented in Figure 3 were obtained. The abscissa axis shows the deviation of fuel element activity from the true one in %. The ordinate axis shows the proportion of fuel elements falling within a given deviation range. All histograms correspond to a noise level of 10%. The color indicates different fuel burnup depth profiles by the volume of the fuel assembly.

Analysis of the presented histograms confirmed the usefulness of the idea using several gamma radiation energy values to determine the activity of fuel elements. In addition, analysis of the histograms for different energy values showed that when reconstructing a tomogram, it is advisable to use the gamma radiation energy values of one isotope, namely ^{134}Cs . The isotope distribution is the same, so this approach allows the best compensation for tomogram reconstruction defects. Thus, for ^{134}Cs , it was found that the deviation of the activity of the reconstructed fuel elements from the true values does not exceed 30%, total number of fuel elements with activity deviations of more than 10% from the true value does not exceed 8 ... 10 pieces.

The results obtained allowed us to assume that if the appropriate reference point is selected, defective fuel rods with a leakage level of more than 30% for fuel rods of inner rows can be identified

on the reconstructed tomograms.

The final analysis of the experimental data involved constructing dependencies for the relative dispersion of fuel δ_i^* rod activity deviation within one row and the maximum activity deviation within one row A_i^{max} . These dependencies are presented in figures 3 and 4, respectively.

The general conclusion that can be made based on the results of the analysis of there is that the greatest reconstruction error is observed in the center of the tomogram. In the extreme rows, which are the most unfavourable from the point of view of the probability of the appearance of a defective fuel element, the accuracy of the tomogram reconstruction is the highest (fig. 4).

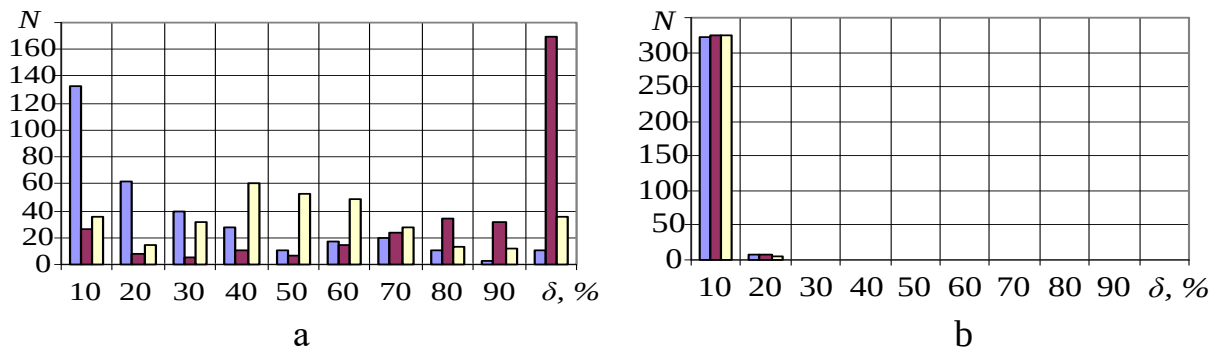


Figure 3 – Histograms of fuel rod activity deviation from the true value for different numbers of N_E energy values and n measurements:

a – $N_E=1, n=720$; b – $N_E>1, n=360,720$

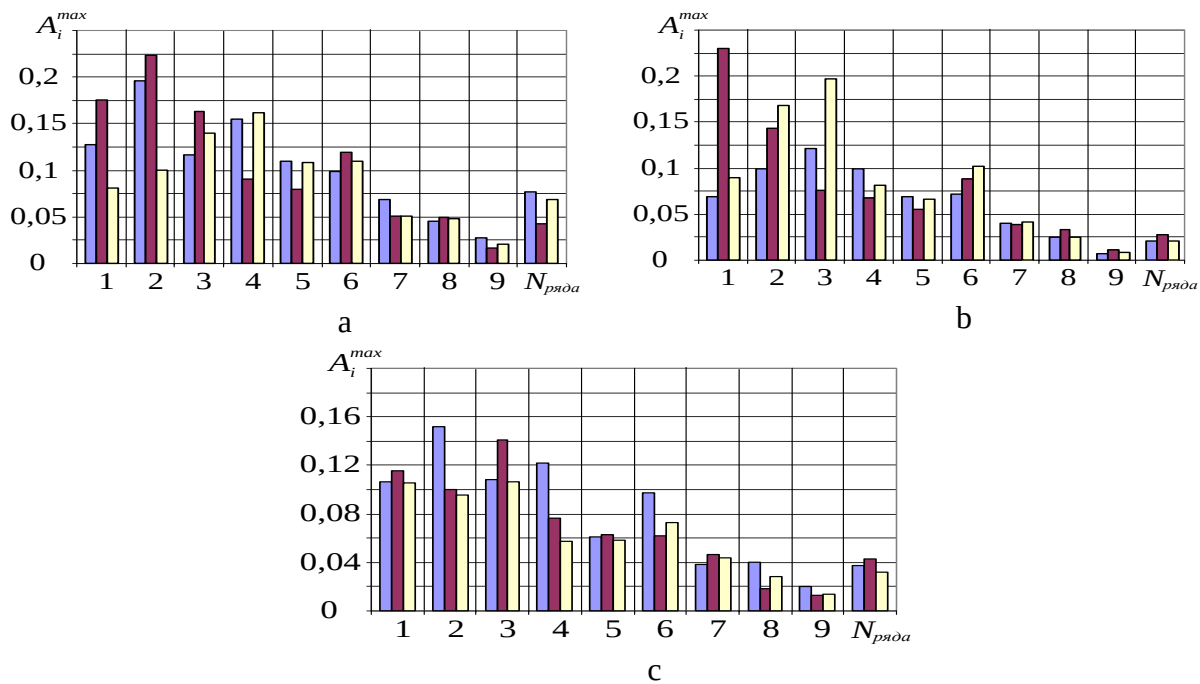


Figure 4 – Histograms of dependence maximum activity deviation A_i^{max} on the number of row

$N_{\text{ряда}}$: a – $N_E=2, n=360$; b – $N_E=3, n=360$;

c – $N_E=4, n=360$

Conclusions. The results of measurements with the help of this system when the reactor is operating at a power of $\approx 100\%$ of the nominal power" are: IR signals themselves, signal power spectral density, cross-correlation function, correlation coefficient and coolant mass flow rate. In

addition to regular measurements of coolant flow at the nominal power level, background measurements and measurements at reduced power levels were carried out.

After the installation of the secondary equipment, measurements of the noise level brought to the input were performed with the input of the amplifier open, i.e. unconnected ionization chamber. The obtained values were $\sim 2 \cdot 10^{-12}$ and $\sim 4 \cdot 10^{-12}$ A in the frequency range $f_b = 0 \dots 10$ and $f_b = 0 \dots 30$ Hz, respectively, i.e. approximately 0.01% of IR output current level. The noise level is determined by the presence of electromagnetic noise and signals from the technological equipment of the power unit in the circuits of the measuring channels, each of which includes a 200-meter coaxial cable of RK-75-4-16 type between the amplifier located near the wall of the hermetic volume and the main amplifier placed in laboratory premises.

REFERENCES:

1. Vavilov V.S. Effect of radiation on semiconductors / V.S. Vavilov, N.P. Kekelidze, L.S. Smirnov. - Moscow: Nauka, 1988. -- 192 p.
2. Lenkov S.V. Physical and technical foundations of radiation technology of semiconductors / S.V. Lenkov, V.A. Mokritsky, D.A. Peregudov, G.T. Tarielashvili. - Monograph. - Odessa: Astroprint, 2002. -- 297 p.
3. Garkavenko A.S. Radiation modification of the physical properties of wide-gap semiconductors and the creation of high-power lasers on their basis / Lvov: ZUKTs, 2012. - 258 p.
4. Banzak O.V. New generation semiconductor detectors for radiation monitoring and dosimetry of ionizing radiation / O.V. Banzak, O.V. Maslov, V.A. Mokritsky: Ed. V.A. Mokritsky, O.V. Maslov. - Monograph. - Odessa, 2013. - Publishing house "VMV". - 220 p.
5. Bouchet J.M. PWR primary flow measurements by correlation analysis of nitrogen-16 fluctuations / J.M. Bouchet, et al. - Progress in Nuclear Energy. - 1982. - Vol. 9.
6. Awadalla S.A. Characterization of detector-grade CdZnTe crystals grown by traveling heater method (THM) / S.A. Awadalla, J. Mackenzie, H. Chen, eds. // Journal of Crystal Growth. - Vol. 312, issue 4. - 2010. - 507-513c.
7. Grybos P. Front-end Electronics for Multichannel Semiconductor Detector Systems; EuCARD Editorial Series on Accelerator Science and Technology, Vol.08 / Institute of Electronic Systems Warsaw University of Technology. - Warsaw: 2010. - 201 p.
8. Dumitrescu A. Comparison of a digital and an analogical gamma spectrometer at low count rates / A. Dumitrescu // U.P.B. Sci. Bull., Series A. - Vol. 73. - Iss. 4, 2011. - P. 127-138.
9. Maslov O. Passive Computer Gamma- Tomography of Nuclear Fuel / O. Maslov, V. Mokritsky, O. Banzak, // ANIMMA. Third International Conference on Advancements in Nuclear Instrumentation Measurement Methods and their Applications - Marseille, June 23-27, 2013. - Book of Abstracts - P. 51.
10. Maslov O.V. The Improved CdZnTe Dose Rate Probe / O.V. Maslov, M.V. Maksimov, L.L. Kalnev // 2008 IEEE Nuclear Science Symposium, Medical Imaging Conference and 16th Room Temperature Semiconductor Detector Workshop - Dresden: 19-25 Oct. 2008. - P. 12-87.
11. Maslov O. Multiple energies passive computer tomography of nuclear fuel / O. Maslov // Proceedings of the International Ukrainian-Japanese Conference on Scientific and Industrial Cooperation - Odesa 24 - 25 October 2013. - P. 114-116.
12. Masuruk K. Dopant incorporation during liquid phase epitaxy / K. Masuruk, T. Bryskewicz // J. Appl. Phys., 1981. - V. 52. - N3. - part 1. - P. 1347-1350.
13. Mokritsky V.A. Methods and means controls of nuclear materials and state of protective barriers at nuclear power plants / V.A. Mokritsky, O.V. Maslov, O.V. Banzak // Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. - K.: MIKNU, 2019. - № 63. - C. 66 - 72.
14. Mokritsky V.A. The detector on basis of CdZnTe-gauge for systems radiating-technological control / V.A. Mokritsky, O.V. Maslov, O.V. Banzak // Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. - K.: MIKNU, 2018. - № 58. - C. 68 - 73.
15. Banzak O.V. Optimum operating mode of cdznte-sensors in the gamma radiation dosimeter / O.V. Banzak, H.V. Banzak, A.A. Gaber // Sur les matériaux de la v conférence scientifique et pratique internationale «Débats scientifiques et orientations prospectives du développement scientifique» - Paris 21-23 June 2023. - P. 77 - 79.

МЕТОДИ ТА ЗАСОБИ КОНТРОЛЮ ЯДЕРНИХ МАТЕРІАЛІВ І СТАН ЗАХИСНИХ БАР'ЄРІВ НА АЕС В УМОВАХ ВІЙСЬКОВОГО ЧАСУ

Рівень розвитку та застосування радіаційних технологій значною мірою визначається станом ядерного приладобудування. За порівняно невеликий період часу ця галузь пройшла кілька етапів розвитку і кожен із них був відзначений появою різних приладів, що реєструють та вимірюють параметри іонізуючого випромінювання ядерних матеріалів: газорозрядних лічильників, сцинтиляторів, напівпровідникових детекторів та інших.

Поява сучасних напівпровідникових радіаційних датчиків уперше пов'язала ядерне приладобудування та електроніку в єдиний комплекс – напівпровідниковий детектор. У ньому поєднуються взаємопов'язані за задачею, що розв'язується та параметрам напівпровідниковий первинний перетворювач іонізуючого випромінювання (датчик), вторинний перетворювач інформації від датчика (електроніка) та програмне забезпечення для обробки цієї інформації. Однак розвиток атомної енергетики, поширення ядерних технологій у різних галузях висунув нові вимоги до контролю та метрології іонізуючих випромінювань, які не можуть бути повною мірою задоволені сучасним рівнем ядерного приладобудування та прикладних ядерно-фізичних досліджень. Створені в цій роботі радіаційні датчики нового покоління та вимірювальні системи на їх основі відкривають раніше невідомі можливості у вирішенні завдань аналізу ядерного палива, збільшення точності та ефективності контролю технологічних параметрів та стану захисних бар'єрів в АЕС, створення засобів для інспекцій МАГАТЕ.

У роботі вперше запропоновано використання методів алгебраїчної реконструктивної пасивної томографії (АРТ) для відновлення зображення внутрішньої структури тепловиділяючих збірок. З цією метою розроблено новий алгоритм пасивної томографії ядерного палива на прикладі ВВЕР-1000, який використовує спосіб кутових проекцій власного випромінювання тепловиділяючих збірок (ТВЗ). Комп'ютерні експерименти томографії даного об'єкта показали, що оптимальними є вимірювання інтенсивності випромінювання в 360 точках розташування детектора щодо осі ТВЗ для двох і більше значень енергії гама-випромінювання ізотопу реперного ¹³⁴Cs. У цьому випадку запропонований метод АРТ дозволяє ідентифікувати на відновлених томограмах дефектні твели з рівнем протікання понад 30%, а також відсутність твелів у ТВЗ.

Ключові слова: радіаційні датчики, іонізуюче випромінювання ядерних матеріалів, пасивна томографія, твели

МЕТОДИКА ВИЗНАЧЕННЯ ВІДДАЛЕНОГО ДЕСАНТУВАННЯ ПАРАШУТНО-РЕАКТИВНОЇ СИСТЕМИ

Сьогодення змушує вирішувати завдання із забезпечення виконання заходів переходу українських Десантно-штурмових військ на стандарти НАТО. Підвищується взаємопартнерство наших воїнів з арміями держав-членів Альянсу. Під час вторгнення з Росії на територію нашої держави наші десантники навчаються вести бойові дії в умовах застосування противником ракетно-авіаційної зброї, високоточних засобів ураження та засобів РЕБ та засобів протиповітряної оборони (ППО). Десантно-штурмові війська розширяють свої можливості – військово-транспортні літаки ЗС України обладнуються для віддалених способів десантування бойової техніки з гранично малих висот.

На шляху набуття військових критеріїв членства в НАТО удосконалюється забезпечення вітчизняних десантних підрозділів. Наявні парашутні системи та керовані системи віддаленого десантування вантажів вже мають код номенклатури відповідно до стандартів НАТО. Такі ж системи стоять на озброєнні ЗС США, провідних країн Європи та Близького Сходу. Вони дозволяють здійснювати точну доставку на поле бою і в тил противника особового складу та вантажів без перетину літаками зони ураження комплексами ППО противника. Апробовано нові умови десантування вантажів парашутним способом, при цьому встановлено мінімально допустиму висоту – 50 метрів. Також ініційовано внесення змін в бортове обладнання літаків військово-транспортної авіації, що дасть можливість десантувати техніку та вантажі з гранично малих висот – 5 метрів.

В роботі розглядаються питання визначення характеристик здійснення десантування важкої техніки з використанням парашутно-реактивної системи (ПРС) з великої висоти та видаленої дистанції від площадки приземлення, що не дає виявити ні сам літак і ПРС системами ППО противника у момент десантування. У роботі пропонується спосіб віддаленого десантування що дозволяє за рахунок збільшення висоти скидання здійснювати горизонтальне переміщення до площадки приземлення на значному віддаленні від точки скидання. Отримані результати дозволяють сформулювати конкретні вимоги до розробки методики оцінки дальності зносу вітром парашутної системи.

Ключові слова: десантування важкої техніки, район застосування, парашутно-реактивні системи, доставка важкої техніки, метод віддаленого десантування.

Вступ та постановка проблеми. Десантування важкої техніки і вантажів з літаків пов'язано з необхідністю доставки її у район застосування за призначенням у найкоротші терміни. На сьогодні найбільшу швидкість, надійність та точність приземлення техніки, яка десантується, забезпечують парашутно-реактивні системи (ПРС). Десантування важких об'єктів з літаків пов'язано з необхідністю їх доставки у район застосування за призначенням у найкоротші терміни [1–3].

При десантуванні важкої техніки з літаків найбільшу швидкість, надійність та точність приземлення об'єкту забезпечують парашутно-реактивна система (ПРС). Застосування ПРС особливо ефективно для десантування об'єктів масою які знаходяться в діапазоні від 6 т до 21 т, висота десантування $H = 300 \dots 5000$ м. Скидання важкої техніки з використанням ПРС здійснюється за рахунок прольоту літака над розрахунковою точкою скидання з висоти,

дозволеної можливостями розкриття парашуту ПРС.

Літаку необхідно знаходитися достатньо низько і безпосередньо в районі десантування для здійснення точної доставки важкої техніки за допомогою ПРС. Використання ПРС для доставки важкої техніки з встановленою висотою (максимальною) скидання не завжди виявляється ефективною через можливість використання противником засобів протиповітряної оборони (далі ППО), скільки більшість сучасних погроз іде від наземного вогню (засобів ППО) противника. Здатність сучасних переносних зенітно ракетних комплексів (далі ПЗРК) дозволяє вражати літаки на максимальній висоті (операційна дальність) до 4600 м, що не дозволяє успішно проводити десантування важкої техніки і вантажів на визначені площадки приземлення. Крім того під час здійснення десантування з малої висоти літак може вказати місто знаходження своїх військ.

Для досягнення максимальної ефективності, десантування важкої техніки необхідно проводити на дистанції видалені до 50 км від площадки приземлення з великої висоти і наступному горизонтальному зміщенні без заходу літаків в зону дії засобів ППО. Десантування з великої висоти практично не дає виявити ні сам літак, ні момент скидання важкої техніки і дозволяє тримати літак за межею виявлення і загрози знищення системами ППО противника. На даний час сучасна технологія зробило можливим реалізацію багатьох інноваційних методів точного скидання, а саме парашутним системам високоточної доставки вантажів.

Аналіз останніх досягнень і публікацій. В іноземній літературі ці системи отримали найменування навідні системи точної повітряної доставки вантажів. Досягнення програми (Joint Precision Aerial Delivery Systems, JPADS) стало створення уніфікованих систем управління, що дозволяє комбінувати їх з різними основними парашутами систем високоточної повітряної доставки.

Історично, повітряна доставка легкої техніки та важких озброєнь виконувалася за допомогою безшумних і порівняно дешевих планерів, здатних швидко долати відстань від лінії фронту до місця приземлення та забезпечувати одночасне приземлення техніки і особового складу в одному місці (що є проблематичним при парашутному способі десантування). Однак розвиток радіолокаційних систем та ракетних систем ППО нівелювали всі переваги даного підходу до десантування.

Як було сказано вище, проблема віддаленого десантування важкої техніки наразі є відкритою, і жодна з провідних армій світу не демонструвала помітних успіхів у цьому напрямку у відкритих джерелах.

Метою статті є розгляд окремих питань та можливі шляхи часткового розв'язання проблеми щодо уникнення наземних загроз (засобів ППО) літаками під час здійснення десантування, які можуть виявитися корисними за планування десантних операцій для підвищення безпечності традиційного парашутного десантування, а також для подальших досліджень та розробці методів віддаленого десантування.

Виклад основного матеріалу. Найбільш простим шляхом десантування техніки без необхідності безпосереднього прольоту військово-транспортного літака над визначеною площадкою приземлення є використання ефекту горизонтального вітру на поведінку парашутно-реактивної системи (далі – ПРС) протягом зниження.

Для оцінки зростання швидкості вітру з висоти (вертикального градієнту) ми застосуємо модель степеневого профілю (рис. 1) яка є більш точною за інші прості моделі на висотах, що перевищують 100 м (тобто протягом переважної частини спуску), та відповідає нейтральному чи стабільному стану повітря над типовою пересіченою сільськогосподарською місцевістю, лісною місцевістю чи населеного пункту забудованого переважно одноповерховими будівлями [5–7].

$$w(h) = w_{\text{ref}} \left(\frac{h}{h_{\text{ref}}} \right)^{\alpha} \quad (1)$$

Під час русу парашута крізь шари повітря, що здійснюють горизонтальний рух з деякою швидкістю, парашут поступово набуватиме тієї ж швидкості горизонтального руху, а швидкість його зниження залишається приблизно сталою (за умови сталої швидкості вітру або її достатньо плавної зміни). Детальний математичний розгляд цього питання можна знайти в звіті.

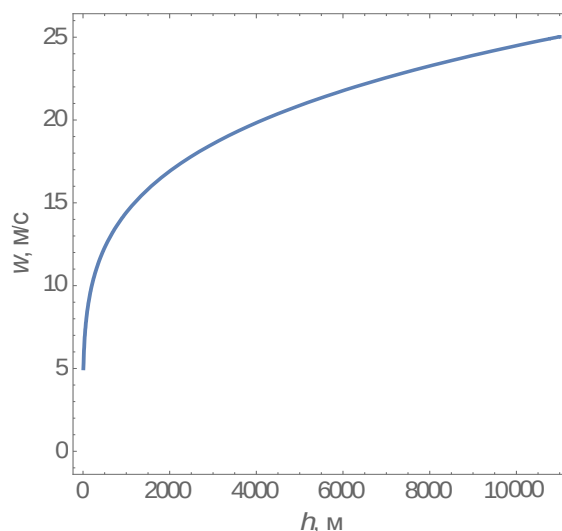


Рисунок 1 – Залежність швидкості горизонтального вітру від висоти над землею ($h_{\text{ref}}=10$ м, $w_{\text{ref}}=5$ м/с, $\alpha=0.23$)

Чим повільніше знижується ПРС, тим швидше горизонтальна компонента її швидкості прямуватиме до горизонтальної швидкості руху повітряних мас. Так при типових швидкостях зниження БМД-2 на системі ПРСМ-915 перехідний період (протягом якого відбуваються встановлення горизонтальної швидкості ПРС) може становити 4-6 с (залежно від величини зміни швидкості вітру), а для багатокупольних систем (далі – БКС) цей процес може відбуватися менше ніж за 2-3 с.

Для оцінки величини зносу (зміщення) ПРС вітром протягом зниження окрім вертикального градієнту горизонтальної компоненти швидкості вітру (1) треба врахувати й зміну швидкості зниження системи внаслідок зміни щільності атмосферного повітря з висотою (цей крок не є необхідним при десантуванні з висот до 1 км), для чого у даній роботі буде застосована міжнародна стандартна атмосфера (International Standard Atmosphere, ISA) – універсальна модель атмосфери, що оцінює значення тиску, температури і щільності атмосферного повітря на заданій висоті виходячи з відомих значень температури і тиску повітря на рівні моря (рис. 2).

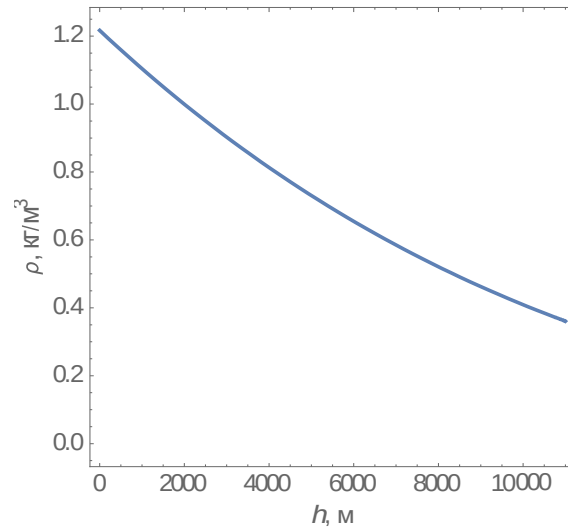


Рисунок 2 – Залежність густини атмосферного повітря від висоти (при температурі й атмосферному тиску на рівні моря $T_{\text{ref}} = 17^\circ\text{C}$ і $P_{\text{ref}} = 101325 \text{ Па}$)

Для спрощення розрахунків і враховуючи плавні зміни швидкості вітру (1) та щільності атмосфери, яка визначає вертикальну швидкість зниження ПРС, далі у цій роботі останню величину ми вважатимемо рівною термінальній швидкості зниження на відповідній висоті за відсутності вітру, а горизонтальну швидкість ПРС рівною горизонтальній швидкості вітру на відповідній висоті (внаслідок цих спрощень отримані нижче значення повного горизонтального зносу по суті є верхньою межею реальних значень величини горизонтального зносу). Величина термінальної швидкості зниження парашутно-реактивної системи $v_{\downarrow}$ визначається балансом сили опору $F_{\text{оп}} = \beta v^2$ повітря та сили тяжіння $F_{\text{тяж}} = mg$, отже:

$$v_{\downarrow} = \sqrt{\frac{mg}{\beta}}, \quad (2)$$

де β – коефіцієнт опору, який визначається характеристичною площею купола A , густиною повітря ρ та коефіцієнтом форми парашутно-реактивної системи c_d (для типових парашутів $c_D \approx 0.8 \dots 1$):

$$\beta = \frac{1}{2} \rho c_d A. \quad (3)$$

Згідно з використаною моделлю атмосфери температура повітря T_{ISA} зменшується на 6.5°C з підйомом на кожен наступний кілометр (на висотах до 11 км), а зниження тиску P внаслідок зменшення товщини розташованого вище шару повітря описується диференціальним рівнянням:

$$\frac{dP_{\text{ISA}}}{dh} = -\frac{P_{\text{ISA}} g}{R_{\text{sp}} T_{\text{ISA}}},$$

де $R_{\text{sp}} \approx 287.1 \text{ Дж} \cdot \text{кг}^{-1} \text{К}^{-1}$ – індивідуальна газова стала для повітря, а густина повітря визначається з його тиску і температури на даній висоті формулою:

$$\rho_{\text{ISA}} = \frac{P_{\text{ISA}}}{R_{\text{sp}} T_{\text{ISA}}}. \quad (4)$$

Повна величина горизонтального зносу Δx_{h_0} парашутно-реактивної системи внаслідок дії вітру може бути визначена шляхом інтегрування:

$$\begin{aligned}
\Delta x_{h_0} &= \int_0^t v_x(t) dt = - \int_{h_0}^0 \frac{v_x(h)}{v_{\downarrow}(h)} dh = \\
&= \int_0^{h_0} w_{\text{ref}} \left(\frac{h}{h_{\text{ref}}} \right)^{\alpha} \sqrt{\frac{c_d A \rho_{\text{ISA}}(h)}{2mg}} dh = \\
&= \frac{w_{\text{ref}}}{h_{\text{ref}}^{\alpha}} \sqrt{\frac{c_d A}{2mg}} \int_0^{h_0} h^{\alpha} \sqrt{\rho_{\text{ISA}}(h)} dh.
\end{aligned} \tag{5}$$

З формули (5) очевидно випливає, що загальна величина зносу у даному наближенні є пропорційною швидкості горизонтального вітру і зростатиме зі збільшенням стабільності повітряних потоків (параметр α) та/або зменшенням середньої швидкості зниження ПРС (яка визначається головним чином температурою повітря, параметрами купола і масою навантаження).

На рис. 3 наведені результати обчислень величини горизонтального зносу ПРС при десантуванні з різних висот для двох значень величини вітру.

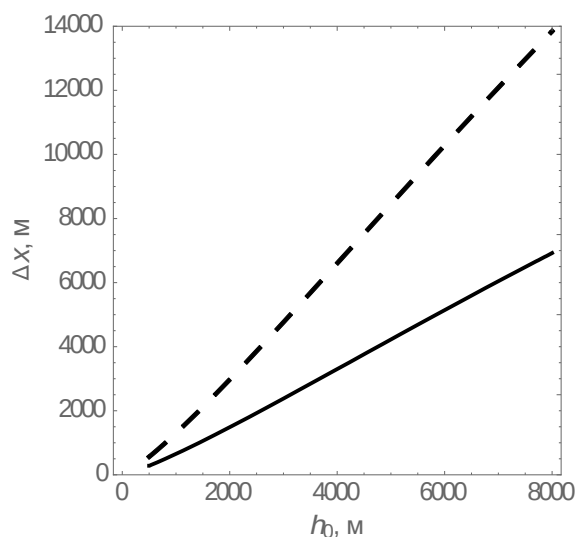


Рисунок 3 – Залежність величини горизонтального зносу вітром від висоти над рівнем моря, з якої проводиться десантування, характеристична площа купола $A = 540 \text{ м}^2$.

суцільна лінія – для швидкості вітру $w_{\text{ref}} = 5 \text{ м/с}$

штрихова лінія – $w_{\text{ref}} = 10 \text{ м/с}$

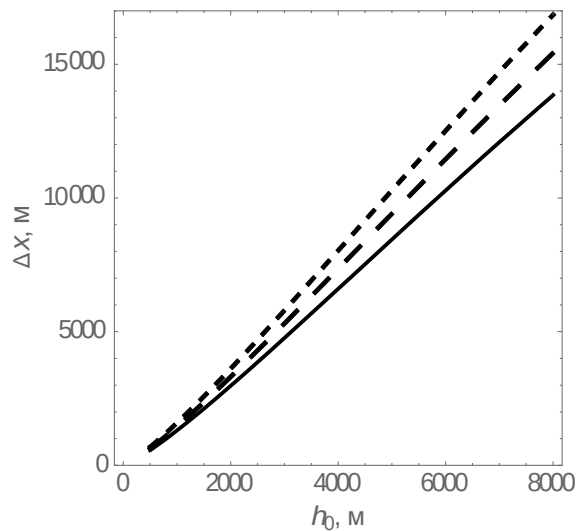


Рисунок 4 – Залежність величини горизонтального зносу вітром від висоти над рівнем моря, з якої проводиться скидання, характеристичній дані: площа купола $A = 540$ м² (суцільна лінія), $A = 670$ м² (штрихова лінія) і $A = 800$ м² (пунктирна лінія),

швидкість вітру $w_{ref} = 10$ м/с

На двох рисунках: $T_{ref} = 17^\circ\text{C}$, $h_{ref} = 10$ м, $\alpha = 0.23$, $m = 8260$ кг, $c_D = 0.8$.

Зменшення швидкості вітру та зменшення вертикальної швидкості ПРС протягом більшої частини зниження компенсують одне одного внаслідок збільшення густини повітря. У наслідок чого залежність величини зносу вітром від висоти десантування має приблизно лінійний характер.

В процесі дослідження спостерігається, що протягом більшої частини траєкторії зниження ПРС зменшення швидкості вітру та зменшення вертикальної швидкості ПРС (внаслідок збільшення густини повітря) компенсують одне одного. В наслідок чого залежність величини зносу вітром від висоти десантування має приблизно лінійний характер.

На рис. 5 наведені траєкторії зниження парашутно-реактивної системи ПРСМ-915 з сумарною масою 8260 кг, площею купола $A = 540$ м² при температурі повітря на рівні моря $T_{ref} = 17^\circ\text{C}$. Траєкторії ПРС побудовані для різних значень висоти, з якої проводиться скидання при здійсненні десантування, та горизонтальної швидкості вітру.

Бачимо, що за швидкості вітру $w_{ref} = 10$ м/с, висотою скидання $h_0 = 1$ км відношення що визначає ефективність зносу $\Delta x_{h_0}/h_0$, становить 1.3 та величина горизонтального зносу вітром буде 1,3 км. Тобто повна величина зносу об'єкту десантування вітром є на 30% більшою за висоту скидання під час здійснення десантування.

При $h_0 = 4$ км значення $\Delta x_{h_0}/h_0$ зростає до 1.65 та величина горизонтального зносу вітром буде 6,5 км, а при $h_0 = 8$ км значення $\Delta x_{h_0}/h_0$ сягає 1.73, величина горизонтального зносу вітром буде 14 км

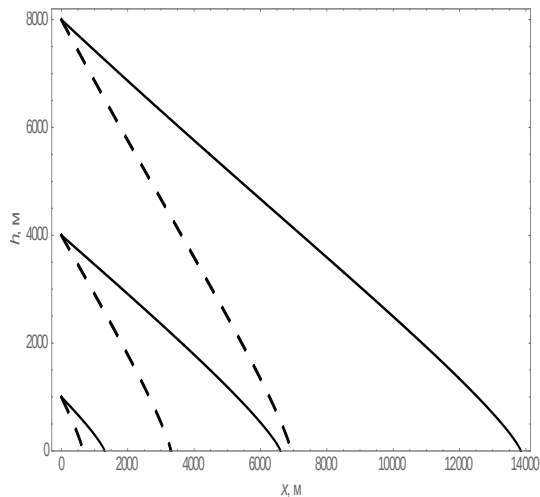


Рисунок 5 – Траєкторії зниження парашутної у вертикальній площині, паралельній до напрямку горизонтального вітру, за різних значеннях висоти десантування (1000 м, 4000 м і 8000 м відповідно) та двох значеннях швидкості горизонтального вітру: штрихові лінії – 5 м/с; суцільні лінії – 10 м/с

Збільшення площі купола парашута ПРС до 800 м² дозволило б збільшити показник $\Delta x_{h_0}/h_0$ до 2,1 (за незмінних інших умов) за рахунок збільшення тривалості зниження. А у випадку специфічних погодних умов, коли швидкість вітру більш інтенсивно зростає зі збільшенням висоти, можна очікувати величин зносу навіть у 2...2,5 більших за початкову висоту десантування.

Результати дослідження демонструють можливість ПРС за рахунок збільшення висоти скидання здійснювати горизонтальне переміщення до площадки приземлення на значному віддаленні від точки скидання. Однак розрахувати конкретну величину переміщення без поточного знання багатьох параметрів, що впливають на швидкість зносу вітром, є значно складнішим. Ці параметри включають головним чином повітряні потоки, з якими зустрічається ПРС, що можуть допомагати або заважати горизонтальному переміщенню.

Сучасні технології зробили можливою реалізацію багатьох інноваційних методів скидання вантажу. З метою зменшення впливу нерівномірності повітряних потоків на точність десантування сьогодні застосовуються системи підвищення точності висотного скидання HARP (high-altitude release point), які враховують динаміку руху повітря, системну балистику та швидкість повітряного судна.

Балістична таблиця (на основі середніх балістичних характеристик цієї парашутної системи) визначає точку скидання бойової машини та розраховує траєкторію вільного падіння при скиданні з великої висоти, враховуючи типові профілі повітряних потоків між точкою скидання і площадкою приземлення.

Після скидання бойової машини повітряні потоки впливають на напрямок її переміщення та тривалість падіння. Комп'ютер на борту повітряного судна розраховує вплив повітряних потоків, використовуючи данні про швидкість польоту, тиск і температуру з бортових датчиків та навігаційних сенсорів. Початкові дані водяться з прогнозу погоди та стану повітря у районі скидання.

Якщо фактичний профіль повітря не змінено та не введено у польотний комп'ютер, то за замовчанням для обчислення помилок у розрахунках HARP застосовується припущення про лінійний профіль повітря. Після того, як ці розрахунки виконані або данні ведені, їх результати записуються у базу даних десантування для використання під час розрахунків у подальших операціях.

Також з метою значного покращення точності скидання з великих висот можливо використання доплерівського лазерного локатора ІК-діапазону для вимірювання швидкості повітряних потоків на різних висотах та створення в реальному часі 3D карт вітрів у районі між повітряним судном і поверхнею площадки приземлення. Такі системи здатні здійснювати вимірювання з типової помилкою менше одного метру в секунду.

Висновки. Отже, у статті розглянуто окремі питання та можливі шляхи часткового розв'язання задачі віддаленого десантування, які можуть виявитися корисними за планування десантних операцій для підвищення безпечності традиційного парашутного десантування, а також у подальших дослідженнях та розробці способів віддаленого десантування ПРС.

За результатами досліджень запропоновано спосіб віддаленого десантування важкої техніки з використанням парашутно-реактивної системи що дозволяє визначити найбільш слабкі властивості системи, оцінити її загальний рівень, який характеризується набором природно-кліматичних показників, зокрема швидкостей вітру на різних висотах, і розробити заходи для підвищення ефективності застосування систем за призначенням.

Використання результатів досліджень на практиці, дозволить підвищити операційні спроможності Десантно-штурмових військ Збройних Сил України, а саме забезпечити швидке розгортання на загрозливих напрямках для стримування противника шляхом віддаленого десантування важкої техніки, що в свою чергу значно підвищить бойовий потенціал бойових підрозділів в оперативно-тактичній глибині оборони противника.

ЛІТЕРАТУРА:

1. Куянов О. Ю., Александров В. Є. Основні напрямки розвитку засобів десантування озброєння та військової техніки. *Наука і техніка Повітряних Сил Збройних Сил України*. 2010. №1(1). С. 49-54.
2. Дмитрієв В. А. Методи випробувань парашутних систем для повітряного десантування. *Наука і техніка Повітряних Сил Збройних Сил України*. 2013. №1(3). С. 41-43.
3. Патент № 111571. Автономна дистанційно керована транспортна модульна платформ супроводження повітряного десанту. Опубл.від 10.05.2016.
4. Manual of the ICAO Standard Atmosphere (extended to 80 kilometres (262 500 feet)) (3rd ed.). International Civil Aviation Organization. 1993. ISBN 92-9194-004-6.
5. Bañuelos-Ruedas F., Angeles-Camacho C. Rios-Marcuello S. Methodologies Used in the Extrapolation of Wind Speed Data at Different Heights and Its Impact in the Wind Energy Resource Assessment in a Region, pp. 97-114.
6. Hsu S., Meindl E., Gilhousen D. Determining the power-law wind-profile exponent under near-neutral stability conditions at sea, J. Appl. Meteorol., Vol. 33, pp. 757-765, 1994.
7. Farm W. Technical Regulations, Potential Estimation and Siting Assessment, Ed. G.O. Suvire, 2011, 248 p.
8. Иванов П. И., Куянов А. Ю., Иванов Р. П. Оценка рассеивания расчетной точки десантирования объекта с летательного аппарата-носителя. *Наука і техніка Повітряних Сил Збройних Сил України*. 2013. № 1(10). С. 42-45.
9. Дмитрієв В. А. Система та методи визначення показників безпеки парашутного десантування особового складу. *Системи озброєння і військова техніка*. 2012. №2 (30). С. 143-146.
10. Дмитрієв В. А. Обґрунтування показників безпеки приземлення військової техніки і вантажів при парашутному десантуванні. *Системи озброєння і військова техніка*. 2013. №3 (35). С. 86–90.
11. Дмитрієв В. А. Методика оцінки ефективності застосування парашутних систем для повітряного десантування. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*. 2020. Вип. 1(3), с. 29-33. <https://doi.org/10.37701/dndivsovt.3.2020.04>.
12. Боднар С. І., Сила І. М., Ряполов І. Є. Методика оцінки характеристик аеродинамічного навантаження двохоболочкових плануючих парашутів. *Комплексне забезпечення якості технологічних процесів та систем: матеріали тез доповідей XIII Міжнар. наук.-практ. конф., м. Чернігів, 25–26 трав. 2023 р. Чернігів, 2023. Т. 1. С. 179.*

REFERENCES:

1. Kuyanov O. Yu., Aleksandrov V. Ye. Osnovni napryamky rozvytku zasobiv desantuvannya ozbroynennya ta viyskovoyi tekhniky. *Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrayiny*. 2010. №1(1). S. 49-54.
2. Dmytriiev V. A. Metody vyprobuvan parashutnykh system dlya povitryanoho desantuvannya. *Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrayiny*. 2013. №1(3). S. 41-43.
3. Patent № 111571. Avtonomna dystantsiyno kerovana transportna modulna platforma suprovodzhennya povitryanoho desantu. Opubl. vid 10.05.2016.
4. Manual of the ICAO Standard Atmosphere (extended to 80 kilometres (262 500 feet)) (3rd ed.). International Civil Aviation Organization. 1993. ISBN 92-9194-004-6.
5. Bañuelos-Ruedas F., Angeles-Camacho C. Rios-Marcuello S. Methodologies Used in the Extrapolation of Wind Speed Data at Different Heights and Its Impact in the Wind Energy Resource Assessment in a Region, pp. 97-114.
6. Hsu S., Meindl E., Gilhousen D. Determining the power-law wind-profile exponent under near-neutral stability conditions at sea, *J. Appl. Meteorol.*, Vol. 33, pp. 757-765, 1994.
7. Farm W. Technical Regulations, Potential Estimation and Siting Assessment, Ed. G.O. Suvire, 2011, 248 p.
8. Ivanov P. I., Kuyanov A. Yu., Ivanov R. P. Otsinka rasseyvannya rozrakhunkovoyi tochky desantuvannya ob'ekta z letalnoho aparata-nosiya. *Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrayiny*. 2013. № 1(10). S. 42-45.
9. Dmytriiev V. A. Systema ta metody vyznachennya pokaznykiv bezpeky parashutnoho desantuvannya osobovoho skladu. *Systemy ozbroynennya i viyskova tekhnika*. 2012. №2 (30). S. 143-146.
10. Dmytriiev V. A. Obgruntuvannya pokaznykiv bezpeky pryzemlennya viyskovoyi tekhniky i vantazhiv pry parashutnomu desantuvanni. *Systemy ozbroynennya i viyskova tekhnika*. 2013. №3 (35). S. 86–90.
11. Dmytriiev V. A. Metodyka otsinky efektyvnosti zastosuvannya parashutnykh system dlya povitryanoho desantuvannya. *Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu vyprobuvan i sertyfikatsiyi ozbroynennya ta viyskovoyi tekhniky*. 2020. Vyp. 1(3), s. 29-33. <https://doi.org/10.37701/dndivsovt.3.2020.04>.
12. Bodnar S. I., Sylva I. M., Ryapolov I. Ye. Metodyka otsinky kharakterystyk aerodynamichnoho navantazhennya dvokhobolochkovykh planuyuchykh parashutiv. *Kompleksne zabezpechennya yakosti tekhnolohichnykh protsesiv ta system: materialy tez dopovidey XIII Mizhnar. nauk.-prakt. konf., m. Chernihiv, 25–26 trav. 2023 r. Chernihiv, 2023. T. 1. C. 179.*

METHODOLOGY FOR DETERMINING THE REMOTE LANDING OF A PARACHUTE-JET SYSTEM

The article discusses certain issues and possible ways to partially solve the problem of remote landing, which may be useful in planning airborne operations to improve the safety of traditional parachute landing, as well as in further research and development of remote landing methods for airborne vehicles.

Based on the results of the research, a method of remote landing of heavy equipment using a parachute-jet system is proposed, which allows to identify the weakest properties of the system, assess its overall level, characterised by a set of natural and climatic indicators, in particular wind speeds at different altitudes, and develop measures to improve the efficiency of the system's intended use. The results of the study demonstrate the ability of the WFD to move horizontally to the landing site at a considerable distance from the point of discharge by increasing the height of the release. However, it is much more difficult to calculate the specific amount of displacement without current knowledge of the many parameters that influence the wind drift rate. These parameters mainly include the air currents encountered by the WTG, which can help or hinder horizontal movement.

Modern technology has made it possible to implement many innovative methods of cargo discharge. In order to reduce the impact of uneven airflows on drop accuracy, HARP (high-altitude release point) systems are now being used to improve the accuracy of high-altitude drops, which take into account airflow dynamics, system ballistics and aircraft speed. The ballistic table (based on the average ballistic characteristics of this parachute system) determines the drop point of the combat vehicle and calculates the free fall trajectory for a high altitude drop, taking into account the typical airflow profiles between the drop point and the landing site. To significantly improve the accuracy of high altitude drops, it is also possible to use an infrared Doppler laser locator to measure airspeed at different altitudes and create real-time 3D wind maps in the area between the aircraft and the landing site surface. Such systems are capable of making measurements with a typical error of less than one metre per second.

The application of the research results in practice will increase the operational capabilities of the Airborne Assault Forces of the Armed Forces of Ukraine, namely, to ensure rapid deployment in threatened areas to deter the enemy by remotely landing heavy equipment, which in turn will significantly increase the combat potential of combat units in the operational and tactical depth of the enemy's defence.

Keywords: landing of heavy equipment, area of application, parachute and jet systems, delivery of heavy equipment, remote landing method.

АНАЛІЗ ЯКОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ НЕЧІТКОГО УПРАВЛІННЯ ЗАСПОКОЮВАЧЕМ ХИТАВИЦІ РЕАКТИВНОЇ ДІЇ

Судно, під час його експлуатації в умовах морського хвилювання, потребує використання додаткових пристроїв та систем для стабілізації свого просторового положення та зменшення негативного впливу різних видів хитавиці на екіпаж та обладнання. Заспокоювачі хитавиці мають чимало варіантів конструкцій, оснований на використанні різних фізичних принципів. Для суден різного цільового призначення використовують як пасивного типу заспокоювачі, які не потребують підведення енергії для свого функціонування, так і активного типу, які, використовують частину потужності судових джерел енергії. Показано, що активні заспокоювачі складають значну частку від всіх їх видів і значно ефективніше зменшують хитавицю, хоча й спричиняють суттєві енергетичні затрати. Відповідно, активні заспокоювачі потребують ефективного управління їх роботою, що має забезпечувати гарні значення параметрів стабілізації просторового положення корпусу судна при допустимих енергетичних затратах.

У даній роботі розглядається система управління різновидом водоструминного заспокоювача хитавиці, який стабілізує корпус судна за рахунок створення механічних моментів від реактивної дії струменів водно-повітряної суміші, що викидаються із заспокоювача у потрібному напрямку.

Доведено, що процес управління роботою заспокоювача комплексної конструкції (яким, зокрема, є водоструминний заспокоювач реактивної дії) є достатньо складним: включає чимало різних за своєю природою вхідних та вихідних змінних, а також зв'язки і залежності між ними, які важко підлягають формалізації та складно ідентифікуються при побудові детермінованої системи управління стабілізації, яка також не може враховувати невизначеності вказаних величин. Показано, що доцільно реалізувати систему управління заспокоювачем хитавиці реактивної дії на базі принципів штучного інтелекту, одним з різновидів якого є використання теорії нечітких множин. У даній роботі проведена реалізація нечіткого контролера для управління заспокоювачем хитавиці водоструминного типу, а також проведено дослідження ефективності його функціонування за допомогою системи Matlab/Simulink. Отримані результати показали, що запропонована нечітка система управління має задовільні показники роботи і може бути рекомендована до реалізації в рамках розробки заспокоювача хитавиці відповідної конструкції.

Ключові слова: заспокоювач хитавиці, водоструминний заспокоювач, fuzzy logic, нечітка система, моделювання, ефективність.

Вступ та постановка задачі. Заспокоювачі хитавиці є важливим елементом сукупності судових пристроїв, що забезпечують комфорт для пасажирів та екіпажу, а також – задовільні режими роботи обладнання судна та належне виконання ним його функціонального призначення. Усі конструкції заспокоювачів можна розділити на пасивні, що потребують затрат енергії на свою роботу, та активні, що їх вимагають. Очевидно, активні заспокоювачі потребують організації раціонального управління, яке дозволяло б мінімізувати (або обмежити) затрати енергії при достатніх (або, відповідно, найкращих) значеннях обраних показників якості їхньої роботи [1]. Таким чином, активні заспокоювачі хитавиці потребують використання автоматизованих систем управління їхньою роботою.

У попередніх публікаціях, наприклад, [2], запропоновано конструкцію і спосіб заспокоєння поздовжньої та поперечної хитавиці судна, оснований на використанні реактивних сил, що діють на корпус судна при викиданні із різних місць у потрібному напрямку водно-повітряної суміші (принцип дії водометних заспокоювачів хитавиці). Така

система має чимало керованих елементів, якими є заслінки та двигуни, які здійснюють нагнітання суміші при подачі у необхідному напрямку. Відповідно, функціональність системи управління подібним заспокоювачем хитавиці є досить складною, а побудова детермінованої математичної моделі автоматичної системи управління може бути утрудненою. У такому випадку доцільно застосувати підхід, заснований на теорії нечітких множин, та будувати нечітку систему управління технічним пристроєм – активним заспокоювачем хитавиці реактивної дії.

Таким чином, необхідно провести реалізацію математичної моделі нечіткої системи управління заспокоювачем хитавиці реактивної дії та на її основі провести аналіз якості її функціонування, впевнившись у відсутності явних недоліків, провести оцінку її основних показників ефективності.

Аналіз останніх досліджень. В цілому, різні принципи роботи сучасних заспокоювачів хитавиці, що описуються, наприклад, у [3], можуть спричинювати доцільність вибору того, чи іншого способу управління заспокоювачем певної конструкції, як описано в [4]. В той же час, у багатьох джерелах для заспокоювачів одного й того ж типу пропонуються різні способи управління.

Так, для заспокоювачів, що працюють на основі виведення із корпусу судна керованих кілів в літературі пропонується використання нейронних мереж (наприклад, у [5]), що, очевидно, пов'язано із бурхливим розвитком та зростанням популярності даного математичного апарату, апробованими застосуваннями. Також, для управління керованими кілями при заспокоєнні поперечної хитавиці пропонуються [6] і більш традиційні підходи, які реалізовані на основі побудови детермінованих математичних моделей. Також оптимізацію роботи заспокоювача хитавиці на основі підводних кілів описано у [7], однак основна частина цієї роботи присвячена саме оптимізації геометрії кілів, що, очевидно, повністю прив'язує її до даного конкретного типу заспокоювача.

Іншою популярною конструкцією заспокоювачів є гіроскопічні, засновані на фізичній здатності масивного тіла, що обертається, зберігати власний момент імпульсу (і, відповідно, загашати коливання корпусу судна, з який гіроскоп є пов'язаним). Так, в роботі [8] описуються нелінійні ефекти, що мають бути враховані при керуванні заспокоювачем подібної конструкції. Однак, застосувати ці відомості до заспокоювача хитавиці реактивної дії не уявляється можливим через особливості його конструкції.

Загальні принципи управління роботою заспокоювача бортової хитавиці приводяться у [9], однак, основою математичної моделі пропонується брати детерміноване диференціальне рівняння (Рікатті 2 порядку), яке не дозволяє врахувати невизначеності, притаманні змінним, які описують процес заспокоєння бортової хитавиці. Аналогічний недолік має і праця [10], де оптимальне керування роботою активного заспокоювача хитавиці (заснованого на керованих кілях) здійснюється на базі лінійно-квадратичного регулятора. Відповідно, більш доцільним є використання методів галузі штучного інтелекту.

Так, наприклад, у [11], пропонується адаптувати до задачі керування заспокоювачем хитавиці такий популярний на сьогоднішній у наукових дослідженнях інструмент, як нейронна мережа. Однак, як відомо, для експлуатації довільної нейронної мережі її спочатку треба навчити, для чого необхідно мати великий обсяг числових даних (дата-сет), що описує процеси керування цільовим технічним пристроєм (заспокоювачем хитавиці) та відповідні реакції корпусу судна. Очевидно, що при розробці системи управління для заспокоювача хитавиці оригінальної конструкції такий дата-сет є відсутнім. Альтернативним підходом з галузі ШІ, що може бути застосований для синтезу системи управління таким заспокоювачем хитавиці, є використання теорії нечітких множин або fuzzy logic, наприклад, [12-14]). Як відомо, такий підхід вимагає розробки бази правил нечітких продукцій, що є вираженням досвіду та логіки управління пристроєм, що отримані від досвідченого фахівця у відповідній галузі (експерта чи їх групи). Таким чином, для синтезу системи управління заспокоювачем хитавиці реактивної дії підхід на базі методів нечіткої логіки видається найбільш

перспективним і тому застосований у даній роботі.

Виклад основного матеріалу. Як відомо, принцип роботи нечіткого контролеру полягає у циклічному повторенні наступної послідовності операцій:

- фазифікація вхідних змінних;
- агрегування підумов для тих правил нечітких продукцій, які мають складні антецеденти;
- активізація підвисновків (тобто застосування усіх активних правил нечітких продукцій);
- акумулювання висновків (для тих змінних, які входять у консеквенти більш ніж одного правила нечітких продукцій);
- дефазифікація вихідних змінних.

Очевидно, що найважливішу роль у роботі нечіткого контролеру має база правил нечітких продукцій, основа якої для випадку, що розглядається у даній роботі була запропонована авторами у [13, 14]. Всього розглядалося 8 нечітких змінних по 3-5 термів у кожній, де всього реалізовано 12 правил, показаних на рис. 1 у вигляді переліку. Значення усіх змінних нормалізовані до одиниці шляхом ділення на максимальне допустиме значення кожної величини. У якості вхідних змінних запропоновано використання швидкості кильової хитавиці (β_7) та бортової хитавиці (β_8). У [13] обґрунтовано, що зважаючи на характер коливань корпусу судна під час обох типів хитавиці у першому наближенні доцільно обмежитися саме кутовими швидкостями коливань корпусу, а не величинами диференту та крену відповідно (чи кутовими прискореннями, які можна взяти до уваги при побудові більш детальної моделі у подальшій перспективі).

У якості вихідних вибрано наступні змінні:

- β_1 – величина отвору лівої повітряної заслінки;
- β_2 – величина отвору правої повітряної заслінки;
- β_3 – величина отвору лівої водної заслінки;
- β_4 – величина отвору правої водної заслінки;
- β_5 – потужність нагнітаючого пристрою лівого борту;
- β_6 – потужність нагнітаючого пристрою правого борту.

Зважаючи на те, що в даному випадку обрано дві вхідних змінних, зручно проаналізувати отримані поверхні нечіткого виводу для вказаних вихідних змінних. Для величин β_1 і β_2 вони показані на рис. 2, для β_3 і β_4 – на рис. 3, для β_5 і β_6 – на рис. 4.

Для дослідження всієї системи управління реалізовано модель об'єкту управління, рис. 5, яка також включає зовнішні впливи у вигляді моментів, що діють на судно з боку хвильової поверхні і розроблену в Simulink на основі матеріалів [14].

Модель всієї системи управління, за допомогою якої проводився аналіз ефективності запропонованих рішень, наведена на рис. 6. У якості Fuzzy Logic Controller використано нечіткий контролер, параметри якого наведені на рисунках 1, ..., 4; у якості об'єкта управління використано модель, наведену на рис. 5. Результати моделювання оцінювалися за допомогою виводу на віртуальні осцилографи, показані на рис. 6, а також на рис. 5.

Аналіз отриманих шляхом моделювання результатів показав наступне:

- заспокоювач ефективно протидіє бортовій хитавиці, зменшуючи її амплітуди до несуттєвих значень (коефіцієнт заспокоєння більше 0,9, тобто досягається зменшення амплітуди на 90 %);
- ефективність протидії кильовій хитавиці є значно меншою, що очевидно спричинюється значно більшою енергією поздовжніх коливань у діаметральній площині судна, і складає не більше 0,6;
- у судна з'являється постійний диферент на корму близько 10-15 градусів, що

спричинено особливостями конструкції заспокоювача, який розглядається (водострумні модулі встановлюються, в основному, у передній частині судна); дана величина не впливає суттєво негативно на роботу обладнання та екіпаж, а з точки зору морехідних характеристик може бути навіть корисною, покращуючи поведінку судна на хвилях;

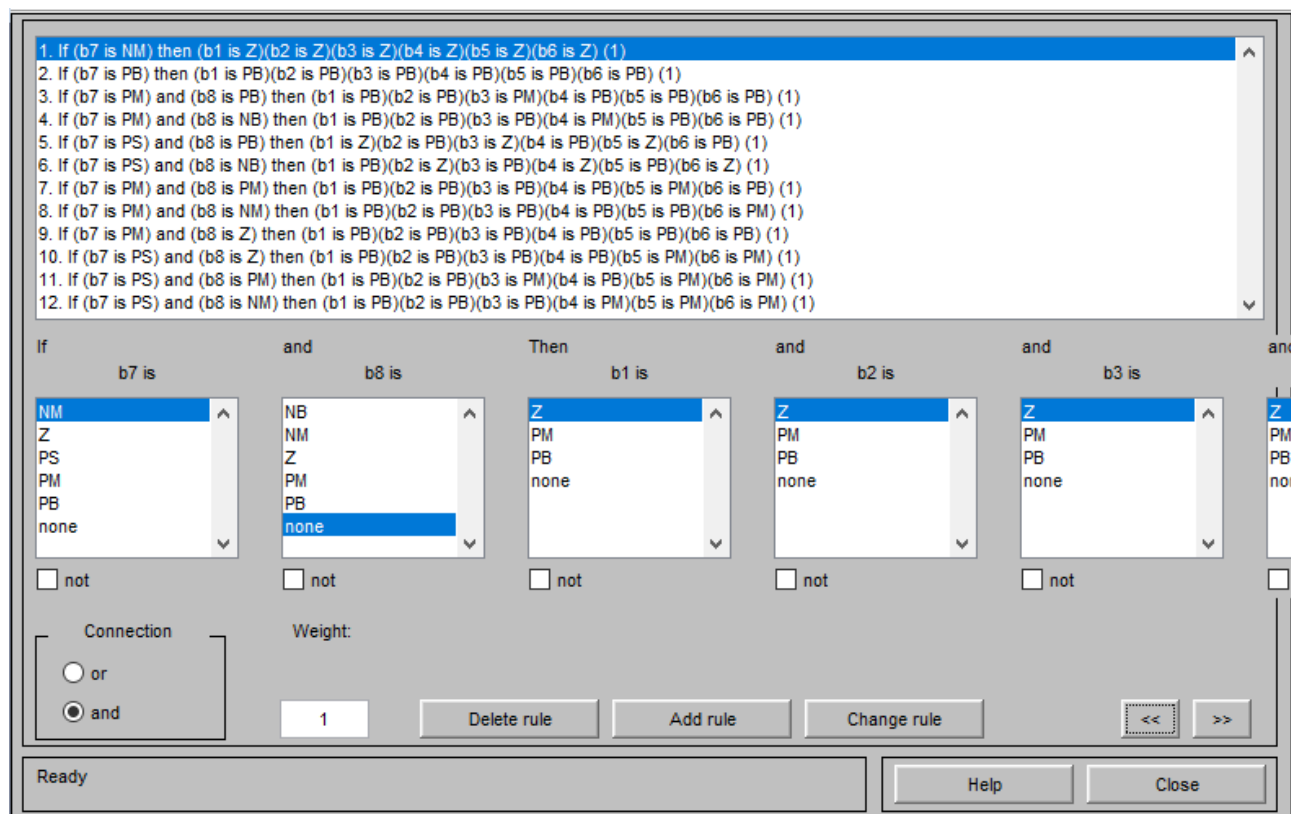


Рисунок 1 – Реалізація бази правил нечітких продукцій

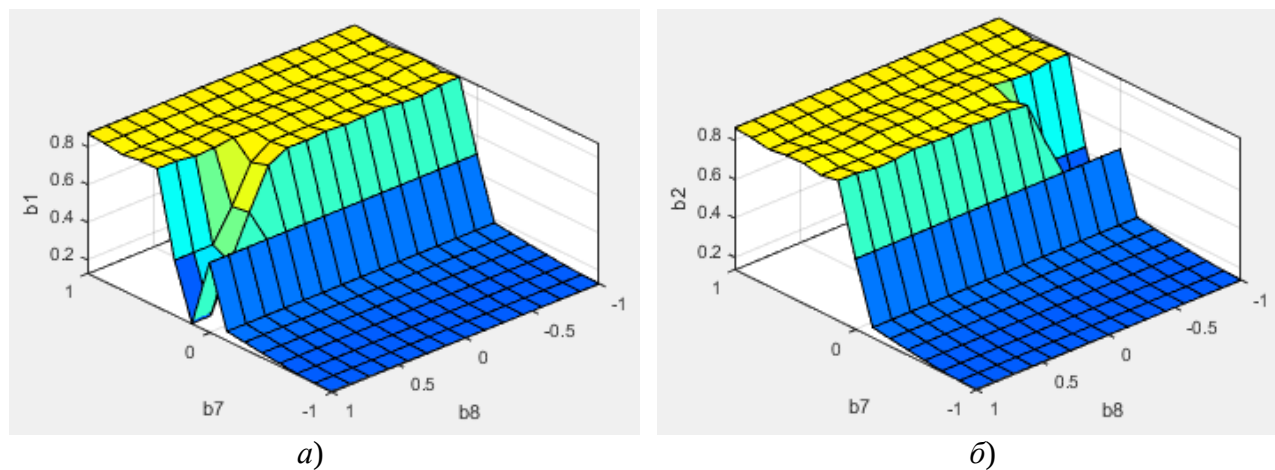
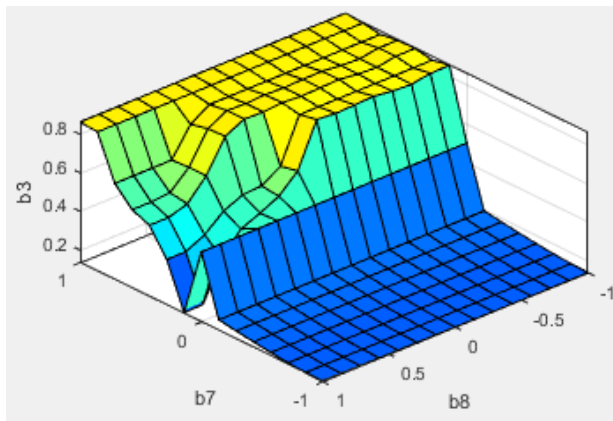
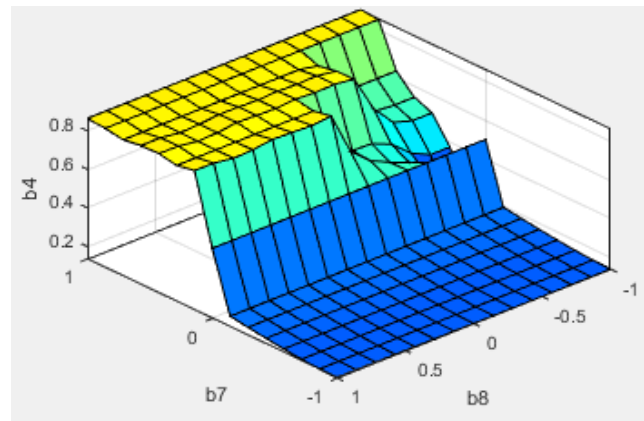


Рисунок 2 – Поверхні нечіткого виводу: a - для змінної β_1 , b - для змінної β_2



а)

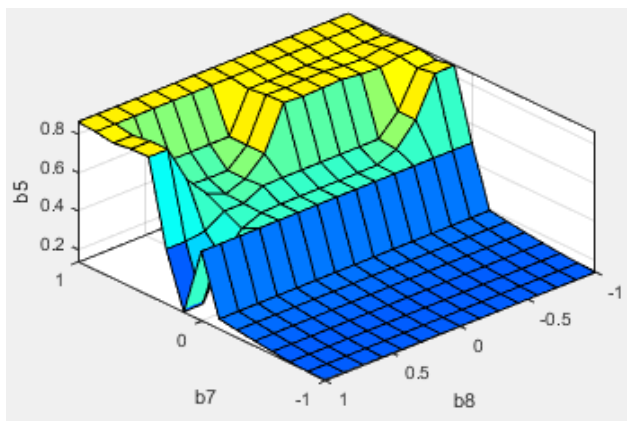


б)

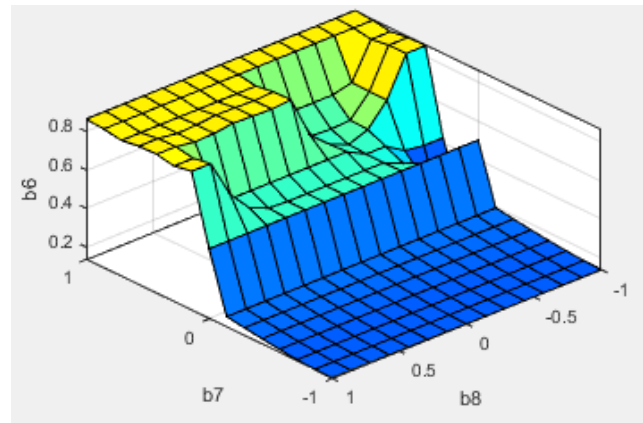
Рисунок 3 – Поверхні нечіткого виводу: а - для змінної β_3 , б – для змінної β_4

- показники якості системи управління знаходяться у допустимих межах, а саме час регулювання (виходу на постійну зменшену амплітуду коливань бортової хитавиці) складає не більше 10 с, а перерегулювання (перевищення амплітуди бортової хитавиці над стаціонарним значенням під час перехідного процесу) складає не більше 20 %;

- енергоспоживання заспокоювача хитавиці, необхідне для його ефективної роботи, може бути досить високим, тому окремою задачею, яка планується у подальшій роботі, є оптимізація режимів роботи пристрою для підвищення його енергоефективності.



а)



б)

Рисунок 4 – Поверхні нечіткого виводу: а - для змінної β_5 , б – для змінної β_6

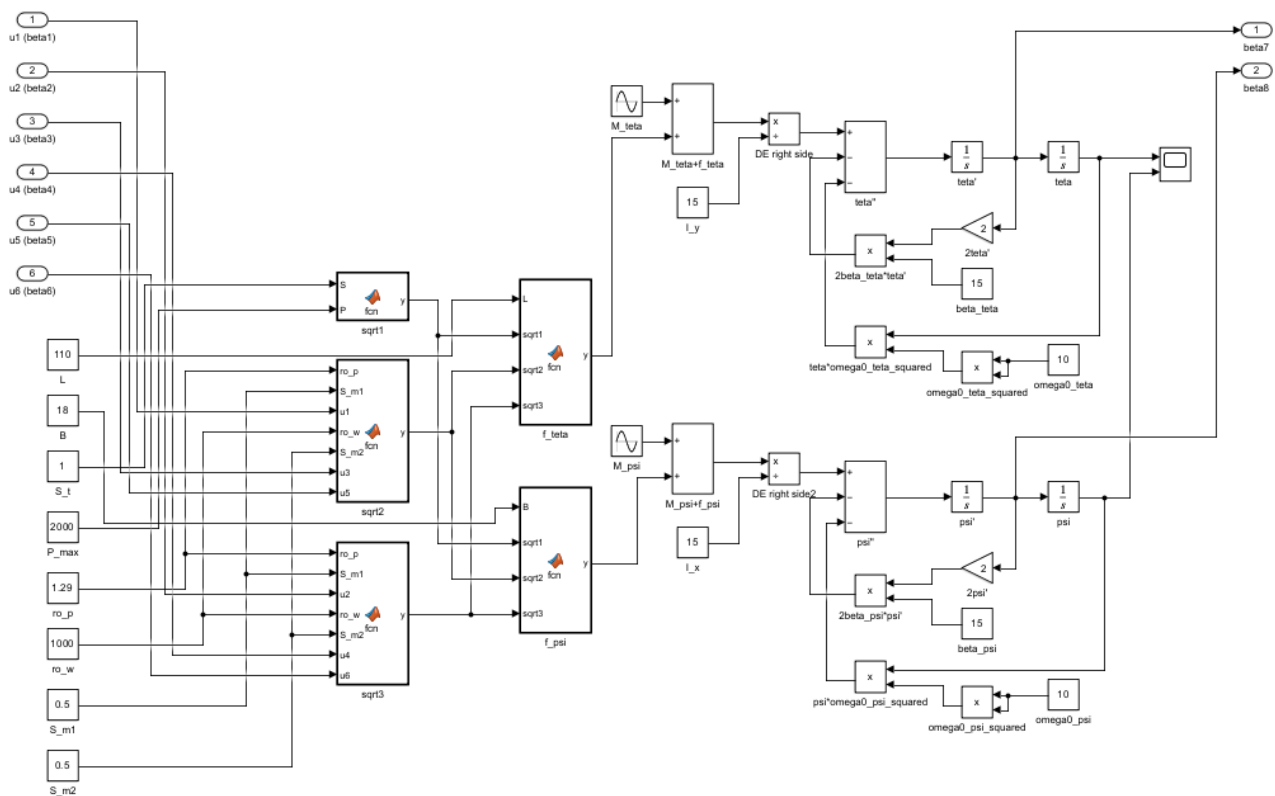


Рисунок 5 – Модель об’єкту управління (корпусу судна, на який діють реактивні сили, спричинені роботою заспокоювача хитавиці), включаючи зовнішні впливи на корпус судна від хвильової поверхні

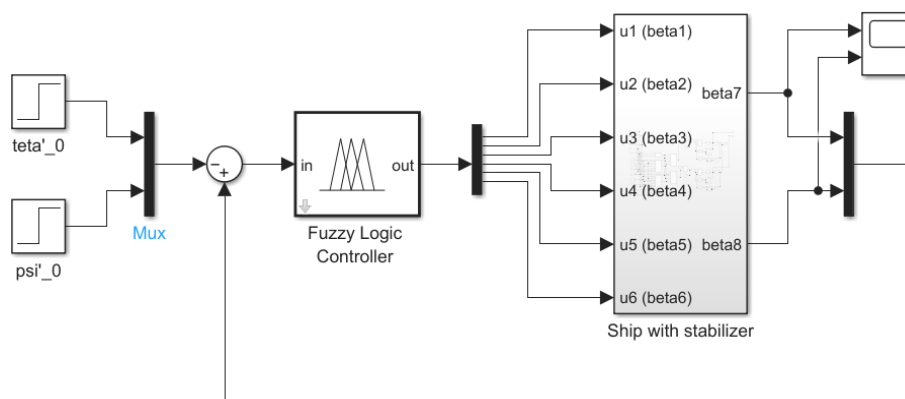


Рисунок 6 – Модель системи управління заспокоювачем хитавиці

Висновки. Таким чином, у даній роботі описано процедуру моделювання системи управління для водоструминного заспокоювача хитавиці реактивної дії. Основою системи управління вибрано контролер, що працює за принципами нечіткої логіки. Проведене дослідження показало, що пристрій задовільно виконує свою задачу, зменшуючи як бортову, так і кильову хитавицю судна (дещо у меншій мірі, через особливості розміщення модулів заспокоювача – в передній частині судна). Показники якості системи управління, визначені на основі дослідження моделі, знаходяться у допустимих межах, тому сама система управління може бути рекомендована до практичної реалізації у прототипі запропонованого водоструминного заспокоювача хитавиці реактивної дії.

ЛІТЕРАТУРА:

1. Kula, K. S. An Overview of Roll Stabilizers and Systems for Their Control. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 2015, Vol. 9, No. 3, pp. 405–414. DOI: <https://doi.org/10.12716/1001.09.03.14>.
2. Гайша О. О. Математичне моделювання ефективності управління реактивним заспокоювачем хитами судна. *Збірник наукових праць ВІ КНУ*. 2013. № 44. С. 27–33.
3. Sinha, T. Different Types Of Roll Stabilization Systems Used For Ships. *Marine Insight*. 2019. URL: <https://www.marineinsight.com/naval-architecture/roll-stabilization-systems/>.
4. Perez, T., Blanke, M. Control of Ship Roll Motion. В: Baillieul, J., Samad, T. (ред.) *Encyclopedia of Systems and Control*. Cham: Springer, 2021. DOI: https://doi.org/10.1007/978-3-030-44184-5_123.
5. Li, R., Li, T., Bai, W., Du, X. An adaptive neural network approach for ship roll stabilization via fin control. *Neurocomputing*, 2016, Vol. 173, pp. 953–957. DOI: <http://dx.doi.org/10.1016/j.neucom.2015.08.050>.
6. Liang, L., Zhao, P., Zhang, S., Yuan, J., Wen, Y. Simulation and analysis of fin stabilizer on ship rolls. 2018.
7. Aboemiera, H., Shehata, A. S., Elsherbiny, K., Mehanna, A. Performance enhancement of the roll stabilization systems used for ships. *AIP Conference Proceedings*, 2023, Vol. 3018, No. 1, p. 020034. DOI: <https://doi.org/10.1063/5.0172425>.
8. Sathit, P., Chatchapol, C., Phansak, I. Non-linearity Analysis of Ship Roll Gyro-stabilizer Control System. *Sustainable Marine Structures*, 2021, Vol. 3, No. 1, pp. 8–21. DOI: <https://doi.org/10.36956/sms.v3i1.316>.
9. Andrikov, D., Dereviankina, A. Control design of ship robust active rolling stabilizer. *Procedia Computer Science*. 2016. DOI: <https://doi.org/10.1016/j.procs.2017.01.027>.
10. Liang, L., Zhao, P., Zhang, S. Research and simulation of ship roll control in turning motion. *Proceedings of the 37th Chinese Control Conference, CCC 2018*, pp. 3841–3846. DOI: <http://dx.doi.org/10.23919/ChiCC.2018.8483223>.
11. Sun, Z., Chen, C., Zhu, G. Adaptive Neural Network Control of Zero-Speed Vessel Fin Stabilizer Based on Command Filter. *Applied Sciences*, 2022, Vol. 12, No. 754. DOI: <https://doi.org/10.3390/app12020754>.
12. Cao, Y., Lee, T. Maneuvering of surface vessels using a fuzzy logic controller. *Journal of Ship Research*, 2003, Vol. 47, pp. 101–130. DOI: <http://dx.doi.org/10.5957/jsr.2003.47.2.101>.
13. Гайша О. О., Гайша О. О. Створення бази правил нечітких продукцій для системи управління реактивного заспокоювача хитами судна. *Збірник наукових праць «Актуальні наукові дослідження в сучасному світі»*, 2017, № 9(29), Ч.1. Переяслав-Хмельницький, 2017, С. 19–23.
14. Melnyk O., Onishchenko O., Onyshchenko S., Shumylo O., Volyanskyy S., Bondar A., Cheredarchuk N. (2023) "Application of fuzzy controllers in automatic ship motion control systems", *International Journal of Electrical and Computer Engineering*, № 13(4), pp. 3948 - 3957. Available at: <http://dx.doi.org/10.11591/ijece.v13i4.pp3948-3957> (Accessed: 6 August 2024).

REFERENCES:

1. Kula, K.S. (2015) "An overview of roll stabilizers and systems for their control", *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 9, No. 3, pp. 405-414. Available at: <https://doi.org/10.12716/1001.09.03.14> (Accessed: 6 August 2024).
2. Haisha, O.O. (2013) "Matematychnе modeliuвання efektyvnosti upravlinnia reaktivnym zaspokoiuvachem khytavytsi sudna", *Zbirnyk naukovykh prats VI KNU*, № 44, S. 27-33.
3. Sinha, T. (2019) "Different types of roll stabilization systems used for ships", *Marine Insight*. Available at: <https://www.marineinsight.com/naval-architecture/roll-stabilization-systems/> (Accessed: 6 August 2024).
4. Perez, T. and Blanke, M. (2021) "Control of ship roll motion", in Baillieul, J. and Samad, T. (eds.) *Encyclopedia of Systems and Control*. Cham: Springer. Available at: https://doi.org/10.1007/978-3-030-44184-5_123 (Accessed: 6 August 2024).
5. Li, R., Li, T., Bai, W. and Du, X. (2016) "An adaptive neural network approach for ship roll stabilization via fin control", *Neurocomputing*, Vol. 173, pp. 953-957. Available at: <http://dx.doi.org/10.1016/j.neucom.2015.08.050> (Accessed: 6 August 2024).

6. Liang, L., Zhao, P., Zhang, S., Yuan, J. and Wen, Y. (2018) "Simulation and analysis of fin stabilizer on ship rolls".
7. Aboemiera, H., Shehata, A.S., Elsherbiny, K. and Mehanna, A. (2023) "Performance enhancement of the roll stabilization systems used for ships", *AIP Conference Proceedings*, Vol. 3018, No. 1, p. 020034. Available at: <https://doi.org/10.1063/5.0172425> (Accessed: 6 August 2024).
8. Sathit, P., Chatchapol, C. and Phansak, I. (2021) "Non-linearity analysis of ship roll gyro-stabilizer control system", *Sustainable Marine Structures*, Vol. 3, No. 1, pp. 8-21. Available at: <https://doi.org/10.36956/sms.v3i1.316> (Accessed: 6 August 2024).
9. Andrikov, D. and Dereviankina, A. (2016) "Control design of ship robust active rolling stabilizer", *Procedia Computer Science*. Available at: <https://doi.org/10.1016/j.procs.2017.01.027> (Accessed: 6 August 2024).
10. Liang, L., Zhao, P. and Zhang, S. (2018) "Research and simulation of ship roll control in turning motion", in *Proceedings of the 37th Chinese Control Conference, CCC 2018*, pp. 3841-3846. Available at: <http://dx.doi.org/10.23919/ChiCC.2018.8483223> (Accessed: 6 August 2024).
11. Sun, Z., Chen, C. and Zhu, G. (2022) "Adaptive neural network control of zero-speed vessel fin stabilizer based on command filter", *Applied Sciences*, Vol. 12, p. 754. Available at: <https://doi.org/10.3390/app12020754> (Accessed: 6 August 2024).
12. Cao, Y. and Lee, T. (2003) "Maneuvering of surface vessels using a fuzzy logic controller", *Journal of Ship Research*, Vol. 47, pp. 101-130. Available at: <http://dx.doi.org/10.5957/jsr.2003.47.2.101> (Accessed: 6 August 2024).
13. Haisha, O.O. and Haisha, O.O. (2017) "Stvorennia bazy pravyl nechitkykh produktsii dlia systemy upravlinnia reaktivnoho zaspokoiuvacha khytavytsi", *Zbirnyk naukovykh prats «Aktualni naukovi doslidzhennia v suchasnomu sviti»*, № 9(29), Ch.1, S. 19-23.
14. Melnyk O., Onishchenko O., Onyshchenko S., Shumylo O., Volyanskyy S., Bondar A., Cheredarchuk N. (2023) "Application of fuzzy controllers in automatic ship motion control systems", *International Journal of Electrical and Computer Engineering*, № 13(4), pp. 3948 - 3957. Available at: <http://dx.doi.org/10.11591/ijece.v13i4.pp3948-3957> (Accessed: 6 August 2024).

Haisha O.O., Doc. of Tech. S. Onishchenko O.A., PhD Haisha O.O.
FUNCTIONING QUALITY ANALYSIS OF THE FUZZY CONTROL SYSTEM OF A REACTIVE
SHIP STABILIZER

A ship during its operation in conditions of sea storm requires the use of additional devices and systems to stabilize its position and reduce the negative impact of various types of rocking on the crew and equipment. The corresponding devices, ship stabilizers, have many design options based on the use of different physical principles. Thus, this work considers a type of water-jet ship stabilizer, which stabilizes the ship's hull by creating mechanical moments from the reactive action of jets of a water-air mixture, which are ejected from the stabilizer in the appropriate direction.

All ship stabilizers can be divided into passive ones, which do not require the supply of energy for their operation, and active ones, which usually use part of the power of the ship's power plant. It should be noted that active stabilizers make up a significant share of all their types and significantly reduce ship oscillations, although they cause significant energy costs. Accordingly, active ship stabilizers require effective control of their work, which should ensure good values of the stabilization parameters of the ship's hull at acceptable energy costs.

It should be noted that the process of control the operation of a complex design stabilizer (which, in particular, is the mentioned reactive water-jet ship stabilizer) is quite complex: it includes many input and output variables of different nature, as well as dependencies between them, which are difficult to formalize during construction deterministic control system, which also cannot take into account the uncertainty of the specified values. Taking this into account, it is advisable to implement a control system for a water-jet ship stabilizer based on the principles of artificial intelligence, one of which is the theory of fuzzy sets. In this work, the implementation of a fuzzy controller for controlling a water-jet-type ship stabilizer was carried out, and its effectiveness was also studied using the Matlab Simulink model. The obtained results showed that the proposed fuzzy control system has satisfactory performance and can be recommended for implementation within the framework of the development of a ship stabilizer of the corresponding design.

Keywords: ship stabilizer, water jet stabilizer, fuzzy logic, fuzzy control, efficiency modeling.

МЕТОДИКА РОЗРАХУНКУ ОСНОВНИХ ПАРАМЕТРІВ ОСКОЛКОВИХ ВИБУХОВИХ ПРИСТРОЇВ НАПРАВЛЕНОЇ ДІЇ ДЛЯ УРАЖЕННЯ ПОВІТРЯНИХ ЦІЛЕЙ ТИПУ БПЛА

За досвідом російсько-Української війни спостерігається тенденція збільшення кількості безпілотних літальних апаратів, які застосовуються для ураження техніки, особового складу та об'єктів інфраструктури. Для цього застосовуються безпілотні літальні апарати типу "баражуючий боєприпас", "камікадзе", для скидів тощо. Частка втрат озброєння та техніки, а також особового складу від дії таких засобів на сьогоднішній стала найбільшою порівняно з іншими засобами ураження. Для протидії таким засобам застосовується різноманітні зенітно-ракетні комплекси, засоби радіоелектронної боротьби та мобільні вогневі групи. Найбільш ефективним способом ураження безпілотних літальних апаратів є ураження їх великою кількістю уражаючих елементів (осколками). Враховуючи співвідношення вартості безпілотних літальних апаратів та засобів їх ураження, зокрема зенітно-ракетних боєприпасів, в роботі за критерієм "ефективність-вартість" пропонується застосування осколкових вибухових пристроїв направленої дії для ураження ударних безпілотних літальних апаратів.

В статті наведений аналіз досліджень ефективності застосування осколкових боєприпасів направленої дії. Проведено дослідження доцільності застосування осколкових інженерних боєприпасів направленої дію типу мін серії МОН. На основі математичної моделі польоту осколка з урахуванням його форми запропоновано методику розрахунку основних параметрів осколкових вибухових пристроїв направленої дії для ураження повітряних цілей типу безпілотних літальних апаратів. Наведені математичні розрахунки визначення основних характеристик осколкових вибухових пристроїв направленої дії для ураження безпілотних літальних апаратів з врахуванням зовнішньо-траєкторних вимірів цілі та факторів, які впливають на формування поля (зони) осколків. Запропоновано схеми розміщення осколкових вибухових пристроїв направленої дії для захисту об'єктів.

Ключові слова: безпілотний літальний апарат, засоби ураження, інженерний осколковий боєприпаси направленої дії, захист об'єктів.

Вступ. В умовах сьогодення постає питання ефективності протидії різним засобам повітряного нападу, особливо безпілотним літальним апаратам (БПЛА), які кардинально змінили форми та методи збройної боротьби. На сьогоднішній день частка уражених ОВТ, об'єктів та особового складу БПЛА ударного типу стала домінуючою у порівнянні з іншими засобами ураження. Основними засобами ураження БПЛА є зенітно-ракетні комплекси, мобільні вогневі групи та засоби РЕБ. Необхідно зазначити, що найбільш ефективними проти БПЛА є саме зенітно-ракетні комплекси. Проте, вартість застосування до них боєприпасів значно перевищує вартість ударних БПЛА, що робить таку протидію недоцільною. В цих умовах гостро постало питання щодо пошуку альтернативних способів протидії ударних БПЛА. Одним з таких напрямків може бути застосування інженерних осколкових боєприпасів направленої дії.

Постановка проблеми. Досвід ведення війни РФ проти України показав, що вразити БПЛА з використанням різних видів стрілецької зброї не завжди вдається, а витрачати зенітні снаряди або коштовні ракети, на порівняно недорогі повітряні цілі типу БПЛА недоцільно.

Проте, враховуючи той фактор, що навіть маловартісний ворожий БпЛА доставляє противнику цінну розвідувальну інформацію та може ефективно уражати особовий склад, військову техніку та різні об'єкти, необхідність їх знищення або блокування роботи являється одним з пріоритетних завдань.

Одним із напрямків ураження БпЛА є використання осколкових інженерних боєприпасів направленої дії. Принципом застосування таких боєприпасів є ураження БпЛА хмарию осколків. Проте, на сьогоднішній день вони застосовуються тільки в горизонтальній площині проти піхоти противника. Припущення щодо ефективності їх застосування проти БпЛА вимагає проведення досліджень щодо визначення параметрів таких боєприпасів з урахування факторів, що впливають на ефективність дії осколка при польоті в вертикальній площині під різними кутами. Все це свідчить про актуальність дослідження та необхідність пошуку нових методів щодо протидії БпЛА.

Для проведення оцінки ефективності осколкової дії інженерних боєприпасів на повітряні цілі необхідно визначити та врахувати: швидкість повітряної цілі; висоту польоту повітряної цілі; швидкість осколків в момент зустрічі з цілю; розміри осколкового поля; форму осколка; кут польоту осколку; убійну дію осколку на різних відстанях. За цих умов необхідно провести теоретичні та практичні дослідження ефективності застосування даних боєприпасів.

Аналіз попередніх досліджень. Аналіз засобів ураження БпЛА осколкової дії свідчить, що основним проблемним питанням у розрахунках є визначення швидкості, напрямку розльоту осколків, визначення числа і щільності розльоту осколків. Так в роботі [1] розглядається питання, які пов'язані з характеристикою уражаючої дії осколків при підриві артилерійського снаряду перед малогабаритною повітряною ціллю та оцінка їх ефективності.

В роботі [2] обґрунтовано концепція універсального боєприпасу осколкової дії здатного забезпечити захист техніки та особового складу від застосування ударних БпЛА. Проведена оцінка уражаючих можливостей боєприпасу, обґрунтовано вибір типу снаряда, ваги та кількості осколків. В роботі [3] проведений аналіз застосування ударних БпЛА та крилатих ракет рф по території України, надано пропозиції щодо доцільності використання осколкових інженерних боєприпасів в якості елемента побудови системи активного захисту військ та об'єктів критичної інфраструктури від ураження засобів повітряного нападу та можливі варіанти їх застосування. Робота [4] присвячена аналізу технічних характеристик та конструктивних особливостей осколкових вибухових пристроїв направленої дії, а також оцінці ефективності ураження повітряних цілей типу БпЛА та визначенню найбільш оптимального варіанту застосування інженерних боєприпасів даного типу.

Проведений аналіз доступних досліджень в даній предметній області в цілому дозволяє визначати показники осколків під час польоту. Проте, не враховуються: зовнішньо-траєкторні показники цілі, що не дає можливості використовувати осколкові боєприпаси для рухомих повітряних цілей; рух осколка у вертикальній площині під впливом сил опору та зміни кута руху; вплив коефіцієнту лобового опору та різних форм осколків для інженерних боєприпасів на дальність ураження цілі; залежність щільності осколкової зони від відділення точки ініціювання інженерних боєприпасів, що впливатиме на імовірність ураження.

Отже **метою статті** є обґрунтування методики розрахунку основних параметрів осколкових вибухових пристроїв направленої дії для ураження БпЛА з врахуванням його зовнішньо-траєкторних параметрів та впливу факторів на рух осколка у повітрі при ураженні повітряної цілі.

Виклад основного матеріалу. Для ураження цілей типу БпЛА доцільно застосовувати осколкові вибухові пристрої направленої дії. В якості таких боєприпасів найбільш

оптимальним варіантом є використання інженерних мін МОН-90 та МОН-200 які мають високі показники імовірності ураження цілі [4].

Осколкові інженерні боєприпаси діють на цілі звичайно на значній відстані, тому, на відміну від мін фугасного і фугасно-осколкового принципів дії, їх віднесено до боєприпасів направленої дії, осколки яких розлітаються в межах малого тілесного кута, у відповідному секторі ураження. При вибуху осколкового боєприпасу ураження цілей здійснюється осколками, які при зустрічі з ціллю повинні мати енергію, необхідну для їх ураження.

Основним показником ефективності ураження повітряної цілі є дальність ураження, яка визначає відстань, на яку осколкові поля уражають цілі. Як було зазначено раніше необхідно розрахувати параметри осколкового вибухового пристрою направленої дії при застосуванні їх для ураження БПЛА з врахуванням зовнішньо-траєкторних вимірів цілі та факторів які будуть впливати на осколкові поля.

За основу методики розрахунку взята теорія впливу механічної енергії на осколок, який рухається у повітрі, використовуючи вираз розрахунку енергії активної маси вибухової речовини, рух осколка розраховується інтегруючи дане рівняння. В якості критерію ураження використовується критерій критичної енергії [5].

Для опису руху осколка у повітрі використовуються фундаментальні поняття розділу механіки, що описують рух матеріальних тіл. На рис. 1 відображено рух осколка у повітрі під кутом α на якого діють сили опору.

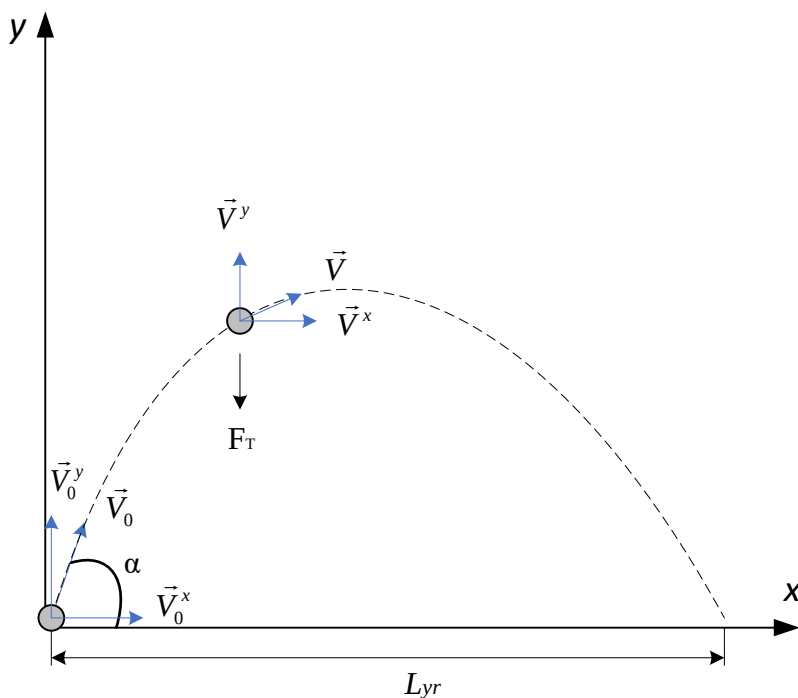


Рисунок 1 - Зниження швидкості рух осколка у повітрі

Рух осколка визначається за його початкову швидкість V_0 . Осколок, отримавши V_0 , рухається у середовищі, що чинить опір, по деякій траєкторії, поки не потрапить в ціль його швидкість постійно зменшується до критичного стану. Зниження швидкості осколка залежить від пройденої відстані що виражається у дальності ураження L_{yr} та сили тяжіння F_T .

Проте дана модель руху осколка буде не зовсім підходити до нашої умови, у зв'язку з великими швидкостями та незначною вагою осколків інженерних боєприпасів сила F_T , визначається як обмеження, та не враховується.

Для вирішення даного питання пропонується розглянути наступну послідовність розрахунку основних параметрів інженерних боєприпасів типу МОН-90, МОН-200.

1. Визначення швидкісних параметрів (V_0 , V_{kr}) та дальності ураження (L_{kr}) осколків.

В роботах [5, 6] проводиться визначення початкової швидкості осколка V_0 , проте не враховано вагу вибухової речовини M , яка суттєво впливає на питому енергію вибухового перетворення Q_0 . Робота, яка утворюється за рахунок вибуху, буде збільшуватися, зі збільшенням маси вибухової речовини. Можна вважати, що ця робота пропорційна енергії Q_0 , тобто енергії яка міститься в одиниці маси вибухової речовини, буде залежити від ваги цієї вибухової речовини [7]. Виходячи з цього початкова швидкість осколка V_0 визначається за наступним виразом:

$$V_0 = \sqrt{2WQ_0M}, \quad (1)$$

де, W – характеристика міцності та інерційних властивостей оболонки і осколків різних боєприпасів, для інженерних боєприпасів знаходиться у діапазоні 0,05...0,12; Q_0 – питома енергія вибухового перетворення, M – вага ВР. [5].

В табл. 1 представлено розрахункові дані початкової швидкості осколка V_0 інженерних боєприпасів МОН-90, МОН-200 з різними коефіцієнтами W .

Таблиця 1

Розрахункові дані V_0 інженерних мін МОН-90, МОН-200

Тип ІБП	Коефіцієнт W							
	0,05	0,06	0,07	0,08	0,09	0,10	0,11	0,12
МОН-90	1661	1819	1965	2101	2228	2349	2404	2573
МОН-200	2244	2459	2656	2839	3011	3039	3329	3477

Для ураження цілі осколок повинен мати певну кінетичну енергію K_e . При вазі осколка $m > 0,5$ г, $K_e = 80 \text{ Дж}$ [8]. Критична швидкість осколка V_{kr} визначається наступним виразом [6]:

$$V_{kr} = \sqrt{\frac{2K_e}{m}}, \quad (2)$$

В табл. 2 представлено розрахункові дані критичної швидкості осколка V_{kr} з різною вагою m .

Таблиця 2

Розрахункові дані V_{kr} з різною вагою осколка m

m , кг	0,002	0,004	0,006	0,008	0,010	0,012	0,014	0,016
V_{kr} , м/с	282	200	163	141	126	115	106	100

Враховуючи характеристики інженерних боєприпасів МОН-90, МОН-200 визначаємо дальність ураження цілі L_{yr} за виразом [5, 6]:

$$L_{yr} = \frac{4}{3C} \cdot \frac{p_m}{p_1} d \cdot \ln \frac{V_0}{V_{kr}}, \quad (3)$$

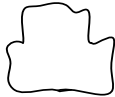
де, C – коефіцієнт лобового опору; p_m – щільність матеріалу, p_1 – щільність повітря; d – діаметр осколка.

Коефіцієнт C є емпіричним коефіцієнтом, який входить у формулу сили лобового опору твердого тіла та залежить від форми тіла. Для деяких найпростіших форм тіл C можна одержати теоретично. Для різної форми осколків коефіцієнт лобового опору C буде становити: для кульки – 1; для циліндра – 1,5; для рваного – 1,75 [6].

В табл. 3 відображено результати дальності ураження цілі L_{yt} з використанням коефіцієнта C для різних форм осколків, при чому V_0 має $W 0,05$.

Таблиця 3

Розрахунки дальності ураження цілі L_{yt} інженерних боєприпасів
з різними формами осколків

Коефіцієнт C	Форма осколка	L_{yt} , м	
		МОН-90	МОН-200
1		102	280
1,5		67	183
1,75		58	159

Отже, відповідно до результатів видно як коефіцієнт лобового опору C та форма осколків змінюють показник L_{yt} .

На пробивну здатність корпусу повітряної цілі будуть впливати швидкість осколка та матеріал корпусу повітряної цілі. Оскільки осколок при русі у повітрі втрачає частину енергії на подолання сил опору, то його критична швидкість повинна бути вищою за швидкості повітряної цілі $V_{kr} > V_{pz}$. Це можна відобразити аналізуючи швидкості руху БпЛА з швидкістю осколка інженерних боєприпасів V_{kr} .

Відповідно до функціональної швидкості польоту БпЛА класифікують наступні типи:

- малошвидкісні – до 55 м/с (максимальна швидкість 69 м/с);
- середньшвидкісні – від 41 до 111 м/с (максимальна швидкість 125 м/с);
- швидкісні – від 97 до 222 м/с (максимальна швидкість 250 м/с) [9].

На рис. 2 показаний порівняльний аналіз швидкісних показників польоту БпЛА та осколків інженерних боєприпасів.

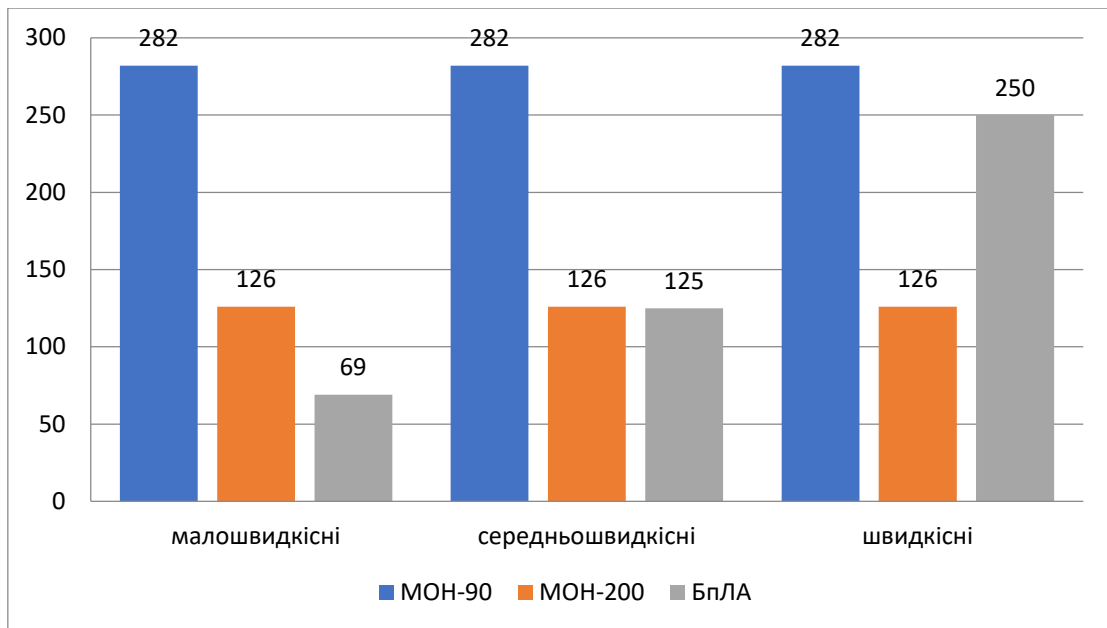


Рисунок 2 – Порівняльна оцінка швидкісних показників БпЛА та осколків інженерних боєприпасів

Враховуючи максимальні показники швидкості польоту БпЛА можна зазначити що інженерні боєприпаси типу МОН-90, МОН-200 можуть ефективно уражати малошвидкісні БпЛА.

2. Визначення впливу механічної енергії та залежність кута руху осколків.

Осколок, який рухається у повітрі має певну енергію, яка визначається законом механічної енергії $\frac{mV^2}{2} = mgh$.

Для визначення висоти h на яку може піднятися осколок зберігаючи своє V_{kr} , проводим інтегрування рівняння закону механічної енергії, де:

$$h = \sqrt{\frac{2mV}{mg}}, \quad (4)$$

визначаємо час за який осколок проходить від початкового до критичної межі (можливість ураження цілі) за виразом $V_{kr} = V_0 - gt$, де:

$$t = \frac{V_0 - V_{kr}}{g}. \quad (5)$$

Показник дальності ураження цілі у вертикальній площині буде також залежати від кута руху осколків інженерних боєприпасів α . При цьому величина кута α буде впливати на висоту ураження повітряної цілі h_{yr} .

Для визначення h_{yr} будемо використовувати вираз:

$$h_{yr} = L_{yr} \cdot \sin \alpha, \quad (6)$$

Показник висоти ураження повітряної цілі h_{yr} інженерними боєприпасами направленої дії з різними значеннями кута α відображено в табл. 4.

Таблиця 4

Розрахункові дані показника висоти ураження повітряної цілі з використанням інженерних боєприпасів у вертикальній площині

Кут α , град.	h_{yr} , м	
	МОН-90	МОН-200
90	90	200
80	89	197
70	84	188
60	78	173
50	69	153
40	58	128

При цьому з постійним зменшенням кута α на 10 град висота ураження повітряної цілі h_{yr} буде зменшуватися в середньому на 10 %. При розрахунках для дальності ураження цілі L_{yr} використані існуючі технічні характеристик інженерних боєприпасів МОН-90, МОН-200 та не враховувалися V_0 , V_{kr} .

3. Визначаємо імовірність ураження повітряної цілі.

Імовірність ураження повітряної цілі інженерними боєприпасами P_{yib} буде залежати від щільності осколкового поля та розмірів проекції площі зустрічі осколків з цілю. Імовірність ураження P_{yib} має вигляд [10]:

$$P_{yib} = 1 - \exp\left(-\Pi \cdot \frac{S_y}{n_{yr}}\right), \quad (7)$$

де, Π – щільність осколків; S_y – площа ураження цілі, м²; n_{yr} – кількість попадань осколків у ціль.

Щільність осколків Π визначається із врахуванням способу формування зон ураження цілей, кутів розльоту уламків та їх кількості, а кількість уламків залежить від способу формування осколкового поля та визначається наступним виразом [10]:

$$\Pi = \frac{N}{S_{cp}}, \quad (8)$$

де, N – кількість осколків; S_{cp} – площа поверхні фронту уламкового поля, м².

Форма фронту осколкового поля може мати вигляд шарового сегменту, тоді його площа визначається [10]:

$$S_{cp} = 2\pi r^2 \left[1 - \cos \frac{\alpha}{2}\right], \quad (9)$$

де, r – відстань від місця ініціювання боєприпасу; α – кут руху осколків.

Для умов рівномірного розподілу осколків в межах сформованого осколкового поля були визначені значення щільності вісісиметричного спрямованого поля осколків, залежність від віддалення від точки ініціювання (рис. 3) [10].

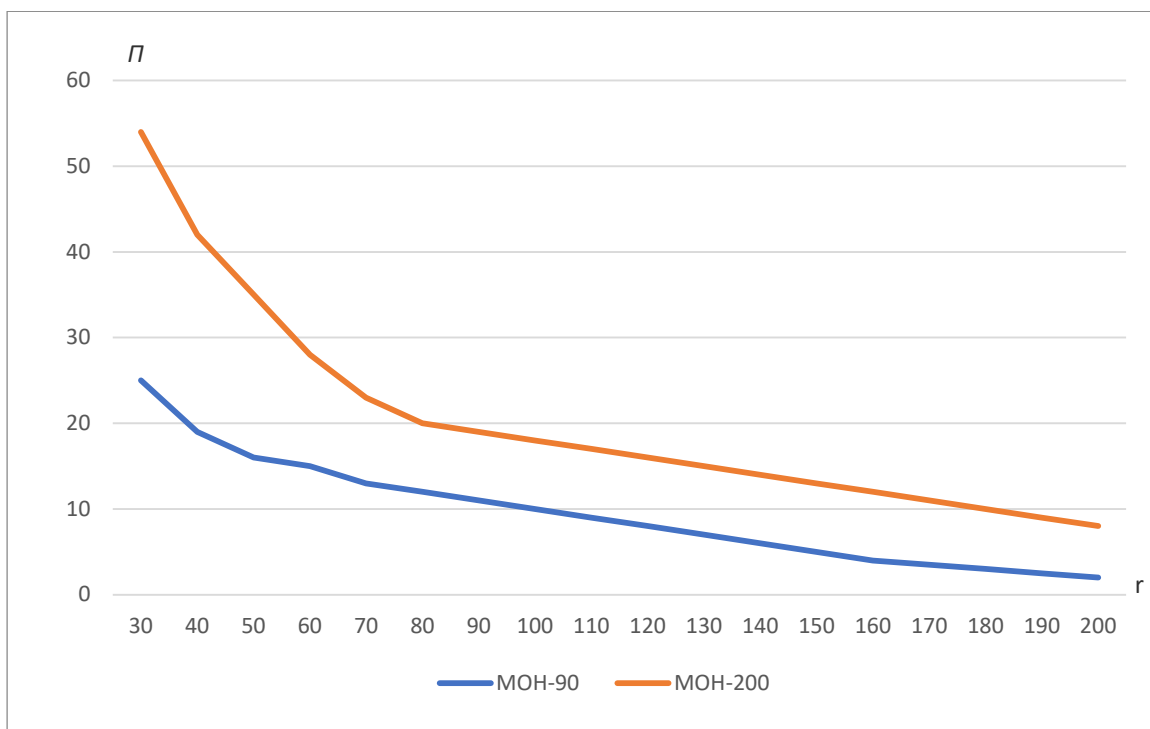


Рисунок 3 – Залежність щільності осколкового поля від віддалення точки ініціювання інженерних боєприпасів

Дослідження показали, що найбільша імовірність ураження цілі досягається при попаданні в її проекцію не менш ніж три осколка на 1 м^2 [11].

Імовірність ураження P_{yib} в корпус повітряної цілі інженерними боєприпасами МОН-90 та МОН-200 в залежності від віддалення місця ініціювання боєприпасу наведено на рис. 4.

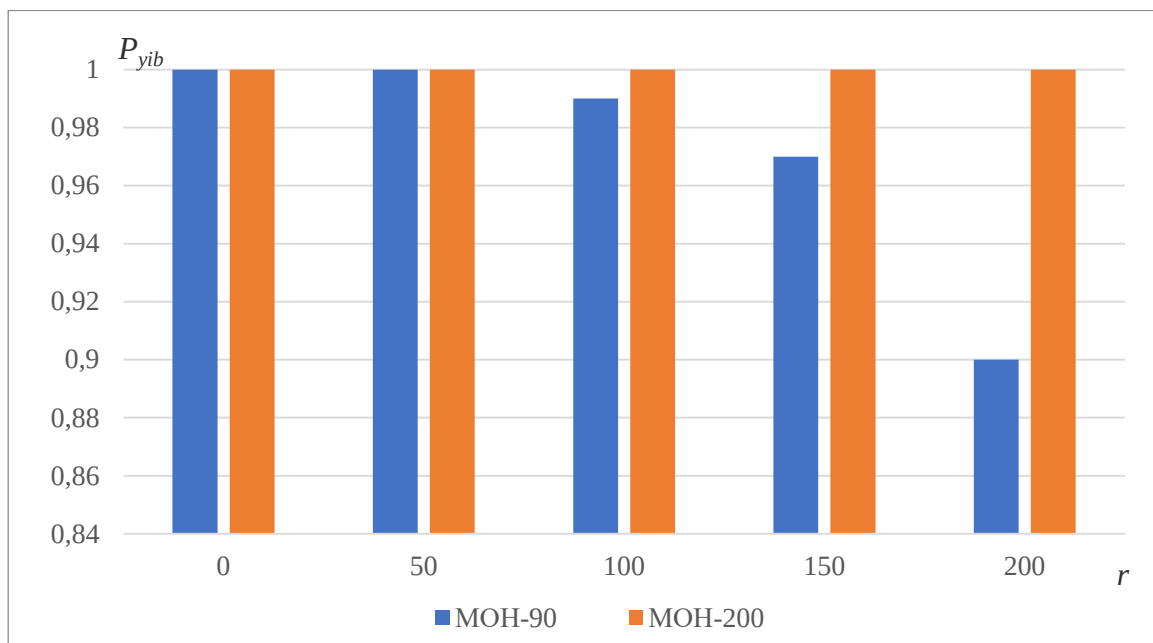


Рисунок 4 – Залежність ймовірності влучення P_{yib} в корпус повітряної цілі

Розрахунки показали, що імовірність ураження повітряної цілі P_{yib} при знаходженні її в зону ураження осколкового вибухового пристрою направленої дії знаходиться в межах середнього показника 0,9. При цьому не враховано дальність ураження цілі L_{yt} інженерними боеприпасами, а основним показником у досягненні таких значень відбувається за рахунок великої щільності осколків Π [11]. Отже, середній показник імовірності ураження повітряної цілі інженерними боеприпасами буде становити 0,9, що досить високий.

За допомогою цього принципу зміни кутових показників та відповідного розміщення інженерних боеприпасів можливо створити “осколковий купол” з використанням осколкового поля навколо об’єкта який підлягатиме захисту від ураження БпЛА.

Для розміщення інженерних боеприпасів направленої дії найбільш доцільним варіантом буде використовувалися фігурних форм, таких як колоподібної та квадратоподібної форми.

Відстань між мінами буде залежати від щільності осколкового поля відповідно до їх форми та розмірів. Ряди МП будуть встановлюватися зі зміщенням, це забезпечить зменшення “сліпих зон” між осколковими полями [12, 13]. Кількість інженерних боеприпасів буде залежит від збільшення дальності встановлення боеприпасів та розміру площі об’єкта.

В подальшому необхідно визначити надходження повітряної цілі в зону ініціації інженерного боеприпасу, з координатами мін (x_n, y_n, z_n) та БпЛА (x_c, y_c, z_c) , що матиме нерівність:

$$\sqrt{(x_c(t) - x_n)^2 + (y_c(t) - y_n)^2 + (z_c(t) - z_n)^2} < R, \quad (10)$$

де, R – відстань до повітряної цілі.

На рис. 5 відображено варіант розміщення осколкового вибухового пристрою направленої дії у фігурних формах.

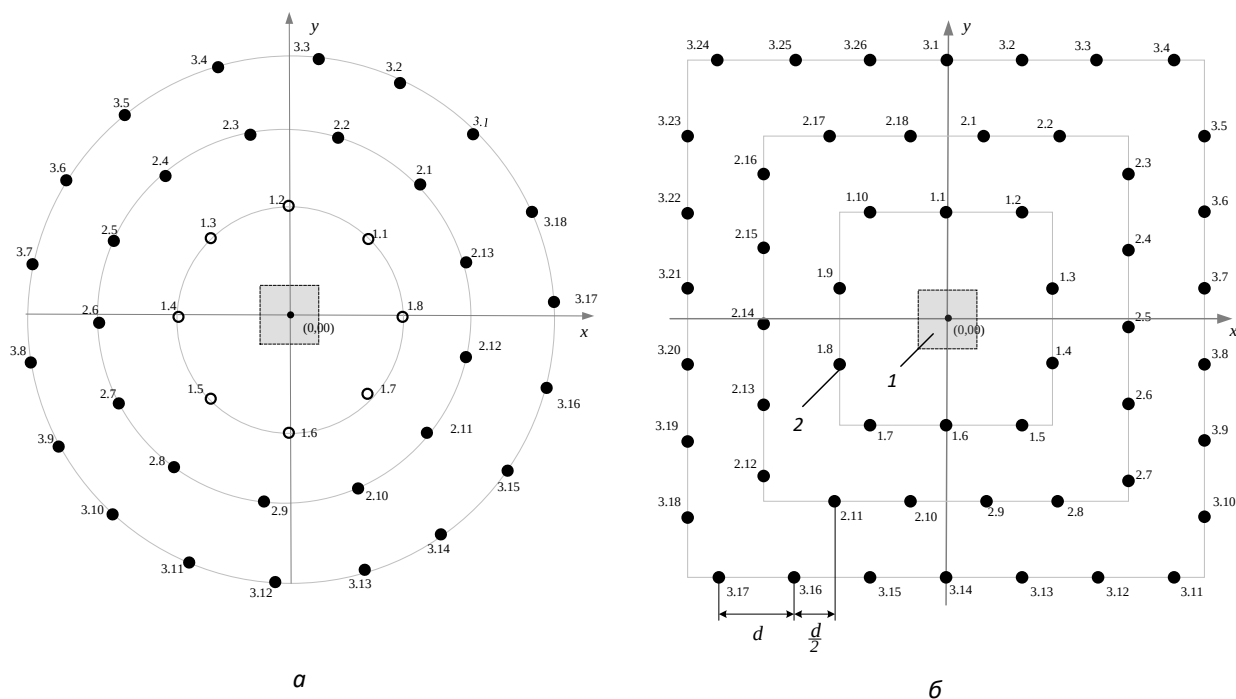


Рисунок 5 – Варіант схеми розміщення осколкового вибухового пристрою направленої дії:

a – колоподібна форма; b – квадратоподібна форма; 1 – площа об’єкта; 2 – інженерний боеприпас; d – відстань між мінами

Таким чином, для ураження повітряної цілі типу БпЛА використання осколкових інженерних боєприпасів направленої дії є доцільним з подальшим створенням системи захисту військ та об'єктів від ураження повітряних цілей.

Результати даних розрахунків дозволяють зробити висновок що осколкові вибухові пристрої направленої дії, або їх аналоги можуть ефективно використовуватися для ураження малозшвидкісних, низьколітаючих повітряних цілей з визначеними характеристиками.

Висновки. Використання осколкових боєприпасів для боротьби з БпЛА на сьогоднішній день є пріоритетним шляхом ефективної протидії даним засобам. Проте, в існуючих дослідженнях недостатня увага звернена до застосування осколкових протипіхотних вибухових пристроїв направленої дії, які знаходяться на озброєнні ЗС України і характеризуються як відносно дешевий та ефективний засіб.

В роботі запропонована методика розрахунку основних параметрів інженерних боєприпасів для ураження БпЛА. Отримано швидкісні параметри осколка, дальність ураження цілі з різними формами осколків та коефіцієнтом C , вирази висоти ураження цілі зі зміною кута руху осколка та імовірність ураження цілі в залежності від щільності осколкового поля та площі цілі. Наведені варіанти розміщення осколкових вибухових пристроїв направленої дії з різним фігурними формами.

Напрямком подальших досліджень може бути розробка активної системи захисту об'єктів та військ від ураження БпЛА з використанням осколкових вибухових пристроїв направленої дії у вигляді захисного купола з осколкових полів.

ЛІТЕРАТУРА:

1. Майстренко О.В., Іваник Є.Г., Прокопенко В.В., Бубенчиков Р.В., Стегура С.І. Методика розрахунку ураження безпілотних літальних апаратів артилерійськими боєприпасами. Збірник наукових праць Національної академії сухопутних військ. Львів. 2018. Вип. 3(10), С 34-40.
2. Мельничук А.И., Горячев Н.В., Юрков Н.К. Способы и средства противодействия беспилотным летательным аппаратам. Надежность и качество сложных систем. 2020, Вип. 4(32). С 131-138. URL: <https://cyberleninka.ru/article/n/sposoby-i-sredstva-protivodeystvia-bespilotnym-letatelny-m-apparatfm> (дата звернення 17.05.2023).
3. Ленков С., Кривцун В., Мірошніченко О., Голушко С., Кольцов Р. Аналіз стану розвитку питання захисту об'єктів критичної інфраструктури з використанням інженерних боєприпасів. *Underwatertechnologiesindustrialandcivilengineering*. 2023. С 81-91.
4. Кривцун В.І., Нагачевський В.Й., Каленик М.М., Голушко С.Л. Використання осколкових протипіхотних вибухових пристроїв направленої дії як один із засобів протидії БпЛА в умовах обмежених ресурсів. Збірник наукових праць НАДПСУ. Хмельницький. 2024, Вип. 94(1). С 152-164.
5. Саламахин Т.М., Мякишев Б.А., Ротт О.Е., Франкевич А.А., Целовальников Е.П., Висящев В.Ю. Основы применения взрыва для решения военно-инженерных задач при ведении боевых действий. \Підручник\ Част. 1. М. 2013, 463с. Доступ до підр.: <https://www.sprtyvg7.com.ua>.
6. Ментус І.Е. Ефективність інженерних боєприпасів. \Навчальний посібник\ – Кам'янець-Подільський: ФВП ПДАТУ, 2008, 80 с.
7. Средства поражения и боеприпасы: учебник / Под ред. В.В. Селиванова. М.: Издательство МГТУ им. Н.Э. Баумана, 2008. – 284 с. Доступ до підр.: <https://ru.scribd.com/search?query>.
8. Бричинський О.В., Окіпняк Д.А., Малюк В.М., Бурашніков О.О., Ковальов Г.Г., Фарбота А.І., Нецадін О.В., Головатий Р.М. Вибухова справа \Підручник\ Львів, НАСВ. 2023, 488с.
9. Гуцул Т., Жежера І., Ткач В. Особливості класифікації та методів вибору БпЛА. *Технічні науки та технології*. 2022. Вип. 4(30), С 201-212.

10. Журавлев А.А., Орлов С.В. Обґрунтування значення площі досвідного ураження цілі в засобах ураження, оснащених осколочно-фугасними боєприпасами. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків. 2012, Вип. 3(9) С. 176-178.

11. Макаренко С.И., Тимошенко А.В. Анализ средств и способов противодействия беспилотным летательным аппаратам. [Електронний ресурс]. Системы управления, связи и безопасности. 2020 Вип. 1, С. 147-197 Режим доступа до журн.: <http://sccs.intelgr.com/archive/2020-01/06-Makarenko.pdf>.

12. Наказ МОУ від 04.01.2017 №2 “Керівництво з застосування інженерних боєприпасів у міністерстві оборони України та Збройних силах України”. Київ, 289 с.

13. Ткачук П.П., Чумакевич В.О., Дробан О.М., Федор Б.С., Евдокимов П.М. Боєприпаси: //Підручник// Львів: АСВ, 2011. – 319 с.

REFERENCES:

1. Maistrenko O.V., Ivanyk Ye.H., Prokopenko V.V., Bubenshchikov R.V., Stehura S.I. (2018). “Metodyka rozrakhunku urazhennia bezpilotnykh litalnykh aparativ artileryiskymy boieprypasamy”. [Methodology for calculating the defeat of unmanned aerial vehicles by artillery ammunition]. Collection of scientific papers of the National Army Academy, No. 3 (10), pp 34-40.

2. Melnychuk A.Y., Horiachev N.V., Yurkov N.K. (2020). “Sposobu y sredstva protyvodeistviya bespylotnym letatelnykh apparatam”. [Ways and means of countering unmanned aerial vehicles]. Reliability and quality of complex systems, No. 4 (32), pp 131-138, <https://cyberleninka.ru/article/n/sposoby-i-sredstva-protivodeystvia-bespylotnym-letatelnykh-apparatam> (accessed 17 may 2023).

3. Lienkov S., Kryvtun V., Miroshnichenko O., Holushko S., Koltsov R. (2023). “Analiz stanu rozvytku pytannia zakhystu ob'ektiv krytychnoi infrastruktury z vykorystanniam inzhenernykh boieprypasiv”. [Analysis of the state of development of the issue of protection of critical infrastructure facilities using engineered munitions]. pp 81-91.

4. Kryvtun V.I., Nahachevskiy V.I., Kalenyk M.M., Holushko S.L. (2023). “Vykorystannia oskolkovykh protypikhotnykh vybukhovykh prystroiv napravlanoi dii yak odyn iz zasobiv protydii BpLA v umovakh obmezhenykh resursiv”. [The use of fragmentation anti-personnel explosive devices as a means of countering UAVs in conditions of limited resources]. Collection of scientific works of NADPSU, No. 94(1), pp 152-164.

5. Salamakhyn T.M., Miakyshev B.A., Rott O.E., Franskevych A.A., Tselovalnykov E.P., Vysiashchev V.Iu. (2013) “Osnovu pryimeneniya vzryva dlia resheniya voenno-ynzhenernykh zadach pry vedenii boevykh deistviy”. [Fundamentals of using explosion to solve military engineering problems in combat operations]. Art. 1. Textbook. P. 463, <https://www.sprtyvg7.com.ua>.

6. Mentus I.E. (2008). “Efektivnist inzhenernykh boieprypasiv”. [Effectiveness of engineered munitions]. Faculty of Military Training at Podilskyi State Agrarian and Technical University. P. 80.

7. V.V. Selyvanov (2008). “Sredstva porazheniya y boieprypasu” [Means of destruction and ammunition] Bauman M. State Technical University Publishing House. 284 p. <https://ru.scribd.com/search?query>.

8. Brychynskiy O.V., Okipniak D.A., Maliuk V.M., Burashnikov O.O., Kovalov H.H., Farbota A.I., Neshchadin O.V., Holovaty R.M. (2023). “Vybukhova sprava” [Explosives business]. Textbook. National Academy of Land Forces. P. 488.

9. Hutsul T., Zhezhera I., Tkach V. (2022). “Osoblyvosti klasyfikatsii ta metodiv vyboru BpLA” [Features of UAV classification and selection methods]. Technical sciences and technologies, No. 4(30), pp 201-212.

10. Zhuravliev A.A., Orlov S.V. (2012). “Obgruntuvannia znachennia ploshchi dosvidnoho urazhennia tsili v zasobamy urazhennia, osnashcheny oskolochno-fugasnymi boieprypasamy” [Substantiation of the value of the area of experimental target destruction in the means of destruction equipped with high-explosive munitions]. Science and Technology of the Air Force of the Armed Forces of Ukraine, No. 3(9), pp 176-178.

11. Makarenko S.Y., Tymoshenko A.V. (2020). “Analiz sredstv y sposobov protyvodeistviya bespylotnym letatelnykh apparatam”. [Analysis of means and methods of countering unmanned aerial vehicles]. Control, communication and security systems, No. 1, pp 147-197, <http://sccs.intelgr.com/archive/2020-01/06-Makarenko.pdf>.

12. Nakaz MOU vid 04.01.2017 №2“Kerivnytstvo z zastosuvannia inzhenernykh boieprypasiv u ministerstvi oborony Ukrainy ta Zbroinykh sylakh Ukrainy”. [Guidelines for the use of engineered munitions in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine]. P. 289.

13. Tkachuk P.P., Chumakevych V.O., Droban O.M., Fedor B.S., Evdokymov P.M. (2011). “Boieprypasy”. [Ammunition]. P. 319.

PhD Kryvtsum V.I., Holushko S.L.

METHODOLOGY FOR CALCULATING THE MAIN PARAMETERS OF FRAGMENTATION EXPLOSIVE DEVICES FOR DESTRUCTION OF AIR TARGETS OF THE BPL TYPE

Based on the experience of the Russian-Ukrainian war, there is a tendency to increase the number of unmanned aerial vehicles used to destroy equipment, personnel, and infrastructure. For this purpose, unmanned aerial vehicles such as barrage munitions, kamikaze, drop drones, etc. are used. The share of losses of weapons and equipment, as well as personnel, caused by such weapons has become the largest compared to other means of destruction. To counteract such means, various anti-aircraft missile systems, electronic warfare equipment and mobile fire groups are used. The most effective way to defeat unmanned aerial vehicles is to hit them with a large number of destructive elements (fragments). Taking into account the ratio of the cost of unmanned aerial vehicles and means of their destruction, in particular anti-aircraft missile munitions, the paper proposes the use of fragmentation explosive devices of directed action to defeat attack unmanned aerial vehicles according to the "effectiveness-cost" criterion.

The article presents an analysis of studies of the effectiveness of the use of directed-action fragmentation munitions. A study of the feasibility of using directed-action fragmentation engineering ammunition of the MON series mines is carried out. On the basis of the mathematical model of the flight of a fragment, taking into account its shape, a methodology for calculating the main parameters of fragmentation explosive devices of directed action for the destruction of air targets such as unmanned aerial vehicles is proposed. Mathematical calculations are presented to determine the main characteristics of fragmentation explosive devices of directed action for defeating unmanned aerial vehicles, taking into account the external trajectory measurements of the target and the factors that affect the formation of the fragmentation field (zone). Schemes of deployment of fragmentation explosive devices of directed action for the protection of objects are proposed.

Keywords: *unmanned aerial vehicle, means of destruction, engineering fragmentation munitions of directed action, protection of objects.*

РОЗВ'ЯЗАННЯ МУЛЬТИМОДАЛЬНОЇ ТРАНСПОРТНОЇ ЗАДАЧІ З УРАХУВАННЯМ ОБМЕЖЕНЬ ЛОГІСТИЧНИХ ПОКАЗНИКІВ

Здійснення військових перевезень усіма видами транспорту передбачає планування, управління, розгортання транспортних комунікацій, розподіл та підготовку видів транспорту, організацію перевезення військ і транспортування військового майна, евакуацію поранених та хворих, пошкодженого озброєння і військової техніки, трофейного майна. В результаті цих дій має бути вирішене питання своєчасної доставки матеріально-технічних засобів з найменшими витратами.

Для вирішення задачі раціонального розподілу доставки матеріально-технічних засобів в умовах оперативного переміщення пунктів зберігання та споживачів, зміни маршрутів постачання та виду транспортних засобів доставки, пропонується розв'язання мультимодальної (трьохіндексної біпланарної) транспортної задачі з урахуванням обмежень логістичних показників: час постачання; наявна вантажопідйомність транспортних засобів різних видів та загальна вартість перевезень. Введення додаткових обмежень в трьохіндексну біпланарну транспортну задачу перетворює її в задачу лінійного програмування загального вигляду. Представлено математичну постановку трьохіндексної транспортної задачі з додатковими логістичними обмеженнями. Надано форму представлення вихідних даних у вигляді розширених транспортних таблиць вартостей перевезень та витрат часу на перевезення вантажів. Показано зручний спосіб розв'язання такої задачі симплекс-методом в надбудові «Пошук розв'язання» табличного процесору Microsoft Excel.

В статті наводяться результати розв'язання мультимодальної транспортної задачі з логістичними обмеженнями в табличному процесорі Microsoft Excel на прикладі доставки матеріально-технічних засобів трьома видами транспорту (автомобільним, залізничним; річковим) з урахуванням обмежень за часом та вартістю доставки. У прикладі застосовані умовні вихідні дані щодо доставки вантажів з трьох міст (пунктів зберігання) до трьох інших міст (пунктів споживання) в межах України.

Ключові слова: військова логістика, мультимодальна транспортна задача, симплекс-метод, цільова функція, обмеження, план перевезень.

Вступ. Питання ефективності логістики пов'язують не лише з наявністю, зберіганням та раціональним розподілом матеріально-технічних засобів (МтЗ) серед споживачів. Найважливішою функцією є здійснення військових перевезень і транспортування усіма видами транспорту, яка полягає в організації планування, управління, розгортання транспортних комунікацій, розподілу та підготовці видів транспорту, організації перевезення військ і транспортування військового майна, евакуації поранених та хворих, пошкодженого озброєння і військової техніки, трофейного майна. Фактично ідеться про вирішення питання своєчасної доставки МтЗ з найменшими витратами.

В умовах сьогодення, під час війни, як ніколи є актуальним твердження, що сучасні війни – це війни економік, які мають найбільший потенціал, вміють враховувати та передбачати ефективність кожного ресурсу витраченого на війну та вкладеного у країну. Поряд з цим значна протяжність фронту, систематичне перегрупування військ та знищення об'єктів зберігання МтЗ висуває певні критерії щодо оперативності та вартості транспортування. Потрібно враховувати обмеження по часу, за який необхідно доставити МтЗ, забезпечуючи

найменшу вартість транспортування за рахунок оптимального вибору виду транспортного засобу (ТЗ) з наявного парку.

Таким чином, раціональність перевезень є ключовим фактором для забезпечення ефективної роботи транспортної системи. Організація перевезень передбачає розробку оптимальних маршрутів, раціональний розподіл наявних транспортних засобів різних видів для доставки МтЗ з мінімальними витратами на транспортування. Разом з цим має досягатися необхідна оперативність доставки військових вантажів до району призначення.

З метою спрощення роботи фахівців служби логістики з планування військових перевезень виникає потреба в інструментарії для розв'язання такої задачі, який повинен бути легкодоступним та простим у використанні.

Аналіз останніх досліджень і публікацій. На початковому етапі організації перевезень значне місце відводиться розрахункам потреби в підвезенні МтЗ, можливостей транспорту і засобів механізації вантажно-розвантажувальних робіт [1]. Для виконання розрахунків з перевезень застосовуються методики, які мають ураховувати конкретну обстановку, характер і види дій, наявність вихідних даних, потрібну точність результатів розрахунків та наявний ліміт часу на планування. Розрахунки, виконані навіть за самими точними методиками, стають непотрібними, якщо результати отримані з запізненням. За наявності часу, розрахунки виконують за методиками, які дозволяють отримати задовільні для практики результати [2-4]. Точність розрахунків значною мірою визначається точністю вихідних даних, які можуть змінюватись у часі.

За обмежень у часі розрахунки, зазвичай, виконуються за допомогою комп'ютерної техніки за методиками, які дозволяють в короткі терміни і з допустимими похибками отримати необхідні результати.

В умовах функціонування територіальної системи логістичного забезпечення, наявні кілька джерел матеріального забезпечення, з яких можуть отримувати матеріальні засоби один або декілька одержувачів. Доставку МтЗ в межах України можливо здійснювати з використанням транспортних засобів різного виду: автомобільного; залізничного; водного, повітряного. Для врахування складних компромісів між різними видами транспорту більш доцільним стає використання мультимодальних перевезень, що інтегрують декілька видів транспорту. Звідси виникає задача оптимального розподілу обсягу перевезень МтЗ за видами транспорту під час проведення операцій оперативних угруповань військ. Розв'язання цієї задачі вкрай важливе з точки зору скорочення часу доставки МтЗ, досягнення мінімальних економічних витрат, ефективного використання наявних транспортних засобів. В рамках розв'язання такого класу задач мають бути попередньо обрані оптимальні маршрути доставки МтЗ з кожного пункту зберігання в пункти споживання для всіх видів транспорту. Для виконання таких розрахунків застосовуються методи теорії графів [5], методи лінійного і динамічного програмування [6-8], методи мережевого планування [9], генетичні алгоритми [10], методи нечіткого програмування [11, 12] та інші. За результатами таких розрахунків або за більш простими практичними розрахунками з урахуванням розкладу руху транспорту обмеженою кількістю можливих маршрутів [10], отримуються числові значення вартостей та часу доставки МтЗ з пунктів зберігання до пунктів споживання. При цьому мультимодальність перевезень також може передбачати наявність проміжних пунктів перевантаження вантажів з одного виду транспорту на інший [12]. В запропонованій нами статті такі варіанти постачання на розглядаються.

Після отримання вихідних даних про вартість і витрати часу на доставку між пунктами зберігання та споживання, наступним кроком є розв'язання задачі знаходження оптимального плану доставки МтЗ з пунктів зберігання в пункти споживання з використанням різних видів транспортних засобів. Для розв'язання таких задач широко застосовуються точні методи лінійного програмування (ЛП), а саме розв'язання транспортної задачі ЛП [13]. На відміну від класичної двохіндексної транспортної задачі щодо оптимального, з точки зору вартості доставки, розподілу однорідних вантажів з пунктів зберігання в пункти споживання,

застосування різних видів ТЗ перетворює її у трьохіндексну. Проблема розв'язання багатойндексних транспортних і розподільних задач ЛП глибоко досліджувалися в [13]. Для випадку трьохіндексної транспортної задачі в [13] надані обчислювальні схеми та приклади її розв'язання. Важливим класом таких задач є трьохіндексні несиметричні транспортні задачі, для розв'язання яких не потрібно застосовувати загальні методи. Урахування специфіки задачі дозволяє отримати простий алгоритм розв'язання. В [13] сформульовано таку задачу та надано спосіб її розв'язання.

Модель задачі: знайти набір $\{x_{ijk}^*\}$, що мінімізує цільову функцію (ЦФ)

$$\min z(\mathbf{X}) = \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^p c_{ijk} x_{ijk}, \quad (1)$$

яка задовольняє обмеженням:

$$\begin{aligned} \sum_{j=1}^n \sum_{k=1}^p x_{ijk} &= a_i, \quad i = 1, \dots, m, \\ \sum_{i=1}^m \sum_{k=1}^p x_{ijk} &= b_j, \quad j = 1, \dots, n, \\ x_{ijk} &\geq 0, \quad i = 1, \dots, m, \quad j = 1, \dots, n, \quad k = 1, \dots, p. \end{aligned} \quad (2)$$

Задача (1), (2) має назву трьохіндексної біпланарної транспортної задачі (Т-2Р) [13]. Необхідною та достатньою умовою існування розв'язку задачі Т-2Р є умова балансу

$$\sum_{j=1}^n b_j = \sum_{i=1}^m a_i = S.$$

В [13] показано, що суттєві індексні елементи оптимального плану цієї задачі відповідають мінімальним значенням коефіцієнтів цільової функції у кожній колонці матриці $\{c_{ijk}\}$, тобто за індексом $k = q_{ij}$. Згідно доведеної в [13] теореми оптимальний план $\{x_{ijk}^*\}$ задачі (1), (2) має наступну структуру:

$$x_{ijk}^* = \begin{cases} x_{ijk} > 0, & i = \overline{1, m}, \quad j = \overline{1, n}, \quad k = q_{ij}; \\ 0, & i = \overline{1, m}, \quad j = \overline{1, n}, \quad k \neq q_{ij}. \end{cases} \quad (3)$$

А мінімальне значення ЦФ

$$\min z(\mathbf{X}) = \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^p c_{ijk} x_{ijk}^*.$$

Властивість (3) задачі Т-2Р дозволяє замість вихідної трьохіндексної задачі (1), (2) розв'язувати допоміжну двохіндексну транспортну задачу будь-яким із відомих методів [13]. Модель транспортної задачі Т-2Р відповідає практичному випадку доставки військових вантажів з кількох пунктів зберігання кільком споживачам і її доцільно застосовувати для пошуку оптимального плану перевезень.

Приклади розв'язання мультимодальної транспортної задачі виду (1), (2) з побудовою опорних планів розглядаються в [4, 14]. В [15] розв'язання мультимодальної транспортної задачі реалізовано за допомогою програмних засобів MS Excel, Mathcad та Matlab. За результатами моделювання отримані ідентичні результати. На користь якого з програмних пакетів віддати перевагу залежить від зручності та швидкодії, особливо за умов зростання розмірності задачі.

Запропонована в [13, 14] постановка мультимодальної транспортної задачі Т-2Р є класичною. Однак, на практиці виникає потреба урахування додаткових обмежень на обсяги

можливих перевезень кожним з видів транспорту k з пункту i в пункт j , а також на витрати часу t_{ijk} на їх виконання.

В [7, 13] розглядається задача мінімізації часу T , за який постачання всіх вантажів буде завершено. Її постановка, як показано в [7], може бути аналогічною звичайній транспортній задачі, однак вагові коефіцієнти в цьому випадку є не транспортними витратами на одиницю маси вантажу, а часом постачання МтЗ з одного пункту зберігання до пункту споживання. Оптимальним буде такий план перевезень (x_{ij}) , за якого час T є мінімальним, тому ЦФ має вигляд

$$T = \max_{x_{ij} > 0} t_{ij} = \min. \quad (4)$$

В такій постановці задача не є задачею ЛП, оскільки величина T не є лінійною функцією змінних x_{ij} , які згідно (4) мають бути більшими за нуль. Така задача може бути розв'язана методом «заборонених клітинок» [7]. Сутність методу полягає у викреслюванні клітинок з найбільшим часом в транспортній таблиці та проведенням оптимізації за мінімумом ЦФ L , яке є мінімальною сумою добутоків для певного плану перевезень (x_{ij}) з обмеженням часу T

$$\min L = \sum_{i=1}^m \sum_{j=1}^n c_{ij} x_{ij},$$

де c_{ij} – вагові коефіцієнти, які дорівнюють t_{ij} для клітинок з незмінними значеннями та $t_{ij} + M$ – для клітинок, в яких $t_{ij} > T$, з доданим великим числом M .

Представляє інтерес пошук розв'язку мультимодальної транспортної задачі Т-2Р за мінімумом вартості перевезень з додатковим урахуванням обмеження на час доставки МтЗ T , а також можливих обмежень на обсяги перевезень для різних видів ТЗ та їх вартість.

Метою статті є розв'язання мультимодальної транспортної задачі з додатковими логістичними обмеженнями щодо строків постачання МтЗ, обсягу перевезень вантажів для різних видів ТЗ та загальної вартості перевезень.

Виклад основного матеріалу. Розглянемо постановку задачі (1), (2) з додатковими обмеженнями на обсяг перевезень для різних видів транспорту у вигляді

$$\sum_{j=1}^n x_{ijk} \leq d_{ik}, i = 1, \dots, m, k = 1, \dots, p, \quad (5)$$

де d_{ik} – загальна вантажопідйомність k -го виду транспорту, який застосовується для одноразового перевезення МтЗ з i -го пункту зберігання усім n споживачам.

В таблиці транспортних витрат для кожного пункту зберігання замість одного рядка для двохіндексної транспортної задачі пропонується ввести p рядків для наявних видів транспорту. Також додамо стовпчик з наявними вантажопідйомностями d_{ik} для кожного виду транспорту. Таблиця витрат для випадку $p = 3$ матиме вигляд, як показано на рис. 1.

Транспортна таблиця для розв'язку задачі матиме аналогічний вигляд (рис. 2). Однак, якщо в таблиці на рис. 1 у стовпчику D_n наведені наявні вантажопідйомності d_{ik} , то на рис. 2. у стовпчику D_v вантажопідйомності d_{ik} є використаними вантажопідйомностями для всіх видів транспорту в кожному з пунктів зберігання. Тобто в цій таблиці вони є сумою мас відповідного рядка згідно з (5) для випадку рівності, наприклад, для першого рядка $d_{11} = \sum_{j=1}^n x_{1j1}$. Введення

додаткових обмежень (5) перетворює задачу Т-2Р в задачу ЛП загального вигляду, яка може бути розв'язана, наприклад, симплекс-методом. Обмеження вантажопідйомностей означає можливість такої ситуації, коли неможливо виконати доставку МтЗ з використання транспортних засобів лише одного виду.

	D_n	B_1	B_2	...	B_n	Пропозиція
A_1	d_{11}	c_{111}	c_{121}	...	c_{1n1}	a_1
	d_{12}	c_{112}	c_{122}	...	c_{1n2}	
	d_{13}	c_{113}	c_{123}	...	c_{1n3}	
A_2	d_{21}	c_{211}	c_{221}	...	c_{2n1}	a_2
	d_{22}	c_{212}	c_{222}	...	c_{2n2}	
	d_{23}	c_{213}	c_{223}	...	c_{2n3}	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$
A_m	d_{m1}	c_{m11}	c_{m21}	...	c_{mn1}	a_m
	d_{m2}	c_{m12}	c_{m22}	...	c_{mn2}	
	d_{m3}	c_{m13}	c_{m23}	...	c_{mn3}	
Попит		b_1	b_2	...	b_n	

Рисунок 1 – Загальний вигляд таблиці транспортних витрат

	D_B	B_1	B_2	...	B_n	Пропозиція
A_1	d_{11}	x_{111}	x_{121}	...	x_{1n1}	a_1
	d_{12}	x_{112}	x_{122}	...	x_{1n2}	
	d_{13}	x_{113}	x_{123}	...	x_{1n3}	
A_2	d_{21}	x_{211}	x_{221}	...	x_{2n1}	a_2
	d_{22}	x_{212}	x_{222}	...	x_{2n2}	
	d_{23}	x_{213}	x_{223}	...	x_{2n3}	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$
A_m	d_{m1}	x_{m11}	x_{m21}	...	x_{mn1}	a_m
	d_{m2}	x_{m12}	x_{m22}	...	x_{mn2}	
	d_{m3}	x_{m13}	x_{m23}	...	x_{mn3}	
Попит		b_1	b_2	...	b_n	

Рисунок 2 – Загальний вигляд таблиці розв'язку транспортної задачі

Урахування часових обмежень пропонується реалізувати за методом заборонених клітинок. Для цього введемо додаткову таблицю часу доставки (рис. 3), яка є подібною до поданої на рис. 1. Відмінностями таблиці, як й у випадку двохіндексної транспортної задачі є заміна вартостей постачання одиниці МтЗ часом доставки з пункту зберігання в пункт споживання відповідним видом транспорту, а також виключення стовпчика D_n .

Для урахування часових обмежень на перевезення вводяться граничні допустимі строки постачання необхідного обсягу МтЗ у кожний з пунктів споживання $T_j, j = \overline{1, n}$. Якщо $T_1 = T_2 = \dots = T_n = T$, тоді йдеться про вимогу виконання всіх поставок в межах загального часу T . В іншому разі обмеження на час постачання МтЗ будуть різними, залежно від потреби.

Після цього в кожному стовпчику таблиці часу доставки вантажів (рис. 3) виконуються порівняння часу t_{ijk} з часовим обмеженням T_j . Якщо $t_{ijk} > T_j$, тоді клітинка вважається забороненою і в неї замість відповідного підставляється велике число. Одночасно велике число додається також у відповідні клітинки в таблиці транспортних витрат (рис. 1). Ці клітинки стають забороненими при виконанні оптимізації за вартістю перевезень в задачі (1), (2). Їх застосування призводить до значного зростання ЦФ, що означає неможливість

задовольнити умовам перевезення з часовими обмеженнями $T_j, j = \overline{1, n}$. На відміну від методу «заборонених клітинок», описаного в [7], в такій постановці задача залишається лінійною відносно вихідної ЦФ виду (1). Логістичний показник витрат часу на перевезення МтЗ з урахуванням їх обмежень є додатковим обмеженням, яке ураховується введенням заборонених клітинок. Таке обмеження може призвести до відсутності розв'язку задачі за умови, коли не можуть бути задоволені обмеження, тобто в процесі оптимізації застосовуються дані із заборонених клітинок. В такому випадку часові обмеження потрібно пом'якшувати збільшенням значень T_j .

	B_1	B_2	...	B_n	Пропозиція
A_1	t_{111}	t_{121}	...	t_{1n1}	a_1
	t_{112}	t_{122}	...	t_{1n2}	
	t_{113}	t_{123}	...	t_{1n3}	
A_2	t_{211}	t_{221}	...	t_{2n1}	a_2
	t_{212}	t_{222}	...	t_{2n2}	
	t_{213}	t_{223}	...	t_{2n3}	
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$
A_m	t_{m11}	t_{m21}	...	t_{mn1}	a_m
	t_{m12}	t_{m22}	...	t_{mn2}	
	t_{m13}	t_{m23}	...	t_{mn3}	
Попит	b_1	b_2	...	b_n	

Рисунок 3 – Загальний вигляд таблиці часу доставки вантажів в транспортній задачі

Розглянемо практичну реалізацію розв'язання транспортної задачі (1), (2) з додатковими логістичними обмеженнями на обсяги вантажопідйомності та строки доставки вантажів в табличному процесорі Excel. Умовні вихідні дані подані в таблицях (рис. 4 і 5), аналогічних представленим на рисунках 1 і 3. Показники вартості та часу доставки подані для трьох пунктів відправлення та трьох пунктів призначення для кожного з трьох видів транспорту (автомобільного, залізничного та річкового). Обмеження за часом доставки МтЗ T_j вводяться у три нижні клітинки таблиці в рядку T_j план (рис. 5).

D4							=IF(K4=\$I\$13;\$B\$13;'Показники ділянок'!G6)
	A	B	C	D	E	F	G
1	Вартість перевезення 1 тони вантажу						
2	Пункти відправлення	Вид транспорту	Наявна вантажопідйомність	Пункти призначення			Запаси
3				Миколаїв	Херсон	Одеса	
4				834,00	956,00	1110,00	
5	Переяслав-Хм	ЗАЛІЗНИЦЯ	1035	696,96	776,45	751,10	480
6		РІЧКА	1800	595,23	530,18	646,91	
7		АВТО	120	636,00	758,00	946,00	
8	Кременчук	ЗАЛІЗНИЦЯ	1035	368,00	446,98	543,74	420
9		РІЧКА	1800	400,00	356,90	474,24	
10		АВТО	120	180,00	312,00	286,00	
11	Вознесеньск	ЗАЛІЗНИЦЯ	1035	122,11	239,62	177,41	300
12		РІЧКА	1800	60,80	121,60	141,06	
13		100000000	Потреба	320	500	380	ТЗ ЗАКРИТА
14							

Рисунок 4 – Таблиця умов мультимодальної транспортної задачі за вартістю доставки

K4						
	H	I	J	K	L	M
1	Час доставки вантажу до пунктів призначення					
2	Пункти відправлення	Вид транспорту	Пункти призначення			
3			Миколаїв	Херсон	Одеса	
4	Переяслав-Хм	АВТО	6,62	7,47	8,16	
5		ЗАЛІЗНИЦЯ	13,75	16,85	15,9	
6		РІЧКА	54,09	48,99	59,11	
7	Кременчук	АВТО	5,68	6,42	8,76	
8		ЗАЛІЗНИЦЯ	6,96	9,95	10,98	
9		РІЧКА	36,11	32,98	41,94	
10	Вознесеньск	АВТО	1,76	2,74	3,67	
11		ЗАЛІЗНИЦЯ	2,94	5,94	2,96	
12		РІЧКА	5,26	10	12,02	
13	10000	Тіплан				
14						

Показники ділянок, які для наочності і зручності користування вводяться на окремому аркуші, показані на рис. 6. За наявності обмеження по часу доставки в стовпчику К (Тіплан), якщо значення часу доставки в клітинці К4 не задовольняє вимогам обмежень в неї буде введено велике число (10000) (рис. 7). За цим принципом вводяться подібні формули в усі клітинки діапазону К4:М12. Значення наявної вантажопідйомності також обчислюються на окремому аркуші і залежить від наявного парку транспортних засобів різних видів в пунктах зберігання та вантажопідйомності окремих одиниць.

Рисунок 6 – Показники часу доставки та вартості перевезення між пунктами відправлення та призначення

S17						
	H	I	J	K	L	M
1		Час доставки вантажу до пунктів призначення				
2		Пункти відправлення	Вид транспорту	Пункти призначення		
3				Миколаїв	Херсон	Одеса
4		Переяслав-Хм	АВТО	6,62	7,47	8,16
5			ЗАЛІЗНИЦЯ	10000	10000	15,9
6			РІЧКА	10000	10000	10000
7		Кременчук	АВТО	5,68	6,42	8,76
8			ЗАЛІЗНИЦЯ	6,96	10000	10,98
9			РІЧКА	10000	10000	10000
10		Вознесеньск	АВТО	1,76	2,74	3,67
11			ЗАЛІЗНИЦЯ	2,94	5,94	2,96
12			РІЧКА	5,26	10000	12,02
13		10000	Тіплан	7	8	17

Рисунок 7 – Заборонені клітинки в таблиці часу доставки з часовими обмеженнями

Наступним кроком зміни вводяться в таблицю умов мультимодальної транспортної задачі (рис. 4). В клітинку B13 введено велике число (100000000) для показників вартості. В клітинку D4 введено формулу “=IF(K4=\$I\$13;\$B\$13;'Показники ділянок'!G6)”, яка у разі заборони клітинки в таблиці умов розрахунку часу доставки (рис. 7) заборонятиме відповідну клітинку (виводити велике число з клітинки B13) в таблицю умов мультимодальної транспортної задачі за вартістю (рис. 4). За таким принципом вводяться формули в усі клітинки діапазону D4:F12.

Відповідні забороненим клітинкам у таблиці умов розрахунку часу доставки (рис. 7) будуть заборонені клітинки в таблиці на рис. 4 умов мультимодальної транспортної задачі, що виключатиме їх із цільової функції (рис. 8).

N15							
	A	B	C	D	E	F	G
1	Вартість перевезення 1 тони вантажу						
2	Пункти відправлення	Вид транспорту	Наявна вантажопідйомність	Пункти призначення			Запаси
3				Миколаїв	Херсон	Одеса	
4	Переяслав-Хм	АВТО	120	834,00	956,00	1110,00	480
5		ЗАЛІЗНИЦЯ	1035	100000000,00	100000000,00	751,10	
6		РІЧКА	1800	100000000,00	100000000,00	100000000,00	
7	Кременчук	АВТО	120	636,00	758,00	946,00	420
8		ЗАЛІЗНИЦЯ	1035	368,00	100000000,00	543,74	
9		РІЧКА	1800	100000000,00	100000000,00	100000000,00	
10	Вознесеньск	АВТО	120	180,00	312,00	286,00	300
11		ЗАЛІЗНИЦЯ	1035	122,11	239,62	177,41	
12		РІЧКА	1800	60,80	100000000,00	141,06	
13		100000000	Потреба	320	500	380	ТЗ ЗАКРИТА
14							

Рисунок 8 – Заборонені клітинки в таблиці умов мультимодальної транспортної задачі за критерієм вартості

Розрахунок цільової функції здійснюється в окремій клітинці, зазвичай нижче таблиці опорного плану перевезень. У нашому випадку в клітинку E30 треба ввести формулу “=SUMPRODUCT(D4:F12;D19:F27)” (рис. 9).

Для урахування обмежень по загальній вартості перевезень в клітинки B30 та B31 вводяться два параметри: максимальної S_{max} та мінімальної S_{min} допустимих вартостей

перевезень (рис. 9). В розглянутому прикладі в ці клітинки введено: в клітинку B30 – занадто велике значення; в клітинку B31 – нуль, що виключило вплив цих обмежень.

N15							
	A	B	C	D	E	F	G
14							
15		ПЛАН ПЕРЕВЕЗЕНЬ					
16							
17	Пункти відправлення	Вид транспорту	Використана вантажопідйомність	Пункти призначення			Запаси
18				Миколаїв	Херсон	Одеса	
19	Переяслав-Хм	АВТО	120		120		480
20		ЗАЛІЗНИЦЯ	360			360	
21		РІЧКА					
22	Кременчук	АВТО	80		80		420
23		ЗАЛІЗНИЦЯ	340	320		20	
24		РІЧКА					
25	Вознесенськ	АВТО					300
26		ЗАЛІЗНИЦЯ	300		300		
27		РІЧКА					
28			Потреба	320	500	380	
29							
30	Smax=	100000000		S =	646277,12		
31	Smin=	0					

Рисунок 9 – Оптимальний план перевезень за критерієм вартості з обмеженням за часом доставки та вантажопідйомністю ТЗ

Наступним кроком необхідно ввести параметри розв’язувача табличного процесору Microsoft Excel. З цією метою на вкладці “Дані” в групі “Аналіз” застосовується команда “Розв’язувач” та розгортається діалогове вікно “Параметри розв’язувача”, в якому вводяться всі необхідні обмеження задачі (1), (2) і додаткові (5). Розв’язання задачі виконується симплекс-методом. Оптимальний план перевезень, який отримано з використанням надбудови “Пошук розв’язання” табличного процесору Microsoft Excel, представлено на рис. 9.

Введені обмеження вплинули на оптимальний розподіл обсягу перевезень за видами транспорту та збільшили вартість перевезення з 459589,76 грн до 646277,12 грн, але при цьому дотримано обмеження за часом доставки (рис. 7).

Таким чином, за допомогою надбудови “Пошук розв’язання” в табличному процесорі Microsoft Excel показано можливість здійснювати оптимальний розподіл обсягу перевезень по видах транспорту за критерієм вартості з урахуванням обмежень за трьома логістичними показниками: наявна вантажопідйомність транспортних засобів; час доставки в пункти призначення, вартість перевезення.

Висновки та перспективи подальших досліджень. Запропоновано постановку та варіант розв’язання мультимодальної транспортної задачі, в якій на відміну від класичної трьохіндексної біпланарної транспортної задачі, додатково ураховуються обмеження таких логістичних показників як строки постачання; наявна вантажопідйомність транспортних засобів різних видів та загальна вартість перевезень.

На умовному прикладі підтверджено можливість проведення розрахунків з розподілу обсягу перевезень МТЗ за видами транспорту з додатковими логістичними обмеженнями симплекс-методом за допомогою надбудови “Пошук розв’язання” в табличному процесорі Microsoft Excel, як поширеному програмному середовищі. Такі розрахунки можуть виконуватись, наприклад, під час проведення операцій оперативних угруповань військ.

Подальшим напрямом досліджень є розробка методики обґрунтування раціонального варіанту розподілу обсягу перевезень за видами транспорту під час проведення операцій оперативними угрупованнями військ, яка б інтегрувалася в систему логістичного забезпечення ЗС України. Це надасть можливість обґрунтовувати найефективніший за вартістю та менш

затратний варіант вибору видів транспорту в ході планування перевезення військ та транспортування військового майна з урахуванням логістичних обмежень. При цьому можуть також розглядатись варіанти доставки МтЗ кількома видами транспорту з перевантаженням вантажів на маршруті перевезення.

ЛІТЕРАТУРА:

1. Настанова “Управління (комендатура) військових сполучень”. ВКДП 4-1-1(03).01. К.: Командування Сил логістики ЗС України, 2020. 48 с.
2. Романченко І. С., Хазанович О. І., Трегубенко С. С. Моделювання системи матеріально-технічного забезпечення: монографія. Львів: НАСВ ЗС України, 2015. 156 с.
3. Романченко І. С., Шуєнкін В. О., Хомчак Р. Б., Трегубенко С. С., Марко І. Ю., Закусило П. С., Хазанович О. І. Розвиток теорії матеріально-технічного забезпечення військ: монографія. Львів: НАСВ ЗС України, 2019. 650 с.
4. Гаврилюк І. Ю. Удосконалена методика розподілу транспортних засобів видів системи транспортного забезпечення оперативного угруповання військ під час операції (бойових дій). К.: ЦНДІ, 2017. 28 с.
5. Христовидес Н. Теория графов. Алгебраический подход. М.: Мир, 1978. 432 с.
6. Таха Х. Введение в исследование операций: В 2-х книгах. Кн. 1. Пер. с англ. М.: Мир, 1985. 479 с.
7. Вентцель Е. С. Исследование операций. М.: “Советское радио”, 1972. 552 с.
8. Зайченко Ю. П. Исследование операций. Издательское объединение “Вища школа”, 1975. 320 с.
9. Ганненко Ю. Удосконалення часткової методики оптимізації маршруту перевезення матеріальних засобів перевезення матеріальних засобів. *Social Development and Security*. 2020. Vol. 10. No. 5. P. 128-134. <https://doi.org/10.33445/sds.2020.10.5.11>.
10. Peng Y., Yong P. and Luo Y. (2021). The route problem of multimodal transportation with timetable under uncertainty: multi-objective robust optimization model and heuristic approach. *RAIRO-Oper. Res.* 55, S3035-S3050. <https://doi.org/10.1051/ro/2020110>.
11. Ebrahimnejad A. (2015). An improved approach for solving fuzzy transportation problem with triangular fuzzy numbers. *J. Intell. Fuzzy Syst.* 29, 963-974. <https://doi.org/10.3233/IFS-151625>.
12. Ge Y., Sun Y. and Zhang C. (2024). Modeling a Multimodal Routing Problem with Flexible Time Window in a Multi-Uncertainty Environment. *Systems*. 12(6):212. <https://doi.org/10.3390/systems12060212>.
13. Раскин Л. Г., Кириченко И. О. Многоиндексные задачи линейного программирования (теория, методы, приложения). М.: Радио и связь, 1982. 240 с.
14. Zabolotnii S., Mogilei S. (2019). Optimization of the method of constructing reference plans of multimodal transport problem. *Technology audit and control systems*. 1/2 (45), 15-20. <https://doi.org/10.15587/2312-8372.2019.154561>.
15. Гончаров А. В., Могілей С. О. Реалізація мультимодальних транспортних задач в різних програмних середовищах. *Вісник Черкаського державного технологічного університету*. 2020. 25(3). С. 67-74. <https://doi.org/10.24025/2306-4412.3.2020.215516>.

REFERENCES:

1. Nastanova “Upravlinnia (komendatura) viiskovykh spoluchen”. VKDP 4-1-1(03).01. K.: Komanduvannia Syl lohistyky ZS Ukrainy, 2020. 48 s.
2. Romanchenko I. S., Khazanovych O. I., Trehubenko S. S. Modeliuvannia systemy materialno-tekhnichnoho zabezpechennia: monohrafiia. Lviv: NASV ZS Ukrainy, 2015. 156 s.
3. Romanchenko I. S., Shuienkin V. O., Khomchak R. B., Trehubenko S. S., Marko I. Yu., Zakusylo P. S., Khazanovych O. I. Rozvytok teorii materialno-tekhnichnoho zabezpechennia viisk: monohrafiia. Lviv: NASV ZS Ukrainy, 2019. 650 s.
4. Havryliuk I. Yu. Udoskonalna metodyka rozpodilu transportnykh zasobiv vydiv systemy transportnoho zabezpechennia operatyvnoho uhrupuvannia viisk pid chas operatsii (boiovykh dii). K.: TsNDI, 2017. 28 s.
5. Xristofides N. Teoriya grafov. Algebraicheskij podhod. M.: Mir, 1978. 432 s.

6. Taxa X. Vvedenie v issledovanie operacij: V 2-x knigax. Kn. 1. Per. s angl. M.: Mir, 1985. 479 s.
7. Ventcel' E. S. Issledovanie operacij. M.: "Sovetskoe radio", 1972. 552 s.
8. Zajchenko Yu. P. Issledovanie operacij. Izdatel'skoe ob'edinenie "Vishha shkola", 1975. 320 s.
9. Hannenko, I. (2020). Improving the partial method of optimizing the route of the material resources transportation. *Social Development and Security*. 10(5), 128-134. <https://doi.org/10.33445/sds.2020.10.5.11>.
10. Peng Y., Yong P. and Luo Y. (2021). The route problem of multimodal transportation with timetable under uncertainty: multi-objective robust optimization model and heuristic approach. *RAIRO-Oper. Res.* 55, S3035-S3050. <https://doi.org/10.1051/ro/2020110>.
11. Ebrahimnejad A. (2015). An improved approach for solving fuzzy transportation problem with triangular fuzzy numbers. *J. Intell. Fuzzy Syst.* 29, 963-974. <https://doi.org/10.3233/IFS-151625>.
12. Ge Y., Sun Y. and Zhang C. (2024). Modeling a Multimodal Routing Problem with Flexible Time Window in a Multi-Uncertainty Environment. *Systems*. 12(6):212. <https://doi.org/10.3390/systems12060212>.
13. Raskin L. G., Kirichenko I. O. *Mnogoindeksnye zadachi linejnogo programmirovaniya (teoriya, metody, prilozheniya)*. M.: Radio i svyaz', 1982. 240 s.
14. Zabolotnii S., Mogilei S. (2019). Optimization of the method of constructing reference plans of multimodal transport problem. *Technology audit and control systems*. 1/2 (45), 15-20. <https://doi.org/10.15587/2312-8372.2019.154561>.
15. Honcharov A. V., Mogilei S. O. (2020). Implementation of multimodal transport tasks in different software environments. *Bulletin of Cherkasy State Technological University*. 25(3), 67-74. <https://doi.org/10.24025/2306-4412.3.2020.215516>.

**Dr. Sci. Prof. Bratchenko H.D., Ph.D. Honcharuk A.A.,
Ph.D. Abramov S.V., Duilovskyi A.O.**

SOLVING OF THE MULTIMODAL TRANSPORTATION PROBLEM TAKING INTO ACCOUNT LIMITATIONS OF LOGISTICS INDICATORS

The implementation of military transportation by all types of transport involves planning, management, deployment of transport communications, distribution and preparation of types of transport, organization of the transportation of troops and military property, evacuation of the wounded and sick, damaged weapons and military equipment, and trophy property. As a result of these actions, the issue of timely delivery of material and technical means with the lowest costs should be resolved.

The solution to the multimodal (three-index biplanar) transportation problem is presented to find the rational distribution and delivery of material and technical means. The proposed solution considers the limitations of logistics indicators, such as delivery time, the available carrying capacity of different types of vehicles, the total cost of transportation in the operational movement of storage points and consumers, changes in supply routes, and delivery vehicle types. Introducing an additional constraint into the three-index biplanar transport problem turns it into a linear programming problem of general form. The three-index transportation problem with extra logistical constraints is given a mathematical formulation. A form of input data presentation in the extended transport tables of transportation costs and time spent on cargo transportation is given. An easy way to solve this kind of problem using the simplex method is demonstrated in the Microsoft Excel spreadsheet processor "Solver" add-on.

The article presents the results of solving a multimodal transportation problem with logistical constraints in Microsoft Excel using the example of the delivery of material and technical means by three types of transport (road, rail, and river), with time and cost constraints. The example uses conditional input data for the simulation of the delivery of cargo from three Ukrainian cities (storage points) to the other three (consumption points).

Keywords: *military logistics, multimodal transportation problem, simplex method, objective function, constraints, transportation plan.*

ОГЛЯД МЕХАНІЗМІВ ROOT CAUSE АНАЛІЗУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Телекомунікаційні мережі є невід'ємною частиною сучасного інформаційного суспільства, забезпечуючи передачу даних та спілкування між мільйонами користувачів по всьому світу. Складність та масштаби цих мереж постійно зростають, що підвищує вимоги до їх надійності та стабільності. Одним з ключових завдань у забезпеченні ефективної роботи телекомунікаційних мереж є виявлення та усунення першопричин збоїв і аномалій, які можуть суттєво вплинути на якість обслуговування кінцевих користувачів. Аналіз першопричин (RCA) є потужним інструментом для виявлення першопричин проблем, запобігання їх повторенню та підвищення загальної надійності телекомунікаційних мереж. У статті представлено детальний огляд сучасних методів та інструментів RCA, що використовуються в телекомунікаційних мережах. Зокрема, розглядаються такі методи, як аналіз діаграми «риб'яча кістка», метод «п'яти причин», аналіз дерева несправностей, а також застосування машинного навчання для аналізу великих об'ємів даних. Кожен з цих підходів має свої переваги та недоліки, а їх комплексне використання дозволяє підвищити точність та ефективність виявлення першопричин проблем. Практичні приклади демонструють ефективність застосування різних методів RCA для вирішення конкретних проблем в телекомунікаційних мережах. Наприклад, використання аналізу діаграми «риб'яча кістка» та методу «п'яти причин» дозволяє виявити основні причини затримок у роботі мережі та проблеми з обладнанням на базових станціях. Впровадження систем прогнозування відмов на основі машинного навчання значно підвищує надійність мережі, дозволяючи на ранніх стадіях виявляти потенційні проблеми та вживати необхідних технічних заходів. Окреслено перспективи розвитку RCA в телекомунікаційних мережах. Основна увага приділяється розробці адаптивних і самонавчальних машинних систем, здатних динамічно реагувати на зміну мережесевих умов. Використання більш складних алгоритмів штучного інтелекту та інструментів прогнозування потенційних проблем дозволить суттєво підвищити ефективність RCA та забезпечити високу якість телекомунікаційних послуг.

Ключові слова: телекомунікації, надійність мереж, аналіз збоїв, машинне навчання, прогнозування проблем, стабільність системи, якість обслуговування, обсяг даних, діагностика мереж.

Вступ. У сучасному світі телекомунікаційні мережі грають ключову роль у забезпеченні безперервного обміну інформацією та підтримці критично важливих комунікаційних послуг. Зростання складності та масштабів цих мереж підвищує вимоги до їх надійності, доступності та якості обслуговування. Одним із головних завдань забезпечення безперебійного функціонування телекомунікаційних мереж є виявлення та усунення першопричин виникнення збоїв та аномалій, що може значно вплинути на якість обслуговування кінцевих користувачів.

Root Cause аналіз (RCA) є ефективним інструментом, що дозволяє ідентифікувати основні причини проблем у мережах, запобігаючи їх повторному виникненню. RCA використовує різні методики та механізми, включаючи машинне навчання, алгоритми штучного інтелекту, аналіз великих даних та інші сучасні технології для глибокого аналізу інцидентів [1].

Аналіз останніх досліджень і публікацій. А. Мащак розглядає моделі для оцінки ризику, надає цінну інформацію про ризики в системах зв'язку [2]. Р. Одарченко досліджує архітектуру сучасних систем моніторингу [3]. С. Сазонова досліджує оцінку ризиків стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки [4]. В. Chen, J. Li та J. Wei пропонують графовий алгоритм для RCA, що є важливим вкладом

у розвиток методів аналізу кореневих причин в телекомунікаційних мережах, демонструє застосування передових алгоритмів для виявлення причин збоїв [5]. А. Gómez-Andrades, Р. Muñoz, І. Serrano та Р. Varco досліджують автоматичний RCA для LTE мереж на основі неконтрольованих технік [6, 7]. Це дослідження є важливим прикладом застосування сучасних методів машинного навчання в RCA. М. Schaaf, G. Wilke, Т. Mikkola, Е. Bunn, І. Hela, Н. Wache та S. G. Grivas досліджують своєчасний RCA для складних ситуацій у великих масштабах телекомунікаційних мереж, що важливо для розуміння складності та масштабів проблем у мережах [8].

Варто зазначити, що існує значна кількість досліджень, які торкаються різних аспектів телекомунікаційних мереж, проте обмежена кількість публікацій, які детально розглядають методи RCA у цьому контексті. Зокрема, роботи, що використовують сучасні підходи, такі як машинне навчання та штучний інтелект для автоматизації процесів RCA, представлені не в повному обсязі. Це свідчить про необхідність подальших досліджень у цій галузі для забезпечення більш ефективного виявлення та усунення корінних причин збоїв у телекомунікаційних мережах.

Мета статті - огляд механізмів Root Cause аналізу телекомунікаційних мереж.

Виклад основного матеріалу. Root Cause аналіз (RCA) у телекомунікаційних мережах використовує різноманітні методики та інструменти для ідентифікації основних причин збоїв та аномалій [4].

Автоматичний пошук кореневої причини несправності вирішує Correlation Engine [6] – спеціалізована платформа для реалізації різних алгоритмів кореляції, аналізу впливу на сервіси (Services Impact Analysis) і відновлення сервісів (Runbook Automation).

Correlation Engine використовує алгоритми машинного навчання для аналізу великих обсягів даних, зібраних з різних елементів телекомунікаційної мережі. Це включає дані про події, журнали системи, показники продуктивності та інші важливі метрики. Використовуючи ці дані, платформа може автоматично виявляти аномалії та кореляції між різними подіями, що дозволяє швидко ідентифікувати кореневі причини несправностей.

Однією з ключових переваг Correlation Engine є її здатність проводити аналіз впливу на сервіси (Services Impact Analysis). Відповідно платформа може визначити, які сервіси і користувачі можуть підлягати впливам певних несправностей. Такий підхід дозволяє операторам мережі визначити пріоритети власних дій, спрямовуючи зусилля на найкритичніші області, що впливають на якість обслуговування кінцевих користувачів [3]. Крім того, Correlation Engine підтримує функції автоматизації відновлення сервісів (Runbook Automation). Це означає, що платформа може автоматично запускати процедури відновлення у випадку виявлення певних типів несправностей. Наприклад, якщо виявлено, що відмова обладнання пов'язана з конкретною проблемою, вона може автоматично виконати сценарій, що передбачає перезапуск обладнання або зміну налаштувань конфігурації, щоб швидко відновити нормальну роботу мережі.

Платформа також підтримує функції зворотного зв'язку та самонавчання, що дозволяє їй постійно покращувати свої алгоритми аналізу та виявлення несправностей на основі нових даних і зворотного зв'язку від операторів мережі. Це забезпечує постійне вдосконалення точності і швидкості ідентифікації кореневих причин проблем, що є критично важливим для підтримання високої надійності та стабільності телекомунікаційних мереж.

Аналіз причинно-наслідкових діаграм (Fishbone Diagram) дозволяє структурувати можливі причини проблем у вигляді діаграми «риб'ячої кістки». Кожна «кістка» відповідає певній категорії можливих причин (наприклад, обладнання, програмне забезпечення, процеси, люди), що дозволяє систематизувати та детально аналізувати кожен фактор [1].

Метод п'яти «чому» (5 Whys) передбачає послідовне задавання питання «чому?» для виявлення корінної причини проблеми. Наприклад, у випадку збоїв у мережі, відповідь на перше «чому?» може вказати на відмову обладнання, а наступні «чому?» допоможуть виявити глибші причини, такі як неправильна конфігурація або неякісне технічне обслуговування.

Аналіз дерева несправностей (Fault Tree Analysis) [2] дозволяє графічно моделювати взаємозв'язки між різними компонентами системи та визначати, як їх відмова може призвести до загальної системної несправності. Цей підхід ефективний для комплексного аналізу складних мережевих систем. Наприклад, в контексті телекомунікаційних мереж, ФТА можна застосувати для аналізу відмови базової станції. Верхній рівень дерева представляє повну відмову базової станції, тоді як нижчі рівні дерева включають можливі причини цієї відмови, такі як збої в електроживленні, програмні збої, апаратні збої та інші. Кожна з цих причин може бути розгалужена на більш дрібні компоненти та події, що можуть спричинити їх.

Цей метод також дозволяє визначити імовірності виникнення кожної з подій, що входять до дерева несправностей. Завдяки цьому можна провести кількісний аналіз ризиків, пов'язаних з роботою мережевої системи. Наприклад, якщо відомі імовірності збоїв окремих компонентів, можна обчислити загальну імовірність системної несправності, що надає можливість визначати пріоритети прикладених зусиль щодо підвищення надійності системи, спрямовуючи ресурси на найбільш критичні вузли та компоненти.

ФТА також дозволяє ідентифікувати так звані «одиничні точки відмови» (single points of failure), які є критичними компонентами системи, відмова яких призведе до загальної несправності. Виявлення таких точок є надзвичайно важливим для проектування та експлуатації надійних телекомунікаційних систем, оскільки їх дублювання або зміцнення може значно підвищити стійкість мережі до збоїв.

Більш того, аналіз дерева несправностей може бути інтегрований з іншими методами аналізу, такими як аналіз впливу та критичності збоїв (Failure Mode and Effects Analysis, FMEA), що дозволяє створити більш детальну та всебічну картину надійності системи. Комбінування різних методів аналізу допомагає забезпечити більш точну і надійну діагностику проблем, а також розробити ефективні стратегії запобігання збоєм.

Використання алгоритмів машинного навчання та аналізу великих даних дозволяє автоматизувати процес виявлення та аналізу корінних причин, що значно підвищує ефективність управління телекомунікаційними мережами. Наприклад, за допомогою кластерного аналізу можна ідентифікувати аномалії у великих обсягах телекомунікаційних даних та визначити патерни, що призводять до збоїв. Це дозволяє операторам мережі не лише швидше виявляти проблеми, але й передбачати їх виникнення.

Одним із прикладів успішного використання алгоритмів машинного навчання є застосування нейронних мереж для прогнозування збоїв. Нейронні мережі здатні аналізувати величезні обсяги даних у реальному часі, виділяючи ключові фактори, що можуть сигналізувати про можливий збій. Зокрема, нейронні мережі можуть враховувати різноманітні параметри, такі як зміни в параметрах сигналу, статистику використання мережевих ресурсів, історичні дані про збої та інші показники. Завдяки цьому, оператори можуть заздалегідь вживати необхідних заходів для запобігання можливим проблемам.

Алгоритми машинного навчання дозволяють створювати моделі прогнозування, які можуть самонавчатися та адаптуватися до змін у мережі, що особливо важливо в умовах постійно зростаючої складності та динамічності телекомунікаційних систем. Моделі можуть автоматично оновлювати свої параметри, враховуючи нові дані та тренди, що з'являються, що дозволяє зберігати їхню ефективність на високому рівні протягом тривалого часу.

Інший приклад ефективного використання алгоритмів машинного навчання – застосування методів глибокого навчання для аналізу журналів подій та логів системи. За допомогою таких методів можна швидко ідентифікувати послідовності подій, що передують збою, та визначити ключові індикатори, що можуть вказувати на наближення проблеми, що дозволяє операторам своєчасно втручатися та проводити необхідні корегувальні дії.

У випадку, якщо у великій телекомунікаційній мережі виявлено періодичні затримки передачі даних, що спричиняло незадоволення користувачів та впливало на якість наданих послуг. Ця проблема має значний вплив на функціонування критично важливих сервісів, таких як відеоконференції, онлайн-ігри та інші реальні часи. Для її вирішення доцільно застосувати

аналіз причинно-наслідкових діаграм та метод п'яти «чому», що дозволило виявити глибинні причини затримок. Розглянемо практичну реалізацію використання методу.

Початковий етап аналізу може виявити, що затримки виникають переважно у пікові години, коли навантаження на мережу є максимальним. Розглянувши діаграму причинно-наслідкових зв'язків, встановлено, що основною причиною затримок є перенавантаженість мережеских вузлів. Метод п'яти «чому» дозволяє глибше дослідити цю проблему.

Затримки передачі даних у пікові години виникають через перенавантаження мережеских вузлів. Отже перше «чому» фокусується на тому, що вузли перевантажуються через високе навантаження на мережу в ці години. Друге «чому» пояснює, що високе навантаження призводить до перенавантаження вузлів через їх недостатню пропускну здатність для обробки всього трафіку в вищезгадані періоди часу. Третє «чому» підкреслює, що вузли мають недостатню пропускну здатність через що й відбувається перенавантаження вузлів. Четверте «чому» вказує на те, що вузли мають недостатню пропускну здатність через неправильно налаштовану маршрутизацію трафіку, яка створює "вузькі місця" в мережі. І п'яте «чому» пояснює, що конфігурації маршрутизаторів не оновлюються через брак ресурсів або недоліки в процесах модернізації мережевого обладнання.

Подальший детальний аналіз підтвердив, що неправильно налаштована маршрутизація трафіку спричиняє накопичення даних у певних вузлах, тоді як інші вузли залишаються недовантаженими. Це призвело до нерівномірного розподілу навантаження по мережі та зумовило затримки у передачі даних.

Для вирішення цієї проблеми доцільним є проведення оновлення конфігурації маршрутизаторів, запровадження нових алгоритмів балансування навантаження, що дозволяють рівномірно розподілити трафік між усіма мережевими вузлами. У результаті, повинна зменшитися затримка у передачі даних та підвищитися загальна ефективність роботи мережі.

Після впровадження цих змін необхідним є проведення моніторингу роботи мережі, який повинен підтвердити стабільне зниження затримок навіть у пікові години. Користувачі мережі мають помітити покращення якості наданих послуг, що в подальшому позитивно вплине на рівень їх задоволеності. Відповідно застосування аналізу причинно-наслідкових діаграм та методу п'яти «чому» дозволяє виявити та усунути ключову проблему, що впливала на якість роботи телекомунікаційної мережі.

В іншому випадку, під час експлуатації базової станції мобільного зв'язку було зафіксовано відмову обладнання, що призвело до втрати покриття в регіоні. Ця ситуація викликала значні незручності для користувачів, оскільки вони втратили можливість здійснювати дзвінки, користуватися мобільним інтернетом та іншими послугами зв'язку. Для вирішення цієї проблеми та запобігання її повторенню використано метод аналізу дерева несправностей.

Перш за все, необхідно створити детальну діаграму дерева несправностей, яка допоможе ідентифікувати та структуровано проаналізувати всі можливі причини відмови. Розглядаються різні фактори, включаючи механічні, електричні та зовнішні умови, які могли спричинити збій.

Додатковий детальний аналіз компонентів джерела живлення може виявити, що проблемою є неякісні кабелі живлення, які не витримували необхідного навантаження і призводять до нестабільної роботи обладнання.

Для запобігання подібним інцидентам у майбутньому, усі неякісні кабелі повинні бути замінені на нові, відповідної якості, що мали сертифікати відповідності стандартам. Крім того, доцільним є впровадження додаткових процедур контролю якості під час закупівлі та встановлення кабельної продукції, що дозволяє своєчасно виявляти та усувати потенційно дефектні компоненти.

Завдяки цим заходам досягається не тільки відновлення нормального функціонування базової станції, але й значно підвищується надійність її роботи в майбутньому. Оператори

зв'язку повинні отримали рекомендації щодо регулярного моніторингу стану джерел живлення та перевірки якості кабельної продукції, що дозволить запобігти виникненню аналогічних проблем в інших регіонах. Аналіз дерева несправностей є ефективним інструментом для ідентифікації та усунення кореневих причин відмов у телекомунікаційних мережах.

Аналізуючи великі обсяги історичних даних про збої та стан обладнання, система здатна ідентифікувати патерни, що передують збоєм. Зокрема, вона здатна виявляти характерні ознаки, такі як частота появи певних помилок, зміни в поведінці мережі або деградація параметрів обладнання, що сигналізують про наближення збою. Крім того, використання таких аналітичних інструментів сприяє оптимізації ресурсів і знижує витрати на технічне обслуговування. Оператори можуть планувати заміну та ремонт обладнання на основі фактичного стану та прогнозованого часу до збою, замість традиційних календарних графіків, що дозволяє уникати зайвих витрат на обслуговування справного обладнання та зосередити ресурси на критичних ділянках мережі.

Представлені приклади демонструють ефективність використання різних методів та інструментів RCA для виявлення та усунення корінних причин проблем у телекомунікаційних мережах. Інтеграція цих підходів у практику експлуатації мереж дозволяє значно підвищити їх надійність та якість обслуговування кінцевих користувачів.

Висновки. Отже, можна зробити висновок, що виявлення та усунення першопричин збоїв у телекомунікаційних мережах є критично важливим завданням для забезпечення їх надійної та ефективної роботи. Огляд сучасних механізмів RCA показав, що використання передових технологій, таких як машинне навчання, аналіз великих даних та штучний інтелект, значно підвищує ефективність і точність виявлення основних причин проблем. Незважаючи на існуючі виклики, пов'язані з інтеграцією та масштабуванням цих технологій, їх подальший розвиток і впровадження обіцяють значні покращення у сфері управління та моніторингу телекомунікаційних мереж.

Подальші дослідження у цій області мають бути спрямовані на розробку більш адаптивних та самонавчальних систем RCA, здатних до динамічного реагування на змінні умови мережі. Це включає інтеграцію більш складних алгоритмів штучного інтелекту, а також розвиток інструментів для прогнозування потенційних проблем на основі аналізу історичних даних. Таким чином, забезпечення високої якості та безперервності телекомунікаційних послуг стане реальністю завдяки вдосконаленню механізмів Root Cause аналізу.

ЛІТЕРАТУРА:

1. Бойко Ю. М., Дружинін В. А., Толюпа С. В. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад. Київ: Логос, 2018. 227 с.
2. Мащак А. В. Моделі для оцінки ризику експлуатації системи радіоуправління безпілотним літальним апаратом: дис.... канд-та тех. наук: 05.12.17. Львів, 2016. 161 с.
3. Одарченко Р. С. Дослідження архітектури сучасних систем моніторингу в мережах стільникового зв'язку. *Наукоємні технології*. 2018. № 2 (38). С. 195–202.
4. Сазонова С. Оцінка ризиків стратегічного управління телекомунікаційними підприємствами в умовах цифрової економіки. *Bulletin of Sumy National Agrarian University*. 2021. № 3 (89). С. 31–37.
5. Chen B., Li J., Wei J. A Graph-Based Algorithm for Root Cause Analysis of Faults in Telecommunication Networks. *IEEE 19th International Conference on Automation Science and Engineering (CASE), Auckland, New Zealand, 2023*. PP. 1–7,
6. Correlation Engine. URL: <https://www.illumina.com/products/by-type/informatics-products/connected-analytics/modules/correlation-engine.html>
7. Gómez-Andrades A., Muñoz P., Serrano I., Barco R. Automatic Root Cause Analysis for LTE Networks Based on Unsupervised Techniques. *IEEE Transactions on Vehicular Technology*. 2016. Vol. 65. № 4. PP. 2369–2386.

8. Schaaf M., Wilke G., Mikkola T., Bunn E., Hela I., Wache H., Grivas S. G. Towards a timely root cause analysis for complex situations in large scale telecommunications networks. *Procedia Computer Science*. 2015. №60. PP. 160–169.

REFERENCES:

1. Boiko Yu. M., Druzhynin V. A., Toliupa S. V. (2018) Teoretychni aspekty pidvyshchennia zavadosiikosti y efektyvnosti obrobky syhnaliv v radiotekhnichnykh prystroiakh ta zasobakh telekomunikatsiinykh system za naiavnosti zavvad [Theoretical aspects of increasing the noise immunity and efficiency of signal processing in radio engineering devices and means of telecommunication systems in the presence of interference]. Kyiv: Lohos. 227 p.
2. Mashchak A. V. (2016) Modeli dlia otsinky ryzyku ekspluatatsii systemy radioupravlinnia bezpilotnym litalnym aparatom [Models for assessing the risk of operation of the radio control system of an unmanned aerial vehicle: dissertation]: dys.... kand-ta tekhn. nauk: 05.12.17. Lviv. 161 p.
3. Odarchenko R. S. (2018) Doslidzhennia arkhitektury suchasnykh system monitorynhu v merezhakh stilnykovoho zviazku [Research of the architecture of modern monitoring systems in cellular networks]. *Naukoiemni tekhnolohii*. vol. 2 (38). pp. 195–202.
4. Sazonova S. (2021) Otsinka ryzykiv stratehichnoho upravlinnia telekomunikatsiinykh pidpriemstvamy v umovakh tsyfrovoy ekonomiky [Assessment of risks of strategic management of telecommunication enterprises in the digital economy]. *Bulletin of Sumy National Agrarian University*. vol. 3 (89). pp. 31–37.
5. Chen B., Li J., Wei J. A (2023) Graph-Based Algorithm for Root Cause Analysis of Faults in Telecommunication Networks. IEEE 19th International Conference on Automation Science and Engineering (CASE), *Auckland, New Zealand*, pp. 1–7.
6. Correlation Engine. URL: <https://www.illumina.com/products/by-type/informatics-products/connected-analytics/modules/correlation-engine.html>
7. Gómez-Andrades A., Muñoz P., Serrano I., Barco R. (2016) Automatic Root Cause Analysis for LTE Networks Based on Unsupervised Techniques. *IEEE Transactions on Vehicular Technology*. vol. 65. № 4. pp. 2369–2386.
8. Schaaf M., Wilke G., Mikkola T., Bunn E., Hela I., Wache H., Grivas S. G. (2015) Towards a timely root cause analysis for complex situations in large scale telecommunications networks. *Procedia Computer Science*. vol. 60. pp. 160–169.

OVERVIEW OF ROOT CAUSE ANALYSIS MECHANISMS FOR TELECOMMUNICATION NETWORKS

Telecommunication networks are an integral part of modern information society, providing data transmission and communication among millions of users worldwide. The complexity and scale of these networks are constantly growing, which increases the demands on their reliability and stability. One of the key tasks in ensuring the efficient operation of telecommunication networks is the identification and elimination of the root causes of failures and anomalies that can significantly affect the quality of service for end users. Root cause analysis (RCA) is a powerful tool for identifying the primary causes of problems, preventing their recurrence, and enhancing the overall reliability of networks. The article provides a detailed review of contemporary methods and tools of RCA used in telecommunication networks. In particular, methods such as fishbone diagram analysis, the «five whys» method, fault tree analysis, and the application of machine learning for big data analysis are considered. Each of these approaches has its advantages and disadvantages, and their comprehensive use allows for higher accuracy and efficiency in identifying the root causes of problems. Practical examples demonstrate the effectiveness of applying various RCA methods to solve specific problems in telecommunication networks. For instance, the use of fishbone diagram analysis and the «five whys» method allows for the identification of the primary causes of network delays and equipment issues at base stations. The implementation of failure prediction systems based on machine learning significantly enhances network reliability by allowing for the early detection of potential problems and the necessary technical measures. The prospects for the development of RCA in telecommunication networks are outlined. The primary focus is on the development of adaptive and self-learning systems capable of dynamically responding to changing network conditions. The use of more complex artificial intelligence algorithms and tools for predicting potential problems will significantly improve the effectiveness of RCA and ensure high-quality telecommunication services.

Key words: telecommunications, network reliability, failure analysis, machine learning, problem prediction, system stability, service quality, data volume, network diagnostics.

МЕТОД БАГАТОСТОРОННІХ ОБЧИСЛЕНЬ КЕРУВАННЯ КРИПТОАКТИВАМИ НА ОСНОВІ ТЕХНОЛОГІЇ MULTI-PARTY COMPUTATION

Розглянута задача побудови ефективного та безпечного криптовалютного гаманця на основі технології багатосторонніх обчислень, який може забезпечити надійне та захищене використання в різних галузях, що працюють з криптовалютами.

Сучасні алгоритми багатосторонніх обчислень, такі як Дженнаро та Голдфедера, Лінделли, Доєрнера, пропонують значні переваги у захисті даних, але вони мають певні обмеження. Основними з них є недостатня ефективність у кількості раундів підпису та відсутність підтримки холодного зберігання. Це підкреслює необхідність подальших досліджень і розробок у сфері технології Multi-Party Computation для досягнення більш високого рівня операційної ефективності та гнучкості.

Метод забезпечення конфіденційності та безпеки криптоактивів на основі технології багатосторонніх обчислень для Ethereum мережі полягає в: забезпеченні високого рівня безпеки для збереження приватних ключів та процесу підписання транзакцій, використовуючи передові методи криптографічного захисту; гарантуванні конфіденційності та приватності користувачів, захищаючи їх особисту інформацію від несанкціонованого доступу або витоку даних; використанні передових технологій, включаючи технологію Multi-Party Computation, для підвищення рівня безпеки та приватності зберігання активів.

На основі проведеного дослідження та аналізу характеристик стандартів протоколів багатосторонніх обчислень запропонований протокол, який враховує наявні покращення та недоліки попередніх протоколів. Для покращення безпеки, у протоколі впроваджено принцип інтервального оновлення спільного секрету.

Система керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв'язку та маршрутизації. Система надає можливість надійного зберігання криптоактивів, зокрема приватних ключів до гаманців Ethereum мережі, з використанням технології Multi-Party Computation, яка може бути використана у різних криптопроектах для безпечного переказу криптоактивів.

Архітектура системи передбачає взаємодію основних компонентів для забезпечення надійної та безпечної роботи. Запропоновано схему встановлення безпечного з'єднання вузлів та описано модель локального сховища, яке забезпечує безпечне зберігання часток ключів, підписів та системних логів.

Ключові слова: криптоактиви, конфіденційна інформація, безпека криптоактивів, технологія multi-party computation, безпечне з'єднання, інформаційна безпека, криптовалюта, цифрові активи, криптовалютний гаманець.

Вступ. З кожним роком популярність використання криптовалюти зростає, так само як і попит на безпечні криптовалютні гаманці. Люди використовують криптовалюту з різних причин: як засіб обміну та збереження вартості, інструмент інвестування та спосіб здійснення міжнародних переказів. Криптовалюти є цифровими активами, які використовують криптографічні протоколи для забезпечення безпеки транзакцій та контролю за створенням нових одиниць цифрової валюти. Вони працюють на базі технології блокчейн, яка дозволяє записувати транзакції у розподіленій базі даних, забезпечуючи безпеку та непідробність операцій [1,2].

Основною перевагою криптовалют є їх децентралізація: вони не контролюються центральними органами управління, такими як уряди чи банки, і можуть бути використані у будь-якій частині світу без обмежень. Додатковими перевагами є анонімність, що дозволяє

користувачам зберігати конфіденційність своїх фінансових операцій, та зручність, що забезпечує швидкі та прості перекази без посередників. Найвідомішою криптовалютою є біткоїн, також існує безліч інших криптовалют, як Ethereum, Ripple, Tether та інші [4,8].

Криптовалютні гаманці є ключовими інструментами для зберігання, відправлення та отримання криптовалюти. Вони можуть бути онлайн-сервісами, програмами для смартфонів або настільними програмами, дозволяючи користувачам відстежувати свої баланси та історію транзакцій. У зв'язку з цим створення ефективного та безпечного криптовалютного гаманця є актуальним завданням для багатьох галузей, які працюють з криптовалютами, таких як фінансові послуги, торгівля, інтернет-магазини, туризм та благодійність [11,13].

Сучасні криптовалютні гаманці розробляють на основі технології Multi-Party Computation (MPC). Використання MPC дозволяє значно підвищити безпеку криптовалютних транзакцій. Дана технологія забезпечує захист даних навіть у випадку компрометації частини учасників системи, оскільки вона розподіляє обробку і зберігання інформації між декількома учасниками, уникаючи центральної точки вразливості. MPC використовує криптографічні методи для розподіленої обробки даних, що дозволяє кільком сторонам виконувати обчислення над даними, не розкриваючи їх один одному. Це гарантує, що жодна сторона не має повного доступу до всієї інформації, що значно знижує ризик витоку даних або зловживань, якщо один або декілька учасників системи будуть зламані або скомпрометовані, конфіденційність та цілісність транзакцій залишаться під захистом [14,18].

Предметом дослідження роботи є створення ефективного та безпечного криптовалютного гаманця на основі технології MPC, який може забезпечити надійне та захищене використання в різних галузях, що працюють з криптовалютами.

Аналіз останніх досліджень та постановка задачі. Блокчейн –децентралізована та розподілена база даних, яка використовується для безпечного, незмінного та прозорого зберігання записів. Ця технологія функціонує на основі принципу послідовного об'єднання блоків даних у ланцюг. Кожен блок містить список транзакцій і пов'язаний з попереднім блоком за допомогою криптографічного хешу, що утворює ланцюг блоків, або блокчейн.

Децентралізація у блокчейні – контроль і повноваження щодо прийняття рішень у мережі розподіляються між її користувачами, а не контролюються однією особою. Це може бути корисним у ситуаціях, коли учасникам необхідно координувати свої дії з незнайомцями або коли вони хочуть подбати про безпеку й цілісність своїх даних [1,2]. У децентралізованій блокчейн-мережі немає центрального органу, який контролює потік даних чи транзакцій. Натомість транзакції перевіряються й записуються розподіленою мережею комп'ютерів, які працюють для підтримки цілісності мережі. Безпека досягається за допомогою криптографічних методів, які захищають дані від несанкціонованого доступу.

У цьому контексті фундаментальне значення мають так звані криптографічні хеш-функції. Хешування – це процес, при якому алгоритм отримує вхідні дані будь-якого розміру і повертає результат, що містить передбачуваний та фіксований розмір. Дана властивість хеш-функцій широко використовується в інформаційній безпеці, зокрема для захисту паролів. Хеші в блокчейнах використовуються як унікальні ідентифікатори для блоків даних і створюють ланцюжок зв'язаних блоків (рис. 1) [2,8].

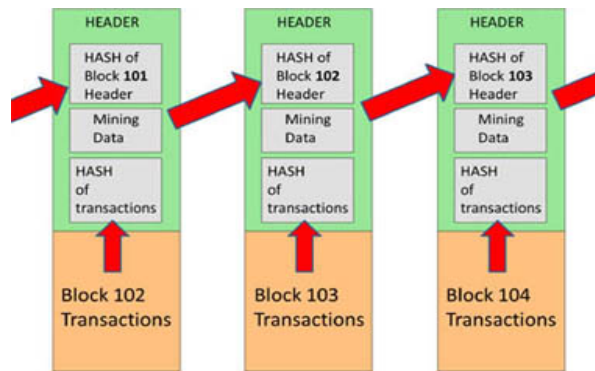


Рисунок 1 – Схематична структура блокчейну

Для обробки транзакцій у блоці використовується метод, відомий як алгоритм дерева Меркла (рис. 2), і в цьому процесі застосовується хешування [4,5].

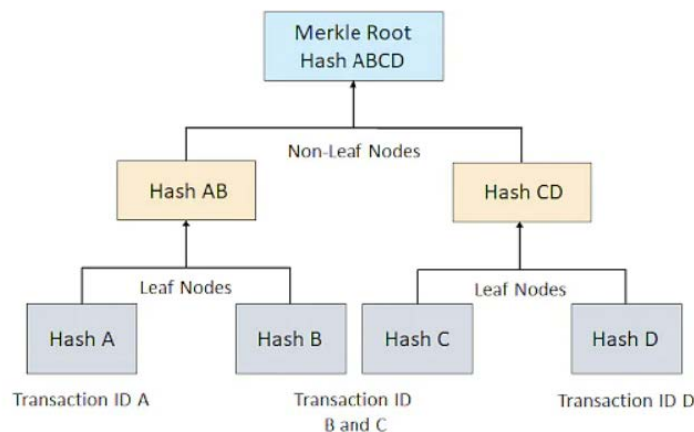


Рисунок 2 – Дерево Меркла

Кожна транзакція в блоці спочатку хешується індивідуально. Потім хеші кожної транзакції об'єднуються і хешуються разом. Якщо кількість транзакцій непарна, останній хеш дублюється і хешується сам із собою, щоб створити парну кількість хешів. Цей процес повторюється поки залишиться лише один кореневий хеш, чи корінь Меркла. Кожен хеш блоку генерується на основі даних в ньому та хешу попереднього блоку (рис. 3) [10].



Рисунок 3 – Схематична структура блоку

Дана взаємозалежність гарантує безпеку та незмінність блокчейну. Хешування також використовується в алгоритмах консенсусу, які в свою чергу використовуються для перевірки транзакцій [2,8].

У блокчейні Bitcoin використовується алгоритм Proof of Work (PoW), процес виконання консенсусу Proof of Work (PoW) полягає у тому, щоб мережа визначала, який блок буде доданий до ланцюжка блоків (blockchain). У спрощеному вигляді, учасники мережі, такі як майнери, змагаються за право знайти блок і додати його до ланцюжка. Для цього вони повинні вирішити складну математичну задачу, яка вимагає великої обчислювальної потужності. PoW, зазвичай базуються на хеш-функції SHA-256. Валідатори мережі повинні знайти створений хеш для нового блоку, який задовольняє певні умови (рис. 4) [10,17].

Саме завдяки консенсусу мережа захищена від атак, таких як подвійне витрачання та модифікація історії транзакцій. Він робить такі атаки вкрай важкими, оскільки будь-яка спроба зміни історії потребує повторного обчислення хешів для всіх попередніх блоків у ланцюжку, а також виграшу у конкуренції з іншими валідаторами для створення нових блоків. Чим більша обчислювальна потужність у мережі, тим важче здійснити подібні атаки, що робить мережу більш стійкою до зловживань.

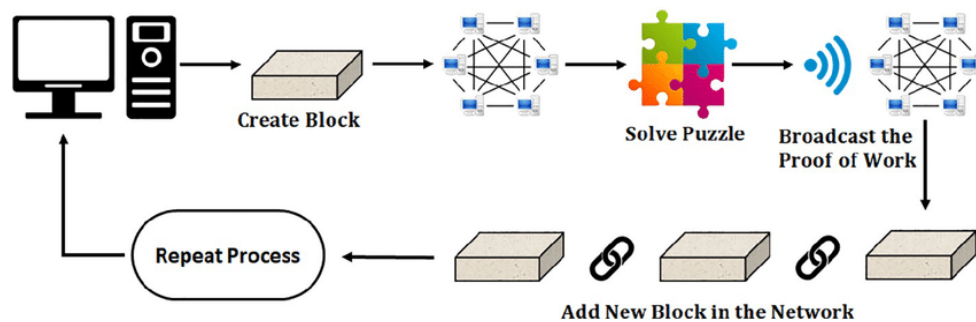


Рисунок 4 – Схематичне зображення Proof of Work (PoW)

Для здійснення будь-яких операцій у мережі, звичайні користувачі, повинні ініціювати криптотранзакції. Для того, щоб відправити криптовалюту, кожному учаснику необхідно мати свій рахунок. Акаунт управляється парою ключів, де відкритий ключ це адреса, яку користувач вказує для отримання цифрових активів, а закритий контролює дії всередині облікового запису, тобто підписує транзакції [18-25]. Кожен рахунок має один закритий ключ [17].

Для підписання транзакції у блокчейн мережі використовується алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) (рис. 5) [17, 26]. Для підписання алгоритм використовує приватний ключ, що є випадковим числом, а публічний ключ генерується за допомогою множення приватного ключа на генераторну точку еліптичної кривої [26]. Перевірка включає використання публічного ключа для перевірки автентичності підпису. Процес полягає в обчисленні двох точок на еліптичній кривій і перевірці, чи збігаються ці точки з підписом та хешем повідомлення. Ефективність та безпека ECDSA забезпечується властивостями еліптичних кривих, які дозволяють досягнути високого рівня стійкості до криптографічних атак при відносно невеликих обчислювальних витратах [11, 26].

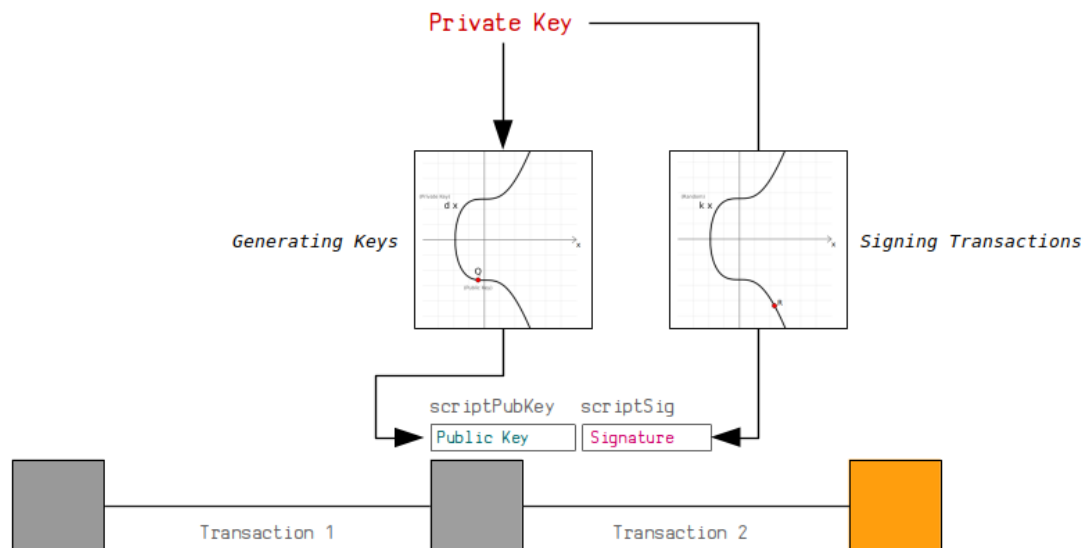


Рисунок 5 – Схематичне зображення роботи алгоритму ECDSA

Весь процес обробки криптовалютних транзакцій (рис. 6) можна поділити на три окремі етапи: створення, підписання, трансляцію та підтвердження (автентифікація та авторизація) [4,6,12].

How does a transaction get into the blockchain?

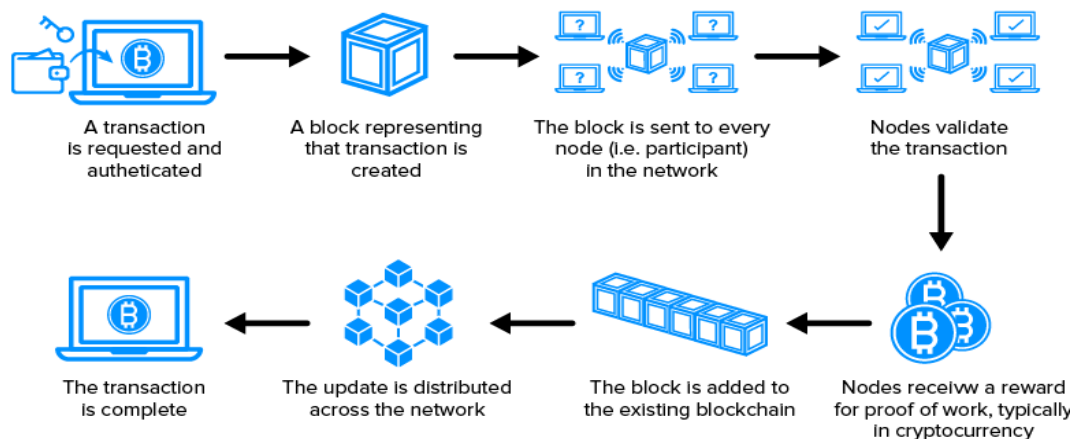


Рисунок 6 – Схематичне зображення взаємодії блокчейна та криптотранзакції

Багатосторонні обчислення MPC (Multi-Party Computation) - набір методів, за допомогою яких декілька учасників можуть спільно вирішувати обчислювальні задачі, не розкриваючи свої вхідні дані один одному. У контексті MPC, кожен учасник має свої власні приватні дані, і мета полягає в тому, щоб вони могли обчислити якийсь результат або функцію, використовуючи ці дані разом, при цьому не розкриваючи їх один одному. Такий тип обчислень стає альтернативою кастодіальним криптогаманцям з мультипідписом, так як дає можливість розділити відповідальність зберігання приватних ключів між декількома сторонами [14,17].

Технологія MPC застосовується для низки варіантів, таких як захист цифрових активів у MPC-гаманцях або збереження певної інформації в таємниці під час цифрових аукціонів.

Основні протоколи MPC, які застосовуються для реалізації кастодіальних криптогаманців:

1. Алгоритм Дженнаро та Голдфедера наразі є одним із найкращих доступних алгоритмів MPC, і багато установ, які захищають свої приватні дані за допомогою MPC, використовують саме цей алгоритм. Однак, незважаючи на його переваги, затримка зв'язку між спільними ресурсами MPC (пристроями, які зберігають ключові спільні ресурси) не досягає найвищого рівня ефективності. Це обумовлено тим, що користувачі повинні чекати до 9 раундів підпису для завершення транзакцій. Крім того, алгоритм Дженнаро та Голдфедера не пропонує жодної гнучкості для установ, яким потрібно використовувати холодне зберігання. Це суттєво обмежує його застосування у сценаріях, де необхідно забезпечити високий рівень безпеки при зберіганні даних офлайн.

2. Алгоритм багатосторонніх обчислень, запропонований Лінделлом та ін., забезпечує незначне зменшення кількості транзакцій, які повинні бути підписані, у порівнянні з алгоритмом Дженнаро та Голдфедера – до 8 раундів. Однак цей алгоритм не досягає рівня операційної ефективності, необхідного для сучасних ринків. Як і алгоритм Дженнаро та Голдфедера, рішення Лінделла також не підтримує холодне зберігання, що обмежує його використання в певних сферах [17,20,21].

3. Алгоритм MPC Доернера та ін. демонструє значний прогрес, досягаючи порогу лише за 6 підписів. Проте, навіть цей рівень ефективності не відповідає потенціалу сучасних технологій. Більше того, подібно до попередніх двох алгоритмів, рішення Доернера також не надає можливості використання холодного зберігання разом із MPC [14].

Таким чином, хоча сучасні алгоритми багатосторонніх обчислень, пропонують значні переваги у захисті даних, вони мають певні обмеження. Основними з них є недостатня ефективність у кількості раундів підпису та відсутність підтримки холодного зберігання. Це підкреслює необхідність подальших досліджень і розробок у сфері MPC для досягнення більш високого рівня операційної ефективності та гнучкості.

Розглянемо алгоритми, які застосовуються для розробки протоколів у MPC гаманцях:

1. Схема розподілу секрету Шаміра (Shamir's Secret Sharing) - дозволяє розділити інформацію на багато часток, при цьому для відновлення оригінального секрету потрібно лише частину з цих часток (рис. 7) [8,11].

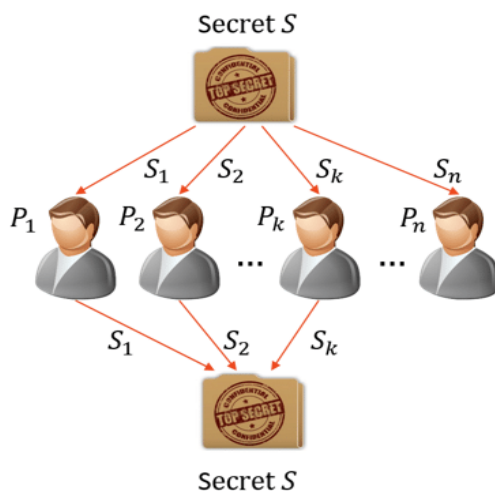


Рисунок 7 – Схематичне зображення роботи схеми розподілу секрету

Для відновлення оригінального секрету, схема Шаміра вимагає мінімальну кількість часток — ця мінімальна кількість називається порогом. Для відновлення секрету необхідно досягти порогу. Якщо кількість часток менша за порогову, секрет не може бути відновлений, що робить схему розподілу секрету Шаміра захищеною від зловмисників з необмеженою обчислювальною потужністю.

2. Порогова схема підпису (Threshold Signature Scheme, TSS) є криптографічним примітивом для розподіленого генерації ключів та підписання (рис 8). Використання TSS у

клієнтах блокчейн, системах зберігання ключів є новою парадигмою, яка може надати численні переваги, особливо в аспекті безпеки. TSS може вплинути на дизайн систем управління ключами (таких як криптогаманці) та прокласти шлях для підтримки нативних випадків використання в DeFi. Втім, варто зазначити, що TSS все ще є новою технологією, тому ризики та обмеження також слід враховувати. Порогові підписи вимагають підмножину сторін, уповноважених створювати підписи від імені групи. Повідомлення вважається підписаним лише в тому випадку, якщо поріг (t із n , де t — поріг підписувачів, а n — кількість усіх підписувачів) підписувачів підписують повідомлення [14].

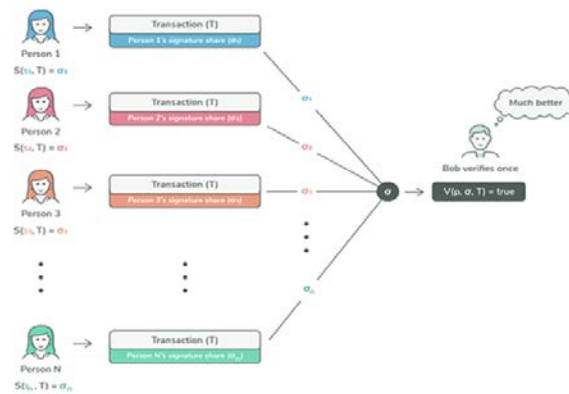


Рисунок 8 – Схематичне зображення роботи протоколу схеми порогового підпису

3. Розподілена генерація ключів (Distributed Key Generation, DKG) - криптографічний протокол, який дозволяє спільно генерувати криптографічні ключі багатьма учасниками, кожен з яких має частину секретного ключа (рис. 9). Розподіляючи процес генерації ключів між групою учасників, DKG гарантує, що жоден суб'єкт не матиме повного контролю, таким чином суттєво сприяючи безпеці та відмовостійкості розподілених систем. За своєю суттю DKG включає групу учасників, які об'єднуються для створення колективного закритого ключа. Процес організований таким чином, що кожен учасник вносить частину ключа, не розкриваючи свій конкретний внесок іншим. Ця криптографічна магія полягає в її здатності поєднувати окремі внески для створення спільного ключа без розкриття точних внесків [15].

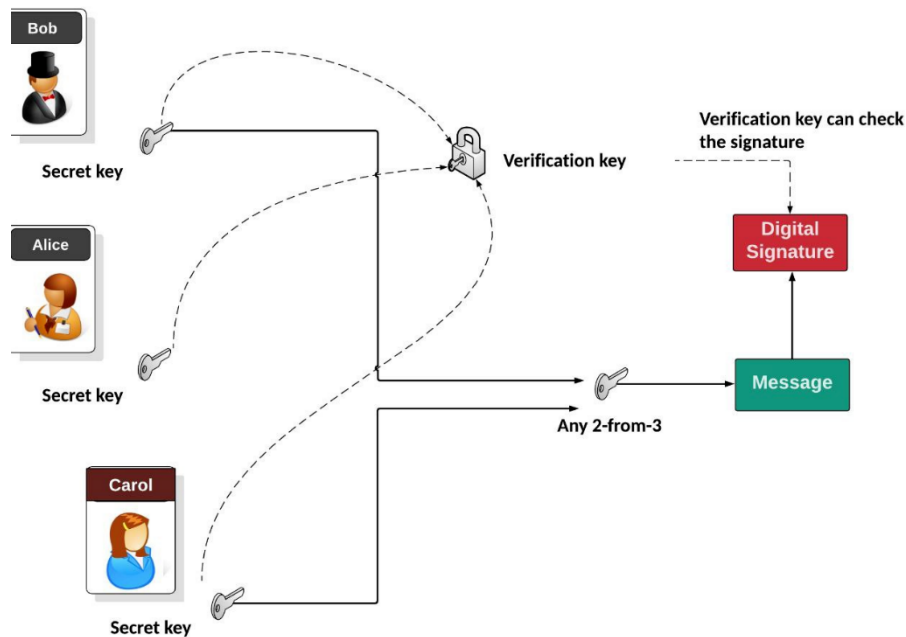


Рисунок 9 – Схематичне зображення розподіленої генерації ключа (DKG)

Порівнюючи розглянуті алгоритми можна виділити те що, SSS (Схема розподілу секрету Шаміра) забезпечує можливість зберігання приватного ключа (ПК) у розподіленому вигляді, що підвищує безпеку. Проте, SSS має недоліки, такі як необхідність "дилера" для генерації частин секрету та вимога для всіх сторін відновити повний ПК для підпису [17,21].

Протокол порогового підпису (TSS) пропонує певні переваги. TSS ґрунтується на чистій криптографії, що робить його незалежним від конкретних реалізацій блокчейн клієнтів. TSS усуває потребу в центральному "дилері", оскільки його роль розподілена, і повний ПК ніколи не зберігається в одному місці. TSS дозволяє розподілене підписання без відновлення частин секрету, покращуючи як безпеку, так і ефективність.

За результатами проведеного дослідження наявних технологій та проблем, пов'язаних з ними, а також з урахуванням зростаючої популярності криптовалют, постає задача розробки та створення системи конфіденційності та безпеки криптоактивів на основі технології багатосторонніх обчислень.

Визначена необхідність розробки системи для надійного зберігання активів, а саме у вигляді приватних ключів до створених користувачем гаманців Ethereum мережі. Це є важливою задачею, що передбачає створення рішення для забезпечення безпеки, приватності та зручності для користувачів.

Метод забезпечення конфіденційності та безпеки криптоактивів на основі технології багатосторонніх обчислень для Ethereum мережі полягає в:

- забезпеченні високого рівня безпеки для збереження приватних ключів та процесу підписання транзакцій, використовуючи передові методи криптографічного захисту;
- гарантуванні конфіденційності та приватності користувачів, захищаючи їх особисту інформацію від несанкціонованого доступу або витоку даних.
- використанні передових технологій, включаючи технологію Multi-Party Computation (MPC), для підвищення рівня безпеки та приватності зберігання активів.

Метод багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation. Протокол багатосторонніх обчислень для системи конфіденційності та безпеки криптоактивів є основою на якій будується принцип контролю приватних ключів користувачів та здійснення усіх необхідних операцій, таких як підписання транзакції та її валідація. При проектуванні таких протоколів необхідно запобігти усіх наявних мінусів попередніх протоколів.

Проблемою алгоритму секретного поділу Шаміра є одна точка відмови, а саме центральний сервер який виконує розподіл і збирання секретного ключа, і цей фактор потрібно врахувати при проектуванні протоколу для системи. Проте перевагою є можливість розділити приватний ключ на частинки з порогом відновлення.

Хоча доведено, що протокол порогового підпису є безпечним, його реалізація також може вимагати деяких додаткових заходів для захисту секретних даних. Тому використовуючи запропоновані варіанти про пороговий протокол ECDSA [26], розширимо протокол додатковими механізмами для досягнення активної безпеки:

1. Механізм оновлення секретного ключ. У пороговій криптографії секрет розподіляється між n сторонами, і щоб використовувати секретний ключ, $t+1$ сторони повинні об'єднати свої частки. З точки зору суперництва, зловмисник повинен порушити $t+1$ сторін, щоб атакувати таку схему. Якщо припустити, що зловмисник порушує сторони одну за одною, механізм оновлення ключа пом'якшує таку атаку, під час оновлення ключа секретні спільні ресурси оновлюються через певний період. Таким чином, якщо зловмиснику вдається порушити деякий відсоток сторін протягом певного періоду та порушувати решту в наступному періоді, вони не можуть розкрити таємницю, оскільки акції поновлюються в кінці першого періоду. Єдиний спосіб для зловмисника досягти успіху - атакувати $t + 1$ сторін одночасно, що набагато складніше.

2. Докази з нульовим знанням. У такому випадку протокол використовує «оптимістичний» підхід і повинен використовувати мінімальну кількість доказів з нульовим знанням у протоколі для отримання кращих результатів продуктивності. Одним із типів доказів нульового знання, є докази діапазону в протоколі MtA (Multiplicative to Additive), які використовуються для підтвердження того, що секретні частки менші за певне число, але через ці перевірки протокол стає відносно дорогим у продуктивності, та впливає на швидкодію програми.

Видалення даних механізмів із протоколу може призвести до витоку інформації про секретний ключ, який обмежений і не впливає на безпеку протоколу. Таким чином, дані механізми можуть бути включені в реалізацію або виключені з неї щодо компромісу між безпекою та продуктивністю.

Для знаходження компромісу між ефективністю та безпекою в системі, для покращення безпеки, використано принцип з інтервальним оновленням спільних поділених частин та не використанню механізму доказів нульової довіри для покращення продуктивності.

Протокол повинен відповідати властивостям багатосторонніх обчислень, а саме конфіденційності, де кожна сторона гарантує, що жодна зі сторін не знає загального секрету, але може гарантувати правильне розподілене обчислення над даними. Це можна досягти за допомогою розподіленої генерації ключа для ECDSA в контексті Ethereum. Такий підхід забезпечує, що приватний ключ ніколи не розкривається жодній стороні, а підписання транзакцій виконується спільно, що підвищує безпеку та конфіденційність. Даний алгоритм необхідно розширити інтервальним оновленням частин секрету, без втрати оригінального секрету, що є важливим аспектом забезпечення довготривалої безпеки в розподілених системах.

Процес розподіленої генерації ключа складається з наступних етапів: ініціалізація; генерація поліному; обрахунок частин ключа; надсилання частин ключа сторонам; обчислення власної частини стороною секрету. Ініціалізація розпочинається з ініціалізації однієї зі сторін протоколу генерації, і тоді кожен учасник генерує свою частину секретного ключа S_i випадковим чином, але так щоб згенероване значення відповідало вимозі, що число додатне та менше за встановлений порядок поля q , де q це кінцева точка обраної еліптичної кривої для системи. У нашому випадку використовується крива secp256k1, що задається рівнянням (1)

$$y^2 = x^3 + ax + b \quad (1)$$

де a, b – параметри, задаються для кривої secp256k1 дорівнюють 0 та 7 відповідно.

Далі відбувається генерація поліному кожною стороною з $f(x)$ ступеня t з випадковими коефіцієнтами a_i , поліном задається наступним виразом (2):

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_tx^t \quad (2)$$

де t – поріг відновлення; a_0 – коефіцієнт який дорівнює S_i (згенерований секрет).

Після того як поліном згенеровано, сторона обчислює частки ключа для кожної іншої сторони передаючи до поліному $f(x)$ порядковий номер вузла у якості параметру x . Згенерований перелік частин власного секретного ключа, сторона розсилає до відповідного учасника через безпечний канал зв'язку. Після того як усі частинки надіслані та отримані сторонами, кожна зі сторін може безпечно обрахувати спільний секретний ключ сумуючи отримані частинки за модулем порядку поля q , цього вистачить для отримання публічного ключа, яким потім можна буде перевірити на валідність транзакцію. Алгоритм розподіленої генерації спільного секретного ключа наведений на рис.10.

Тепер необхідно розробити механізм інтервального оновлення часток секретного ключа, опираючись на математичні операції які застосовувались для їх генерації. Опираючись на

поділ секрету Шаміра [17] можна виділити наступні кроки оновлення часток спільного секретного ключа: ініціалізація; генерація та розподіл; обчислення нових часток.

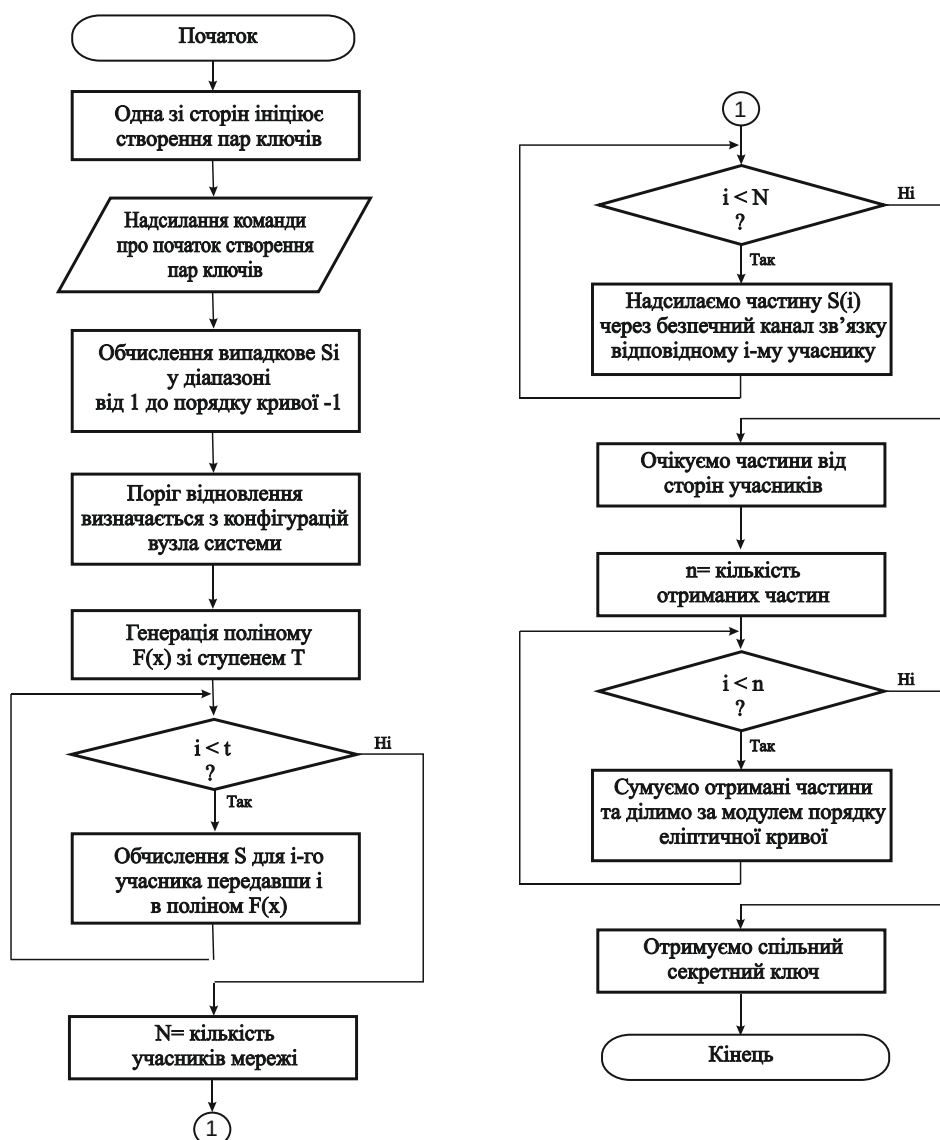


Рисунок 10 – Алгоритм розподіленої генерації спільного секретного ключа

Оновлення ключа розпочинається з того, що один із учасників повідомляє інших про початок раунду оновлення часток. Тоді кожен учасник повинен згенерувати випадкове число n_i , відповідно до того яке він генерував для власного секретного ключа. Це випадкове число буде використано для зміни його частки секретного ключа. Згенеровані частки обмінюються між учасниками через безпечний канал зв'язку. Після обміну новими частками ключа, учасники повинні обрахувати свій новий спільний ключ (3):

$$s'_i = s_i + \sum_{j=i} n_j - n_i \quad (3)$$

де s_i — це поточна частка учасника j ; s'_i — оновлена частка ключа.

Сума n , що надходить від інших учасників, додається, а своє власне n віднімається, щоб зберегти загальну суму секретного ключа незмінною. Алгоритм оновлення часток приватного ключа учасника протоколу наведено на рис.11.

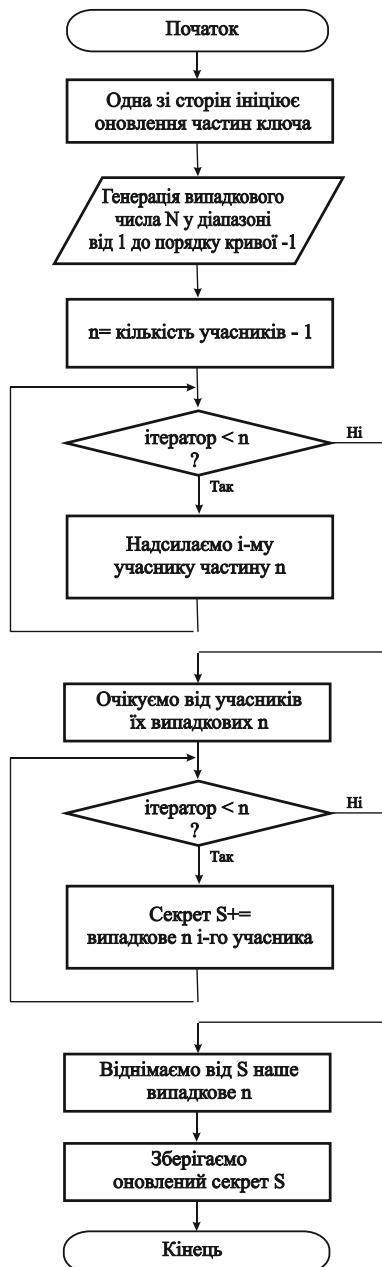


Рисунок 11 – Алгоритм оновлення частинок приватного ключа учасника протоколу

Таким чином можемо досягти регулярного оновлення часток секретного ключа, зменшуючи ризики компрометації і підтримуючи високий рівень безпеки в розподілених системах. Шляхом розробки та впровадження протоколу багатосторонніх обчислень з ключами, розподіленими та періодично оновлюваними - ефективно покращуємо рівень безпеки, у порівнянні з традиційними методами зберігання ключів у єдиному місці, наш підхід забезпечує значно вищий ступінь захисту від потенційних атак. Замість того, щоб мати один централізований пункт доступу, який може стати мішенню для зловмисників, ми розподіляємо ключі між декількома довіреними елементами системи. Кожен ключ періодично оновлюється або змінюється, ускладнюючи можливість несанкціонованого доступу. Цей підхід не лише робить процес взлому системи значно складнішим завданням, але й активно захищає систему від потенційних атак, надаючи більшу впевненість у безпеці та надійності обчислень.

Система багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation. Система реалізована як однорангова (peer-to-peer, P2P) мережа для забезпечення децентралізації та підвищеної безпеки. Комп'ютерні мережі типу P2P засновані на принципі рівноправності учасників і характеризуються тим, що їх елементи

можуть зв'язуватися між собою, кожен вузол виконує роль учасника в процесі генерації та оновлення ключів, а також підписання транзакцій [4,16].

Для забезпечення комунікації між вузлами у системі використана технологія веб-сокетного з'єднання. Використання WebSocket дозволяє побудувати надійний та ефективний механізм обміну даними між вузлами. При використанні WebSocket можливо реалізувати різні типи повідомлень для обміну даними між центральним сервером і вузлами, такі як запити на підпис транзакцій, генерацію приватних ключів, а також статусні повідомлення для синхронізації даних між вузлами, дозволяє побудувати розширені механізми керування підключеннями, автентифікацію та авторизацію, що може бути корисним для забезпечення безпеки та надійності комунікації між центральним вузлами.

Важливим пунктом у організації такого з'єднання, є встановлення безпечного та конфіденційного каналу зв'язку між вузлами. Загальну схему встановлення безпечного каналу зв'язку між двома вузлами наведено на рис.12.



Рисунок 12 - Загальна схема встановлення безпечного зв'язку

Схема описує процес встановлення безпечного з'єднання між двома вузлами (A і B) у одноранговій мережі з використанням асиметричної криптографії RSA, складається з наступних кроків: початок з'єднання; перевірка ID; передача відкритого ключа; шифрування пароля; передача шифрованого пароля; дешифрування та верифікація.

Процес встановлення безпечного зв'язку між вузлами (A і B) у одноранговій мережі:

1. Вузол A звертається до Вузла B з проханням про початок з'єднання. Вузол A надсилає унікальний ідентифікатор (ID), який використовується для автентифікації, його встановлює адміністратор системи при розгортанні.

2. Після отримання запиту, Вузол B перевіряє надісланий ID. Якщо ID вірний, Вузол B генерує пару ключів RSA, яка складається з відкритого і приватного ключів.

3. Вузол B відправляє свій відкритий ключ до Вузла A. Відкритий ключ буде використовуватись для шифрування повідомлень з паролем мережі від Вузла A до Вузла B.

4. Вузол A отримує відкритий ключ і використовує його для шифрування пароля.

5. Шифрований пароль передається через мережу до Вузла B.

6. Вузол B отримує шифрований пароль, дешифровує його за допомогою свого приватного ключа RSA. Після успішного дешифрування Вузол B перевіряє правильність отриманого пароля. Якщо пароль вірний, Вузол B надсилає відповідь "ОК" до Вузла A, що підтверджує успішне встановлення безпечного з'єднання. Тоді обидва вузли можуть безпечно шифрувати та дешифрувати дані використовуючи пароль мережі, з використанням алгоритму симетричного шифрування AES.

Для кожної операції генерації адреси або підписання транзакції у системі вузла буде реалізована відповідна кінцева точка.

Загальну схему взаємодії компонентів системи наведено на рис.13. Мережевий компонент відповідає за зв'язок з іншими вузлами, забезпечуючи прийом і відправку повідомлень, таких як запити на підписання або частки ключів. Інтерфейс для ініціалізації з'єднань з вузлами дозволяє вузлу ефективно взаємодіяти в одноранговій мережі. Також цей компонент відповідає за API взаємодію з кінцевим клієнтом.

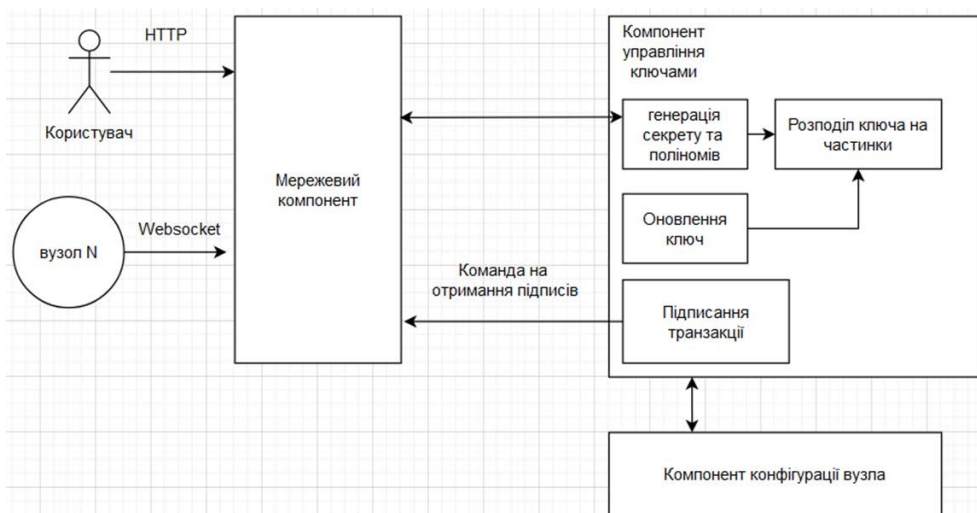


Рисунок 13 - Схема взаємодії компонентів архітектури вузла програмного забезпечення системи

Компонент управління ключами виконує генерацією поліномів та розподілом часток ключів. Компонент шифрує частки ключів перед їх передачею іншим вузлам та дешифровує отримані частки, забезпечує безпеку ключової інформації під час її обміну між вузлами мережі. Компонент також включає в себе оновлення ключа та своєчасне виконання протоколу багатосторонніх обчислень для оновлення часток секретного ключа.

Компонент підписання відповідає за генерацію часток підпису. Виконує верифікацію часток підпису, отриманих від інших вузлів, і комбінує їх для створення загального підпису. Це критично важливий процес, який забезпечує цілісність та авторитетність транзакцій у системі.

Компонент конфігурації налаштовує параметри безпеки, такі як шифрування та генерація ключів, а також параметри мережевого з'єднання, включаючи IP-адреси та порти. Параметри порогової криптографії, зокрема кількість учасників, інтервал оновлення частинок ключа та поріг, також налаштовуються через даний компонент. Це дозволяє вузлу функціонувати в рамках визначених безпекових політик та забезпечує гнучкість системи.

Розгортання системи керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв'язку та маршрутизації.

Система керування криптоактивами, використовує технології багатосторонніх обчислень, дозволяє генерувати ключі та підписувати транзакції, виконуючи операції між різними вузлами. Це дозволяє підвищити безпеку активів, адже приватний ключ перебуває у розподіленому стані.

Висновки. Проведено дослідження предметної області та запропонований метод багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation. Шляхом розробки та впровадження протоколу багатосторонніх обчислень з ключами, розподіленими та періодично оновлюваними - ефективно покращуємо рівень безпеки. У порівнянні з традиційними методами зберігання ключів у єдиному місці, наш підхід

забезпечує значно вищий ступінь захисту від потенційних атак. Замість централізованого пункту доступу, який може стати мішенню для зловмисників, ми розподіляємо ключі між декількома довіреними елементами системи. Кожен ключ періодично оновлюється або змінюється, ускладнюючи можливість несанкціонованого доступу. Даний підхід не лише робить процес взлому системи значно складнішим завданням, але й активно захищає систему від потенційних атак, надаючи більшу впевненість у безпеці та надійності обчислень.

Системи керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв'язку та маршрутизації. Система надає можливість надійного зберігання криптоактивів, зокрема приватних ключів до гаманців Ethereum мережі, з використанням технології MPC, яка може бути використана у різних криптопроектах для безпечного переказу криптоактивів.

На основі проведеного дослідження та аналізу характеристик стандартів протоколів багатосторонніх обчислень запропонований протокол, який враховує наявні покращення та недоліки попередніх протоколів. Для покращення безпеки, у протоколі було впроваджено принцип інтервального оновлення спільного секрету.

Архітектура системи передбачає взаємодію основних компонентів для забезпечення надійної та безпечної роботи. Запропоновано схему встановлення безпечного з'єднання вузлів та описано модель локального сховища, яке забезпечує безпечне зберігання часток ключів, підписів та системних логів.

ЛІТЕРАТУРА:

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.
2. What Makes a Blockchain Secure? Академія Binance: веб-сайт. URL: <https://academy.binance.com/en/articles/what-makes-a-blockchain-secure> (дата звернення: 20.02.2024).
3. Бем, М. В. Стандарти захисту персональних даних в соціальній сфері. / М. В.Бем, І. М. Городиський -Львів:, 2018р. - 110 с.
4. Що таке транзакції у блокчейні? Incrypted : веб-сайт. URL: <https://incrypted.com/tranzakcii-v-blokcheyn/> (дата звернення: 20.02.2024).
5. Голубєв, О.В. Програмно-технічні засоби захисту даних від комп'ютерних злочинів / О. В. Голубєв– Запоріжжя : «Павел», 2018. – 145 с.
6. Горбулін, В. П. Проблеми захисту інформаційного простору України / М.М. Биченок, В.П. Горбулін – К.: Інтертехнологія, 2019. – 138 с.
7. Ленков, С.В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Ленков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.
8. What Is a Merkle Tree & What Is Its Role in Blockchain? Learn ByBit: веб-сайт. URL: <https://learn.bybit.com/blockchain/what-is-merkle-tree/>(дата звернення: 20.02.2024).
9. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Селюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.
10. Proof of Work (PoW) Process flow. ResearchGate : веб-сайт. URL: https://www.researchgate.net/figure/Proof-of-Work-PoW-Process-flow-Latif-et-al-2021_fig2_374870812 (дата звернення: 20.02.2024).
11. Why is so Much Important to have Digital Signatures? Medium: веб-сайт. URL: <https://saurabh57788.medium.com/why-is-so-much-important-to-have-digital-signatures-8583abec63d1> (дата звернення: 20.02.2024).
12. Ємельянов, С.Л. Основи інформаційної безпеки. / С.Л. Ємельянов– Одеса: Фенікс, 2019р.– 357 с.

13. Кастодіальні та некастодіальні гаманці: у чому різниця? Академія Binance : веб-сайт. URL: <https://academy.binance.com/uk/articles/custodial-vs-non-custodial-wallets-what-s-the-difference> (дата звернення: 20.02.2024).
14. An overview of Multi-Party Computation (MPC), Threshold Signatures (TSS) and MPC-TSS wallets. Medium : веб-сайт. URL: <https://mmasoudi.medium.com/an-overview-of-multi-party-computation-mpc-threshold-signatures-tss-and-mpc-tss-wallets-4253adacd1b2> (дата звернення: 20.02.2024).
15. Secure multi-party computation. Wikipedia : веб-сайт. URL: https://en.wikipedia.org/wiki/Secure_multi-party_computation (дата звернення: 20.02.2024).
16. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсєєв, О.Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.
17. Building A New Digital World: Threshold Signing and Key Distribution Generation. Medium : веб-сайт. URL: <https://medium.com/asecuritysite-when-bob-met-alice/building-a-new-digital-world-threshold-signing-and-key-distribution-generation-a1235390b6aa> (дата звернення: 20.02.2024).
18. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.
19. Рибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. – с.57-62
20. Threshold Signatures Explained. Академія Binance : веб-сайт. URL: <https://academy.binance.com/uk/articles/threshold-signatures-explained> (дата звернення: 20.02.2024).
21. Multisig vs. (SSS vs. TSS). Typefully : веб-сайт. URL: <https://typefully.com/tomkowalczyk/JAfJzji> (дата звернення: 20.02.2024).
22. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.
23. WebSocket. Wikipedia : веб-сайт. URL: <https://uk.wikipedia.org/wiki/WebSocket> (дата звернення: 20.02.2024).
24. Хорошко, В.О. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браїловський - Київ., 2019р. 164 с.
25. Proactive Secret Share for Eigen Secret Recovery. EigenLab. 2021. URL: <https://www.pdau.edu.ua/sites/default/files/node/4518/pravylaoformlennyaspyshkuvykorystanyhdzherel.pdf> (дата звернення: 20.02.2024).
26. Jens Groth and Victor Shoup. Design and analysis of a distributed ECDSA signing service. Cryptology ePrint Archive, Paper 2022/506. 2022. URL: <https://eprint.iacr.org/2022/506> (дата звернення: 20.02.2024).

REFERENCES:

1. Doktryna informatsiinoi bezpeky Ukrainy, zatverdzhenoї Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku № №47/2017, 15s.
2. What Makes a Blockchain Secure? Akademia Binance: veb-sait. URL: <https://academy.binance.com/en/articles/what-makes-a-blockchain-secure> (data zvernennia: 20.02.2024).
3. Bem, M. V. (2018) Standarty zakhystu personalnykh danykh v sotsialnii sferi. / M. V. Bem, I. M. Horodyskyi -Lviv - 110 s.
4. Shcho take tranzaktsii u blokcheini? Incrypted : veb-sait. URL: <https://incrypted.com/tranzakcii-v-blokcheyn/> (data zvernennia: 20.02.2024).
5. Holubiev, O.V. (2018) Prohramno-tekhnichni zasoby zakhystu danykh vid kompiuternykh zlochyniv / O. V. Holubiev– Zaporizhzhia : «Pavel» – 145 s.
6. Horbulin, P.V. (2019) Problemy zakhystu informatsiinoho prostoru Ukrainy / M.M. Bychenok, P.V. Horbulin – K.: Intertekhnolohiia – 138 s.
7. Lenkov, S.V.(2023), Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv / S.V. Lienkov, V.M. Dzhulii, A.M. Bernaz, I.V. Muliar, I.V. Pampukha // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnogo universytetu imeni Tarasa Shevchenka. – K.: VIKNU -. №78. – С. 123-134.
8. What Is a Merkle Tree & What Is Its Role in Blockchain? Learn ByBit: веб-сайт. URL: <https://learn.bybit.com/blockchain/what-is-merkle-tree/> (data zvernennia: 20.02.2024).

9. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoї informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.
10. Proof of Work (PoW) Process flow. ResearchGate : веб-сайт. URL: https://www.researchgate.net/figure/Proof-of-Work-PoW-Process-flow-Latif-et-al-2021_fig2_374870812 (data zvernennia: 20.02.2024).
11. Why is so Much Important to have Digital Signatures? Medium: веб-сайт. URL: <https://saurabh57788.medium.com/why-is-so-much-important-to-have-digital-signatures-8583abec63d1> (data zvernennia: 20.02.2024).
12. Yemelianov, S.L. (2019) Osnovy informatsiinoї bezpeky./S.L.Yemelianov– Odesa: Feniks – 357s.
13. Kastodialni ta nekastodialni hamantsi: u chomu riznytsia? Akademiia Binance : veb-sait. URL: <https://academy.binance.com/uk/articles/custodial-vs-non-custodial-wallets-what-s-the-difference> (data zvernennia: 20.02.2024).
14. An overview of Multi-Party Computation (MPC), Threshold Signatures (TSS) and MPC-TSS wallets. Medium : veb-sait. URL: <https://mmasmoudi.medium.com/an-overview-of-multi-party-computation-mpc-threshold-signatures-tss-and-mpc-tss-wallets-4253adacd1b2> (data zvernennia: 20.02.2024).
15. Secure multi-party computation. Wikipedia : veb-sait. URL: https://en.wikipedia.org/wiki/Secure_multi-party_computation (data zvernennia: 20.02.2024).
16. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.
17. Building A New Digital World: Threshold Signing and Key Distribution Generation. Medium : веб-сайт. URL: <https://medium.com/asecuritysite-when-bob-met-alice/building-a-new-digital-world-threshold-signing-and-key-distribution-generation-a1235390b6aa> (data zvernennia: 20.02.2024).
18. Buriachok, V. L. (2016) Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby : posibnyk / V. L. Buriachok, S. V. Toliupa, V. V. Semko – K. : DUT-KNU – 178 s.
19. Rybalchenko, L.V., Kosychenko, O.O. (2019) Problemy bezpeky personalnykh danykh v Ukraini / Rehionalna ekonomika / Zaporizhzhia – s.57-62
20. Threshold Signatures Explained. Академія Binance : веб-сайт. URL: <https://academy.binance.com/uk/articles/threshold-signatures-explained> (data zvernennia: 20.02.2024).
21. Multisig vs. (SSS vs. TSS). Typefully : веб-сайт. URL: <https://typefully.com/tomkowalczyk/JAfJzji> (data zvernennia: 20.02.2024).
22. Honchar, S. F. (2019) Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obektiv krytychnoi infrastruktury : monohrafiia. / S. F. Honchar. – Kyiv – 175 s.
23. WebSocket. Wikipedia : veb-sait. URL: <https://uk.wikipedia.org/wiki/WebSocket> (data zvernennia: 20.02.2024)
24. Khoroshko, V.O. Zakhyst system elektronnykh komunikatsii: navch. posib. / V.O. Khoroshko, O.V. Kryvoruchko, M.M. Brailovskyi - Kyiv., 2019r. 164 s.
25. Proactive Secret Share for Eigen Secret Recovery. EigenLab. 2021. URL: <https://www.pdau.edu.ua/sites/default/files/node/4518/pravylaoformlennypyskuvykorystanyhdzherel.pdf> (data zvernennia: 20.02.2024).
26. Jens Groth and Victor Shoup. Design and analysis of a distributed ECDSA signing service. Cryptology ePrint Archive, Paper 2022/506. 2022. URL: <https://eprint.iacr.org/2022/506> (data zvernennia: 20.02.2024).

METHOD OF MULTI-PARTY COMPUTATION MANAGEMENT OF CRYPTOASSETS BASED ON MULTI-PARTY COMPUTATION TECHNOLOGY

The task of building an efficient and secure crypto-currency wallet based on multi-party computing technology, which can provide reliable and secure use in various industries working with cryptocurrencies, is considered.

Modern algorithms of multilateral calculations, such as those of Gennaro and Goldfeder, Lindella, Doerner, offer significant advantages in data protection, but they have certain limitations. The main ones are insufficient efficiency in the number of signature rounds and lack of cold storage support. This highlights the need for further research and development in the field of Multi-Party Computation technology to achieve higher levels of operational efficiency and flexibility.

The method of ensuring the confidentiality and security of cryptoassets on the dream technology of multilateral computing for the Ethereum network consists in: ensuring a high level of security for the storage of private keys and the process of signing the transaction, using advanced cryptographic protection methods; guaranteeing the confidentiality and privacy of users, protecting their personal information from unauthorized access or data leakage; using advanced technologies, including Multi-Party Computation technology, to increase the level of security and privacy of asset storage.

On the basis of the conducted research and analysis of the characteristics of multiparty computing protocol standards, a protocol is proposed that takes into account the existing improvements and shortcomings of previous protocols. To improve security, the protocol implements the principle of interval update of the shared secret.

A cryptoasset management system based on multilateral computing includes several important stages: choosing cloud providers, creating and configuring instances, containerizing applications, configuring secure communication and routing. The system provides the possibility of reliable storage of cryptoassets, in particular, private keys to wallets of the Ethereum network, using the Multi-Party Computation technology, which can be used in various cryptoprojects for the safe transfer of cryptoassets.

The architecture of the system involves the interaction of the main components to ensure reliable and safe operation. A scheme for establishing a secure connection of nodes is proposed and a local storage model is described, which provides secure storage of key shares, signatures, and system logs.

Keywords: cryptoassets, confidential information, cryptoasset security, multi-party computation technology, secure connection, information security, cryptocurrency, digital assets, cryptocurrency wallet.

АНАЛІЗ СУЧАСНИХ ТА ТРАДИЦІЙНИХ МЕТОДІВ ПРОЕКТУВАННЯ І ВИРОБНИЦТВА ВІЙСЬКОВОЇ ТЕХНІКИ З ВИКОРИСТАННЯМ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

В статті авторами виконано один із видів аналізу існуючих та перспективних методів проектування і виробництва військової техніки з використанням автоматизованих інформаційних систем. Відомо, що програмне забезпечення АІС має характерні ознаки складної системи і підпорядковується законам науки про складні системи. Сучасний етап розвитку складних інформаційних систем характеризується тим, що тенденція до різкого збільшення складності завдань управління все в більшому ступені виявляється в об'ємності програмного забезпечення систем управління технічними об'єктами, технологічними процесами і виробництвом. В роботі зроблено класифікацію програм, відповідно до SPE, яка, являє собою «модель деякої іншої моделі в рамках теорії абстрактного уявлення окремих об'єктів». Вона може бути віднесена до одного з трьох класів: S-клас – це програми, функції яких формально визначаються специфікаціями і впливають із них. Відповідність між входом і виходом є визначальною і будь-яка зміна, створює нову програму. Р-клас – складають програми, прийнятність рішення яких оцінюється шляхом порівняння з реальною обстановкою, тобто програми цього класу повинні постійно змінюватися залежно від зміни навколишнього середовища, уточнення даних тощо. Програми Е-класу самі стають частиною реалізації обстановки, яку вони моделюють, тобто в ще більшому ступені, ніж Р-програми схильні до змін.

Розглянуті основні фази життєвого циклу АІС і визначені їх особливості: визначення, проектування, реалізації, впровадження, експлуатації.

Визначено концептуальну єдність підходів, що використані на етапах отримання системних специфікацій, проектування модульної структури та реалізації модулів, дозволила об'єднати прийняття окремих рішень в єдину методiku проектування коректного спеціального програмного забезпечення, основними відмінностями якої є: пошированість, яка досягається використанням принципу абстрагування (ієрархії); об'єднання процесу проектування з процесом моделювання, що досягається застосуванням графових моделей, які отримуються в процесі проектування, та можливістю використання кожного рівня ієрархії в якості моделі СПЗ; безперервність процесу проектування, яка забезпечується сумісністю моделей, які отримуються на різних етапах, участю системного програміста в розробці з начального етапу і можливістю початку кодування з першого етапу.

Ключові слова: автоматизовані інформаційні системи, системи управління технічними об'єктами, концептуальна єдність підходів, безперервність процесу проектування.

Вступ та аналіз останніх досліджень. Коли мова йде про якість програмного забезпечення автоматизованої інформаційної системи (АІС), об'єктом дослідження стають не стільки власне програми (тексти, що написані мовою, яка сприймається комп'ютером), скільки саме математичне забезпечення АІС, тобто сукупність методів, моделей і алгоритмів для розв'язання задач і опрацювання інформації з застосуванням обчислювальної техніки. Тому в

результаті розроблення математичного забезпечення в остаточному підсумку і з'являється сукупність програм, які реалізують задум проектувальника: сукупність функцій АІС, забезпечуючих функціонування комплексу технічних засобів і бажаний розвиток системи, тобто програмне забезпечення.

Програмне забезпечення АІС має характерні ознаки складної системи і підпорядковується законам науки про складні системи [1,2]. Сучасний етап розвитку складних інформаційних систем характеризується тим, що тенденція до різкого збільшення складності завдань управління все в більшому ступені виявляється в об'ємності програмного забезпечення систем управління технічними об'єктами, технологічними процесами і виробництвом. Обсяг опрацьованої інформації в системах цього типу зростає більш інтенсивно, ніж збільшення обсягів самого виробництва або підвищення його техніко-економічних показників [3-5].

Аналіз підходів до проектування АІС військового призначення. Розв'язання задач прискорення створення і використання вимог по підвищенню ефективності АІС на базі розробки пакетів практичних прикладних програм (типових алгоритмічних модулів), моделювання і управління технологічними процесами розроблення типових та уніфікованих елементів забезпечення, способів і методик їх розробки.

Задачі оптимізації вирішуються за допомогою моделей, тому їх ієрархія задач відповідає ієрархії моделей керованих підсистем відповідних комплексів. Автори виділили основні рівні ієрархії таких складних технологічних комплексів [5,6]:

- побудова моделей керування;
- вирішення задач керування, по рівню складності рішення;
- побудова ієрархії технічних засобів.

Перший вид визначає обробку інформації з метою ідентифікації керованих об'єктів.

Другий – характеризує процес аналізу рішень в системі керування і відповідає дереву цілей системи.

При побудові системи керування найважливішою проблемою є синтез ієрархічної структури. Ці проблеми зводяться до вибору алгоритмів розв'язання задач, оцінки побудови структури, і розроблення правил їх формування.

Саме формалізація методів і алгоритмів побудови АІС є основою застосування сучасної теорії складних систем до проектування математичного забезпечення АІС[7-9].

Класифікація програм, відповідно до SPE, що була запропонована В.Турським [10], являє собою «модель деякої іншої моделі в рамках теорії абстрактного уявлення окремих об'єктів». Вона може бути віднесена до одного з трьох класів:

S-клас – це програми, функції яких формально визначаються специфікаціями і впливають із них. Відповідність між входом і виходом є визначальною і будь-яка зміна, створює нову програму;

P-клас – складають програми, прийнятність рішення яких оцінюється шляхом порівняння з реальною обстановкою, тобто програми цього класу повинні постійно змінюватися залежно від зміни навколишнього середовища, уточнення даних тощо.

Програми E-класу самі стають частиною реалізації обстановки, яку вони моделюють, тобто в ще більшому ступені, ніж P-програми схильні до змін.

Звісно, що спеціальне програмне забезпечення СПЗ АІС відбиває деяку модель або піддається постійним змінам, або згодом утрачає свою корисність. При його синтезі практичні задачі управління включають екстраполяцію наслідків упровадження на перспективи розвитку системи. При конструюванні СПЗ в роботі [11] стверджується, що до програм типів P та E доцільно додати наступну структуру, що всі їх елементи будуть S-програмами. Тобто проектування СПЗ АІС в цьому можна уявити як розвиток специфікацій.

Традиційними технологіями виготовлення СПЗ систем реального часу тривалий час були інструментально-орієнтовані технології, засновані на розвинутих засобах для написання програм, але недостатньо обґрунтовані методологічно. До них варто віднести використання

процедурно-орієнтованих мов реального часу і проблемно-орієнтованих пакетів (пакетів прикладних програм).

Сукупність мови, програмних засобів трансляції, налагодження, документування та обслуговування програм в процесі їхньої розробки й експлуатації складають систему програмування – основу технології при використанні процедурно-орієнтованих мов. Мови виступають і як засіб формалізованого опису і як інструментарій для одержання кінцевого програмного продукту.

Основною якістю програм мов реального часу можна вважати наступні:

- доцільність управління поведінкою операційної системи розвинутими механізмами рівнобіжних обчислень і синхронізації гілок апарату синхронізації обчислювального процесу з зовнішніми подіями, тощо;
- використання досить потужного обчислювального апарата, широкого набору типів і спеціалізованих структур даних;
- використання достатня гнучких різноманітних методологій проектування і підтримку модульного і структурного програмування.

Пакети прикладних програм служать для заміни програмування конструюванням СПЗ з готових елементів і підрозділяються на: бібліотеки програм; системи програмування з використанням спеціалізованих мов; мета системи, що дозволяють генерувати ППП для конкретних застосувань по їх описах.

Добре знайомі традиційні методи проектування ПЗ виділяють два наступних: "униз" (аналітичні підходи) і "нагору" (синтетичний підхід) [10-13]. Проектування методом "униз" полягає у постановленні задачі і розвитку шляхом розбивки задачі на підзадачі. Розробка методом "нагору" починається з оцінки рівня базових понять і подалі розвиває формування більш абстрактних понять, у кінцевому рахунку приводячи до термінів яких легко висловити рішення всієї задачі.

Такі підходи не дають вирішення на кожному кроці, проте забезпечують повний спектр можливостей, які подаються базовим прошарком. Такий підхід до проектування орієнтований скоріше на обслуговування об'єкту, ніж на розв'язання конкретних задач. Цей підхід використовується при побудові операційних систем та інструментальних засобів. Разом з тим, проектування алгоритмічної структури звичайно велося методом «униз».

Одним із різновидів аналітичних підходів є покрокова розробка (ПР) [14] і проектування вертикальними прошарками (ПВС) [15].

Серед відомих методів важливу групу складають методи структурного проектування, які засновані на аналізі потоку інформації. Вони з одного боку, відображають потік даних, а з іншого – перетворення вхідних даних у вихідні. Такі методи описані Джексоном [16] та Уорнером [17]. Вони ефективні при розробці інформаційних систем, тому що орієнтовані на виявлення відповідності вхідних файлів вихідним.

Всі розглянуті традиційні методи лягли в основу нових і дають можливість боротися зі складністю – декомпозицією у рівнях абстракції, що по суті є єдиним способом одержання надійного тобто коректного ПЗ. Слід зазначити, що як аналітичний, так і синтетичний підходи призводять до поняття модульності.

Основна аналітична частина дослідження. Аналіз та розуміння того або іншого методу програмування неможливо поза розглядом поняття моделі життєвого циклу програми – системи процедур, правил і інструментальних засобів, використовуваних для розроблення програмної системи. Життєвий цикл програмної системи спершу визначає вимоги до неї користувачів і закінчується аналізом експлуатації системи цими користувачами в рамках їхнього власного оточення.

Як правило, в життєвому циклі є наступні фази:

1. Визначення:
 - а) вироблення вимог;
 - б) розроблення специфікацій.

2. Проектування:
 - а) проектування архітектури;
 - б) детальне проектування.
3. Реалізація (конструювання):
 - а) кодування;
 - б) інтеграція;
 - в) тестування (сертифікація).
4. Впровадження.
5. Експлуатація (супровід).

Фаза визначення

Під час фази визначення виявляються властивості, які повинна мати система в остаточному варіанті, тобто створюється задум системи. Розроблювач визначає детальну картину зовнішніх властивостей готового виробу: описуються функції, що буде виконувати система; характеристики інтерфейсу, забезпечуваного системою. Під час цієї фази приймаються рішення щодо розмірів, часу відгуку, продуктивності та інших параметрів системи.

Визначення здійснюється за допомогою двох основних категорій – вимог і специфікацій. При цьому розрізняють опис необхідних властивостей (вимоги) і опис об'єкта, що володіє цими властивостями (специфікації).

Вимога – це властивість, необхідна для рішення проблеми або досягнення цілі. При описі використовуються такі поняття, як якість, можливості або інші характеристики системи, гаданого її використання або середовища. Як правило, вимоги розробляються з метою виявлення місця утворюваної системи в рамках раніше визначеної організації або середовища.

Це середовище використання може не мати формального опису, а робота організації користувача майже завжди ґрунтується на інтуїтивному розумінні робочого середовища робітниками даної організації. Тому найкращою мовою опису вимог, що забезпечують суворе, точне і всеосяжне експертне їхнє висловлення, є професійно-природна мова експертів у сфері діяльності організації користувача, тобто вимоги можуть бути розроблені, зрозумілі і перевірені тільки експертами в даній області застосування.

Специфікація – опис на мові розроблювача зовнішньо відомих характерних рис поведінки системи.

Функціональна специфікація програми містить у собі:

- мету програми;
- граничні умови;
- опис функції (що програма повинна робити і, що, можливо, буде робити);
- специфікацію вхідних і вихідних даних;
- верифікаційні вимоги.

Фаза проектування

Вхідною інформацією для проектування є специфікації, написані на підставі вимог користувача. Базуючись на цілях проекту, вимогах до поведінки, планованої документації, специфікаціях дуже високого рівня, різноманітних вихідних формах для користувача, проектувальник здійснює архітектурне і детальне проектування.

Проектування архітектури (первинна або загальна стадія проектування) закінчується декомпозицією специфікацій у структуру системи. При цьому забезпечується подання на модульному рівні, що припускає оцінку, уточнення, модифікацію на самому ранньому етапі розвитку програми. Поряд з описом загальної структури, результатом етапу є специфікації на модуль, що складаються, як правило, з імені/мети, неформального опису, посилань, входу/виходу, алгоритму, приміток.

Ім'я/мета. У цій секції дається ім'я модуля й одне речення, яке описує, що має робити модуль. З ім'ям звичайно дають формальні параметри, асоційовані з модулем. Формальний параметр це параметр, що вказується в полі операндів процедури або макрокоманди. При

виконанні процедури формальний параметр заміщується реальним параметром.

Неформальний опис. Секція містить загальний огляд дій модуля. Потрібно старанно підходити до глибини деталізації опису, приведеного в цій частині. Легко скотитися до поверхневої багатослівності, через що секція стане марною. З іншого боку, легко написати так мало, що стане неясним, що повинен робити модуль.

Посилання. Існують дві категорії посилань: модулі, що прямо посилаються на даний модуль, і модулі, на які посилається даний модуль. Обидві категорії важливі, тому що якщо модуль буде змінюватися, стає ясным, на яких модулях це відіб'ється. Ці посилання також забезпечують можливість перехресних перевірок. З'являється гарантія того, що модулі, на які є посилання, дійсно знають, що на них посилаються. Можна також перевірити, що якщо передбачається, що деякі модулі посилаються на даний модуль, вони дійсно це роблять.

Вхід/вихід. Якщо є формальні параметри, вони повинні бути описані в цій секції. Те саме стосується значення функції, класів змінних і системних констант. Використовуються три специфічних класи змінних:

- а) глобальні змінні, до яких мають доступ усі модулі;
- б) локальні змінні, відомі тільки даному модулю;
- в) змінні, що відомі тільки деяким модулям. Цей останній клас змінних може йти під різними іменами, але важливо відокремити його від перших двох. Інший метод класифікації змінних використовує права доступу. Системні константи – це фіксовані значення, до яких звертаються за символічними іменами.

Алгоритм. Ця частина модуля описує дії модуля. Вони повинні бути зрозумілими розроблювачу. Алгоритм повинний бути структурований. Тут утримуються корисні коментарі. Наприклад, тимчасові характеристики, незвичні ситуації, що призводять до помилкових умов тощо.

На цьому етапі системна структура трансформується в процедурний опис (логіку) програми. Відбувається аналіз, та оцінюється алгоритм для запуску даного модуля. Всі деталі і рішення стосовно кожного модуля повинні бути добре визначені.

Фаза реалізації

Під час цієї фази реалізується переклад проекту у форму програми для конкретної ЕОМ, складання системи та її перевірка в умовах тестових і реальних умов роботи з метою визначення відповідності експлуатаційних характеристик заявленим у специфікації.

Фаза впровадження

Під час цієї фази провадиться повне, упорядковане, координоване користувачем залучення до реального середовища нової або зміненої системи. Варто одержати підтвердження відповідності висунутим раніше вимогам до системи.

Фаза експлуатації

Під час цієї фази життєвого циклу програмної системи здійснюється оцінка працюючої системи і підтримка її працездатності в заданих межах. При випуску програми як товарної продукції для загального користування завершальною фазою є супровід, що полягає в таких діях:

- знаходження і виправлення помилок;
- додання нових функцій і модифікація існуючих;
- включення програми в нову систему;
- поліпшення показників роботи.

Супровід великої програми може коштувати в 2–3 рази дорожче, ніж її розробка. Найбільші витрати йдуть на своєчасне (синхронне) коригування документації і носіїв у користувача.

Під час проектування архітектури специфікації перетворюються в структуру системи. Засоби, що працюють на цій стадії, розділяють на дві групи: ті, що здійснюють опрацювання й ті, що орієнтовані на дані. Методології, спрямовані на опрацювання, надають особливого значення процесу і структурі в створенні архітектури програми. Методології, орієнтовані на

дані, роблять основний акцент на даних.

Методології, що орієнтовані на опрацювання

Найбільше відомі такі методології, орієнтовані на опрацювання: модульне програмування, метод функціональної декомпозиції, метод проектування потоку даних, метод проектування структур даних, метод НІРО [5,7].

Модульне програмування. Основні концепції модульного програмування:

кожний модуль розроблено до єдиної незалежної функції;

кожний модуль має єдину систему вхід/вихід;

розмір модуля повинен бути мінімальним;

кожний модуль може бути спроектований і закодований різноманітними програмістами і може бути окремо протестований;

При такому підході система розділяється на декілька частин, одночасно утворюваних різноманітними програмістами. Кожний модуль реалізує єдину функцію. Розмір модуля невеликий, тому тестування кероване і може бути проведено ретельно. Після кодування і тестування всіх модулів відбувається їхня інтеграція і тестується вся система. При супроводі тестується й налагоджується тільки той модуль, що погано працює. Очевидні переваги в полегшенні написання і тестування програм, зменшується вартість їх супроводу.

Модуль не повинний змінювати команди іншого модуля і, як правило, не повинний зберігати історію своїх викликів (хоча остання властивість істотно спрощує трасування при збої). Відомі позитивні якості модульних програм:

легкість упорядкування і налагодження, функціональні компоненти такої програми пишуться й налагоджуються порізно, можливе добре структуроване налагодження як “нагору”, так і “униз”;

легкість супроводу і модифікації;

можливість розподілу модулів між програмістами різноманітної кваліфікації відповідно до рівня складності;

можливість створювати бібліотеки найбільше вживаних програм;

спрощення процедури завантаження в оперативну пам'ять великої задачі, що потребує сегментації

виникнення численних природних контрольних точок для спостереження за просуванням програми, використовуваних для підвищення усталеності СПЗ.

Передача управління в модульній структурі відбуваються лише по вертикальних лініях, що з'єднує модулі в схемі ієрархії.

Будь-який модуль може активізувати підпорядкований модуль і одержати керування після завершення його роботи. Модуль більш низького прошарку не може викликати модуль більш високого прошарку. Модуль зобов'язаний повернути управління тому модулю, що його викликав. Прийняття рішень модулями нижчого рівня за модулі вищого рівня не припускається. Надмірна кількість аргументів, що подаються модулю, указує на необхідність поділу функції (основна мета при цьому – скорочення числа аргументів).

Функціональна декомпозиція. Функціональна декомпозиція істотно базується на стратегії "розділай і керуй". Відомий фахівець в галузі методології програмування Парнас, формалізував процедуру функціональної декомпозиції у формі покрокової деталізації, у якості критерію декомпозиції системи запропонував концепцію приховування інформації. При використанні цього параметру досліджуваній модуль визначається автором суб'єктивно. Другою важливою ідеєю є проектування програмної системи у вигляді набору віртуальних машин замість традиційного підходу, що використовує блок-схеми. Перевага функціональної декомпозиції в її придатності. Хиби – непередбачуваність і мінливість.

Проектування з використанням потоку даних. Ці методи використовують потік даних як рушійну силу процесу проектування програми. При цьому використовуються різноманітні функції відображення, що перетворюють потік інформації в структуру програми.

Структурне проектування засноване на концепції, яка висунута в роботах Йодана і

Майерса. Метод намагається боротися з хибою, властивою методу функціональної декомпозиції, при використанні якого не можна управляти якістю декомпозиції функції. Підхід полягає у відображенні потоку даних проблеми в структуру програми з використанням деяких способів аналізу проекту. Зазвичай прийнята така процедура:

- ідентифікується потік даних і відтворюється граф потоку даних;
- ідентифікуються вхідні, центральні і вихідні перетворюючі елементи;
- формується ієрархічна структура програми, що використовує ці елементи. Після цього оптимізується структура програми.

Цей підхід застосовується при відсутності яскраво виражених структур даних.

Технологія структурного аналізу проекту SADT, заснована на структурному аналізі, запропонованому Россом.

SADT застосовується в різноманітних практичних і військових галузях. Метод особливо ефективний на стадіях розвитку системи.

Метод перетворення графів. Метод заснований на одержанні системної специфікації у вигляді графа керування задачами з графа інформаційного зв'язку між ними. У основі методу – використання причинно-наслідкових зв'язків між задачами системи, заснованої на їхній взаємній залежності за даними. Основна мета – одержати схему виконання задач, вільну від конфліктів, породжених відсутністю синхронізації даних.

Методологія Уорнера [4,5]. Вона подібна методології Джексона в тому, що ключем до проекту програми є структури даних. Проте процедура проектування більш деталізована. Використовуються чотири види подання проекту: діаграми організації даних, діаграми логічного проходження, список інструкцій, псевдокод. Діаграма організації даних описує вхідні і вихідні дані. Діаграми логічного проходження подають логічний потік цих даних. Список інструкцій містить команди, що використовуються в проекті. Псевдокод потрібний при описі кінцевих результатів проектування. Методологія Уорнера може бути узагальнена в такий спосіб:

- ідентифікувати усі вхідні дані системи;
- організувати вхідні дані в ієрархічну форму;
- визначити детальний формат кожного елемента вхідного файлу і зафіксувати число їх появ;

- повторити кроки 1–3 для вихідних даних;

- специфікувати деталі програми, ідентифікуючи типи команд, що містяться в проекті, в такому порядку: читання, розгалуження, обчислення, входи, виходи, виклик підпрограм;

- використовувати діаграми типу блок–схем для показу логічної послідовності інструкцій, використовуючи спеціальні символи для подання початку процесу, кінця процесу, розгалуження і вкладення;

- пронумерувати елементи логічної послідовності і розкрити їх за допомогою інструкцій, записаних у кроку 5.

НІРО (Ієрархія плюс Вхід, Опрацювання, Вихід). Метод ієрархічних діаграм, розвинений фірмою ІВМ. Основні характеристики:

- спроможність подавати зв'язок між вхідними/вихідними даними і процесом опрацювання;

- можливість декомпонувати систему ієрархічно, не залучаючи зайві дрібні деталі;

- використання трьох елементів: вхід, опрацювання, вихід.

Опрацювання (процес) специфікується як центральний блок діаграми, вона сполучена з елементами, що відображають вхід і вихід.

Основна процедура проектування з використанням НІРО:

- почати з найвищого рівня абстракції;

- ідентифікувати вхід, вихід і опрацювання;

- з'єднати кожний елемент входу і виходу з відповідним опрацюванням;

- документувати кожний елемент системи, використовуючи НІРО діаграми;

деталізувати діаграму, використовуючи кроки 1–4.

Методології, орієнтовані на дані. У цих методологіях виділяються компоненти проекту, засновані на даних. Це так звані об'єктно-орієнтована методологія проектування і методологія проектування концептуальних баз даних. Оскільки обидві технології належать до методу формалізації специфікацій, спочатку розглянемо концепцію методів формальних специфікацій.

Програми можуть бути побудовані методично (систематично), виходячи з формальних специфікацій на дані, з якими вони працюють. Базуючись на формальних специфікаціях, можна розробити засоби автоматичного програмування і докази слушності програм. Особлива увага в літературі приділяється абстракціям даних. Відомі математичні основи доказу коректності з використанням алгебраїчних і аксіоматичних специфікацій. У багатьох роботах формальні специфікації в сполученні з технікою верифікації використані для виявлення помилок на ранніх стадіях життєвого циклу ПЗ.

Об'єктно-орієнтована методологія проектування. Заснована на концепціях приховування інформації й абстрактних типів даних. Такий підхід розглядає всі такі ресурси, як дані, модулі і системи в якості об'єктів.

Кожний об'єкт містить деяку структуру даних (або тип даних), обрамлену набором процедур, що знають як маніпулювати з цими даними. Використовуючи цю методологію, проєктант може створити свій власний абстрактний тип і відобразити проблемну частину у ці створені проєктантом абстракції замість традиційного відображення проблемної частини у визначені керуючі структури і структури даних мови реалізації. Подібний підхід рекламується як більш природний, чим методології, орієнтовані на опрацювання (на процес).

Через можливість створювати в процесі проектування різноманітні види абстракції типів даних на цьому шляху проєктант може сконцентруватися на проєкті системи, не турбуючись про деталі інформаційних об'єктів, використовуваних у системі. Повний поділ між специфікаціями і реалізацією в мовах АДА і МОДУЛА-2 роблять їх найбільше пристосованими для використання в даній методології. Основні дії, реалізовані методологією:

- визначити проблему;

- розвинути неформальну стратегію, що подає загальну послідовність кроків, яка задовольняє вимогам до системи;

- формалізувати стратегію (ідентифікувати об'єкти і їхні атрибути; ідентифікувати операції над об'єктами; встановити інтерфейси; реалізувати операції).

Методологія, що заснована на проектуванні концептуальних баз даних. Належить до класу методологій, орієнтованих на дані, і покликана дати проєктувальнику методичні вказівки в процесі трансляції специфікацій у концептуальну схему бази даних. Цей підхід ставить своєю метою встановити уніфіковану концептуальну модель з більш багатим семантичним значенням і використовувати концепцію абстракцій даних для спрощення проектування. Процес проектування розглядається як процес побудови моделі. Запропоновано методи конструювання концептуальної моделі, засновані на способах узагальнення/спеціалізації. Передбачається, що проєктант починає з визначення найбільше загальних природно виникаючих класів об'єктів і подій предметної галузі. Подальші деталі програмної системи вводяться послідовними ітераціями описом підкласів уже поданих класів і спеціалізації взаємодій у цих класах. Проте, ця галузь, що торкається взаємозв'язку між способами концептуального моделювання, поданням знань і механізмом абстрагування потребує подальших досліджень.

Основи методології проектування якісного спеціального програмного забезпечення автоматизованих інформаційних систем воєнного призначення. Вказаній методології присвячено багато наукових джерел, наприклад [5-9, 19-22] та інші. Базою методології створення якісного СПЗ є використання наступних етапів, на кожному з яких розроблення ведеться пошарово на обмеженому наборі допустимих структур.

I – етап проектування системних зв'язків (системна специфікація). Змістом цього етапу є тривимірна функціонально-подійно-режимна декомпозиція СПЗ на задачі. При цьому у доповнення до класичної функціональної декомпозиції здійснюється декомпозиція за принципом реакції на події з об'єкту та за режимами роботи системи.

II – етап виділення функціонального ядра кожної задачі. Особливістю такого виділення є забезпечення незалежності даної частини задачі від обраної операційної системи і обраного методу міжзадачного зв'язку за даними. При цьому всі функції зв'язку покладаються на частину задачі, що залишилася – інтерфейс. Задача-інтерфейс – основний об'єкт операційної системи, за допомогою якої здійснюється зв'язок функціональних ядер за управлінням та інформацією. Починаючи з даного етапу, розроблення ведеться за двома зустрічними напрямками: проектування ядер ведеться “згори донизу” (аналітичний підхід), остаточна інтеграція - збирання системи за допомогою інтерфейсів – “знизу вгору” (синтетичний підхід).

III – етап полягає в пошаровому модульному проектуванні, який є подальшою декомпозицією функціональних ядер.

IV – етап виражається деталізація модулів з використанням структурних примітивів структурного програмування.

Слід відзначити, що на першому етапі проектування здійснюється функціонально-подійно-режимна декомпозиція (ФПР-декомпозиція) СПЗ на задачі - виділення окремих задач, які реалізують певну часткову функцію системи управління, що виконується при виникненні конкретної події в одному з режимів роботи системи.

Оскільки будь-яка зміна ситуації у часі, що змінює поточний стан потоку управління в системі, називається подією, до початку декомпозиції необхідно мати ситуаційну модель – відображення множини ситуацій, які можуть виникнути на об'єкті, у множину зовнішніх подій для системи управління. Прикладом зовнішньої події є активізація ініціативної кнопки оператором системи. Режим розуміється як регламент роботи системи, що зберігає структуру управління. Введення системи в роботу, “програмний відступ” при виявленні непрацездатності елементів СПЗ, закінчення роботи відбуваються при переході з одного режиму на інший. Функція - сукупність дій СПЗ, спрямованих на досягнення певної мети (проведення розрахунків для отримання сукупності результатів).

Після розбиття СПЗ на задачі здійснюється опис вхідних та вихідних даних для кожної з отриманих задач, що реалізують певний режим.

Подання задачі z_j у вигляді двох наборів даних (вхідних $\{Ind\}$ і вихідних $\{Od\}$) дозволяє побудувати орієнтований граф інформаційних зв'язків між задачами системи L_I , в якому множина вершин графа збігається з множиною задач, а дуга, що зв'язує вершини z_i та z_j , існує тоді, коли

$$\{Od_i\} \cap \{Ind_j\} \neq \emptyset. \quad (1)$$

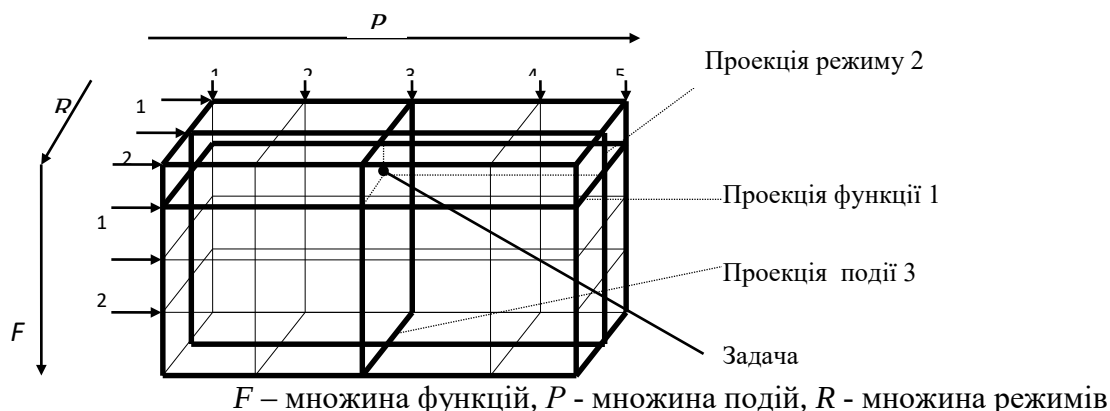


Рисунок 1 - Схема функціонально-подійно-режимної декомпозиції СПЗ на задачі

Наявність в інформаційному графі сильно зв'язаних компонент свідчить про нерозумну декомпозицію на першому етапі проектування. З точки зору ефективності організації обчислювального процесу більш раціональним є об'єднання задач, що утворюють сильно зв'язану компоненту, в одну задачу. Дана процедура відповідає розкладанню графа на максимально сильно зв'язані підграфи.

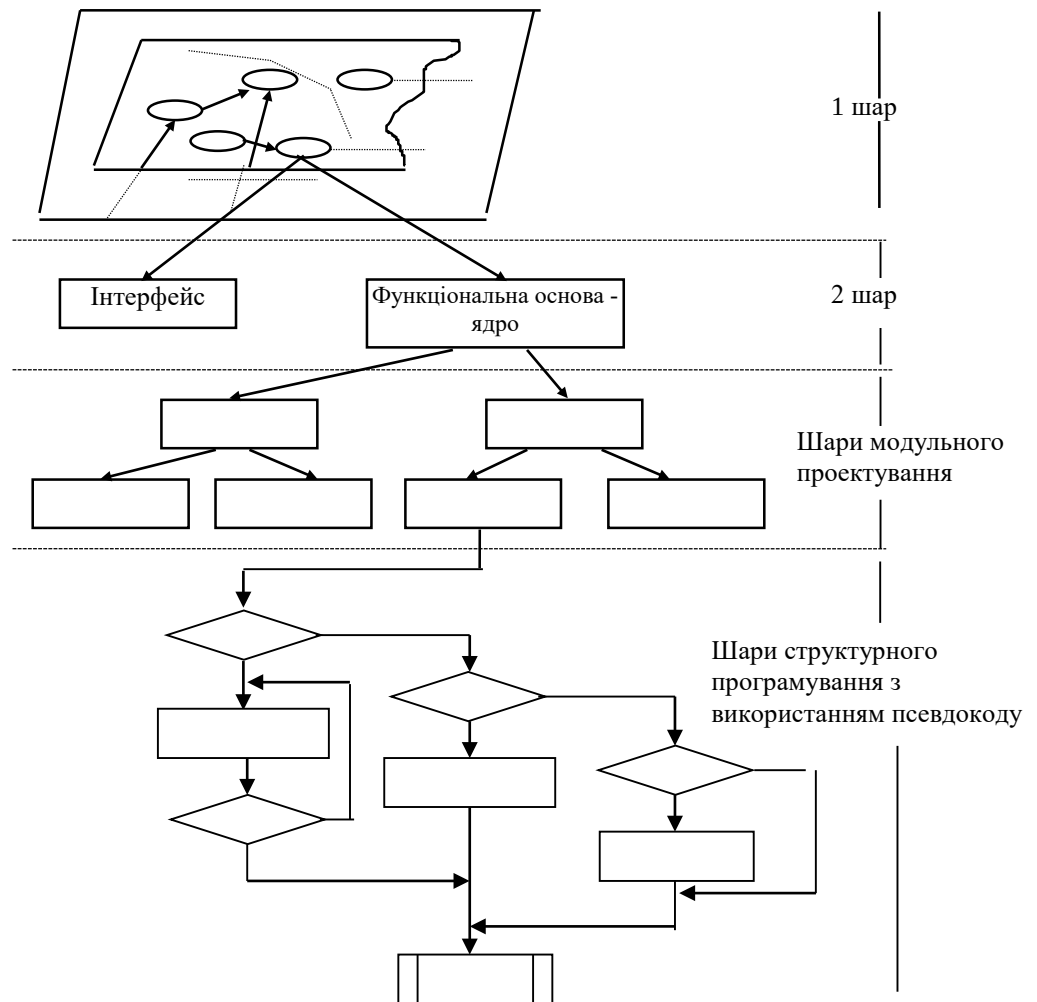


Рисунок 2 – Схема пошарового структурного проектування СПЗ для одного режиму

У графі управління, що буде отриманий з перетвореного графа інформаційних зв'язків, міжзадачних циклів не буде, а циклічність виконання окремих задач буде виражена петлею при вершині. На рис. 3 показано приклад перетворення графа та об'єднання задач. Задачі z_5, z_6, z_7 об'єднані в нову задачу Z_5' , z_{11}, z_{12}, z_{13} — в Z_6' , z_3, z_8, z_9 — в Z_3' .

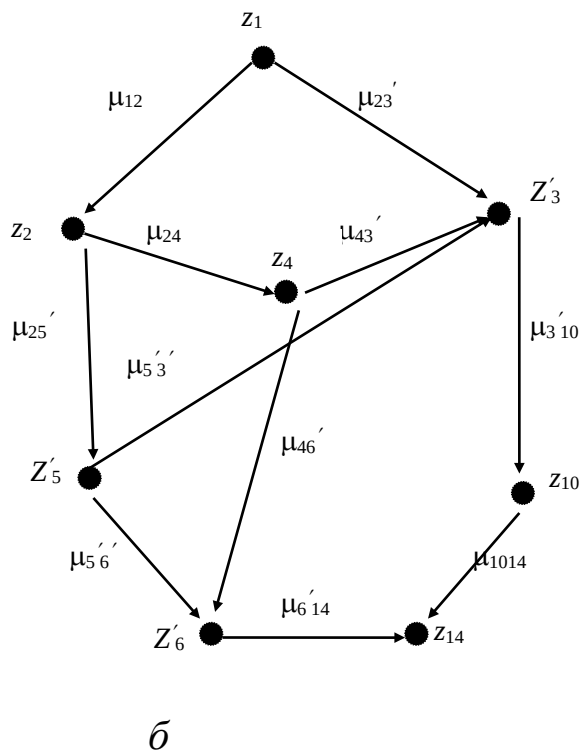
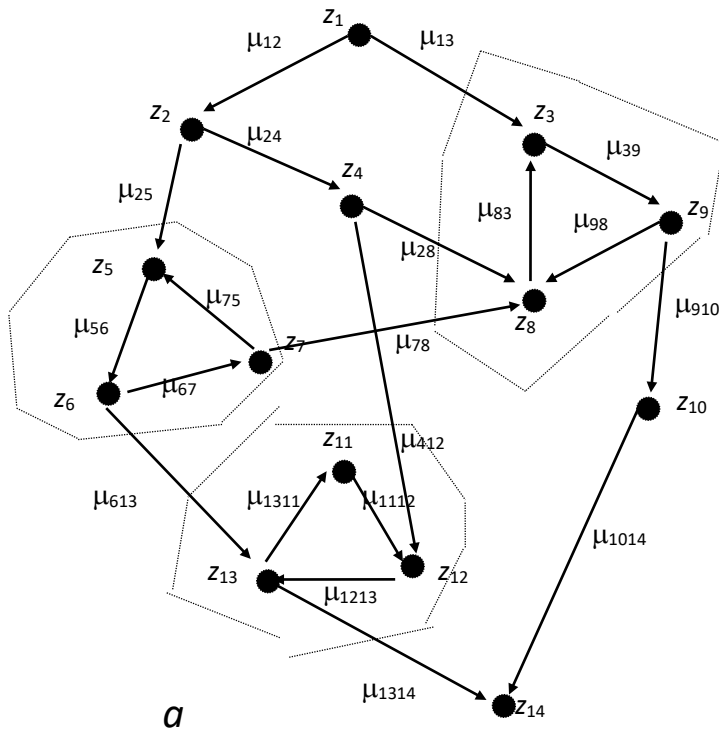


Рисунок 3 – Перетворення графа інформаційних зв'язків (об'єднання задач):
a – вихідний граф; *б* – перетворений граф

Етап модульного проектування по суті є етапом функціональної декомпозиції. Рівні абстракції або шари готового продукту на цьому етапі проектування набувають статус рівней модулів у створюваній програмі, відбиваючи майбутню ієрархію системи. До цього часу існують різночитання поняття модульності. У роботі прийнято визначення, згідно з яким модульним називається таке програмне забезпечення, в якому можна змінити будь-яку частину логічної структури, не викликаючи змін в інших частинах. Під модулем розуміється послідовність логічно зв'язаних фрагментів, які оформлені як окрема частина програми.

Визначальна властивість модуля - незалежність відносно логічної структури СПЗ, аргументів (параметрів) модуля, констант, тощо. Будемо розрізняти Ф-модулі (акції – функціональні дії), І-модулі (інтерфейси) і ОСД-модулі (операції над структурами даних). Введення ОСД-модулів пояснюється тим, що правильне використання структур даних грає дуже важливу роль при проектуванні та визначає ефективність СПЗ.

На конструкцію модуля накладаються такі обмеження:

модуль повинен мати один вхід і один вихід;

модуль не повинен змінювати команди іншого модуля;

модуль не повинен зберігати історію своїх викликів (хоча її наявність спрощує трасування при збоях роботи СПЗ);

в ідеалі кожний модуль повинен реалізувати одну функцію цілком.

Програми, які розроблені за модульним принципом, мають такі переваги:

легкі у складанні і налагодженні а, отже, в супроводі і модифікації;

існує можливість розподілу модулів для програмування між програмістами різної кваліфікації;

можливість створення бібліотек найбільш вживаних програм;

спрощення процедури завантаження в оперативну пам'ять великої задачі, яка вимагає сегментації;

можливість підвищення стійкості СПЗ за рахунок виникнення численних природних контрольних точок для спостереження за роботою програми.

Суттєві обмеження на глибину модульності програм накладає підвищення витрат обчислювальних ресурсів системи за часом роботи центрального процесора й обсягом пам'яті. Додаткові обмеження на реалізацію модульних програм полягають в наступному. Передачі управління між модулями відбуваються по вертикальних лініях, що з'єднують модулі у схемі ієрархії. Модуль, що активізує підлеглий модуль, отримує управління після завершення його роботи (зворотне не вірно — модуль більш низького рівня ієрархії не може викликати модуль більш високого рівня). Модуль завжди повертає управління тому модулю, що його викликав. Прийняття рішень модулями нижчого рівня за модулі вищого рівня не допускається. Надто велика кількість аргументів, що надаються модулю, тягне необхідність розподілу функцій. Пропонується обчислювати кількість модулів, виходячи з залежності $M=\eta/6$, де M — кількість модулів, η — кількість єдиних за змістом вхідних і вихідних параметрів, які включені в алгоритм. Дана залежність базується на припущенні, що кількість параметрів ідеального модуля дорівнює 6. Введення певних правил модульного проектування, опис їх у термінах формальної теорії дозволяє побудувати формальні моделі ієрархічних модульних структур і провести їх верифікацію.

Структурне програмування припускає використання певних принципів розроблення програм, яким відповідає набір жорстких правил для полегшення тестування, поліпшення читаності програм і підвищення продуктивності праці проектувальників. Методи структурного програмування базуються на відмові від використання оператора GO TO в явному вигляді і реалізації сукупності цілком певних структурованих операторів передачі управління (керуючих структур) у поєднанні з принципами спадного (зверху вниз) проектування.

Розрізняють декілька класів керуючих структур. Основний (базовий) клас утворюють D -структури, що являють собою програми, які складені з структурних примітивів з одним входом і одним виходом (оператори призначення, виклики процедур, оператори вводу-виводу, умовні конструкції форми IF P THEN S_1 ELSE S_2 , цикли форми WHILE P DO S). Наступний клас керуючих структур – D' -структури (оператори IF P THEN S з однією гілкою, цикли REPEAT S UNTIL P , оператори CASE з гілками).

Наступні класи являють собою узагальнення розглянутих вище структур, які пов'язані з наявністю багатьох входів і виходів.

Серед них є BJ_n -структури, що складені з основних дій, композицій, структур IF P THEN

S_1 ELSE S_2 і одновхідних-одновихідних структур Ω_k ($k \leq n$).

У Ω_k -структурі є k послідовних предикатів і дій з k виходами, по одному на кожний предикат.

Наступний клас складають RE_n , REC_n , DRE_n , $DREC_n$ -структури.

RE_n -структура включає основні дії, композиції, структури IF_THEN_ELSE, команди виходу форми EXIT(c) (c – позитивна ціла константа) і конструкції REPEAT_END.

REC_n -структура подібна RE_n -структурі з тією відзнакою, що у неї є додаткова команда формування циклу CYCLE(c).

DRE_n -структура являє собою сукупність RE_n -структури з доданням структур WHILE_DO.

$DREC_n$ -структури визначаються як DRE_n -структури з доданням операторів CYCLE(c).

У цілому RE_n -структурам і їх варіантам відповідають програми, в яких передача управління може здійснюватися тільки у початок або у кінець вкладеного циклу управління.

GP_n - і L -структури складають наступний клас структур. При цьому GP_n -структура – така структура, в якій всі підструктури з одним входом і одним виходом мають не більш n різноманітних предикатів. L -структура — будь-яка структура без обмежень на кількість або конфігурацію предикатів, дій і передач управління. Дана структура відповідає програмі з вільним використанням міток і операторів GO TO.

Основними результатами теорії структурного програмування є результати досліджень з теоретичної повноти D -структур [107] і результати щодо ієрархії структурних класів [106].

Сенс першого результату зводиться до того, що доведена можливість перетворення будь-якої L -структури у функціонально еквівалентну D -структуру, тобто для проектування програм достатньо D -структур (оператор GO TO виявляється теоретично непотрібним): послідовної композиції, IF_THEN_ELSE та WHILE_DO. При цьому L -структура може бути зведена до D -структури без введення нових булевих перемінних або зміни конкретних дій і предикатів програм тільки тоді, коли вона не містить циклів з двома роздільними виходами.

Другий результат показує, які структури і в якому ступені можуть бути зведені до інших (рис. 4). Безперервна спрямована вгору лінія на даному рисунку означає суворе зведення структур нижнього класу до структур верхнього класу (наприклад, клас C_1 зведений до класу C_2 , якщо кожна структура в C_1 може бути перетворена у структури з C_2 , але не навпаки). З'єднання штриховою лінією означає, що нижній клас зведений до верхнього, при цьому кожна структура нижнього класу може бути перетворена до структури верхнього, але не обов'язково навпаки. Еквівалентність класів ($C_1 \sim C_2$) означає, що кожна структура C_1 може бути перетворена в структуру C_2 і навпаки.

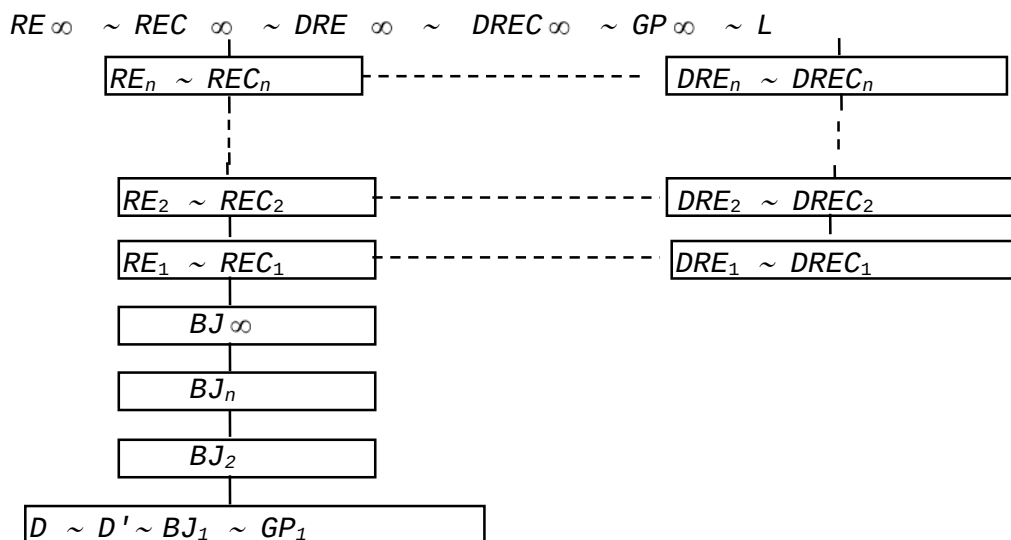


Рисунок 4 – Ієрархія класів управляючих структур

Аналіз практичного застосування структур при використанні принципів структурного програмування показує, що для потреб практики виявляється достатнім використання класів D і D' . Застосування більш високих структур суперечить принципу ясності. При цьому D' -структури часто виявляються більш корисними, ніж D -структури. Окрім основних переваг структурного програмування (ієрархічність, видимість, наочність, скорочення термінів проектування), його реалізація дозволяє ввести контроль правильності програм на рівні керуючих структур. Дотримання принципу незалежності (структури нижнього рівня не можуть користуватися інформацією про верхні рівні) дозволяє не тільки пошарово проектувати і модифікувати ППЗ, але й побудувати ієрархічну схему локалізації помилок: ситуація – система задач – задача – функціональне ядро – модуль – керуючі структури.

Для зменшення ймовірності виникнення помилок в СПЗ технологія проектування повинна бути прозорою, простою для супроводження та дозволяти ефективне управління розробкою. Крім того, вона повинна враховувати особливості предметної галузі, для якої розробляються програми.

З цією метою технологічний процес проектування може бути диференційований на ряд етапів-процедур. Ці процедури упорядковані та застосовуються у певній послідовності і дозволяють вести проектування крок за кроком. При цьому інформація, що отримується в результаті виконання певної процедури, є вхідною для наступних.

Висновки. В роботі проведено аналіз сучасних та традиційних методів проектування і виробництва військової техніки з використанням автоматизованих інформаційних систем.

Програмне забезпечення АІС має характерні ознаки складної системи і підпорядковується законам науки про складні системи. Сучасний етап розвитку складних інформаційних систем характеризується тим, що тенденція до різкого збільшення складності завдань управління все в більшому ступені виявляється в об'ємності програмного забезпечення систем управління технічними об'єктами, технологічними процесами і виробництвами. Обсяг опрацьованої інформації в системах цього типу зростає більш інтенсивно, чим збільшення обсягів самого виробництва, або підвищення його техніко-економічних показників.

Базою методології створення якісного СПЗ є використання етапів, на кожному з яких розроблення ведеться пошарово на обмеженому наборі допустимих структур.

Перший етап – етап проектування системних зв'язків (системна специфікація). Змістом цього етапу є тривимірна функціонально-подійно-режимна декомпозиція СПЗ на задачі. При цьому у доповнення до класичної функціональної декомпозиції здійснюється декомпозиція за принципом реакції на події з об'єкту та за режимами роботи системи.

Другий етап – виділення функціонального ядра кожної задачі. Особливістю такого виділення є забезпечення незалежності даної частини задачі від обраної операційної системи і обраного методу міжзадачного зв'язку за даними. При цьому всі функції зв'язку покладаються на частину задачі, що залишилася - інтерфейс. Задача-інтерфейс - основний об'єкт операційної системи, за допомогою якої здійснюється зв'язок функціональних ядер за управлінням та інформацією. Починаючи з даного етапу, розроблення ведеться за двома зустрічними напрямками: проектування ядер ведеться “згори донизу” (аналітичний підхід), остаточна інтеграція - збирання системи за допомогою інтерфейсів - “знизу вгору” (синтетичний підхід).

Третій етап полягає в пошаровому модульному проектуванні, який є подальшою декомпозицією функціональних ядер.

На четвертому етапі виробляється деталізація модулів з використанням структурних примітивів структурного програмування.

Таким чином, концептуальна єдність підходів, що використані на етапах отримання системних специфікацій, проектування модульної структури та реалізації модулів, дозволила об'єднати прийняття окремих рішень в єдину методику проектування коректного спеціального програмного забезпечення, основними відмінностями якої є:

пошаровість, яка досягається використанням принципу абстрагування (ієрархії); об'єднання процесу проектування з процесом моделювання, що досягається застосуванням графових моделей, які отримуються в процесі проектування, та можливістю використання кожного рівня ієрархії в якості моделі СПЗ;

безперервність процесу проектування, яка забезпечується сумісністю моделей, які отримуються на різних етапах, участю системного програміста в розробці з начального етапу і можливістю початку кодування з першого етапу.

З метою виявлення та діагностування помилок при передачі управління між структурними елементами системи за допомогою "методу паролів" найбільша ефективність застосування паролів досягається їх рівномірним розподілом по всіх шарах СПЗ.

Метод "тестових інтерфейсів" дозволяє удосконалити процес проектування програмного забезпечення за рахунок застосування діагностичної системи контролю за цілісністю програм.

Тестування є одним з найважливіших методів контролю якості СПЗ, і практично єдиним з них, що може бути доступним кінцевим користувачам. Жоден з інших відомих методів, жодна будь-яка їх комбінація не можуть повністю замінити тестування, оскільки тільки метод тестування дозволяє отримати оцінки якості СПЗ по коду що виконується.

ЛІТЕРАТУРА:

1. Основы инженерии качества программных систем / Ф.И. Андон, Г.И. Коваль, Г.М. Коротун, В.Ю. Суслов: НАНУ, Институт программных систем. – К.: Академперіодика, 2002, 504 с.
2. Де Марко Т., Листер Т. Человеческий фактор. Успешные проекты и команды. – М.: Символ-Плюс, 2012, 288 с.
3. Інформаційні технології. Оцінювання процесів життєвого циклу програмних засобів. – Офіційне видання. – К.: Держспоживачстандарт, 2001, (Національний стандарт України).
4. Толубко В.Б., Сбітнев А.І., Пермьков О.Ю., Методологічні основи проектування прикладного забезпечення до АСУ воєнного призначення. Монографія. – К.: НАОУ 2004 р. 248 с.
5. Гришак О.М. Проектування спеціального програмного забезпечення авто-матизованих інформаційних систем (аналітичний огляд)// Комп'ютерні інформаційні технології та системи. Вісник ЧДТУ. Черкаси - 2008. №2 - 075 с. 3-5
6. Ленков С.В., Гришак О.М., Жиров Г.Б., Пампуха І.В. Оцінка "практичності" та "коректності" спеціального програмного забезпечення автоматизованих інформаційних систем воєнного призначення // Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2022. - №74. – С.83 – 89. DOI: 10.17721/2519-481X/2022/74-09.
7. Ленков С.В., Селюков О.В., Гусак Ю.А., Пампуха І.В., Солодєєва Л.В. Оцінка "здатності до супроводу" та "здатності до переміщення" спеціального програмного забезпечення автоматизованих інформаційних систем воєнного призначення // Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2022. - №75. – С. 23 – 30. DOI: 10.17721/2519-481X/2022/75-04.
8. Ленков С.В., Бойченко О.В. Оцінка вірогідності даних автоматизованої системи управління // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2014. – № 45. – С. 46 – 51.
9. Ленков С.В., Джулій В.М., Муляр І.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи // Журна «Сучасна спеціальна техніка», м.Київ, 2016. – 2(45). – С.59 – 67.
10. Турский В. Методология проектирования программ. - М.: Мир, 1981. -265с.;
11. Lehman M. Programs, Life Cycle and Laws of Software Evolution// Proc. of IEEE. - 1980. - Vol. 68. - pp. 26-46.
12. Йодан Э. Структурное проектирование и конструирование программ. - М.: Мир, 1979. -415с.
13. Миллс Х. Программирование больших систем по принципу "сверху-вниз"// Средства отладки больших систем. - М.:Статистика. - 1977.
14. Wirth N. Program Development by Step-Wise Refinement//Comm. ACM. - 1971. - Vol. 14. - pp. 221-229.

15. Фуксман А.Л. Технологические аспекты создания программных систем. - М.: Статистика, 1979. - 184с.
16. Jakson M.A. Principles of Program Design. - N.Y.: Academic Press. - 1975. - p.238.
17. Liskov B.H. A Design Methodology for Reliable Software Systems // Fall Joint Computer Conf., AFIPS. – 1972. – Vol. 41. – P. 191-199.
18. В.А. Кашканова, А.А. Кашканова, Б.П. Кукец Інформаційні системи і технології на автомобільному транспорті: Навчальний посібник. – Вінниця: ВНТУ, 2020-104с.
19. Семчак О.М., Богданова О.Г. Проблеми та перспективи розвитку автоматизованих систем управління цілевказання // Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2024. - №82. – С. 94 – 102. DOI: [DOI:https://doi.org/10.17721/2519-481X/2024/82-11](https://doi.org/10.17721/2519-481X/2024/82-11).
20. Кацалап В.О., Омелянчук А.В., Сивак О.В. Обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України // Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2027. - №77. – С. 45 – 100. DOI: <https://doi.org/10.17721/2519-481X/2022/77-04>.
21. Фесьоха В.В., Нерознак Є.І., Сова О.Я. Удосконалена модель оптимального використання серверних ресурсів кластерної системи військового призначення на основі рівноваги неша // Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2023. - №79. – С. 159 – 171. DOI: <https://doi.org/10.17721/2519-481X/2023/79-15>.
22. Khlaponin Y.I., Qasim N. H., Tarasiuk D.M.// Збірник наукових праць Військового інституту Київського університету імені Тараса Шевченка. – Київ, - 2023. - №80. – С. 91 – 97. DOI: <http://doi.org/10.17721/2519-481X/2023/80-10>.

REFERENCES:

1. Osnovy inzhenerii kachestva programnykh system / F.I. Andon, H.I. Koval, H.M. Korotun, V.Yu. Suslov: NANU, Instytut prohrannykh system. – K.: Akademperiodyka, 2002, 504 s.
2. De Marko T., Lister T. Chelovecheskiy faktor. Uspeshnye proekty i komandy. – M.: Simvol-Plyus, 2012, 288 s.
3. Informatsiyni tekhnolohiyi. Otsinyuvannya protsesiv zhyttyevoho tsykladu prohrannykh zasobiv. – Ofitsiine vydannya. – K.: Derzhspozhyvachstandart, 2001, (Natsionalnyy standart Ukrayiny).
4. Tolubko V.B., Sbitniev A.I., Permyakov O.Yu., Metodolohichni osnovy proektuvannya prykladnoho zabezpechennya do ASU voyennoho pryznachennya. Monohrafiya. – K.: NAOU 2004 r. 248 s.
5. Hryshchak O.M. Proektuvannya spetsialnoho prohrannoho zabezpechennya avtomatyzovanykh informatsiynykh system (analychnyy ohlyad)// Komp'yuterni informatsiyni tekhnolohiyi ta systemy. Visnyk ChDTU. Cherkasy - 2008. №2 - 075 s. 3-5.
6. Lenkov S.V., Hryshchak O.M., Zhyrov H.B., Pampukha I.V. Otsinka “praktychnosti” ta “korektnosti” spetsialnoho prohrannoho zabezpechennya avtomatyzovanykh informatsiynykh system voyennoho pryznachennya // Zbirnyk naukovykh prats Viys'kovoho instytutu Kyivskoho universytetu imeni Tarasa Shevchenka. – Kyiv, - 2022. - №74. – S.83 – 89. DOI: [10.17721/2519-481X/2022/74-09](https://doi.org/10.17721/2519-481X/2022/74-09).
7. Lenkov S.V., Selyukov O.V., Husak Yu.A., Pampukha I.V., Solodyeyeva L.V. Otsinka “zdatnosti do suprovodu” ta “zdatnosti do peremishchennya” spetsialnoho prohrannoho zabezpechennya avtomatyzovanykh informatsiynykh system voyennoho pryznachennya // Zbirnyk naukovykh prats Viys'kovoho instytutu Kyivskoho universytetu imeni Tarasa Shevchenka. – Kyiv, - 2022. - №75. – S. 23 – 30. DOI: [10.17721/2519-481X/2022/75-04](https://doi.org/10.17721/2519-481X/2022/75-04).
8. Lenkov S.V., Boychenko O.V. Otsinka virohidnosti danykh avtomatyzovanoyi systemy upravlinnya // Zbirnyk naukovykh prats Viys'kovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K., 2014. – № 45. – S. 46 – 51.
9. Lenkov S.V., Dzhuliy V.M., Mulyar I.V. Dynamichni pokaznyky otsinky rivnya funktsionalnoyi bezpeky informatsiynykh system.
10. Turskiy V. Metodolohiya proektyrovaniya prohrann. - M.: Myr, 1981. -265s.
11. Lehman M. Programs, Life Cycle and Laws of Software Evolution// Proc. of IEEE. - 1980. - Vol. 68. - pp. 26-46.
12. Yodan Э. Strukturnoe proektyrovanye y konstruyrovanye prohrann. - M.: Myr, 1979. -415s.
13. Mylls X. Prohrannyrovanye bolshykh system po pryntsypu "sverkhu-vnyz"// Sredstva otladky bolshykh system. - M.:Statystyka. - 1977.

14. Wirth N. Program Development by Step-Wise Refinement//Comm. ACM. - 1971. - Vol. 14. - pp. 221-229.
15. Fuksman A.L. Tekhnolohycheskye aspekty sozdaniya prohrammnykh system. - M.: Statystyka, 1979. - 184s.
16. Jakson M.A. Principles of Program Design. - N.Y.: Academic Press. - 1975. - p.238.
17. Liskov B.H. A Design Methodology for Reliable Software Systems // Fall Joint Computer Conf., AFIPS. – 1972. – Vol. 41. – R. 191-199.
18. V.A. Kashkanova, A.A. Kashkanova, B.P. Kukets Informatsiini systemy i tekhnolohii na avtomobilnomu transporti: Navchalnyi posibnyk. – Vinnytsia: VNTU, 2020-104s.
19. Semchak O.M., Bohdanova O.H. Problemy ta perspektyvy rozvytku avtomatyzovanykh system upravlinnia tsilevkazannia // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho universytetu imeni Tarasa Shevchenka. – Kyiv, - 2024. - №82. – S. 94 – 102. DOI: <https://doi.org/10.17721/2519-481X/2024/82-11>.
20. Katsalap V.O., Omelianchuk A.V., Syvak O.V. Obhruntuvannia pokaznykiv vidmovostiikosti avtomatyzovanoi systemy upravlinnia tsentru operatyvnoho kerivnytstva Zbroinykh Syl Ukrainy // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho universytetu imeni Tarasa Shevchenka. – Kyiv, - 2027. - №77. – S. 45 – 100. DOI: <https://doi.org/10.17721/2519-481X/2022/77-04>.
21. Fesokha V.V., Neroznak Ye.I., Sova O.Ia. Udoshkonalena model optymalnoho vykorystannia servernykh resursiv klasternoi systemy viiskovoho pryznachennia na osnovi rivnovahy nesha // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho universytetu imeni Tarasa Shevchenka. – Kyiv, - 2023. - №79. – S. 159 – 171. DOI: <https://doi.org/10.17721/2519-481X/2023/79-15>.
22. Khlaponin Y.I., Qasim N. H., Tarasiuk D.M.// Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho universytetu imeni Tarasa Shevchenka. – Kyiv, - 2023. - №80. – S. 91 – 97. DOI: <http://doi.org/10.17721/2519-481X/2023/80-10>.

ANALYSIS OF MODERN AND TRADITIONAL METHODS OF DESIGNING AND MANUFACTURING MILITARY EQUIPMENT USING AUTOMATED INFORMATION SYSTEMS

In the article, the authors perform one type of analysis of existing and prospective methods of designing and manufacturing military equipment using automated information systems. It is known that AIS software has the characteristic features of a complex system and is subject to the laws of complex systems science. The current stage of development of complex information systems is characterized by a sharp increase in the complexity of management tasks, which is increasingly reflected in the volume of software for managing technical objects, technological processes, and production. The work classifies programs according to SPE, which represents “a model of another model within the theory of abstract representation of individual objects.” It can be classified into one of three classes: S-class - these are programs whose functions are formally defined by specifications and follow from them. The correspondence between input and output is decisive, and any change creates a new program. P-class - these are programs whose solution acceptability is assessed by comparison with the real situation, meaning that programs of this class must constantly change depending on the environment, data refinement, etc. E-class programs themselves become part of the implementation of the situation they model, meaning they are even more prone to changes than P-programs.

The main phases of the AIS life cycle are considered, and their features are defined: definition, design, implementation, deployment, and operation.

The conceptual unity of approaches used at the stages of obtaining system specifications, designing the modular structure, and implementing modules allowed for the integration of individual decisions into a single methodology for designing correct special software, the main differences of which are: layering achieved through the use of the abstraction principle (hierarchy); combining the design process with the modeling process achieved through the application of graph models obtained during design, and the possibility of using each level of the hierarchy as a model of the special software; continuity of the design process ensured by the compatibility of models obtained at different stages, the participation of the system programmer from the initial stage, and the possibility of starting coding from the first stage.

Keywords: automated information systems, technical object management systems, conceptual unity of approaches, continuity of the design process.

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ СТРУКТУРОВАНИХ АНАЛІТИЧНИХ МЕТОДІВ У РОЗВІДУВАЛЬНІЙ ІНФОРМАЦІЙНІЙ РОБОТІ

Структуровані аналітичні методи – невід’ємний складові для всіх спеціалістів аналітичної діяльності, які прагнуть впроваджувати прозорість, науковість у свої повсякденні аналітичні роботи, надавати обґрунтування для прийняття розвідувальних рішень та уникати сюрпризів. Добрий аналіз та передбачення означають, що нам постійно потрібно ставити під сумнів себе. Ці дослідження доводять нам, як це робити в структурований та систематичний спосіб. Вони легкі у використанні, орієнтовані на практику та переконують навіть скептиків у необхідності застосування структурованих технологій. Структуровані аналітичні методи, дослідження яких пропонується в роботі, стимулюють уяву, підвищують вимогливість та застосовуються до вирішення складних розвідувальних проблем, а також інших областей, які вимагають суттєвого аналізу. Це нове, розширене дослідження та обов’язковий ресурс для щоденного використання будь-яким серйозним аналітиком які займаються розвідувальною діяльністю. В роботі відмічено, що незважаючи на те, як інтенсивно вивчалася та критикувалася розвідувальна інформаційна робота, мало уваги традиційно приділялося аналізу розвідувальної діяльності. Більшість оцінок зазвичай зосереджуються на таких питаннях, як таємні зарубіжні операції та прихована діяльність, можливо, тому, що вони легше узгоджуються з популярними уявленнями про світ розвідки, але аналіз, можливо, ніколи не був більш важливою частиною професії або не потрібний розвідникам. У порівнянні з біполярною динамікою холодної війни, у цьому новому світі наближається загроза від недорозвинених держав, розповсюдження небезпек, регіональних криз, зростаючих сил і небезпечних недержавних акторів. Звичайно, існують цінні таємниці, які має розкрити розвідка – речі, які можна знати та відкрити. Але цей світ також багатий на таємниці, пов’язані з майбутнім напрямком подій та намірами ключових акторів. Такі речі малоймовірно освітлюються за допомогою одного лише шматка секретної розвідувальної інформації; це обов’язково теми для аналізу.

Ключові слова: структурний аналіз, аналітичні методи, ресурс, розвідувальна діяльність, таємні операції, біполярна динаміка, держава.

Вступ. Сучасний досвід проведення розвідувальної інформаційної роботи показує, що для ефективного та швидкого впровадження структурованого аналізу потрібно крок-за-кроком відображати мислення індивідуального аналітика так, щоб це було легко зрозуміло іншим, тим самим дозволяючи його обмінювати, розвивати та критикувати іншими. При сполученні з інтуїтивним судженням фахівців у галузі, такий структурований та прозорий процес може значно зменшити ризик аналітичної помилки. Наш поточний високотехнологічний глобальний оточуючий світ все більше потребує співпраці між аналітиками з різними областями експертизи та різними організаційними перспективами. Структуровані аналітичні методи ідеально підходять для такої взаємодії. Кожен крок у методиці спонукає до відповідної дискусії, і, як правило, це генерує більше розбіжної інформації та більше нових ідей, ніж будь-який неструктурований груповий процес [1]. Процес структурованих аналітичних методів організовує взаємодію між аналітиками у невеликій аналітичній групі чи команді таким чином, щоб уникнути множинних пасток та помилок, які часто погіршують ефективність роботи групи чи команди. Структурований аналіз є механізмом, за допомогою якого внутрішні

процеси відображаються зовні в систематичний та прозорий спосіб, щоб їх можна було спільно використовувати, розвивати та легко критикувати іншими. Кожна техніка залишає слід, за яким інші аналітики та керівники можуть слідкувати, щоб побачити основи аналітичного судження. Ці техніки використовуються індивідуальними аналітиками, але, можливо, найкраще застосовуються у командних або групових зусиллях, у яких кожен етап аналітичного процесу відкриває учасникам різноманітні або протилежні перспективи. Ця прозорість допомагає забезпечити, що різниці у поглядах серед аналітиків будуть вислухані та серйозно враховані на початковому етапі аналітичного процесу. Аналітики повідомляють нам, що це одна з найцінніших переваг будь-якої структурованої техніки. Структурований аналіз допомагає аналітикам забезпечити, що їх аналітична основа – фундамент, на якому вони формують свої аналітичні судження, – максимально надійний. Допомагаючи розкрити конкретну аналітичну проблему на її складові частини та вказати крок за кроком процес обробки цих частин, структуровані аналітичні техніки допомагають організувати аморфну масу даних, з якою повинні боротися більшість аналітиків. Такі техніки роблять наше мислення більш відкритим та доступним для оцінювання та критики як самими аналітиками, так і іншими учасниками процесу. Ця прозорість сприяє ефективній комунікації на робочому рівні, що є важливим для співпраці військовослужбовців, які займаються розвідувальною діяльністю [2].

Аналіз останніх досліджень. Аналіз публікацій в області структурованих аналітичних методів розвідувально-інформаційної роботи, викладено у багатьох літературних джерелах [1-3]. Питання інформаційно-аналітичної діяльності розглядається у таких публікаціях як: Варенко В. М. Інформаційно-аналітична діяльність: навчальний посібник; Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова AJP-2.1 (видання В, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с. Але, на думку вчених сучасна техніка без спеціального програмного забезпечення не здатна задовольнити постійно зростаючі потреби підвищення ефективності розвідувальної діяльності. На думку військових вчених шлях вирішення даної проблеми є утворення спеціальних автоматизованих інформаційних систем (AIC). В залежності від предметної галузі, вони можуть дуже відрізнятися між собою за функціями, архітектурою, реалізацією. Структуровані аналітичні техніки для аналізу розвідки від Хойера та Ферсона стали класикою в розвідувальній літературі. Вже стандартний підручник у безлічі університетів та урядових агентств по всьому світу, друге видання буде продовжувати бути обов'язковою літературою для поточних та майбутніх аналітиків розвідки Данії. Її техніки викладаються у Копенгагенському університеті, а книга представляє собою основну літературу для вправ з симуляції аналізу, у яких студенти-магістри факультету політичних наук вправляються в мистецтві та науці аналізу розвідки під керівництвом старших аналітиків урядових розвідувальних структур. Існує багато літератури щодо когнітивних упереджень, Робота Річарда Хьюера для ЦРУ в кінці 1970-х та 1980-х років, а пізніше його книга «Психологія аналізу розвідки», вперше опублікована у 1999 році, застосовували уявлення Тверські та Канемана до проблем, з якими стикалися аналітики розвідки. З моменту публікації «Психології аналізу розвідки» інші автори, пов'язані з Розвідувальною спільнотою США (включаючи Джеффри Купера та Роба Джонстона), визначили когнітивні упередження як основну причину аналітичних невдач у ЦРУ.

Мета статті. Провести дослідження структурованого аналізу його механізмів, за допомогою яких внутрішні процеси розвідувальної інформаційної роботи відображаються зовні в систематичний та прозорий спосіб, щоб їх можна було спільно використовувати, розвивати та легко критикувати іншими. Кожна техніка залишає слід, за яким інші аналітики та керівники можуть слідкувати, щоб побачити основи структурованого аналітичного судження.

Виклад основного матеріалу. Протягом останніх двадцяти років були зроблені важливі досягнення в психологічних дослідженнях щодо людського судження. Теорія подвійного процесу використовувалась як переважний підхід, передбачаючи дві системи прийняття рішень, які називаються Системою 1 та Системою 2. Основне відмінності між Системою 1 та Системою 2 полягає у інтуїтивному та аналітичному мисленні. Система 1 є інтуїтивною, швидкою, ефективною і часто несвідомою. Вона природно використовує наявні знання, минулі досвіди і часто довгострокову ментальну модель того, як люди або речі працюють в конкретному середовищі. Мислення Системи 1 дуже спокусливе, оскільки воно потребує мало зусиль, і дозволяє людям швидко і ефективно вирішувати проблеми та приймати рішення. Часто воно точне, але інтуїтивне мислення також є поширеним джерелом когнітивних упереджень та інших інтуїтивних помилок, які призводять до неправильного аналізу. Мислення Системи 2 є аналітичним [3]. Це повільне, обдумане, свідоме мислення. До нього входять всі види аналізу, такі як критичне мислення та структуровані аналітичні техніки, а також весь спектр емпіричних та кількісних методів. Структуровані аналітичні техніки, як тип аналітичної техніки, допомагає протистояти одному чи кільком типам когнітивних упереджень та інших поширених інтуїтивних помилок, пов'язаних з мисленням Системи 1. Існує багато типів упереджень, всі з яких можна розглядати як когнітивні упередження, оскільки вони усі формуються та виявляються через діяльність Системи 1 у мозку. Потенційні причини упереджень включають професійний досвід, що призводить до засвоєння аналітичної ментальності, навчання або освіти, характер виховання, тип особистості, видимий особистий досвід або особистий інтерес у певному рішенні. Усі упередження, крім, можливо, особистого упередження до особистих інтересів, є результатом швидкого, несвідомого та інтуїтивного мислення (Система 1), а не результатом обдуманого міркування (Система 2). Мислення Системи 1 зазвичай правильне, але часто впливають на аналіз та прийняття рішень в багатьох галузях, таких як психологія, політологія, медицина, економіка, бізнес та освіта, починаючи з моменту, коли Амос Тверські та Даніель Канеман вперше ввели концепцію когнітивних упереджень на початку 1970-х років. У роботі Річарда Хьюера «Психологію аналізу розвідки», детально описано багато упереджень, які впливають на розвідувальний аналіз. З тих пір сотні когнітивних упереджень були описані у науковій літературі за допомогою різних термінів. Як зауважив Хьюер багато років тому: «Когнітивні упередження подібні до оптичних ілюзій у тому, що помилка залишається переконливою навіть тоді, коли особа повністю усвідомлює її природу. Саме усвідомлення упередження не породжує більш точне сприйняття» Тому когнітивні упередження дуже важко подолати. Наприклад, Емілі Пронін, Деніел І. Лін та Лі Росс виявили у трьох різних дослідженнях, що люди більше помічають існування та функціонування когнітивних та мотиваційних упереджень у інших, ніж у самих себе. Це пояснює, чому так багато аналітиків вважають, що їх власне інтуїтивне мислення (Система 1) є достатнім. Існує багато літератури щодо когнітивних упереджень, іноді називаних «евристиками», яка пояснює, як вони впливають на мислення людини у багатьох галузях. Кожна з п'ятдесяти п'яти структурованих аналітичних технік, надає дороговказ для уникнення одного або декількох конкретних когнітивних упереджень, а також інших поширених інтуїтивних пасток [4].

Структуровані аналітичні техніки є техніками деупередження. Вони не замінюють інтуїтивне судження. Їх роль полягає в тому, щоб піддавати сумнівам інтуїтивні судження, ідентифікуючи більший спектр варіантів для розгляду аналітиками. Наприклад, ключові припущення. Перевірка передбачає ідентифікацію та розгляд додаткових припущень. Аналіз конкуруючих гіпотез передбачає ідентифікацію альтернативних гіпотез, акцент на спростуванні, а не підтвердженні гіпотези, та більш систематичний аналіз доказів. Усі структуровані техніки, описані у цій книзі, мають розділ «Додаткова вартість», що описує, як ця техніка сприяє поліпшенню аналізу та допомагає зменшити когнітивні упередження та

інтуїтивні пастки, часто роблені розвідниками та пов'язані з мисленням Системи 1. Для багатьох технік користь є очевидною. Жодна з них не претендує на завжди бути правильною відповіддю. Вони ідентифікують альтернативи, які заслуговують на серйозний розгляд. Звичайна критика структурованих аналітичних технік полягає в тому, що «у мене немає достатньо часу, щоб їх використовувати». Досвід багатьох аналітиків показує, що ця критика не має підстав. Багато технік забирають дуже мало часу. Будь-яка нова річ потребує часу на вивчення; але, дуже засвоєна, використання структурованих аналітичних технік заощаджує час аналітиків. Це може допомогти індивідуальним аналітикам працювати більш ефективно, особливо на початку проекту, коли аналітик може інакше трохи блукати, намагаючись зрозуміти, як продовжувати дослідження. Структуровані техніки полегшують групові процеси, покращуючи комунікацію, а також полегшують збір та інтерпретацію доказів. І, в кінцевому підсумку, структурована техніка створює продукт, в якому міркування за висновками є більш прозорим і більш легко приймається, ніж той, який отримано за допомогою інших методів. Це заощаджує час, швидко відзначаючи його рецензентами та редакторами, та тим самим стискаючи процес координації. Аналітичні методи є важливими, але сам метод далекий від того, щоб гарантувати аналітичну точність або значення. Метод повинен бути поєднаний з субстантивною експертизою та допитливим та уявним розумом. І ці, у свою чергу, повинні підтримуватися і стимулюватися організаційним середовищем, в якому виконується аналіз [5].

Сучасне бачення майбутнього аналізу розвідки взаємодіє з баченням Директора Національної розвідки «Візія 2015», в якій аналіз розвідки все більше стає спільним підприємством, зі зміною акценту «від координації проектних продуктів до регулярного обговорення даних та гіпотез на ранніх етапах дослідження». Це є великою зміною по відношенню до традиційного концепту розвідувального аналізу як переважно індивідуальної діяльності, а координацію як останній етап процесу [6].

У спільному підприємстві структуровані аналітичні техніки є процесом, через який відбувається співпраця. Так само, як ці техніки надають структуру нашим індивідуальним розумовим процесам, вони також можуть структурувати взаємодію аналітиків у малій команді або групі. Оскільки розумовий процес у цих техніках є прозорим, кожний крок у техніці спонукає до обговорення в команді. Таке обговорення може генерувати та оцінювати значно більше різноманітної і нової інформації, ніж група, яка не використовує структурований процес. Коли команда має справу з складною проблемою, синергія кількох розумів, які використовують структурований аналіз, зазвичай є ефективнішою, ніж думка одного аналітика [7]. Структуровані аналітичні техніки, коли вони поєднуються з програмним забезпеченням, також можуть надати каркас для керування міжагентурною співпрацею та координацією, з'єднуючи членів команди в різних офісах, агентствах, частинах перенасичених транспортними пробками мегаполісів, навіть по всьому світу. Командний аналіз, звичайно, може приносити новий набір викликів, еквівалентний когнітивним упередженням та іншим пасткам, з якими зіштовхується індивідуальний аналітик [8]. Однак відомі проблеми групового процесу мінімізуються за допомогою структурованих технік, які керують взаємодією між учасниками команди або групи. Це допомагає уникнути відхилень від обговорення та полегшує викликання альтернативних точок зору всіма членами команди. Аналітики також виявили, що використання структурованого процесу допомагає використовувати аргументи без прив'язки до особистостей в разі розбіжностей у поглядах. Крім того, сьогодині технології та програми соціального обміну даними роблять структуровану співпрацю набагато простішою, ніж коли-небудь раніше. Коли у 2000 році була створена Шерманська школа з аналізу розвідки в ЦРУ для покращення ефективності аналізу розвідки, Джон МакЛлофлін, тодішній заступник директора з розвідки, доручив школі об'єднати техніки, що тоді називалося «альтернативним аналізом». У відповідь на завдання МакЛлофліна, Школа Кента розробила компіляцію технік, і Директорат розвідки ЦРУ почав викладати ці

техніки на курсі, який пізніше перетворився на Семінар з передових аналітичних інструментів та технік. Пізніше курс був розширений, щоб включити аналітиків з Агентства розвідки оборони та інших складових Розвідувальної спільноти США [9]. Різноманітні комісії щодо розслідувань, які були створені після несподіваних терористичних атак 11 вересня 2001 року, а потім помилкового аналізу щодо наявності у Іраку зброї масового знищення, збільшили тиск на проведення більш альтернативних підходів до аналізу розвідки. Наприклад, Закон про реформу розвідки 2004 року поклав на Директора Національної розвідки «відповідальність за забезпечення того, що, відповідно, елементи розвідувальної спільноти проводять альтернативний аналіз інформації та висновків у аналізі розвідки» [10]. Проте з часом аналітики, які неправильно сприйняли або протистояли цьому підходу, почали розуміти альтернативний аналіз просто як альтернативу звичайному способу ведення аналізу, що вказує на те, що ці альтернативні процедури потрібні лише винятково у виняткових обставинах, коли аналіз є критично важливим. Інструктори Школи Кента повинні були пояснити, що ці техніки не є альтернативою традиційному аналізу, але є центральними для хорошого аналізу і повинні бути інтегровані в звичайну робочу рутину – вдосконалюючи суворість і структуру в повсякденну роботу аналітиків. У 2004 році, коли Школа Кента вирішила оновити свої навчальні матеріали на основі отриманих у попередні кілька років уроків та опублікувати *«Основи майстерності»*, Рендольф Х. Ферсон та Роджер З. Джордж були серед авторів [11].

«Існувало враження, що назва «альтернативний аналіз» є занадто обмеженою і не достатньо описовою. Принаймні десяток різних аналітичних технік були об'єднані в один термін, тому було вирішено знайти назву, яка була б більш всеохоплюючою та відповідала б цьому широкому спектру підходів до аналізу.» Кеті Ферсон отримує заслугу за виникнення терміну «структуровані аналітичні техніки» під час розмови за обіднім столом зі своїм чоловіком, Ренді. Роджер Джордж організував техніки у три категорії: діагностичні техніки, контр аргументаційні техніки та техніки уяви. Термін «структуровані аналітичні техніки» став офіційним у червні 2005 року, коли оновлені навчальні матеріали були офіційно затверджені.

Вище керівництво Директорату розвідки стало сильним прихильником структурованих аналітичних технік і вжило активні заходи для полегшення та просування цього підходу. Термін зараз використовується в усій Розвідувальній спільноті США – і все більше в академії та багатьох розвідувальних службах по всьому світу [12].

Висновки та напрямки подальших досліджень. Таким чином, в результаті дослідження можливостей структурованих аналітичних методів у розвідувальній аналітичній роботі визначено роль та обсяг структурованих аналітичних технік як окремої аналітичної методології, яка забезпечує крок за кроком процес роботи з неповними, двозначними та іноді обманливими даними, з якими аналітикам доводиться працювати. Структурований аналіз є механізмом, за допомогою якого внутрішні розумові процеси відображаються зовні в систематичний та прозорий спосіб, щоб їх можна було спільно використовувати, розвивати та легко критикувати іншими. Кожна техніка залишає слід, за яким інші аналітики та керівники можуть слідкувати, щоб побачити основи аналітичного судження. Ці техніки використовуються індивідуальними аналітиками, але, можливо, найкраще застосовуються у командних або групових зусиллях, у яких кожен етап аналітичного процесу відкриває учасникам різноманітні або протилежні перспективи. Ця прозорість допомагає забезпечити, що різниці у поглядах серед аналітиків будуть вислухані та серйозно враховані на початковому етапі аналітичного процесу. Аналітики повідомляють нам, що це одна з найцінніших переваг будь-якої структурованої техніки.

Структурований аналіз допомагає аналітикам визначити, що їх аналітична основа – фундамент, на якому вони формують свої аналітичні судження, – максимально надійний. Допомагаючи розкрити конкретну аналітичну проблему на її складові частини та вказати крок за кроком процес обробки цих частин, структуровані аналітичні техніки допомагають організувати аморфну масу даних, з якою повинні боротися більшість аналітиків. Такі техніки

роблять наше мислення більш відкритим та доступним для оцінювання та критики як самими аналітиками, так і іншими учасниками процесу. Ця прозорість сприяє ефективній комунікації на робочому рівні, що є важливим для співпраці як всередині офісу, так і між установами. Ці методи називаються «техніками», оскільки вони зазвичай спрямовані на надання аналітику можливості думати про проблему, а не надати йому остаточну відповідь, як це можна було б очікувати від методу. Однак загалом структуровані аналітичні техніки складають методологію – набір принципів і процедур для якісного аналізу тих видів невизначеностей, з якими зустрічаються багато аналітиків щоденно. Треба відмітити, що у подальших дослідженнях структуровані аналітичні методи, можуть використовуватися незалежно або в поєднанні з іншими методами. З метою зручності уявлення, необхідно розподілили методи на групи, або області, в залежності від переважного фокусу та призначення кожного методу. Структуровані аналітичні методи є важливою частиною процесу, за допомогою якого інформація ділиться, і аналітики з різних підрозділів часто співпрацюють під час виконання спільних завдань. Існує базовий набір методів та навичок критичного мислення, які команди або групи співпраці регулярно використовують на початку більшості проектів для створення спільного фундаменту для їхньої комунікації та спільної роботи.

ЛІТЕРАТУРА:

1. Війна в Україні: розвідка Британії розкрила ключовий у найближчий час фактор. <https://www.unian.ua/war/viy-na-rosiji-proti-ukrajini>
2. Ненсі Діксон «Проблема і виправлення уроків, вивчених агентствами розвідки США», 2009 р., <http://www.nancydixonblog.com/2009/07/the-problem-and-the-fix-for-the-us-intelligence-agencies-lessons-learned.html>.
3. bintel.org.ua/nukma/rozviduvalnij-proces-nato/
4. <https://www.nato.int/docu/review>
5. Левченко О. В., Вінник В. В., Устименко О. В. Розвідка та іноземні армії. Інформаційна робота : навчальний посібник / — Київ: «КНТ», 2022. — 124 с.
6. Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення. – К. : Міністерство оборони України, 2015. – 26 с.
7. Варенко В. М. Інформаційно-аналітична діяльність : навчальний посібник. – К. : Університет «Україна», 2014. – 417 с.
8. Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова АJP–2.1 (видання В, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с.
9. Основи розвідувально-інформаційної діяльності: настанова Штабу розвідки Міністерства оборони Великобританії. – К. : ГУР МО України, 2015.– 51 с.
10. [/defpol.org.ua/index.php/produkt-y-tsentru/49-shliakh-ukrainy-do-nato/1084](http://defpol.org.ua/index.php/produkt-y-tsentru/49-shliakh-ukrainy-do-nato/1084)
11. "Ситуація бентежна": у ГУР назвали єдиний безпечний варіант для росіян в Криму. Анжеліка Байбак 17:29, 27 вересня 2023 р. https://24tv.ua/chornomorskiy-flot-sevastopoli-vibuhi-rozvidtsi-dali-poradu-rosiyanam_n2400724
12. Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). – К. : ГУР МО України, 2018. – 118 с.

REFERENCES:

1. The war in Ukraine: British intelligence revealed a key factor in the near future. <https://www.unian.ua/war/viy-na-rosiji-proti-ukrajini>
2. Nancy Dixon, The Problem and Fix Lessons Learned by US Intelligence Agencies, 2009, <http://www.nancydixonblog.com/2009/07/the-problem-and-the-fix-for-the-us-intelligence-agencies-lessons-learned.html>.
3. bintel.org.ua/nukma/rozviduvalnij-proces-nato/

4. <https://www.nato.int/docu/review>
5. Levchenko O. V., Vinnyk V. V., Ustymenko O. V. Intelligence and foreign armies. Information work: study guide / — Kyiv: "KNT", 2022. — 124 p.
6. Military standard 01.101.004. Edition 2. Military intelligence. Intelligence and information activities. Terms and definitions. - K.: Ministry of Defense of Ukraine, 2015. - 26 p.
7. Varenko V. M. Information and analytical activity: study guide. - K.: "Ukraine" University, 2014. - 417 p.
8. Intelligence activity processes. NATO standard. Allied Joint Instruction AJP-2.1 (edition B, version 1)/ NATO Standardization Office, 2016. – 80 p.
9. Basics of intelligence and information activities: instruction of the Intelligence Staff of the Ministry of Defense of Great Britain. – K.: GUR Ministry of Defense of Ukraine, 2015. – 51 p.
10. /defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084
11. "The situation is embarrassing": the GUR named the only safe option for Russians in Crimea. Anzhelika Baibak 17:29, September 27, 2023 https://24tv.ua/chornomorskiy-flot-sevastopoli-vibuhi-rozvidtsi-dali-poradu-rosiyanam_n2400724
12. Methodological recommendations for the development of intelligence assessments (according to the standards of leading NATO member countries). - K.: GUR Ministry of Defense of Ukraine, 2018. - 118 p.

**Ph.D. Maksimenko Yu.A., Ph.D., Mamich V.V.,
Ph.D. Didyk V.O., Sharshatkin D.Y., Korol D. A.**

RESEARCH OF THE POSSIBILITIES OF STRUCTURED ANALYTICAL METHODS IN INTELLIGENCE INFORMATION WORK

Structured analytical methods are an integral component for all analytical specialists who seek to introduce transparency, scientificity into their daily analytical work, provide justification for making intelligence decisions and avoid surprises. Good analysis and foresight means that we constantly need to question ourselves. These studies show us how to do this in a structured and systematic way. They are easy to use, practice-oriented and convince even skeptics of the need to use structured technologies. The structured analytical methods explored in the work stimulate the imagination, raise the level of demandingness, and are applied to solving complex intelligence problems, as well as other areas that require significant analysis. This is a new, expanded study and a must-have resource for daily use by any serious intelligence analyst. The work noted that despite the intensive study and criticism of intelligence information work, little attention was traditionally paid to the analysis of intelligence activities. Most assessments tend to focus on issues such as covert foreign operations and covert activities, perhaps because they align more easily with popular perceptions of the intelligence world, but analysis has perhaps never been a more important part of the profession or needed by intelligence officers. Compared to the bipolar dynamics of the Cold War, in this new world the threat of underdeveloped states, spreading dangers, regional crises, rising powers and dangerous non-state actors is looming. Of course, there are valuable secrets to be discovered by intelligence - things to know and discover. But this world is also rich with mysteries related to the future course of events and the intentions of key actors. Such things are unlikely to be illuminated by a single piece of classified intelligence; these are necessarily topics for analysis.

Key words: structural analysis, analytical methods, resource, intelligence activity, covert operations, bipolar dynamics, state.

МЕТОДИКА ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ SIEM-СИСТЕМОЮ В БАЗАХ ДАНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В умовах інтеграції інформаційно-комунікаційних систем у процеси військової діяльності, питання їх кіберзахисту стає все більш актуальнішим. Основною ціллю для кібератак є бази даних, що переважно містять конфіденційну інформацію. Одним із найефективніших підходів до забезпечення кіберзахисту баз даних інформаційно-комунікаційних систем військового призначення є використання інтелектуальних можливостей SIEM-системи. SIEM дозволяє в режимі реального часу здійснювати моніторинг, аналіз та реагування на потенційні кіберінциденти. У статті запропоновано методику виявлення кіберінцидентів SIEM-системою у базах даних інформаційно-комунікаційних систем військового призначення. Основний акцент зроблено на багаторівневому захисті баз даних, який включає захист на рівні операційної системи, рівні бази даних та системи керування базами даних, а також мережевому рівні захисту. З метою підвищення ефективності виявлення кіберінцидентів на рівні аналізу даних SIEM-системи застосовується удосконалена методика на основі апарату нечіткої логіки. Удосконалення методики досягається шляхом введення ваг антецедентів у нечітких правилах, що дозволяє, у деяких випадках, точніше ідентифікувати кіберінциденти у порівнянні з існуючими моделями та методами. Безпосередньо ваги антецедентів нечітких правил визначаються за допомогою методу парних порівнянь на основі рангових оцінок, здійснених за 9-бальною шкалою Сааті. Представлено алгоритм прийняття рішень щодо ідентифікації кіберінцидентів, який базується на аналізі нечітких правил та ваг їх антецедентів. Наведено приклад розрахунку ваг антецедентів нечітких правил використовуючи метод парних порівнянь на основі рангових оцінок.

Ключові слова: база даних, інформаційно-комунікаційна система, кіберзахист, кіберінцидент, кібербезпека, кібератака, SIEM-система, теорія нечітких множин, нечіткі правила, метод парних порівнянь.

Вступ. У сучасному цифровому світі інформаційно-комунікаційні системи військового призначення (ІКСВП) знаходяться під постійним загрозливим тиском від кібератак, які можуть призвести до порушення безпеки проведення військових операцій, розголошення конфіденційної інформації та завдання збитків військовій інфраструктурі [1-4]. Кіберпростір став не лише ареною для інформаційної війни, але й стратегічним полем битви, де навіть одна успішна кібератака може мати серйозні наслідки. Від протидії кібератакам залежить ефективність виконання військових операцій, захист конфіденційної інформації, а також безпека особового складу та працездатність обладнання інформаційно-комунікаційної системи. Тому розвиток та застосування ефективних засобів виявлення та реагування на кіберінциденти стає невідкладною необхідністю для будь-якої країни чи військової організації.

Одним з основних структурних елементів будь-якої ІКСВП є база даних (БД), яка виконує важливі функції зберігання, організації та доступу до інформації, необхідної для функціонування системи [5]. У ІКСВП БД можуть містити різноманітну інформацію, включаючи дані про військову діяльність, плани, обладнання, персонал, розташування військових об'єктів та інші дані, необхідні для прийняття оперативних рішень та забезпечення безпеки [6]. Оскільки БД зберігає великий обсяг критичних даних, забезпечення безпеки їх стає надзвичайно пріоритетною задачею.

Найбільш ефективним рішенням в контексті кіберзахисту БД ІКСВП є використання системи управління інформацією та подіями безпеки (SIEM-системи) [7, 8]. SIEM-система забезпечує комплексний підхід до кіберзахисту, поєднуючи в собі моніторинг, аналіз та

реагування на потенційні кіберзагрози в реальному часі. Її засоби дозволяють виявляти аномальність у поведінці користувачів та систем, а також аналізувати великі обсяги даних для виявлення підозрілих подій.

У БД ІКСВП, де конфіденційність та цілісність даних є критичними, SIEM-системи виявляються особливо корисними. Вони дозволяють відслідковувати доступ до конфіденційної інформації, виявляти спроби несанкціонованого доступу та інші, а також забезпечувати швидке реагування на кіберінциденти.

Однак, важливо зауважити, що процеси обробки та аналізу даних у SIEM-системах не є завжди досконалими. Незважаючи на те, що ці системи здатні виявляти багато типів кіберінцидентів, вони можуть пропускати нові, наприклад, раніше не відомі типи кібератак, а також є ризик виникнення надмірної генерації сповіщень про потенційні кіберінциденти, що може призвести до ігнорування реально небезпечних подій. Тому процес постійного покращення і оптимізації процесів аналізу та реагування на кіберінциденти у SIEM-системах є важливим та актуальним.

Використання новітніх технологій штучного інтелекту, машинного навчання, обробки великих обсягів даних, а також постійне вдосконалення кореляційних алгоритмів їхнього аналізу може забезпечити більш точне виявлення кіберінцидентів SIEM-системою, що покращить кіберзахист БД ІКСВП у цілому.

Аналіз останніх досліджень. У публікації [9] запропоновано архітектуру інтелектуальної SIEM-системи для виявлення кіберінцидентів у БД ІКСВП. Вона складається з наступних рівнів: рівень збору даних, рівень управління даними, рівень аналізу даних і рівень прийняття та реалізації рішень. Рівень аналізу даних є головним і критичним елементом архітектури [10]. Він забезпечує можливість ефективного виявлення та реагування на кіберінциденти у реальному часі.

У наукових публікаціях процесам аналізу даних у SIEM-системах приділяється велика увага. Це пояснюється тим, що ефективність SIEM-систем безпосередньо залежить від якості цих процесів. Вдосконалення моделей та методів аналізу є постійним процесом, який потребує інноваційних підходів та адаптації до нових кіберзагроз.

У [11] зроблено акцент на важливості впровадження та удосконалення технологій SIEM-систем для підвищення рівня захисту ІКС. Проведено огляд методів кореляції, які можуть бути впроваджені в SIEM-системах для більш ефективного аналізу та протидії кіберінцидентам.

Публікація [12] присвячена використанню моделей машинного та глибокого навчання для виявлення мережових кібератак, з акцентом на ефективність різних класифікаторів та їх здатність виявляти різні типи кіберінцидентів на основі набору даних UNSW-NB15.

Робота [13] присвячена оптимізації інфраструктури SIEM-системи за допомогою кореляційно-регресійного аналізу подій. Представлено, зменшення кількості помилкових спрацьовувань і підвищення здатності SIEM-системи виявляти кіберінциденти за рахунок покращення нормалізації журналів подій та ефективного використання правил кореляції.

Таким чином, аналіз сучасних досліджень та публікації щодо кореляції та аналізу подій безпеки в SIEM-системах, вказує значний прогрес у цій області. Однак, постійний розвиток кібератак, вимагає подальшого вдосконалення моделей і методів кіберзахисту ІКСВП. Це підкреслює важливість даної роботи для сфери кібербезпеки, зокрема для ефективного виявлення нових типів кібератак/кіберінцидентів SIEM-системами.

Метою роботи є розробка методики виявлення кіберінцидентів SIEM-системою, пов'язаних з БД інформаційно-комунікаційних систем військового призначення.

Виклад основного матеріалу. Для досягнення поставленої мети, доцільно застосувати підхід, який представлено у [14, 15]. Суть даного підходу полягає у введенні вагових коефіцієнтів для антецедентів нечітких лінгвістичних правил, що описують кіберінциденти у базі знань, які можуть виникнути під час функціонування ІКСВП. Ці коефіцієнти є числами з інтервалу $[0, 1]$, відображають значимість ознак кіберінциденту у системі нечіткого логічного виводу.

Отже, задача виявлення кіберінцидентів у БД ІКСВП матиме наступний вигляд (1):

$$F_l^* = (f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*) \rightarrow c_j \in C = (c_1, c_2, \dots, c_m) \quad (1)$$

де F_l^* – множина ознак кіберінциденту, пов'язаному з функціонуванням БД ІКСВП, отриманих з різних рівнів кіберзахисту БД [12].

Область зміни ознак кіберінцидентів $f_{il} \in [\underline{f_{il}}, \overline{f_{il}}]$, $i = 1 \dots n$, $l = 1 \dots L$, які отримуються з різних рівнів кіберзахисту БД $l = 1 \dots L$ і вихідного значення ідентифікації $c_j \in [\underline{c_j}, \overline{c_j}]$, $j = 1 \dots m$.

Відповідно $\underline{f_{il}}$, $\overline{f_{il}}$ – нижнє (верхнє) значення ознак кіберінциденту f_{il} , l -го рівня кіберзахисту БД, $i = 1 \dots n$, $l = 1 \dots L$; $\underline{c_j}$, $\overline{c_j}$ – нижнє (верхнє) значення результату ідентифікації c_j .

Для вирішення задачі, вхідні і вихідні змінні розглядаються, як лінгвістичні змінні, що задані на універсальних множинах (2) [16, 17]:

$$f_{il} = [\underline{f_{il}}, \overline{f_{il}}], c_j = [\underline{c_j}, \overline{c_j}] \quad (2)$$

Для оцінки (3) доцільно використовувати якісні терми, які входять до множин термів:

$A_{il} = \{a_{il}^1, a_{il}^2, \dots, a_{il}^k\}$ – терм-множина змінної f_{il} , де a_{il}^k – k -й лінгвістичний терм змінної f_{il} , $k = 1 \dots k_i$, $i = 1 \dots n$ l -го рівня кіберзахисту БД $l = 1 \dots L$;

$\Delta = \{\delta_1, \delta_2, \dots, \delta_m\}$ – терм-множина змінної c_j , де δ_j , $j = 1 \dots m$ – лінгвістичний терм змінної c_j , m – число можливих класів кіберінцидентів, пов'язаних з БД.

Таким чином, лінгвістичні терми $a_{il}^k \in A_{il}$, $k = 1 \dots k_i$, $i = 1 \dots n$, $l = 1 \dots L$ та $\delta_j \in \Delta$, $j = 1 \dots m$ можна розглядати як нечіткі множини, які задані на універсальних множинах f_{il} , c_j .

Експертні дані можуть бути представлені у вигляді багатовимірної матриці знань про кіберінциденти (табл.1).

Таблиця 1

Багатовимірна таблиця ознак кіберінцидентів у БД ІКСВП і класів, що їм відповідають з урахуванням ваги антецедентів у межах окремих правил

Номер вхідної комбінації значень	Ознаки кіберінцидентів, отримані з різних рівнів кіберзахисту БД										Клас кіберінциденту
	f_{1l}	Ω_{1l}	f_{2l}	Ω_{2l}	...	f_{il}	Ω_{il}	...	f_{nl}	Ω_{nl}	c
11	α_{1l}^{11}	Ω_{1l}^{11}	α_{2l}^{11}	Ω_{2l}^{11}	...	α_{il}^{11}	Ω_{il}^{11}	...	α_{nl}^{11}	Ω_{nl}^{11}	δ_1
12	α_{1l}^{12}	Ω_{1l}^{12}	α_{2l}^{12}	Ω_{2l}^{12}	...	α_{il}^{12}	Ω_{il}^{12}	...	α_{nl}^{12}	Ω_{nl}^{12}	
...	...	...	...	...	...	...	...	...	...	...	
$1k_1$	$\alpha_{1l}^{1k_1}$	$\Omega_{1l}^{1k_1}$	$\alpha_{2l}^{1k_2}$	$\Omega_{2l}^{1k_2}$	...	$\alpha_{il}^{1k_1}$	$\Omega_{il}^{1k_1}$	...	$\alpha_{nl}^{1k_1}$	$\Omega_{nl}^{1k_1}$	
...	...	...	...	...	...	...	...	...	...	...	...
$j1$	α_{1l}^{j1}	Ω_{1l}^{j1}	α_{2l}^{j1}	Ω_{2l}^{j1}	...	α_{il}^{j1}	Ω_{il}^{j1}	...	α_{nl}^{j1}	Ω_{nl}^{j1}	δ_j
$j2$	α_{1l}^{j2}	Ω_{1l}^{j2}	α_{2l}^{j2}	Ω_{2l}^{j2}	...	α_{il}^{j2}	Ω_{il}^{j2}	...	α_{nl}^{j2}	Ω_{nl}^{j2}	
...	...	...	...	...	...	...	...	...	...	...	
jk_j	$\alpha_{1l}^{jk_j}$	$\Omega_{1l}^{jk_j}$	$\alpha_{2l}^{jk_j}$	$\Omega_{2l}^{jk_j}$	...	$\alpha_{il}^{jk_j}$	$\Omega_{il}^{jk_j}$	...	$\alpha_{nl}^{jk_j}$	$\Omega_{nl}^{jk_j}$	
...	...	...	...	...	...	...	...	...	...	...	...
m_1	α_{1l}^{m1}	Ω_{1l}^{m1}	α_{2l}^{m1}	Ω_{2l}^{m1}	...	α_{il}^{m1}	Ω_{il}^{m1}	...	α_{nl}^{m1}	Ω_{nl}^{m1}	δ_m
m_2	α_{1l}^{m2}	Ω_{1l}^{m2}	α_{2l}^{m2}	Ω_{2l}^{m2}	...	α_{il}^{m2}	Ω_{il}^{m2}	...	α_{nl}^{m2}	Ω_{nl}^{m2}	
...	...	...	...	...	...	...	...	...	...	...	
mk_m	$\alpha_{1l}^{mk_m}$	$\Omega_{1l}^{mk_m}$	$\alpha_{2l}^{mk_m}$	$\Omega_{2l}^{mk_m}$	...	$\alpha_{il}^{mk_m}$	$\Omega_{il}^{mk_m}$	...	$\alpha_{nl}^{mk_m}$	$\Omega_{nl}^{mk_m}$	

Тоді, з врахуванням ваг ознак кіберінцидентів у БД ІКСВП, нечітка база знань, яка представлена сукупністю нечітких правил “ЯКЩО-ТО”, що зв’язують лінгвістичні оцінки ознак кіберінцидентів з результатами їхньої ідентифікації, прийме наступний вигляд [14, 15]:

$$\begin{aligned}
 & \text{ЯКЩО } (f_{il} = \alpha_{1l}^{11} \text{ з вагою } \Omega_{1l}^{11}) \text{ ТА } (f_{2l} = \alpha_{2l}^{11} \text{ з вагою } \Omega_{2l}^{11}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{11} \text{ з вагою } \Omega_{nl}^{11}) \text{ АБО} \\
 & (f_{il} = \alpha_{1l}^{12} \text{ з вагою } \Omega_{1l}^{12}) \text{ ТА } (f_{2l} = \alpha_{2l}^{12} \text{ з вагою } \Omega_{2l}^{12}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{12} \text{ з вагою } \Omega_{nl}^{12}) \text{ АБО} \\
 & (f_{il} = \alpha_{1l}^{1k_1} \text{ з вагою } \Omega_{1l}^{1k_1}) \text{ ТА } (f_{2l} = \alpha_{2l}^{1k_1} \text{ з вагою } \Omega_{2l}^{1k_1}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{1k_1} \text{ з вагою } \Omega_{nl}^{1k_1}) \\
 & \text{ТО } (c=\delta_1), \dots \\
 & \dots, \text{ЯКЩО } (f_{il} = \alpha_{1l}^{j1} \text{ з вагою } \Omega_{1l}^{j1}) \text{ ТА } (f_{2l} = \alpha_{2l}^{j1} \text{ з вагою } \Omega_{2l}^{j1}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{j1} \text{ з вагою } \Omega_{nl}^{j1}) \text{ АБО} \\
 & (f_{il} = \alpha_{1l}^{j2} \text{ з вагою } \Omega_{1l}^{j2}) \text{ ТА } (f_{2l} = \alpha_{2l}^{j2} \text{ з вагою } \Omega_{2l}^{j2}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{j2} \text{ з вагою } \Omega_{nl}^{j2}) \text{ АБО} \\
 & (f_{il} = \alpha_{1l}^{jk_j} \text{ з вагою } \Omega_{1l}^{jk_j}) \text{ ТА } (f_{2l} = \alpha_{2l}^{jk_j} \text{ з вагою } \Omega_{2l}^{jk_j}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{jk_j} \text{ з вагою } \Omega_{nl}^{jk_j}) \\
 & \text{ТО } (c=\delta_j), \dots \\
 & \dots, \text{ЯКЩО } (f_{il} = \alpha_{1l}^{m1} \text{ з вагою } \Omega_{1l}^{m1}) \text{ ТА } (f_{2l} = \alpha_{2l}^{m1} \text{ з вагою } \Omega_{2l}^{m1}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{m1} \text{ з вагою } \Omega_{nl}^{m1}) \text{ АБО} \\
 & (f_{il} = \alpha_{1l}^{m2} \text{ з вагою } \Omega_{1l}^{m2}) \text{ ТА } (f_{2l} = \alpha_{2l}^{m2} \text{ з вагою } \Omega_{2l}^{m2}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{m2} \text{ з вагою } \Omega_{nl}^{m2}) \text{ АБО} \\
 & (f_{il} = \alpha_{1l}^{mk_m} \text{ з вагою } \Omega_{1l}^{mk_m}) \text{ ТА } (f_{2l} = \alpha_{2l}^{mk_m} \text{ з вагою } \Omega_{2l}^{mk_m}) \text{ ТА...ТА } (f_{nl} = \alpha_{nl}^{mk_m} \text{ з вагою } \Omega_{nl}^{mk_m}) \\
 & \text{ТО } (c=\delta_m), \tag{3}
 \end{aligned}$$

де α_{il}^{jk} - лінгвістична оцінка ознаки кіберінциденту у БД ІКСВП $f_{il}, i = 1 \dots n ; l=1 \dots L$ у рядку k j -ої диз’юнкції, що визначається на терм-множині $A_i = \{\alpha_{il}^1, \alpha_{il}^2, \dots, \alpha_{il}^{k_i}\}$;

$\delta_j \in \Delta, j = 1 \dots m$ - лінгвістична оцінка класу кіберінциденту у БД ІКСВП, що визначається на терм-множині $\Delta = \{\delta_1, \delta_2, \dots, \delta_m\}$,

Ω_{nl}^{mk} - вага ознак кіберінцидентів у межах правил.

З урахуванням вагових коефіцієнтів антецедентів у межах нечітких правил, нечітка база знань (3), може бути представленою модифікованою системою нечітких рівнянь (4) наступним чином:

$$\mu^{\delta_j}(f_{1l}, f_{2l}, \dots, f_{nl}) = V_{k=1}^{k_j} \left\{ \bigwedge_{i=1}^n \left[\mu^{\alpha_{il}^{jk}}(f_{il}) \Omega_{il}^{jk} \right] \right\}, j = 1 \dots m \tag{4}$$

Шляхом заміни операцій $\wedge$ та $\vee$ на операції $\min$ та $\max$, які їм відповідають, модифікована модель нечіткої ідентифікації кіберінцидентів SIEM-системами [13] із зваженими антецедентами нечітких правил прийме наступний вигляд:

$$\mu^{\delta_j}(f_{1l}, f_{2l}, \dots, f_{nl}) = \max_{k=1, k_j} \left\{ \min_{i=1, n} \left\{ \mu^{\alpha_{il}^{jk}}(f_{il}) \Omega_{il}^{jk} \right\}, j = \overline{1, m} \right\}. \tag{5}$$

Дана модель є основою для розробки правило-орієнтованого методу виявлення кіберінцидентів, пов’язаних з БД SIEM-системи із врахуванням ознак кіберінцидентів, отриманих з різних рівнів кіберзахисту БД ІКСВП.

Графічно задачу ідентифікації кіберінцидентів можна представити наступним чином (рис.1):



Рисунок 1 – Графічна інтерпретація задачі ідентифікації кіберінцидентів в БД ІКСВП

Основними труднощами, які виникають під час вирішення наведеної задачі є:

1. Обробка та аналіз великих обсягів даних є дуже ресурсомісткою і потребує значної обчислювальної потужності. Відповідно до цього, для виявлення кіберінцидентів у великих масивах даних необхідно застосовувати методи і алгоритмів, здатні швидко обробляти накопичену інформацію.
2. Дані про події у системі містять велику кількість неструктурованих або нерелевантних даних, що ускладнює ідентифікацію дійсно важливих подій.
3. Дані можуть надходити з різних джерел, які мають різні формати та структури. Об'єднання та кореляція таких даних може бути складним завданням.
4. Відомості про кіберінциденти можуть бути неповними або фрагментованими. Відсутність достатньої кількості ознак може ускладнити ідентифікацію і кореляцію подій.
5. Налаштування та тренування моделей машинного навчання потребує значних ресурсів і знань. Постійна адаптація моделей до нових загроз є необхідною, що може бути складним процесом.

Наведене підтверджує доцільність створення у складі SIEM-системи інтелектуальної підсистеми підтримки прийняття рішень, в основу функціонування якої має бути покладена модель ідентифікації кіберінцидентів на основі нечітких правил та нечіткого логічного виводу.

При цьому, для її розробки необхідно враховувати лінгвістичний характер типу кіберінциденту (вихідна змінна) та його ознак (вхідні змінні). У свою чергу, причинно-наслідкові зв'язки між кіберінцидентом та його ознаками повинні бути описані експертом зрозумілою мовою, а після цього, формалізовані у вигляді множини нечітких логічних правил.

Слід зауважити, що при великій кількості ознак кіберінцидентів, доцільно побудувати дерево логічного виводу, яке визначає порядок вкладення висловлювань одне в одне [16, 17].

На рис. 2 наведено дерево логічного виводу для нечіткого кореляційного правила: якщо на одному сервері баз даних з тією самою IP-адресою відбулося п'ять спроб доступу до різних таблиць, які завершилися невдало протягом п'яти хвилин, при цьому використовувалися різні ідентифікатори користувачів БД, а також було здійснено успішний доступ до будь-якої таблиці з тієї ж самої IP-адреси протягом цього часу, то ця подія повинна бути розглянута офіцером з безпеки.

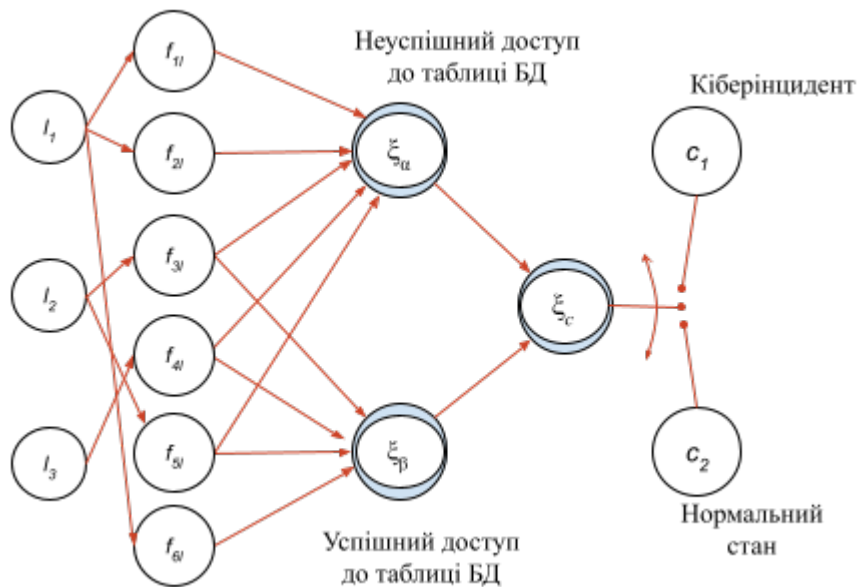


Рисунок 2 - Дерево логічного виводу для нечіткого кореляційного правила

У даному прикладі рівні кіберзахисту БД відтворено через $l_1 \div l_3$ (табл. 2), а ознаки кіберінциденту БД через $f_{11} \div f_{61}$ (табл. 3).

Таблиця 2

Рівні кіберзахисту БД

Рівень	Зміст рівня
l_1	Рівень БД та СКБД
l_2	Рівень ОС
l_3	Рівень мережі

Таблиця 3

Ознаки кіберінциденту БД відповідно її рівнів захисту

Ознака	Рівні кіберзахисту БД	Зміст ознаки	Тип
f_{11}	l_1	Кількість невдалих спроб доступу до таблиць	Числовий
f_{21}	l_1	Кількість ідентифікаторів користувачів БД	Числовий
f_{31}	l_2	Тривалість за часом спроб входу до системи	Числовий
f_{41}	l_3	Кількість IP-адрес, що задіяні під час доступу до таблиць	Числовий
f_{51}	l_2	Кількість серверів баз даних, що задіяні під час доступу до таблиць	Числовий
f_{61}	l_1	Кількість вдалих спроб доступу до таблиць	Числовий

Відповідно, через c_1 та c_2 позначено тип події, що відбувається у БД ІКСВП (табл. 4)

Таблиця 4

Ознаки кіберінциденту БД ІКСВП

Подія	Зміст події
α	Неуспішний доступ до таблиці БД
β	Успішний доступ до таблиці БД
c_1	Кіберінцидент
c_2	Нормальний стан системи

Структура дерева логічного виводу відповідає відношенням (6) – (8):

$$c = \xi_c(\alpha, \beta), \quad (6)$$

$$\alpha = \xi_\alpha(f_{1l}, f_{2l}, f_{3l}, f_{4l}, f_{5l}), \quad (7)$$

$$\beta = \xi_\beta(f_{3l}, f_{4l}, f_{5l}, f_{6l}). \quad (8)$$

Таблиця 5

Багатовимірна матриця знань про кіберінциденти

Ознака	Значення	Тип	Кіберінцидент
		α	
f _{1l}	В	В	C ₁
f _{2l}	В		
f _{3l}	Н		
f _{4l}	Н		
f _{5l}	вС		
Ознака	Значення	β	
f _{3l}	нС	В	
f _{4l}	Н		
f _{5l}	В		
f _{6l}	Н		
Ознака	Значення	α	C ₁
f _{1l}	вС	вС	
f _{2l}	вС		
f _{3l}	нС		
f _{4l}	Н		
f _{5l}	С		
Ознака	Значення	β	
f _{3l}	нС	вС	
f _{4l}	Н		
f _{5l}	вС		
f _{6l}	Н		

Для оцінки значень лінгвістичних змінних $f_{1l} \div f_{6l}$, α , β застосовується єдина шкала якісних термів: Н – низький; нС – нижче за середній; С – середній; вС – вище за середній; В – високий. Кожний з цих термів задається відповідною функцією належності.

З формальної точки зору задача ідентифікації кіберінцидентів на основі нечітких правил відповідає математичній моделі ідентифікації об'єкту з дискретним виходом [16, 17]. Так, для ідентифікації кіберінцидента c_1 , співвідношення має наступний вигляд:

$$\mu^{c_1}(c) = [\mu^B(\alpha) \wedge \mu^B(\beta)] \vee [\mu^{6C}(\alpha) \wedge \mu^{6C}(\beta)], \quad (9)$$

$$\text{де } \mu^B(\alpha) = [\mu^B(f_{1l}) \wedge \mu^B(f_{2l}) \wedge \mu^H(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^{6C}(f_{5l})],$$

$$\mu^B(\beta) = [\mu^{нС}(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^B(f_{5l}) \wedge \mu^H(f_{6l})];$$

$$\mu^{6C}(\alpha) = [\mu^{6C}(f_{1l}) \wedge \mu^{6C}(f_{2l}) \wedge \mu^{нС}(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^C(f_{5l})],$$

$$\mu^{6C}(\beta) = [\mu^{нС}(f_{3l}) \wedge \mu^H(f_{4l}) \wedge \mu^{6C}(f_{5l}) \wedge \mu^H(f_{6l})];$$

У загальному випадку, наведені нечіткі логічні рівняння дозволяють приймати рішення щодо ідентифікації кіберінциденту за наступним алгоритмом (рис. 3):

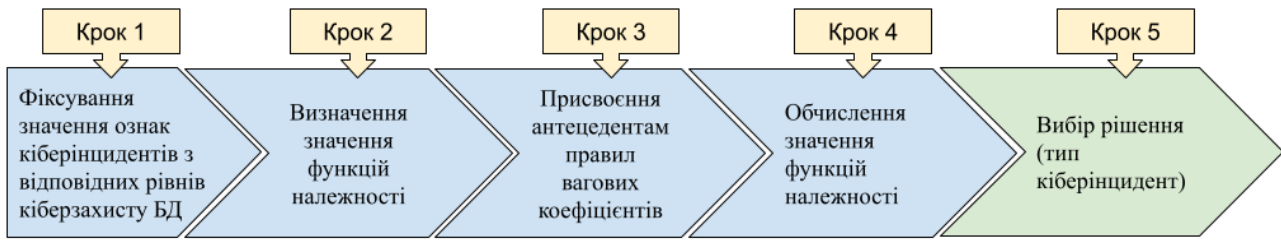


Рисунок 3 – Алгоритм ідентифікації кіберінциденту

Крок 1. Фіксуються значення ознак кіберінцидентів $F^* = (f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*)$.

Крок 2. Визначаються значення функцій належності $\mu^k(f_{il}^*)$ при фіксованих значеннях параметрів $f_{il}^*, i = \overline{1, n}; k = \overline{1, K_i}$.

Крок 3. Присвоїти антецедентам правил вагові коефіцієнти Ω_i^k .

Крок 4. На основі логічних рівнянь (3.16) обчислюються значення функцій належності $\mu^{c_j}(f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*)$ за вектором ознак $F^* = (f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*)$ для всіх типів кіберінцидентів $c_1, c_2, \dots, c_m$.

Логічні операції І ($\wedge$) та АБО ($\vee$) над функціями належності замінюються операціями $\min$ та $\max$:

$$\mu^k(f_{il}^*) \Omega_i^k \wedge \mu^k(f_{jl}^*) \Omega_j^k = \min [\mu^k(f_{il}^*) \Omega_i^k, \mu^k(f_{jl}^*) \Omega_j^k]; i \neq j, \quad (10)$$

$$\mu^k(f_{il}^*) \Omega_i^k \vee \mu^k(f_{jl}^*) \Omega_j^k = \max [\mu^k(f_{il}^*) \Omega_i^k, \mu^k(f_{jl}^*) \Omega_j^k]; i \neq j, \quad (11)$$

Крок 5. Вибір рішення c_j^* (тип кіберінцидента) за умови:

$$\mu^{c_j}(f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*) = \max [\mu^{c_j}(f_{1l}^*, f_{2l}^*, \dots, f_{nl}^*)]. \quad (12)$$

Слід зауважити, що вирішення задачі присвоєння вагових коефіцієнтів антецедентам правил може бути зведеною до визначення степенів належності елементів до множини й побудові на їх основі функцій належності (ФН). Цьому присвячено роботу [16]. Проте, для її ефективного вирішення, необхідно зробити правильний вибір необхідного метода побудови ФН з метою використання подальших методів її обробки. Тому, дане питання потребує більш глибокого дослідження. Задача визначення вагових коефіцієнтів антецедентів нечітких правил може бути сформульованою наступним чином.

Дано: нечітка база знань, що містить нечіткі правила виду (3).

Необхідно: для кожної пари антецедентів правила визначити ступінь переваги та побудувати ФН нечіткій множині “важливість”, яка характеризує “ступінь важливості” антецедента в правилі та представляє собою умову його домінування.

Для методів формування ФН характерним є [18]:

способом опитування (індивідуальний (d_1), груповий (d_2));

видом процедури збору даних (порівняння (p_1), оцінювання об’єктів (p_2), порівняння пар об’єктів (p_3));

типологією експертної інформації (ранжування (e_1), парне або послідовне порівняння (e_2));

уявленням про характер порівняння або оцінювання (порівняння здійснюється за ступенем виразності певної характеристики (v_1) чи за ступенем віддаленості від ідеальної точки (v_2));

інтерпретацією експертної інформації (розгляд результатів порівняння або оцінювання як детермінованих (N) так й імовірнісних (D)).

Крім того, з точки зору практичної реалізації до наведеного переліку слід додати: простоту та зручність (трудомісткі (T) та простоту й компактність у реалізації(L)).

Отже, для обґрунтованого вибору методу побудови ФН нечітких множин для рішення конкретної практичної задачі, його слід розглядати, як кортеж вигляду:

$$M = \langle \alpha, \beta, \gamma, \phi, \sigma, \theta, \rangle, \quad (13)$$

де α – спосіб експертного опитування;

β – вид процедури збору даних;

γ – тип експертної інформації, яка використовується;

ϕ – характер порівняння або оцінювання;

σ – інтерпретація даних експертного опитування;

θ – простота та зручність.

Крім того, основними вимогами до процедури побудови ФН [18] є наступні.

Опитування експертів повинно здійснюватися при наявності ясної фізичної інтерпретації поняття степені приналежності в режимі “оператор-комп’ютер”.

Процедури побудови ФН не повинні нав’язувати експерту апіорних обмежень на його відповіді (наприклад, вимагати транзитивних оцінок).

Кількість запитань до експерта повинно бути невеликим. Наприклад, для застосування методу парних порівнянь число об’єктів, які порівнюються не повинно перевищувати 15.

Визначення ФН повинно здійснюватися при фіксованій множині термів відповідної лінгвістичної змінної.

Процедура повинна включати алгоритми формалізації нечітких множин як з числовою, так й нечислової областями визначення.

Аналіз поставленої задачі та характеру діяльності офіцерів з безпеки показує, що для її вирішення може бути застосований метод типу (14) [19]:

$$\langle d_1, p_3, e_2, v_1, N, L \rangle, \quad (14)$$

де d_1 –індивідуальний спосіб опитування;

p_3 –процедура збору даних – порівняння пар об’єктів;

e_2 –типологія експертної інформації – парне або послідовне порівняння;

v_1 – характер порівняння або оцінювання – порівняння здійснюється за ступенем виразності певної характеристики;

N – інтерпретація експертної інформації – розгляд результатів порівняння або оцінювання, як детермінованих;

L – простота та зручність у реалізації.

Визначеним вимогам відповідає метод, який базується на ідеї розподілу ступенів належності елементів універсальної множини відповідно до їх рангів або метод парних порівнянь на основі рангових оцінок [16, 17, 19-21].

Отже, для вирішення задачі, під рангом антецеденту $f_{jl} \cdot l_{f_{jl}k_{f_j}} \in O^T$ будемо розуміти число $r_\Omega(f_{jl} \cdot l_{f_{jl}k_{f_j}})$, яке характеризує значимість антецеденту у формуванні правила, яке описується нечітким термом Ω . Припускаємо, що виконується правило: чим більшим є ранг елемента, тим більшою є ступінь його належності.

Уведемо наступні позначення (15):

$$r_\Omega(f_{jl} \cdot l_{f_{jl}k_{f_j}}) = r_j, \quad \mu_\Omega(f_{jl} \cdot l_{f_{jl}k_{f_j}}) = \mu_j, \quad j = \overline{1, n}. \quad (15)$$

Тоді правило розподілу ступенів приналежності задається у вигляді співвідношення: $\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} \dots \frac{\mu_n}{r_n}$, з умовою нормування: $\mu_1 + \mu_2 + \dots + \mu_n = 1$.

Враховуючи це, отримуються співвідношення (15), які дають змогу обчислити ступені приналежності $\mu_{\Omega}(f_{jl}, l_{f_{jlkf_j}})$ антецедентів $f_{jl}, l_{f_{jlkf_j}} \in F^T$ до нечіткого терму Ω шляхом використання відносних оцінок рангів $\frac{r_i}{r_j} = a_{ij}, i, j = \overline{1, n}$.

$$\left. \begin{aligned} \mu_1 &= \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \dots + \frac{r_n}{r_1}\right)^{-1} \\ \mu_2 &= \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + \dots + \frac{r_n}{r_2}\right)^{-1} \\ &\dots \\ \mu_n &= \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \dots + 1\right)^{-1} \end{aligned} \right\} \quad (16)$$

За допомогою них створюється матриця (17), яка може інтерпретуватися як матриця парних порівнянь рангів. Для експертних оцінок елементів цієї матриці можна застосувати 9-ти бальну шкалу Сааті [18] (табл. 6):

1 – при відсутності переваги r_j над r_i ;

3 – при слабій перевазі r_j над r_i ;

5 – при суттєвій перевазі r_j над r_i ;

7 – при явній перевазі r_j над r_i ;

9 – при абсолютній перевазі r_j над r_i ;

2, 4, 6, 8 – проміжні порівняльні оцінки.

$$A = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \dots & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \dots & \frac{r_n}{r_2} \\ \dots & \dots & \dots & \dots \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \dots & 1 \end{bmatrix} \quad (17)$$

Таким чином, на основі матриці (17) у відповідності до формул (16) можна визначити вагові коефіцієнти відносної важливості $\omega(f_{jl}, l_{f_{jlkf_j}})$ антецедентів $f_{jl}, l_{f_{jlkf_j}} \in F^T$ та побудувати функцію належності нечіткого терму Ω .

Таблиця 6

Шкала відносної важливості

Інтенсивність важливості	Якісна оцінка	Пояснення
0	Незрівнянність	Немає сенсу порівнювати елементи.
1	Рівна важливість елементів, що порівнюються	Елементи є рівними за значимістю.
3	Помірна (слаба) перевага одного над іншим	Існують показання про перевагу одного елемента над іншим, але вони не є переконливими.
5	Сильна (суттєва) перевага	Існують гарні докази і логічні критерії, котрі можуть показати, що елемент є більш важливим.
7	Очевидна перевага	Існує переконливий доказ більшої значимості одного елемента над іншим.
9	Абсолютна перевага	Максимально підтверджується відчутність одного елемента над іншим.
2, 4, 6, 8	Проміжні значення між двома сусідніми оцінками	Коли є необхідним компроміс.

Для прикладу візьмемо нечітке правило: Якщо кількість підозрілих SQL-запитів є Високою та Частота запитів є Високою та використання ресурсів СКБД є Високим, то це кіберінцидент, пов'язаний з БД.

Крок 1: Оцінювання парних порівнянь

Побудова матриці, в якій експерт оцінює важливість кожного антецедента порівняно з іншими антецедентами в нечіткому правилі. Наприклад, відповідно до наведеного правила:

A1: Кількість підозрілих SQL-запитів є Високою

A2: Частота запитів є Високою

A3: Використання ресурсів СКБД є Високим

Матриця парних порівнянь має виглядати наступним чином, де експерт (аналітик з кібербезпеки) оцінює важливість одного антецедента в порівнянні з іншим (табл. 7).

Таблиця 7

Матриця парних порівнянь антецедентів нечіткого правила

	A1	A2	A3
A1	1	5	1/3
A2	1/5	1	3
A3	3	1/3	1

В цій матриці кожне число показує, як експерт оцінює важливість одного антецедента в порівнянні з іншими в нечіткому правилі. Якщо експерт вважає, що антецедент A1 (Кількість підозрілих SQL-запитів) важливіший за антецедент A2 (Частота запитів), він ставить 5 балів, що вказує на цей відносний ранг.

Крок 2: Нормалізація матриці парних порівнянь

Після того, як матриця побудована, потрібно її нормалізувати, щоб отримати відносні ваги кожного антецедента.

Спочатку обчислимо суми кожного стовпця:

Сума стовпця A1: $1 + 1/5 + 3 = 4,2$

Сума стовпця A2: $5 + 1 + 1/3 = 6,33$

Сума стовпця A3: $1/3 + 3 + 1 = 4,33$

Для подальшої нормалізації значення у кожному стовпці ділимо на загальну суму оцінок у цьому стовпці (табл. 8).

Таблиця 8

Нормалізована матриці парних порівнянь

	A1	A2	A3
A1	0,23	0,79	0,07
A2	0,05	0,15	0,69
A3	0,71	0,05	0,23

Крок 3: Отримання оберненої матриці

Виходячи з того, що логічні операції І ($\wedge$) та АБО ($\vee$) над функціями належності замінюються операціями $\min$ та $\max$, то для врахування “ступені важливості” антецедента, доцільно значення ваг зробити оберненими (табл. 9):

Таблиця 9

Обернена матриця парних порівнянь

	A1	A2	A3
A1	0,77	0,21	0,93
A2	0,95	0,85	0,31
A3	0,29	0,95	0,77

Крок 4: Визначення вектору ваг

Далі обчислюється середнє значення кожного рядка нормалізованої матриці:

Вага для A1: $(0,77 + 0,21 + 0,93) / 3 \approx 0.6$

Вага для A2: $(0,95 + 0,85 + 0,31) / 3 \approx 0.7$

Вага для A3: $(0,29 + 0,95 + 0,77) / 3 \approx 0.7$

Крок 5: Створення нечіткого правила з вагою антецедентів

Якщо кількість підозрілих SQL-запитів є Високою з вагою 0,6 і Частота запитів є Високою з вагою 0,6 та використання ресурсів СКБД є Високим з вагою 0,7, то це кіберінцидент у БД.

Висновки. Запропонована методика виявлення кіберінцидентів в БД ІКСВП, на відміну від існуючих, дозволяє, шляхом застосування нечіткої моделі з вагами антецедентів правил, усунути невизначеність під час логічного виводу для прийняття рішень офіцером безпеки у деяких ситуаціях. Для визначення ваги антецедентів нечітких правил запропоновано використання методу парних порівнянь на основі рангових оцінок. Експериментальна перевірка застосування запропонованої методики на практиці дозволяє зробити висновок про підвищення точності виявлення кіберінцидентів у ІКСВП. Практична цінність методики полягає у можливості виявлення кіберінцидентів SIEM-системами в умовах неповноти та нечіткості інформації про них.

ЛІТЕРАТУРА:

1. Фесьоха В.В., Кисиленко Д.Ю., Нестеров О.М. Аналіз спроможності існуючих систем антивірусного захисту та покладених у їхню основу методів до виявлення нового шкідливого програмного забезпечення у військових інформаційних системах / Системи і технології зв'язку, інформатизації та кібербезпеки 2023. Т. 3. С. 143–151.
2. Байдур О., Вдосконалення кіберзахисту збройних сил з урахуванням досвіду протидії військовим кіберопераціям російської федерації в 2022 році, Кібербезпека: освіта, наука, техніка 2022, 1, 31-45. URL: [https:// doi.org/10.28925/2663-4023.2022.17.3145](https://doi.org/10.28925/2663-4023.2022.17.3145).
3. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році [Електронний ресурс]. – Режим доступу: <https://scrc.gov.ua/uk/articles/334>
4. Герасимов, Б.М., Субач, І.Ю., Хусаїнов, П.В., Міщенко, В.О. (2008) Аналіз задач моніторингу інформаційних мереж та методів підвищення ефективності їх функціонування. Сучасні інформаційні технології у сфері безпеки та оборони, 3(3), 24–27.
5. Субач І., Власенко О. Інформаційні технології захисту баз даних від кібератак в інформаційних системах військового призначення. Collection «Information Technology and Security».2022. No 10 (2). С. 177–193. URL: <https://doi.org/10.20535/2411-1031.2022.10.2.270412>.
6. Субач,І., Герасимов,Б. (2008). Показники якості інформаційного забезпечення та їх вплив на ефективність застосування ІСППР. Вісник Національного університету ім. Тараса Шевченка,20, 27–29.
7. O. Podzins, A. Romanovs, Why SIEM is Irreplaceable in a Secure IT Environment?, Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2019, pp. 1-5, URL: <https://doi.org/10.1109/eStream.2019.8732173>.
8. Granadillo, Gustavo Gonzalez. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel, Switzerland) 21. 2021: n. pag. URL: [https:// doi.org/10.3390/s21144759](https://doi.org/10.3390/s21144759).
9. Субач І., Власенко О., Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-телекомунікаційних системах військового призначення. Збірник наукових праць ВІТІ. 2023. No4. С. 82–92. URL: [https:// doi.org/10.58254/viti.4.2023.07.82](https://doi.org/10.58254/viti.4.2023.07.82).
10. Самохвалов, Ю., Толюпа, С. (2017). Кореляція подій у SIEM-системах з урахуванням немонотонного виводу. Захист інформації, 19(1), 5-9.

11. O. Sievierinov, M. Ovcharenko, Analysis of correlation rules in Security information and event management systems, Fourth International Scientific and Technical Conference «COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES», – Kharkiv: NURE, 2020. – С. 24–25.
12. K.A. Dhanya, Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T. Senthil Kumar, T. Gireesh Kumar, Detection of Network Attacks using Machine Learning and Deep Learning Models, *Procedia Computer Science*, Volume 218, 2023, Pages 57-66, <https://doi.org/10.1016/j.procs.2022.12.401>.
13. Thursday Ehis, A.- mudu. (2023). Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture. *Archives of Advanced Engineering Science*, 1–10. <https://doi.org/10.47852/bonviewAAES32021068>.
14. Субач І., Власенко О., Нечіткі моделі виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення. Збірник наукових праць ВІТІ. 2024. №5. С. 165–180. URL: <https://doi.org/10.58254/viti.5.2024.15.165>.
15. Субач,І, Здоренко,Ю., Фесьоха,В. (2018). Методика виявлення кібератак типу JS(HTML) / Scrinject на основі застосування математичного апарату теорії нечітких множин. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут, 4, 125–131
16. Rotshtein A. P. Medical diagnostics using fuzzy logic. Vinnitsa: Continent-PRIM, 1996. 132 p.
17. Rothstein A. Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks. Vinnytsia: UNIVERSUM, 1999.
18. Borisov A.N., Krumberg O.A., Fedorov I.P. Decision-making based on fuzzy models: examples of use. - Riga: Znanie, 1990. - 184 с.
19. Субач, І. і Микитюк, А. (2023) «Методика формування нечітких асоціативних правил із зваженими атрибутами з бази даних SIEM-системи для виявлення кіберінцидентів в спеціальних інформаційно-комунікаційних системах», Collection "Information Technology and Security", 11(1), с. 47–59. <https://doi.org/0.20535/2411-1031.2023.11.1.283575>.
20. Шапочка М. К., Макарюк О. В. Застосування експертних оцінок при прийнятті рішень за умов невизначеності. Механізм регулювання економіки. 2006. № 4. С. 142-148.
21. Дебела, І. (2024). Проблеми синтезу рішення за нечітких умов: узгодження індивідуальних експертних оцінок. *Економічний простір*, (191), 174-177. <https://doi.org/10.32782/2224-6282/191-28>.

REFERENCES:

1. Fesokha V.V., Kysylenko D.Iu., Nesterov O.M. Analiz spromozhnosti isnuichykh system antyvirusnoho zakhystu ta pokladykh u yikhniu osnovu metodiv do vyivlennia novoho shkidlyvoho prohramnoho zabezpechennia u viiskovykh informatsiinykh systemakh / Systemy i tekhnolohii zviazku, informatyzatsii ta kiberbezpeky 2023. T. 3. S. 143–151.
2. Baidur O., Vdoskonalennia kiberzakhystu zbroinykh syl z urakhuvanniam dosvidu protydiv viiskovym kiberobratsiam rosiiskoi federatsii v 2022 rotsi, Kiberbezpeka: osvita, nauka, tekhnika 2022, 1, 31-45. URL: <https://doi.org/10.28925/2663-4023.2022.17.3145>.
3. Statystychnyi zvit za rezultatamy roboty Systemy vyivlennia vrazlyvosti i reahuvannia na kiberintsydeny ta kiberatomy v 2023 rotsi [Elektronnyi resurs]. – Rezhym dostupu: <https://scpc.gov.ua/uk/articles/334>
4. Herasymov, B.M., Subach, I.Iu., Khusainov, P.V., Mishchenko, V.O. (2008) Analiz zadach monitorynhu informatsiinykh merezh ta metodiv pidvyshchennia efektyvnosti yikh funktsionuvannia. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 3(3), 24–27.
5. Subach I., Vlasenko O. Informatsiini tekhnolohii zakhystu baz danykh vid kiberatak v informatsiinykh systemakh viiskovoho pryznachennia. Collection «Information Technology and Security».2022. No 10 (2). S. 177–193. URL: <https://doi.org/10.20535/2411-1031.2022.10.2.270412>.
6. Subach,I., Herasymov,B. (2008). Pokaznyky yakosti informatsiinoho zabezpechennia ta yikh vplyv na efektyvnist zastosuvannia ISPPR. Visnyk Natsionalnoho universytetu im. Tarasa Shevchenka,20, 27–29.
7. O. Podzins, A. Romanovs, Why SIEM is Irreplaceable in a Secure IT Environment?, Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2019, pp. 1-5, URL: <https://doi.org/10.1109/eStream.2019.8732173>.
8. Granadillo, Gustavo Gonzalez. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel, Switzerland) 21. 2021: n. pag. URL: <https://doi.org/10.3390/s21144759>.

9. Subach I., Vlasenko O., Arkhitektura intelektualnoi SIEM-systemy dlia vyavlennia kiberintsydyntiv u bazakh danykh informatsiino-telekomunikatsiinykh systemakh viiskovoho pryznachennia. Zbirnyk naukovykh prats VITI. 2023. No4. S. 82–92. URL: <https://doi.org/10.58254/viti.4.2023.07.82>.
10. Samokhvalov, Yu., Toliupa, C. (2017). Koreliatsiia podii u SIEM-systemakh z urakhuvanniam nemonotonnoho vyvodu. Zakhyst informatsii, 19(1), 5–9.
11. O. Sievierinov, M. Ovcharenko, Analysis of correlation rules in Security information and event management systems, Fourth International Scientific and Technical Conference «COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES»,– Kharkiv: NURE, 2020. – C. 24–25.
12. K.A. Dhanya, Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T. Senthil Kumar, T. Gireesh Kumar, Detection of Network Attacks using Machine Learning and Deep Learning Models, Procedia Computer Science, Volume 218, 2023, Pages 57–66, <https://doi.org/10.1016/j.procs.2022.12.401>.
13. Thursday Ehis, A.- mudu. (2023). Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture. *Archives of Advanced Engineering Science*, 1–10. <https://doi.org/10.47852/bonviewAAES32021068>.
14. Subach I., Vlasenko O., Nechitki modeli vyavlennia kiberintsydyntiv u bazakh danykh informatsiino-komunikatsiinykh system viiskovoho pryznachennia. Zbirnyk naukovykh prats VITI. 2024. No5. S. 165–180. URL: <https://doi.org/10.58254/viti.5.2024.15.165>.
15. Subach, I., Zdorenko, Iu., Fesokha, V. (2018). Metodyka vyavlennia kiberatak typu JS(HTML) / Scrinject na osnovi zastosuvannia matematychnoho aparatu teorii nechitkykh mnozhyn. Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii imeni Heroiv Krut, 4, 125–131
16. Rotshtein A. P. Medical diagnostics using fuzzy logic. Vinnitsa: Continent-PRIM, 1996. 132 p.
17. Rothstein A. Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks. Vinnytsia: UNIVERSUM, 1999.
18. Borisov A.N., Krumberg O.A., Fedorov I.P. Decision-making based on fuzzy models: examples of use. - Riga: Znanie, 1990. - 184 c.
19. Subach, I. i Mykytiuk, A. (2023) «Metodyka formuvannia nechitkykh asotsiatyvnykh pravyl iz zvazheny my atrybutamy z bazy danykh SIEM-systemy dlia vyavlennia kiberintsydyntiv v spetsialnykh informatsiino-komunikatsiinykh systemakh», Collection "Information Technology and Security", 11(1), s. 47–59. <https://doi.org/0.20535/2411-1031.2023.11.1.283575>.
20. Shapochka M. K., Makariuk O. V. Zastosuvannia ekspertnykh otsinok pry pryiniatti rishen za umov nevyznachenosti. Mekhanizm rehuliuвання ekonomiky. 2006. № 4. S. 142–148.
21. Debela, I. (2024). Problemy syntezy rishennia za nechitkykh umov: uzghodzhennia indyvidualnykh ekspertnykh otsinok. Ekonomichnyi prostir, (191), 174–177. <https://doi.org/10.32782/2224-6282/191-28>.

METHODOLOGY FOR DETECTING CYBER INCIDENTS BY SIEM IN DATABASES OF MILITARY INFORMATION AND COMMUNICATION SYSTEMS

With the integration of information and communication systems into military operations, the issue of their cyber defense is becoming increasingly important. The main target for cyberattacks are databases that mostly contain confidential information. One of the most effective approaches to ensuring cybersecurity of databases of military information and communication systems is to use the intelligent capabilities of a SIEM system. SIEM allows real-time monitoring, analysis and response to potential cyber incidents. The article proposes a methodology for detecting cyber incidents by a SIEM system in databases of military information and communication systems.

The main emphasis is placed on the multi-level protection of databases, which includes protection at the operating system level, the database level and the database management system, as well as the network level of protection. In order to improve the efficiency of cyber incident detection at the level of SIEM data analysis, an improved methodology based on fuzzy logic is used. Improvement of the methodology is achieved by introducing weights of antecedents in fuzzy rules, which allows, in some cases, to identify cyber incidents more accurately compared to existing models and methods. The weights of the antecedents of fuzzy rules are determined using the method of pairwise comparisons based on the rankings made on the 9-point Saaty scale. A decision-making algorithm for identifying cyber incidents based on the analysis of fuzzy rules and the weights of their antecedents is presented. An example of calculating the weights of antecedents of fuzzy rules using the method of pairwise comparisons based on rank estimates is given.

Keywords: database, information and communication system, cyber protection, cyber incident, cybersecurity, cyber attack, SIEM system, fuzzy set theory, fuzzy rules, pairwise comparison method.

СОЦІОКУЛЬТУРНИЙ АНАЛІЗ ТРАНСФОРМАЦІЙ ГЕНДЕРНОЇ СТРУКТУРИ ВІЙСЬКОВОЇ СФЕРИ: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД

В статті розглядається проблематика гендерної інтеграції як у сфері національної безпеки і оборони, так і її загальносвітові тенденції розвитку, що залежать від традицій, культури та політичних пріоритетів кожної держави. Реалізація принципу гендерної рівності та механізму його забезпечення в українському війську потребує врахування не лише світового досвіду військової фемінізації, але й можливості його практичного застосування з урахуванням реалій сучасної війни. Соціокультурний підхід до реалізації гендерної політики у військовій сфері передбачає досягнення гендерної паритетності відповідно до існуючих у суспільстві соціокультурних орієнтирів з метою забезпечення рівних умов для реалізації прав та можливостей для збройного захисту держави представниками обох статей без обмежень, пов'язаних із жорстко закріпленими гендерними ролями. Рівність між жінками та чоловіками розглядається як питання прав людини та як необхідна умова повноцінного членства України в Альянсі, що не може бути досягнута без належного представництва різних соціальних та гендерних груп у силових структурах. За результатами проведеного дослідження з'ясовано, що за час військових дій з 2014 року гендерний склад українського війська суттєво змінився – кількість жінок в армії зросла майже втричі, і вона продовжує збільшуватися. Спостерігається також позитивна тенденція подолання гендерних стереотипів у суспільстві, підвищення рівня соціальної свідомості та гендерної компетентності військовослужбовців. Аналіз вимог нормативно-правових актів засвідчив, що жінки в Україні мають відносно однакові права та обов'язки, але при цьому в армії зберігаються певні ознаки гендерного дисбалансу, притаманні в цілому українському суспільству. У зв'язку з цим зусилля уряду і суспільства щодо формування ефективної гендерної політики у військовій сфері мають бути спрямовані на мінімізацію проявів дискримінації за ознакою статі в українському війську, створення сприятливих умов для професійної реалізації жінок в армії, зміцнення відповідних інституційних механізмів з урахуванням міжнародних правових норм з метою скорочення розриву між декларативним та реальним впровадженням гендерної рівності та її адаптації відповідно до конкретних потреб оборонного сектору.

Ключові слова: гендерна політика, гендерна рівність, дискримінація, стереотипи, Збройні Сили України, фемінізація, жінки-військовослужбовці.

Вступ та постановка проблеми. Ще до початку повномасштабної збройної агресії російської федерації в Україні окреслилася стійка тенденція подолання гендерної дискримінації, ґрунтована на досягнутому суспільному визнанні архаїчності та шкідливості патріархального розподілу гендерних ролей [1]. У сучасних умовах проблематика формування національного механізму забезпечення гендерної рівності у військовій сфері набуває особливого значення і зумовлена необхідністю якісного комплектування особового складу Сил безпеки і оборони країни, міжнародними зобов'язаннями України, її європейським вибором, світовими політичними процесами та іншими чинниками. Необхідність забезпечення рівних прав та можливостей жінок і чоловіків у секторі безпеки та оборони потребує напрацювання ефективних управлінсько-правових засобів викорінення гендерних стереотипів та пошуку інноваційних підходів до формування і реалізації гендерної політики у Збройних Силах України.

У науковій літературі гендерна політика визначається як комплексна, цілеспрямована діяльність держави, міжнародних і недержавних організацій, яка здійснюється ними

безпосередньо та опосередковано на національному та регіональному рівнях і спрямована на впровадження гендерного підходу в усі сфери суспільного життя як засіб уникнення дискримінації за ознакою статі та досягнення рівного розподілу економічних, соціальних і політичних ресурсів між жінками і чоловіками. У свою чергу, гендерна політика у Збройних Силах України є складовою загальної гендерної політики держави, її “проекцією” на військове середовище. Життєдіяльність війська ґрунтується на статусних засадах, зокрема, на статусно-посадових відмінностях різних категорій військовослужбовців, що значною мірою формує соціальний потенціал кожної окремої особистості. Тобто предметом гендерної політики у силових структурах є статусні взаємодії між військовослужбовцями обох статей та статусно-рольові відмінності між ними, їх вплив на рівень бойової готовності і боєздатності військ (сил) [2]. Отже, гендерна політика у Збройних Силах України має забезпечувати гарантії рівних прав та можливостей для військовослужбовців незалежно від їх статі для реалізації ними своїх професійних та життєвих прагнень, створювати умови для їх конструктивної взаємодії та сприяти формуванню гендерної моделі, що відповідатиме сучасним світовим стандартам.

Поняття “гендер” є відносно складним за змістом. Так, гендер можна розглядати як організовану модель соціальних відносин між чоловіками і жінками в усьому просторі соціуму: від сім’ї до вищих інститутів влади. Якщо термін “стать” використовується для визначення біологічних відмінностей між особами чоловічої та жіночої статей, то категорія “гендер” означає соціально-культурні відмінності між чоловіками і жінками, обумовлені суспільними нормами і традиціями, що можуть різнитися як в окремих країнах і культурах, так і в різних групах одного суспільства [3]. Тобто в межах соціокультурного підходу зміщується акцент з аналізу відношень статі на механізм взаємодії принципів рівноправності та універсальності прав людини як важливого фактору розвитку суспільства [4].

Слід зазначити, що у контексті гендерної рівності у ЗС України досягнення гендерного балансу не має на меті забезпечення рівної репрезентації чоловіків і жінок в особовому складі. Мова йде про те, що у демократичному суспільстві кожен громадянин повинен мати можливість максимально ефективно реалізувати свої професійні здібності, навички та досвід, у тому числі для захисту держави, незалежно від гендерних ознак. У цьому контексті проведення подальших наукових досліджень щодо визначення гендерної стратегії у збройних силах, активне вивчення вітчизняного і зарубіжного досвіду гендерної політики у військовій сфері має суттєве теоретичне й практичне значення.

Аналіз останніх досліджень і публікацій. Поширення принципів гендерної рівності у військовій сфері сприяло активізації наукових досліджень, присвячених вивченню гендерної складової розвитку національних збройних сил, зокрема, українських. Ретроспективний аналіз наукової літератури свідчить, що гендерна проблематика була актуальною здавна, проте теорія та практика інтегрування гендерних підходів у військову сферу потребує сучасної наукової оцінки та пошуку шляхів і засобів оптимізації професійної діяльності жінок в армії. Зокрема, висвітленню цих питань присвячені праці таких науковців як В. Арнаутова, Б. Андресюк, Н. Вавілова, І. Грицай, О. Давидюк, Н. Дубчак, Ю. Калагін, І. Коросташова, Н. Клименко, Л. Кринець, В. Кротиков, В. Малюга, М. Мірошніченко, В. Топальський та ін. Питання формування зваженої гендерної політики у силових структурах України перебуває на стадії активного наукового обговорення і потребує подальшого різноаспектного наукового аналізу, який при цьому дещо ускладнений обмеженим доступом до інформації військового характеру, необхідністю адаптації зарубіжного досвіду до вітчизняних умов тощо.

Метою статті є дослідження процесу інтеграції жінок до військових формувань як невід’ємної складової реалізації принципів гендерної політики, зокрема, у Силах безпеки і оборони з урахуванням реалій сучасної війни та загальносвітових тенденцій розвитку гендерних відносин у силових структурах.

Виклад основного матеріалу. Фемінізацію військової сфери можна розглядати, виходячи з різних теоретичних аспектів. На певних етапах розвитку суспільства

функціональне призначення жінок у військових формуваннях залежало від суспільної формації і полягало в основному у виконанні сімейно-побутових, духовно-рекреативних обов'язків, господарських та медичних функцій. Будь-які соціальні, економічні, політичні перетворення призводили до змін у соціальному порядку і змушували переглядати гендерні контракти. В індустріальному суспільстві жінки стали брати участь у бойових кампаніях, переважно не вступаючи у прямий контакт із противником, в якості медичного персоналу, зв'язківців, комірників і т.д., тобто у професійній діяльності запроваджується концепція рівних потенційних можливостей у процесі самореалізації людини незалежно від статевої належності. У сучасних умовах розширення можливостей служби жінок у Збройних силах обумовлюються, з одного боку, редукцією функцій чоловіків у суспільстві в цілому і в армії зокрема, а з іншого – зростанням технічної оснащеності військ, модернізацією зброї, появою складних технічних комплексів, тобто інтелектуалізацією всіх сфер життя. Використання нових технологій при веденні бойових дій, дистанційних методів управління зброєю відсувають на другий план природні “чоловічі” ознаки сили і мужності. Більшого значення набувають такі якості як стресостійкість, уважність, спостережливість, витривалість, організованість. Для освоєння професійних компетенцій військовослужбовець має бути мотивований до здійснення своєї діяльності, прагнути професійного зростання, бути комунікабельним, виконувати норми та вимоги, успішно вирішувати поставлені перед ним завдання. Таким чином, трансформаційні процеси, які відбуваються сьогодні в суспільстві, прискорили інтеграцію жінок до військових структур, що, безумовно, є значним кроком на шляху забезпечення гендерної рівності. Однак на практиці поширеними залишаються випадки, коли жінки стикаються з низкою сталих стереотипних суджень, які часто заважають освоєнню професії та продукують практики виключення з армійського соціуму. Зокрема, часто чоловіки скептично оцінюють професійні якості жінок-військовослужбовців, аргументуючи це тим, що жінки мають менше фізичної та моральної сили, менш витривалі, схильні до паніки в екстрених ситуаціях через надмірну емоційність; поранена або вбита жінка на полі бою більше деморалізує солдатів, оскільки спрацьовують гендерні стереотипи. Крім того, жінка не вписується у специфічні умови військової служби, оскільки апіорі інакше сприймає як систему домінантних відносин в армії, так і певні елементи армійської культури, що в результаті ускладнює повсякденні ритуальні практики чоловічої спільноти, якщо там з'являється жінка. Водночас дослідження військових психологів показують, що присутність у колективі жінок значно пом'якшує морально-психологічну атмосферу, покращує комунікаційні навички, змушує командирів бути стриманішими, а головне – зростає культура взаємовідносин між військовослужбовцями у самому колективі, знижується рівень напруженості у конфліктних ситуаціях [5]. При цьому відсоток порушень військової дисципліни або злочинів, скоєних жінками-військовослужбовцями, – мінімальний. Соціологічні дослідження, проведенні за останні 10 років, свідчать, що саме жінки-військовослужбовці найбільш старанно виконують службові обов'язки [6]. Крім цього, визнаним є факт, що наявність жінок у контингентах з підтримання миру сприяє поліпшенню відносин військових з населенням приймаючої країни, а також підвищує можливості миротворців щодо взаємодії з жінками і дітьми та їх захисту [7]. Паритетне представлення жінок у секторі безпеки сприяє більшій довірі до нього населення.

Слід відзначити, що за результатами загальнонаціональних комплексних та інших соціологічних досліджень в Україні спостерігається трансформація гендерних стереотипів, яка відзначається посиленням егалітарних і ослабленням традиційних установок у суспільстві [8-10]. Якщо у 2018 році ідею рівноправності жінок і чоловіків в армії підтримували 53% респондентів, то у 2023 році підтримка зросла до 80%. При цьому жінки вище оцінюють рівень можливостей для жінок у силових структурах, ніж чоловіки. 85% громадян України позитивно ставляться до жінок, які служать у Збройних Силах, 81% погоджуються, що жінка може командувати бойовим підрозділом так само, як і чоловік. Тобто можна стверджувати, що за час військових дій з 2014 року національна та соціально-політична свідомість українців

зазнала фундаментальних змін, що призводить до поступової відмови від пострадянських стереотипів мислення і російських наративів, якими є шовінізм, дискримінація за національними і гендерними ознаками та агресивна гомофобія. Як наслідок такої трансформації, підвищився рівень соціальної відповідальності та самосвідомості військовослужбовців, що, зокрема, виражається у глобальній європеїзації ментальності військовослужбовців Збройних Сил України [11]. Разом із цим, все ще поширеними у суспільстві залишаються упереджені погляди щодо жінок в армії: більше половини респондентів погодилися з тим, що жінкам краще займатися небойовими задачами, ще 40% поділяють думку про більші проблеми у сім'ях жінок-військовослужбовиць порівняно із цивільними жінками. На думку експертів, виправити гендерні стереотипи у суспільстві складніше, ніж расові чи етнічні забобони [12].

В цілому можна констатувати, що з кожним роком кількість жінок у Збройних силах збільшується, створюючи нові гендерні моделі в армійських структурах та змінюючи вигляд військових формувань. Багато сучасних дослідників відмічають той факт, що нарешті жінку-військовослужбовця в Україні почали сприймати не як виняток, а як професіонала, що добровільно опановує обрану спеціальність.

Проблема гендерної інтеграції в армії викликала широкий резонанс у рамках світової демократизації соціальних структур і активно обговорюється з двох протилежних позицій: консервативної та ліберальної. Консерватори вважають, що Збройні сили повинні зберігати свою специфіку та особливу функціональну призначеність. Ліберали ж стверджують, що армія має адекватно відображати мінливі цінності громадянського суспільства та поширення в ньому багатьох “інституційних субкультур”, у тому числі побудованих за гендерним принципом. Прибічник ліберального підходу Б. Мюллер зауважував, що “жінки не можуть з повним правом вимагати рівних прав у всіх сферах життя, не визнаючи водночас права на захист своєї країни” [13]. Л. Дефлер та Р. Уорнер, аналізуючи соціально-економічний та соціально-психологічний вплив військової служби на жінок, дійшли висновку, що військовослужбовці-жінки досягають більш високих статусних позицій у порівнянні з цивільними жінками, оскільки мають можливість отримувати зарплату, еквівалентну чоловічій, а також задоволені тим, що їхня робота перебуває у сфері безпеки країни, отже, більш важлива для досягнення різних благ у суспільстві [14]. Тому жінки-військовослужбовці мають прагматичні очікування від служби в армії та намагаються реалізувати свій життєвий шлях із максимальною вигодою. Горизонти для гендерної рівноправності в арміях світу розширюються також у зв'язку з тенденцією переходу до комплектування Збройних сил на контрактній основі, тобто створенням професійної армії.

Фемінізація Збройних сил має загальносвітові тенденції розвитку, але існують і специфічні риси цього процесу, що залежать від традицій, культури, політичних пріоритетів кожної окремої держави. У цьому контексті цікавим є порівняння існуючої гендерної структури в арміях різних країн світу. Так, в Ізраїлі, наприклад, який є беззаперечним лідером щодо аналізованого питання, кожен третій солдат армії – жінка [6]. З 1948 р. держава взяла участь у вісьмох визнаних війнах та низці конфліктів, тому Ізраїль має постійно утримувати велику, навчену та добре озброєну армію (ЦАГАЛ). Не зважаючи на постійні дискусії серед представників релігійних організацій щодо служби жінок в армії, в країні запроваджена обов'язкова мобілізація всіх громадян по досягненню 18 років, у тому числі жінок. Отримати відстрочку/звільнення від служби в армії жінки можуть лише у зв'язку з одруженням, вагітністю або за релігійними переконаннями. Військова служба для ізраїльтянок триває 21 місяць (для чоловіків – 36). Спочатку вони служили в тилу на посадах медсестер, вчителів тощо, однак у 1995 році Верховний суд дозволив жінкам вступати у бойові підрозділи та брати участь у бойових діях. Жінкам дозволяється служити практично в усіх частинах ізраїльської армії, за винятком лише окремих видів військ, що становлять не більше однієї п'ятої загальної чисельності з'єднань Армії оборони Ізраїлю. Наразі жінки служать у сухопутних військах, у флоті та авіації, але здебільшого – в артилерії або прикордонних військах. Станом на 2021 рік

жінки складали до 40% призовників Армії оборони Ізраїлю та обіймали 25% офіцерських посад. Кількість позицій, відкритих для ізраїльтянок, також зростає. У 1980-х роках жінкам були доступні 55% військових посад, у 1995 – 73%, а з 2012 року – 86%. Статистика свідчить, що кількість жінок-піхотинців зросла на 350% з 2013 по 2017 рік, а загальна кількість військовослужбовиць збільшилась всемеро з 2005-го [15].

Норвегія ухвалила закон про обов'язковий військовий обов'язок для обох статей у 2014 році, ставши за цим показником першою в країнах НАТО та першою європейською країною. У Норвегії жінки мають право виконувати військові функції з 1938 року. Під час Другої світової війни жінки-рядові та жінки-офіцери служили в усіх родах Збройних сил. У 1947-му їх перевели на тиллові позиції, однак з 1976 року жінкам було дозволено служити у збройних силах за власним бажанням. У 1985 році парламент ухвалив законодавство про рівні можливості для жінок та чоловіків у військах, таким чином Норвегія стала першою країною НАТО, яка дозволила жінкам займати бойові позиції у збройних силах, включаючи службу на підводних човнах, відповідно до законодавства країни про рівні гендерні можливості. Вже у 2020-му жінки становили 33% від загальної кількості людей, які пройшли обов'язкову військову службу. Громадян Норвегії призивають в армію у віці 19 років. Чоловіки та жінки зобов'язані з'явитись у місця збору, але лише 15% з них відбирають на службу, яка триває 12-16 місяців. На сьогодні жінки нарівні з чоловіками проходять військову службу. Вони не лише разом тренуються на полігонах та виконують бойові завдання, а й проживають під одним дахом на маневрах та у пунктах постійної дислокації. Адже декілька років тому було прийнято рішення об'єднати чоловічі та жіночі казарми, щоб усі військовослужбовці проживали на одній території незалежно від статі. При цьому у норвезькій армії не існує такого ганебного явища, як випадки домагань [16]. Станом на 2017 рік в армії країни було 12% військовослужбовиць, але міністерство оборони Норвегії планує довести кількість жінок в армії до 20% від загальної чисельності збройних сил, і ключовим аргументом цієї політики є просування гендерної рівності в усіх аспектах життєдіяльності країни.

З 1989 року у Швеції немає гендерних обмежень на доступ до військової підготовки або посад у Збройних силах. Жінки мають право служити в усіх родах військ та на всіх позиціях, у тому числі й бойових. Систему призову в армію як для чоловіків, так і для жінок у Швеції запустили у 2017 році. Служба у війську триває 11 місяців. Перед цим вона не була обов'язковою для громадян протягом семи років, оскільки в армії вистачало добровольців. У 2018-му жінки складали 15% від загальної кількості солдатів, які проходили навчання у шведській армії та обіймали менше 7% офіцерських посад.

У ФРН жінки у погонах становлять 10% від усього особового складу, такий самий гендерний склад в армії Великобританії. Тим часом Бундесвер (армія Німеччини) стала доступна для жінок з 2001 року після змін, внесених до конституції країни. Німеччина досить довго чинила опір участі жінок у бойових діях на передовій. Зміни у конституції призвели до того, що кількість жінок в армії суттєво збільшилась. Але проведене міністерством оборони Німеччини через десять років опитування показало, що половина з тих жінок, які скористалися своїм знову набутим правом, визнали, що помилилися у виборі професії.

У Європі найбільш “фемінізованою” є французька армія (понад 22% жінок). З 1995 року жінкам Франції дозволено пілотувати всі види літаків. З 2014 року французькі жінки можуть брати участь у бойових діях. В Іспанії жінки служать в армії нарівні з чоловіками, їхня частка складає близько 14% від усього особового складу. У Франції, Румунії та Польщі кількість жінок, які беруть участь у бойових діях, залишається досить низькою. Так само, як і в Новій Зеландії, яка дозволила жінкам брати участь у боях на передовій у 2001 році, кількість добровольців на бойові позиції залишається вкрай низькою. Австралія пішла цим шляхом у 2013 році, понад 60 жінок негайно підписали контракти на участь у бойових діях. Деякі з них вступили до елітних підрозділів спецназу, які брали участь в операціях в Афганістані. При цьому загальна кількість жінок у збройних силах Австралії становить 14%, близько 10% служать у частинах, розміщених у зоні бойових дій за кордоном.

У США з 1 липня 1973 року було введено добровільну систему комплектування Збройних сил, що кардинальним чином змінило їхній гендерний склад. Так, з моменту запровадження контрактної служби кількість жінок-військовослужбовців у загальній структурі Збройних сил зросла з 42 тис. осіб у 1973 р. до 363 тис. у 2022 р., що становить 17,5% від загальної чисельності війська Сполучених Штатів [17]. Однією з найбільших змін подальших років можна вважати надання у 2015 році після років дебатів дозволу жінкам служити у будь-яких військових частинах США та на будь-яких посадах. Тепер усі військові посади у Збройних силах США, включно з бойовими в елітних загонах, відкриті для жінок, за умови їх відповідності стандартам та наявності необхідної кваліфікації. Зауважимо, що за даними досліджень, проведених Pew Research Center, гендерних відмінностей у виборі професії військового виявлено не було. І чоловіки, і жінки орієнтувалися на можливість служити своїй країні, пильги для здобуття освіти, перспективи побачити світ та розвинути професійні навички. Не зважаючи на ідентичні очікування від військової служби та декларовані рівні стартові можливості, як і раніше, спостерігається гендерний дисбаланс при кадровому розміщенні, хоча зміни в цій галузі очевидні. У даний час жінки в США задіяні у всіх родах збройних сил і можуть знаходитись на лінії фронту. З кожним роком жінок у військах стає все більше, вони продовжують обіймати посади, які довгі роки вважалися лише чоловічими. У Штатах служба в армії є добровільною, останній призов у країні був під час війни у В'єтнамі у 70-х роках. У 2021-му у Палаті представників США пропонували внести поправку до закону та зобов'язати жінок також ставати на військовий облік, але її не підтримали.

У канадській армії жінки почали служити з 1895 року. Канада стала однією з перших країн світу, які допустили жінок на передову у 1989 році згідно рішення Суду з прав людини щодо повної інтеграції жінок у Канадські збройні сили. Однак, наприклад, до служби на підводних човнах жінок не допускали аж до 2000 року, а перша жінка капітан військового корабля з'явилася в канадському ВМФ лише у 2003 році. Наразі жінки становлять близько 15% від усіх канадських військовослужбовців, але керівництво Збройних сил активно намагається збільшити їх кількість, аби до 2026 року цей показник досягнув 25%.

Жінки служать також в арміях Бельгії, Данії, Швейцарії, Нідерландів, Туреччини, Іспанії, Португалії, Люксембургу, Польщі, Греції, Шрі-Ланки, Пакистану, Північної Кореї, Китаю, Еритреї та інших країн.

Поруч із загальносвітовою тенденцією збільшення кількості жінок у силових структурах, детермінуючим фактором зміни гендерного складу в українському війську стала зовнішня військова агресія та гостра потреба захисту Батьківщини. Після повномасштабного вторгнення РФ кількість жінок, що долучилися до лав ЗС України та інших військових формувань, значно зросла. Так, у 2014 році загальна чисельність жінок у ЗС України становила 49 926 осіб, із них військовослужбовиць – 16 557. На початок 2024 року в українській армії служило вже 45 587 жінок, тобто майже втричі більше, і їх кількість продовжує збільшуватися [18]. Загалом, наразі більше 7% чисельності особового складу Збройних Сил України становлять жінки і більше 5% – саме військовослужбовиці, зокрема: офіцерський склад – 6,6%, сержантсько-старшинський склад – 6,6%, солдати – 4,4%, курсанти – 18,1%. Близько 5 тисяч військовослужбовиць виконують завдання в районі проведення бойових дій, більше 13 тисяч – мають статус УБД [19]. Такі цифри є показовими навіть у порівнянні України з країнами-членами НАТО, частка військовослужбовиць в арміях яких коливається від 0,3 % до 20 %. Це свідчить про те, що роль жінки в українській армії помітно зросла, але зберігаються певні ознаки гендерного дисбалансу, притаманні в цілому українському суспільству.

Військова агресія російської федерації змусила переглянути роль та права жінок у силових структурах України з точки зору існуючих законодавчих обмежень, наприклад, щодо участі у бойових діях, виконання окремих завдань, доступу до посад та військових звань тощо. Результатом стало прийняття у 2018 році Закону України № 2523-VIII “Про внесення змін до деяких законів України щодо забезпечення рівних прав і можливостей жінок і чоловіків під

час проходження військової служби у Збройних Силах України та інших військових формуваннях” [20], що закріпив принцип рівноправного проходження служби жінками та чоловіками і скасував необґрунтовані обмеження стосовно служби жінок у запасі та проходженні військових зборів. Наразі в Україні дозволена участь жінок у бойових операціях, для жінок відкритий доступ практично на всі бойові спеціальності, жінки можуть служити по контракту (до 60 років, як і чоловіки), управляти військовою технікою, займати керівні армійські посади, офіційно встановлена форма одягу для військовослужбовиць. З 2019-го року уряд дозволив дівчатам вступати до військових ліцеїв, тепер жінки мають доступ до усіх рівнів військової освіти. Регулярно проводяться тренінги, наради, семінари, круглі столи, освітні заходи за участю міжнародних організацій й фахівців з питань рівноправності в українському війську; усі документи, які розробляє МОУ, проходять гендерну експертизу; здійснюється імплементація гендерного компоненту у навчальні програми; введені посади штатних та позаштатних радників з гендерних питань у системі Міноборони та ЗС України. У відповідь на виклики, з якими зіткнулися військовослужбовиці під час проходження служби, у Національному університеті оборони України було розроблено та розміщено в електронній бібліотеці “Порадник з протидії гендерної дискримінації у Збройних Силах України”, в якому містяться рекомендації щодо забезпечення прав жінок в армії з урахуванням досвіду сучасної війни та підкреслюється актуальність просвітницької роботи серед військовослужбовців [21, 22]. Такий підхід відповідає концептуальним засадам сучасної політики гендерної рівності, що полягає у комплексному підході “gender mainstreaming” як стратегії її досягнення і має на меті зробити інтереси та досвід жінок і чоловіків невід’ємним аспектом проектування, реалізації, моніторингу та оцінювання будь-якої ініціативи [23].

З точки зору імплементації у правове поле України міжнародних принципів гендерної рівноправності важливим кроком стало прийняття Кабінетом Міністрів у 2016 році першого Національного плану дій з виконання Резолюції Ради Безпеки ООН 1325 “Жінки, мир, безпека”. Резолюція стала інституційною рамкою для інтеграції жінок до безпекового сектору. Її основні положення визначають важливість залучення досвіду жінок у вирішенні конфліктів, розбудові миру, захисті жінок від гендерно зумовленого насильства під час конфліктів. Україна стала першою країною в світі, де документ було прийнято в умовах збройного конфлікту [24]. Вже у 2021 році був ухвалений другий Національний план дій, у рамках якого Міністерством оборони України був розроблений План заходів з реалізації в Міністерстві оборони України Національного плану дій з виконання резолюції Ради Безпеки ООН 1325 “Жінки, мир, безпека” на період до 2025 року [25], де визначені стратегічні та оперативні цілі впровадження положень резолюції, зокрема в секторі безпеки і оборони. Після повномасштабного вторгнення були також ухвалені зміни до ст. 1 Закону України “Про військовий обов’язок і військову службу” (№ 2664-IX від 7.10.2022) щодо порядку взяття жінок на військовий облік [26]. Вони передбачають, що українки певних професій, споріднених з відповідними військово-обліковими спеціальностями, можуть ставати на військовий облік за власним бажанням. Зазначимо, що наразі питання щодо обов’язкової мобілізації жінок в Україні на порядку денному не стоїть – жінки можуть мобілізуватися до Сил оборони винятково добровільно.

Не зважаючи на те, що державна політика щодо досягнення гендерної рівності в секторі безпеки й оборони України реалізується відповідно до міжнародних зобов’язань та національного законодавства, для подальшого ефективного її впровадження необхідно посилювати заходи щодо подолання існуючих гендерних стереотипів та зміцнювати відповідні інституційні механізми. Наприклад, наразі у Збройних Силах України лише 9 % офіцерських посад обіймають жінки, і лише три жінки мають генеральське звання [27]. Для жінок усе ще діє заборона на прийом на посади офіцерського складу, що пов’язані з використанням бойових патронів, водолазними роботами. Також для жінок залишаються закритими всі посади на підводних човнах і надводних кораблях, в управлінні бригад надводних кораблів, підрозділах пожежогасіння, які передбачають непряме гасіння пожеж, а

також підрозділах тилового забезпечення з використанням вибухонебезпечних реактивів. Посади для жінок також відсутні у військових частинах спеціального призначення [28]. Тому насамперед потрібні законодавчі ініціативи щодо забезпечення кар'єрного розвитку жінок в армії відповідно до їх рівня освіти, досвіду і результатів службової діяльності; розширення можливостей, зокрема, за рахунок збільшення кількості посад, у тому числі командних, які можуть займати жінки на військовій службі; крім цього, актуальним є створення гендерно орієнтованої побутової інфраструктури в армії, поліпшення доступу до медичного обслуговування та психологічної підтримки для військовослужбовиць з урахуванням специфічних жіночих потреб, забезпечення їх формою і амуніцією на державному рівні; удосконалення корпоративної етики у військах, протидія проявам сексизму. Також важливо, щоб воєначальники прагнули до розвитку власних навичок застосування гендерного підходу до всіх аспектів командування збройними силами, наприклад, через використання практики залучення фахових інструкторів [29]. Збройні сили можуть використовувати знання і досвід громадських організацій, національних правозахисних інститутів та міжнародних організацій з метою їх практичного застосування, зокрема, в умовах збройного конфлікту. Можливо, на даний час наше суспільство ще не готове до запровадження обов'язкової строкової військової служби для всіх громадян, як в Ізраїлі, або до застосування однакових нормативів з фізичної підготовки незалежно від гендерної ознаки, як у Великобританії, чи до впровадження спільної території проживання чоловіків і жінок під час проходження військової служби, як у Норвегії та Фінляндії, – але виклики часу вимагають створити сприятливі умови реалізації здібностей та можливостей для збройного захисту держави тими жінками, які до цього дійсно готові [30]. Якщо у більшості інших країн було чимало часу, аби інтеграція жінок у військо здійснювалася поступово і послідовно, то українська армія в умовах протидії збройній агресії вимушена розвиватися швидко.

Висновки. Отже, аналіз гендерних відносин у військах свідчить про те, що на різних етапах розвитку суспільства роль жінки у військовій сфері змінювалася – від повного неприйняття жінок у чоловічому армійському соціумі до рівноправності у виборі військової професії. Важливими віхами фемінізації в арміях всього світу стали світові війни, коли жінки почали брати участь у бойових діях поряд із чоловіками на підставі мобілізації. Крім того, модифікація системи призову у бік відмови від масових армій та актуалізації набору на контрактній основі дозволила трансформувати існуючі гендерні пропорції. Не зважаючи на це, досить сталими у суспільстві залишаються стереотипні гендерні судження. Зокрема вважається, що присутність жінок на полі бою негативно впливає на боєздатність армії; жінок доцільно зберігати як “мирний сегмент” суспільства; місце жінки – “на кухні” не лише у цивільному житті, а й у війську. З іншого боку, багато противників сегрегації вважають відсутність жінок у бойових підрозділах ознакою сексизму і дискримінації, що глибоко вкоренилися в армійському середовищі. При цьому слід враховувати, що реалізація стратегії гендерної рівності має здійснюватися без підміни понять “рівність” і “однаковість”, оскільки фізіологічні, психологічні та інші відмінності між жінками і чоловіками існують, тому їх треба брати до уваги на всіх етапах формування гендерної політики з орієнтиром на рівний розподіл соціальних, економічних та професійних можливостей. Перспектива подальшого удосконалення інституційної спроможності гендерної інтеграції в секторі оборони загалом полягає в налагодженні механізму моніторингу, оцінювання та координації гендерних питань, імплементації міжнародних антидискримінаційних правових норм, формування гендерної компетентності особового складу з метою викорінювання гендерних стереотипів та формування гендерно нейтральної військової субкультури. Хоча й на сьогодні обов'язки жінок-військовослужбовців лежать здебільшого у сферах служби тилу, командно-штабних (військкомати, фінансові органи), медичних, інженерно-технічних чи виховних структурах, тенденція на егалітарність у системі формування Збройних сил свідчить про те, що в армійському соціальному просторі і надалі будуть поширюватися принципи гендерної рівності.

ЛІТЕРАТУРА:

1. Проневіч О. Інституційно-правові імперативи забезпечення гендерної рівності у секторі оборони. Гендерна політика в умовах воєнного стану: правовий вимір : зб. тез доповідей міжнародної наук.-практ. конф. (Київ, 15 червня 2023 р.). Одеса : Видавництво “Юридика”, 2023. С. 162-168.
2. Актуальні проблеми гендерної політики у Збройних Силах України: навч.-метод. посіб. [В.П. Кроти́ков, В.Л. Топальський, В.М. Малюга та ін.]; за заг. ред. Б.П. Андресюка. К.: НДЦ ГП ЗС України, 2011. 112 с.
3. Практическое руководство по внедрению гендерного подхода / Методология. Обзор по секторам. Сборник примеров из практики. 3-е изд. Братислава: ПРООН, 2007. 295 с.
4. Мірошніченко М.І., Черняхівська В.В. Гендерна політика в державному управлінні України: методологія, теорія, історія : монографія. Київ: Вадекс, 2019. 226 с.
5. Жінки. Мир. Безпека: Інформаційно-навчальний посібник з гендерних аспектів конфліктів для фахівців сектору безпеки / Колектив авторок. Київ, 2017. 264 с. ISBN 978-966-2310-95-5
6. Стожар П. Обов'язковий призов жінок в армію: міжнародний досвід. URL : <https://uain.press/articles/605256-605256> (дата звернення: 14.05.2024).
7. Антаутова В., Лукічов В., Нікітюк Т. Путівник гендерної інтеграції у Збройних Силах України : Формування гендерної компетентності військового професіонала. К., 2020. 236 с.
8. Дискримінація різних соціальних груп у ЗСУ: результати комплексного дослідження березень-квітень 2023. URL : https://nako.org.ua/storage/pdf/2023-06-06--07:30:08-for%20print%20UA%20RG_NAKO_ComprehensiveResearch.pdf (дата звернення: 09.05.2024).
9. Стан реалізації у Збройних Силах України гендерної політики держави : аналіт. звіт за результ. соціол. дослідж. (заключний) / НДЦ ГП ЗС України; викон. О.В. Шевчук, В.С. Михайлов, О.Д. Деточка та ін. К.: 2020. 61 с.
10. Давидюк О.О. Інтеграція жінок до силових структур в Україні: соціологічний вимір. Демографія та соціальна економіка. 2021. №4(46). С. 116-133. DOI: <https://doi.org/10.15407/dse2021.04.116>
11. Крimeць Л.В. Гендерна рівність в контексті формування позитивного іміджу Збройних Сил України. Гендерна політика в умовах воєнного стану: правовий вимір : зб. тез доповідей міжнародної наук.-практ. конф. (Київ, 15 червня 2023 р.). Одеса : Видавництво “Юридика”, 2023. С. 105-108.
12. Тінін Д.Г. Деякі аспекти гендерної рівності у воєнний час: як війна змінює роль жінок у суспільстві. Науковий вісник Ужгородського Національного Університету. Серія Право. 2023. Вип. 80. Ч. 2. С. 432-437. DOI: <https://doi.org/10.24144/2307-3322.2023.80.2.69>
13. Moller B. Conscription and its alternatives. COPRI Working Paper. 1999. №25.
14. Defleur L. B., Warner R. L. Socioeconomic and social-psychological effects of military service on women. J. of Political and Military Sociology. 1985. Vol. 13. P. 195-208.
15. Смуток Б. Жінки в армії: як проходить служба в різних країнах. URL : <https://chas.news/current/zhinki-v-armii-yak-prohodit-sluzhba-v-riznih-krainah> (дата звернення: 15.05.2024).
16. Норвегія та гендерна рівність. Україна до НАТО. URL : <https://ukrainetonato.com.ua/henderna-polityka/norvehiia-ta-henderna-rivnist/> (дата звернення: 26.04.2024).
17. Defense Department Report USA. URL : <https://www.defense.gov/News/Releases/Release/Article/3580676/defense-department-report-shows-decline-in-armed-forces-population-while-percen/> (дата звернення: 30.04.2024).
18. Богданьок О. В Україні зростає число жінок у ЗСУ. URL : <https://suspilne.media/701262-ponad-45-tisac-vijskovosluzbovic-v-ukraini-zrostaе-cislo-zinok-u-zsu/> (дата звернення: 02.05.2024).
19. Гамалій І. Нині на полі бою в Україні ми маємо найбільшу кількість жінок в новітній світовій історії. URL : https://lb.ua/society/2023/11/20/585125_zsu_sluzhat_ponad_62_tis_zhinok_z.html (дата звернення: 18.04.2024).
20. Про внесення змін до деяких законів України щодо забезпечення рівних прав і можливостей жінок і чоловіків під час проходження військової служби у Збройних Силах України та інших військових формуваннях: Закон України від 06.09.2018 №2523-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2523-19#Text> (дата звернення: 23.04.2024).
21. Крimeць Л.В. Порадник з протидії гендерної дискримінації у ЗСУ. К.: НУОУ, 2022. 20 с.

22. Кримець Л.В., Саєнко О.Г., Телелим І.В. Соціально-психологічні аспекти протидії гендерної дискримінації у Збройних Силах України під час війни. Вісник Національного університету оборони України імені Івана Черняхівського. 2022. №4(68). С. 70-79.
23. Компанцева Л.Ф. Гендерна перспектива інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2019. №2. С. 115-125.
24. Гендерна рівність. Національна соціальна сервісна служба України [офіційний сайт]. URL: <https://nssu.gov.ua/genderna-rivnist> (дата звернення: 11.05.2024).
25. Гендерні питання у сфері оборони. Міністерство оборони України [офіційний сайт]. URL: <https://www.mil.gov.ua/diyalnist/genderni-pitannya-u-sferi-bezpeki/> (дата звернення: 18.04.2024).
26. Про військовий обов'язок і військову службу: Закон України від 25.03.1992 №2232-XII. URL : <https://zakon.rada.gov.ua/laws/show/2232-12#Text> (дата звернення: 14.04.2024).
27. Прокопій Д. Гендерна рівність у ЗСУ після повномасштабного вторгнення РФ в Україну. URL : <https://niss.gov.ua/news/komentari-ekspertiv/henderna-rivnist-u-zsu-pislya-povnomasshtabnoho-vtorhnennya-rf-v-ukrayinu> (дата звернення: 15.04.2024).
28. Ніколаєнко А. Жінки на сторожі безпеки: оборонному сектору бракує гендерної рівності. URL : <https://mind.ua/openmind/20253660-zhinki-na-storozhi-bezpeki-oboronnomu-sektoru-brakue-gendernoyi-rivnosti> (дата звернення: 30.04.2024).
29. Грицай І.О. Механізм забезпечення принципу гендерної рівності: теорія та практика: монографія. К.: "Хай-Тек Прес", 2018. 560 с. ISBN 978-966-910-033-7.
30. Хардель Р., Хардель М. Гендерний аспект комплектування сил оборони України особовим складом в умовах воєнного стану. Гендерна політика в умовах воєнного стану: правовий вимір : зб. тез доповідей міжнародної наук.-практ. конф. (Київ, 15 червня 2023 р.). Одеса : Видавництво "Юридика", 2023. С. 162-168.

REFERENCES:

1. Pronevych, O. (2023), "Instytutsiino-pravovi imperatyvy zabezpechennia gendernoi rivnosti u sektori oborony" [Institutional and legal imperatives of ensuring gender equality in the defense sector], *Genderna polityka v umovakh voiennoho stanu: pravovyi vymir : zb. tez dopovidei mizhnarodnoi nauk.-prakt. konf.* (Kyiv, 15 chervnia 2023 r.), Yurydyka, Odessa, pp. 162-168.
2. Krotikov, V.P., Topalskyi, V.L., Maliuha, V.M. ta in., za zah. red. B.P. Andresiuka (2011), "Aktualni problemy gendernoi polityky u Zbroinykh Sylakh Ukrainy: navch.-metod. posib." [Actual problems of gender policy in the Armed Forces of Ukraine], NDTs HP ZS Ukrainy, Kyiv, 112 p.
3. *Praktycheskoe rukovodstvo po vnedrenniu gendernoho podkhoda / Metodolohyia. Obzor po sektoram. Sbornyk prymerov yz praktyky. 3-ye yzd.* Bratislava: PROON, 2007. 295 p.
4. Mirosnichenko, M.I., Cherniakhivska, V.V. (2019), "Genderna polityka v derzhavnomu upravlinni Ukrainy: metodolohiia, teoriia, istoriia", monohrafiia [Gender policy in public administration of Ukraine: methodology, theory, history], Vadeks, Kyiv, 226 p.
5. "Zhinky. Myr. Bezpeka: Informatsiino-navchalnyi posibnyk z gendernykh aspektiv konfliktiv dlia fakhivtsiv sektoru bezpeky" [Women. Peace. Security] / Kolektiv avtorok. Kyiv, 2017. 264 p. ISBN 978-966-2310-95-5.
6. Stozhar, P. Oboviazkovyi pryzov zhinok v armiiu: mizhnarodnyi dosvid" [Compulsory conscription of women into the army: international experience]. URL : <https://uain.press/articles/605256-605256>
7. Antautova, V., Lukichov, V., Nikitiuk, T. (2020), "Putivnyk gendernoi intehratsii u Zbroinykh Sylakh Ukrainy : Formuvannia gendernoi kompetentnosti viiskovoho profesionala [Guide to gender integration in the Armed Forces of Ukraine: Formation of gender competence of a military professional], Kyiv, 236 p.
8. *Dyskryminatsiia riznykh sotsialnykh hrup u ZSU: rezultaty kompleksnoho doslidzhennia berezen-kviten* 2023. URL : https://nako.org.ua/storage/pdf/2023-06-06--07:30:08-for%20print%20UA%20RG_NAKO_ComprehensiveResearch.pdf
9. "Stan realizatsii u Zbroinykh Sylakh Ukrainy gendernoi polityky derzhavy", analit. zvit za rezult. sotsiol. doslidzh. (zakliuchnyi) [State of implementation of the state's gender policy in the Armed Forces of Ukraine] / NDTs HP ZS Ukrainy; vykon. O.V. Shevchuk, V.S. Mykhailov, O.D. Dietochka ta in. Kyiv, 2020, 61 p.
10. Davydiuk, O.O. (2021), "Intehratsiia zhinok do sylovykh struktur v Ukraini: sotsiolohichni vymir" [Integration of women into law enforcement agencies in Ukraine: the sociological dimension], *Demohrafiia ta sotsialna ekonomika*, №4(46), pp. 116-133. DOI: <https://doi.org/10.15407/dse2021.04.116>.

11. Krymets, L.V. (2023), "Genderna rivnist v konteksti formuvannia pozytyvnoho imidzhu Zbroinykh Syl Ukrainy [Gender equality in the context of forming a positive image of the Armed Forces of Ukraine], Genderna polityka v umovakh voiennoho stanu: pravovyi vymir : zb. tez dopovidei mizhnarodnoi nauk.-prakt. konf. (Kyiv, 15 chervnia 2023 r.), Yurydyka, Odesa, pp. 105-108.
12. Tinin, D.H. (2023), "Deiaki aspekty gendernoї rivnosti u voiennoi chas: yak viina zminiue rol zhinok u suspilstvi" [Some Aspects of Gender Equality in Wartime: How War Changes the Role of Women in Society]. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriya Pravo, Vyp. 80, Ch. 2, pp. 432-437. DOI: <https://doi.org/10.24144/2307-3322.2023.80.2.69>.
13. Moller, B. (1999), "Conscription and its alternatives" // COPRI Working Paper, №25.
14. Defleur, L.B., Warner, R.L. (1985), "Socioeconomic and social-psychological effects of military service on women" // J. of Political and Military Sociology. Vol. 13. pp. 195-208.
15. Smutok, B. "Zhinky v armii: yak prokhodyt sluzhba v riznykh krainakh" [Women in the army: how is the service in different countries]. URL : <https://chas.news/current/zhinky-v-armii-yak-prohodit-sluzhba-v-riznih-krainah>
16. Norvehiia ta genderna rivnist. Ukraina do NATO. URL : <https://ukrainetonato.com.ua/henderna-polityka/norvehiia-ta-henderna-rivnist/>
17. Defense Department Report USA. URL : <https://www.defense.gov/News/Releases/Release/Article/3580676/defense-department-report-shows-decline-in-armed-forces-population-while-percen/>
18. Bohdanok, O.V. "Ukraini zrostaie chyslo zhinok u ZSU" [The number of women in the Armed Forces is increasing in Ukraine]. URL : <https://suspilne.media/701262-ponad-45-tisac-vijskovosluzbovic-v-ukraini-zrostaie-cislo-zinok-u-zsu/>
19. Hamalii, I. "Nyni na poli boiu v Ukraini my maiemo naibilshu kilkist zhinok v novitnii svitovii istorii" [Currently, we have the largest number of women on the battlefield in Ukraine in recent world history]. URL : https://lb.ua/society/2023/11/20/585125_zsu_sluzhat_ponad_62_tis_zhinok_z.html.
20. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zabezpechennia rivnykh prav i mozhlyvostei zhinok i cholovikiv pid chas prokhodzhennia viiskovoї sluzhby u Zbroinykh Sylakh Ukrainy ta inshykh viiskovykh formuvanniakh: Zakon Ukrainy vid 06.09.2018 № 2523-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2523-19#Text>
21. Krymets, L.V. (2022), "Poradnyk z protydii gendernoї dyskryminatsii u ZSU" [Adviser on combating gender discrimination in the Armed Forces], NUOU, Kyiv, 20 p.
22. Krymets, L.V., Saienko, O.H., Telelim, I.V. (2022), "Sotsialno-psykholohichni aspekty protydii gendernoї dyskryminatsii u Zbroinykh Sylakh Ukrainy pid chas viiny" [Socio-psychological aspects for elimination of gender discrimination in the Armed Forces of Ukraine during the war], Visnyk Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho, №4 (68), pp. 70-79.
23. Kompantseva L.F. (2019), "Henderna perspektyva informatsiinoї bezpeky" [Gender perspective of information security], Informatsiina bezpeka liudyny, suspilstva, derzhavy, №2, pp. 115-125.
24. Genderna rivnist. Natsionalna sotsialna servisna sluzhba Ukrainy [ofitsiyni sait]. URL: <https://nssu.gov.ua/genderna-rivnist>
25. Genderni pytannia u sferi oborony. Ministerstvo oborony Ukrainy [ofitsiyni sait]. URL: <https://www.mil.gov.ua/diyalnist/genderni-pitannya-u-sferi-bezpeki/>
26. Pro viiskovy oboviazok i viiskovu sluzhbu: Zakon Ukrainy vid 25.03.1992 № 2232-XII. URL : <https://zakon.rada.gov.ua/laws/show/2232-12#Text>
27. Prokopii, D. "Genderna rivnist u ZSU pislia povnomasshtabnoho vtorhnennia RF v Ukrainu" [Gender equality in the Armed Forces after the full-scale invasion of the Russian Federation into Ukraine]. URL : <https://niss.gov.ua/news/komentari-ekspertiv/henderna-rivnist-u-zsu-pislya-povnomasshtabnoho-vtorhnennya-rf-v-ukrayinu>
28. Nikolaenko, A. "Zhinky na storozhi bezpeky: oboronnomu sektoru brakuie gendernoї rivnosti" [Women on guard: the defense sector lacks gender equality]. URL : <https://mind.ua/openmind/20253660-zhinky-na-storozhi-bezpeki-oboronnomu-sektoru-brakue-gendernoyi-rivnosti>
29. Hrytsai, I.O. (2018) "Mekhanizm zabezpechennia pryntsyphu gendernoї rivnosti: teoriia ta praktyka: monohrafiia" [The mechanism for ensuring the principle of gender equality: theory and practice], Khai-Tek Pres, Kyiv, 560 p. ISBN 978-966-910-033-7
30. Khardel, R., Khardel, M. (2023), "Gendernyi aspekt komplektuvannia syl oborony Ukrainy osobovym skladom v umovakh voiennoho stanu" [The gender aspect of staffing the defense forces of Ukraine under martial law], Genderna polityka v umovakh voiennoho stanu: pravovyi vymir: zb. tez dopovidei mizhnarodnoi nauk.-prakt. konf. (Kyiv, 15 chervnia 2023 r.), Yurydyka, Odesa, pp. 162-168.

SOCIO-CULTURAL ANALYSIS OF TRANSFORMATIONS OF THE GENDER STRUCTURE OF THE MILITARY SPHERE: DOMESTIC AND FOREIGN EXPERIENCE

Gender integration both in the field of national security and defense, as well as its global development trends, which depend on the traditions, culture and political priorities of each state are examined in the article. Implementation of the gender equality principle and the mechanism of its provision in the Ukrainian army requires taking into account not only the world experience of military feminization, but also the possibility of its practical application, taking into account the realities of modern war. The socio-cultural approach to the implementation of gender policy in the military sphere involves the achievement of gender parity in accordance with the existing socio-cultural guidelines in society in order to ensure equal conditions for the exercise of rights and opportunities for the armed protection of the state by representatives of both sexes without restrictions associated with rigidly fixed gender roles. Equality between women and men is considered a human rights issue and a necessary condition for Ukraine's full membership in the Alliance, which cannot be achieved without proper representation of various social and gender groups in the power structures. According to the results of the conducted research, it was found that during the military operations since 2014, the gender composition of the Ukrainian army has changed significantly - the number of women in the army has almost tripled, and it continues to increase. There are also positive dynamics regarding gender stereotypes in society, increasing the level of social awareness and gender competence of military personnel. The analysis of the requirements of the normative legal acts proved that women in Ukraine have relatively equal rights and duties, but at the same time certain signs of gender imbalance, characteristic of the Ukrainian society as a whole, remain in the army. In this regard, the efforts of the government and society to form an effective gender policy in the field of defense should be aimed at minimizing the manifestations of discrimination based on gender in the Ukrainian army, which requires the development of effective administrative and legal means to eradicate gender stereotypes, the implementation of relevant legislative initiatives, the search for innovative approaches to the formation and implementation of gender policy in the Armed Forces of Ukraine with the aim of reducing the gap between declarative and real implementation of gender equality and its adaptation in accordance with the specific needs of the defense sector.

Keywords: gender policy, gender equality, discrimination, stereotypes, Armed Forces of Ukraine, feminization, female military personnel, NATO member countries.

Дані про авторів

Адамов Юрій Іванович, начальник науково-дослідного відділу Військової академії, м. Одеса, ORCID: 0000-0002-7355-777X.

Абрамов Станіслав Вікторович, кандидат технічних наук заступник начальника наукового центру Військової академії, м. Одеса, ORCID: 0000-0002-1522-4248.

Банзак Оксана Вікторівна, доктор технічних наук, професор, професор кафедри Електроніки, транспортних технологій та логістики Державного університету інтелектуальних технологій і зв'язку, м. Одеса ORCID: 0000-0002-6649-5013.

Братченко Геннадій Дмитрович, доктор технічних наук, професор провідний науковий співробітник наукового центру Військової академії, м. Одеса, ORCID: 0000-0002-0314-8188.

Власенко Владислав Володимирович, аспірант кафедри телекомунікацій Інституту телекомунікаційних систем Київського політехнічного інституту імені Ігоря Сікорського, ORCID: 0009-0009-4648-5342.

Власенко Олександр Володимирович, ад'юнкт, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, ORCID: 0000-0001-6671-870X.

Габер Антоніна Анатоліївна, кандидат технічних наук, доцент, завідувач кафедри Метрології, якості та стандартизації Державного університету інтелектуальних технологій та зв'язку, м. Одеса, ORCID: 0000-0001-7670-9911.

Гайша Олена Олександрівна, в.о. завідувача кафедри інженерних технологій Міжнародного класичного університету імені Пилипа Орлика, ORCID: 0009-0000-4543-912X, SCOPUS ID – 57202193987.

Гайша Олександр Олександрович, кандидат технічних наук, доцент, доцент кафедри інженерних технологій Міжнародного класичного університету імені Пилипа Орлика, ORCID: 0000-0003-3711-547X, SCOPUS ID – 55338466100.

Германенко Людмила Миколаївна, кандидат економічних наук, доцент, старший науковий співробітник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки, м. Черкаси, ORCID: 0000-0002-6238-6290.

Голушко Сергій Леонідович, ад'юнкт штатний науково-організаційного відділу Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, ORCID: 0000-0003-1585-8504.

Гончарук Антон Антонович, кандидат технічних наук, старший науковий співробітник, начальник наукового центру, Військової академії, м. Одеса, ORCID: 0000-0002-4445-6574

Гришак Олег Миколайович, кандидат технічних наук, доцент, Національний університет оборони України

Джудий Володимир, кандидат технічних наук, доцент, доцент кафедри кібербезпеки Хмельницького національного університету, ORCID: 0000-0003-1878-4301, SCOPUS ID: 57192704936.

Дідик Валентин Олександрович, доктор філософії, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія, м. Одеса, ORCID: 0000-0003-4267-9122.

Дуйловський Андрій Олександрович старший науковий співробітник наукового центру Військової академії, м. Одеса, ORCID: 0009-0008-1155-4080.

Завальнюк Володимир Вікторович, кандидат фізико-математичних наук доцент кафедри Військової академії, м. Одеса, ORCID: 0000-0002-3193-9569.

Король Дмитро Анатолійович, викладач кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військової академії, м. Одеса, ORCID: 0009-0002-1649-3770.

Кривцун Володимир Іванович, кандидат технічних наук, старший науковий співробітник, докторант Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів, ORCID: 0000-0002-3907-5320.

Ленков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-7689-239x, Scopus ID: 58061035100.

Максименко Юрій Анатолійович, кандидат технічних наук, начальник кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія, м. Одеса, ORCID: 0000-0002-1227-2009.

Маміч Віктор Володимирович, кандидат технічних наук, доцент, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія, м. Одеса, ORCID: 0000-0001-5574-0901.

Міночкін Дмитро Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри телекомунікацій Інституту телекомунікаційних систем Київського політехнічного інституту імені Ігоря Сікорського, ORCID: 0000-0003-4988-7098.

Онищенко Олег Анатолійович, доктор технічних наук, професор, професор кафедри технічної експлуатації флоту Національного університету "Одеська морська академія", ORCID: 0000-0002-3766-3188, SCOPUS ID – 57192820689.

Охрамович Михайло Миколайович, кандидат технічних наук, старший дослідник, начальник відділу-заступник начальника управління Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-8776-3937.

Сєлюков Олександр Васильович, доктор технічних наук, професор, Лауреат Державної премії України в галузі науки і техніки, професор аерокосмічної школи Сиянського університету Цзяотун, Сіян, Китай, ORCID: 0000-0001-7979-3434, Scopus ID 57205509194.

Сотніков Євгеній Олегович, науковий співробітник науково-дослідного відділу військово-технічних та інформаційних досліджень науково-дослідного управління інформаційно-психологічних, геоінформаційних, військово-технічних досліджень науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0009-0005-8133-0750.

Субач Ігор Юрійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, ORCID: 0000-0002-9344-713X.

Філюк Євген магістр кафедри кібербезпеки Хмельницького національного університету.

Шаршаткін Данило Юрійович, старший викладач кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія, м. Одеса, ORCID: 0000-0002-3362-2469.

Шинкаренко Ольга Миколаївна, кандидат економічних наук, науковий співробітник Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки м. Черкаси, ORCID: 0000-0002-7621-7017

Алфавітний покажчик

Адамов Ю.І.	17	Гончарук А.А.	47	Міночкін Д.А.	58
Абрамов С.В.	47	Грищак О.М.	82	Онищенко О.А.	27
Банзак О.В.	7	Джулій В.	65	Охрамович М.М.	82
Братченко Г.Д.	47	Дідик В.О.	100	Сєлюков О.В.	7
Власенко В.В.	58	Дуйловський А.О.	47	Сотніков Є.О.	82
Власенко О.В.	107	Завальнюк В.В.	17	Субач І.Ю.	107
Габер А.А.	7	Король Д.А.	100	Філюк Є.В.	65
Гайша О.О.	27	Кривцун В.І.	35	Шаршаткін Д.Ю.	100
Гайша О.О.	27	Лєнков С.В.	7,82	Шинкаренко О.М.	122
Германенко Л.М.	122	Максименко Ю.А.	100		
Голушко С.Л.	35	Маміч В.В.	100		

РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ

ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ «ЗБІРНИКА ВІКНУ»

Редакційна політика «Збірника ВІКНУ» заснована на принципах об'єктивності та неупередженості при відборі статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності при відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

У «Збірнику ВІКНУ» сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах «Збірника ВІКНУ»: <http://miljournals.knu.ua/index.php/zbirnuk>; <http://mil.univ.kiev.ua/page/lib/31>

ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, що вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності:

- керується принципами неупередженості, наукової етики рецензування, захисту – інтелектуальної власності,
- несе відповідальність за рівень наукового наповнення журналу,
- виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;
- залишає за собою право направити рукопис на розгляд сторонньому рецензенту, у тому числі ретельний відбір через «сліпе» рецензування, відхилити статтю або повернути її на доопрацювання;

- може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення,
- має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про даний факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проекту не можуть бути відтворені повністю або частково в будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. При використанні опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

- несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань а також за те, що в матеріалах не міститься інформація з обмеженим доступом;
- повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у даній роботі, якщо вони не були отримані самим автором;
- забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, і бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

УВАГА!

Для авторів статей дещо доопрацьовані вимоги щодо особистих даних.

Ці данні подаються українською та англійською мовами в такій послідовності: Прізвище

Ім'я_

По батькові (за бажанням)_ Науковий ступінь та вчене звання_ Місце роботи та посада_

ORCID 0000-0001-3215-4400

SCOPUS ID 57193059215 (при наявності) Індекс DBLP 10 (при наявності)

e-mail: __ моб.телефон_

Надсилати скановані рисунки, формули та таблиці не допускається.

Вся стаття оформлюється одним шрифтом **Times New Roman** вказаними нижче розмірами, зверніть увагу на формули, таблиці та рисунки.

РЕДАКЦІЙНА КОЛЕГІЯ «ЗБІРНИКА ВІКНУ» ЗДІЙСНЮЄ НЕЗАЛЕЖНЕ («СЛІПЕ») ЕКСПЕРТНЕ РЕЦЕНЗУВАННЯ НАДАНИХ ДО ДРУКУ РУКОПИСІВ ТА ПЕРЕВІРКУ ЇХ НА ПЛАГІАТ. РЕЦЕНЗУВАННЯ ЗДІЙСНЮЄТЬСЯ ЗА АНОНІМНОЮ ФОРМОЮ ЯК ДЛЯ АВТОРІВ, ТАК І ДЛЯ РЕЦЕНЗЕНТІВ.

ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

Загальні вимоги до технічного оформлення статей:

Обсяг рукопису - рекомендується не менше 12 повних аркушів українською або англійською мовами.

Формат аркуша - **A4 (210 x 297 мм)**.

Розмір полів: верхнє, нижнє, праве, ліве - **2 см**.

Шрифт тексту - **Times New Roman №12**, через міжрядковий інтервал - **1,0**.

Абзац має становити **10 мм**.

Стаття повинна мати такі необхідні елементи:

УДК;

назва статті, яка лаконічно відображає зміст та новизну статті;

анотація та ключові слова;

вступ та постановка задачі чи проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано **розв'язання даної проблеми** і на які спирається автор, визначення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання мети статті;

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

висновки з даного дослідження і перспективи подальшого розвитку у даному напрямку.

список літератури,

References,

дані про авторів двома мовами.

Анотація до статті виконується українською та англійською мовами загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова.

Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (5–7 термінів).

Список літератури (References) повинен включати не менш 12 джерел, з яких 50 % видані за останні 10 років. При цьому не менш 25 % джерел повинно відноситися до іноземної періодики. Самоцитування авторів у списку літератури повинно бути, як правило, не більш за 25 %.

Якщо основною мовою статті є українська, то оформлюються два списки літератури: перший (список літератури мовою оригіналу джерела) – згідно наказу МОН від 12.01.2017 № 40 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН від 12.01.2017 № 40 та міжнародного Гарвардського стилю BSI (British Standards Institution).

На адресу редколегії (03022, м. Київ, вул. Ю. Здановської, 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:

експертний висновок, про можливість відкритого публікування, завірений печаткою, сканкопія надсилається на е-[mail: lenkov_s@ukr.net](mailto:lenkov_s@ukr.net)

Відомості про авторів див. на стор.150. Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

– запис завжди починається з прізвища автора, потім, через кому, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються «and» без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлено «and» без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводять у "лапках";

– назва журналу або книги завжди виділяється курсивом;

- ім'я видавця вказується перед місцем видання;
- коми використовують для поділу елементів запису;
- для джерел українською або російською мовою, що наводяться у References, назви статей журналів, глав в книгах наводять латиницею (транслітерацією) у "лапках" та перекладом на англійську мову у квадратних дужках. Онлайн-конвертер з української мови для транслітерації: <http://translit.kh.ua/?passport>.

Приклади оформлення References за стилем Harvard British Standards Institution

Книга (ДСТУ 8302:2015)

Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х. : Вид. Рожко С.Г., 2017. 276 с.

Книга (Harvard style BSI)

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "Informatsiino-psykholohichna borotba u voiennii sferi: monohrafiia" [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

Стаття із періодичного видання (ДСТУ 8302:2015)

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75–78.

Стаття із періодичного видання (Harvard style BSI)

Karpenko, D.V. (2017), "Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75–78.

Дисертація (ДСТУ 8302:2015)

Белозеров, І.В. Религиозная политика: дис. ... канд. ист. наук: 07.00.02; захищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

Дисертація (Harvard style BSI)

Belozerov, I.V. (2002), "Relyhyoznaia polytyka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7–15. Режим доступа до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7–15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution можна знайти на сайті *Національної бібліотеки України імені В.І. Вернадського* та онлайн генератора посилань *Cite This For Me*.

Редакційна колегія: e-mail: lenkov_s@ukr.net

Шрифт

СХЕМА ОФОРМЛЕННЯ СТАТЕЙ У «ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ВІКНУ»

УДК

науковий ступінь, вчене звання

ініціали та прізвище автора (співавторів)

Місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. Степанов С.В. (ВІКНУ)

к.т.н., с.н.с. Українець О.В. (ВІКНУ)

к.т.н. Саленко В.Д. (ВІКНУ)

12 пт

жирний

КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ ЖЕСТІВ

Анотація до статті виконується українською та англійською мовами (загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова).

11 пт

курсив,
жирний

Для керування електронними пристроями, для сучасного користувача важливими критеріями є такі, як: зручність та простота керування. Для того щоб надати користувачу такі можливості та зручності в використанні, є досить доцільною розробка системи, яка б надавала такі можливості. Керування системою, яка працює на основі жестів, є надзвичайно перспективним, та може суттєво полегшити користувачу роботу з нею, тому що, жести які потрібні для керування системою, можуть бути інтуїтивно зрозумілими користувачу, порівняно з іншими системами які працюють за допомогою комбінацій клавіш.

Для вирішення задач керування за допомогою жестів, пропонується програмно-апаратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу виконує відповідну роль в системі, наприклад знаходить точку інтересу з множини чи вираховує глибину сцени. Також в системі є ядро, яке відповідає за аналіз модифікаторів та жестів. На основі даних модулів стає можливо створити систему, яка б працювала на основі жестів. Але для створення даної системи, потрібно вирішити певні задачі, такі як: сегментація, скелетизація, спостереження. Кожна з яких містить в собі відповідні математичні моделі та визначення. Запропонований програмно-апаратний комплекс для керування природними жестами. Суть програмно-апаратного комплексу полягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував роботу знаходячись частково віддалено від робочого місця, чи маніпулював інструментами на відстані, тобто за допомогою жестів. Використання запропонованого програмно-апаратного комплексу дозволить покращити показники стерильності в операційних, підвищити технічну безпеку під час виконання безпосередньої роботи користувача з приладами.

Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, точка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, спостереження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ

12 пт

НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ: вступ та постановка проблеми (задачі) у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями; аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується дана стаття, формулювання цілей статті (постановка завдання), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів; їх практичного значення та результатів експерименту чи впровадження; висновки з даного дослідження і перспективи подальших досліджень у даному напрямку. Література. References.

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно розміщувати по центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт – **Times New**

Roman № 12). Рисунки повинні бути виконані за допомогою редактора Word, згруповані і являти собою один графічний об'єкт. Формули та позначення по тексту обов'язково набирати за допомогою Equation Editor - редактора формул Word, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний

12 pt, великі індекси – **10 pt**, малі індекси – **7 pt**, великі символи – **14 pt**, малі символи

10 pt: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт Times New Roman, для решти стилів – шрифт Symbol, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно наказу МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 пт

ЗРАЗОК

1. Ленков С.В., Толлок І.В., Цицарев В.М., Ленков Є.С. Моделювання процесів витрачання та поповнення ресурсу угруповання технічних об'єктів. Системи озброєння і військова техніка. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Ленков Є.С., Цицарев В.М., Проценко Я.М. Моделювання процесу відмов об'єктів, що відновлюються з ієрархічною конструктивною структурою. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

11 пт

ЗРАЗОК

1. Lienkov, S.V., Tolok, I.V., Tsytsarev, V.N. and Lenkov, Ye.S. (2018), "Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv" [Modeling of processes of expenditure and resource replenishment grouping of technical objects], Systems of Arms and Military Equipment, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Lenkov, Ye.S., Sytsarev, V.M. and Prochenko, Ya.M. (2017), "Modeljuvannja procesu vidmov ob'ektiv, shho vidnovljujut'sja z ierarhichnoju konstruktivnoju strukturoju" [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 55, pp. 30-39

For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene. Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.

Keywords: artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.

Дані про авторів див.стор.150

ЗРАЗОК

11 пт

Степанов Сергій Вікторович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1202-6512-1234, ORCID ID 0000-0001-3215-4400, SCOPUS ID 57193059215 (при наявності), індекс DBLP 10 (при наявності), e-mail:stepanov@ukr.net, тел. 068 652 26 62.

Українець Олексій Васильович, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1204-6512-1235, ukr@ukr.net, 073 556 6776. SCOPUS ID 57193059215 (при наявності), індекс DBLP 10 (при наявності), e-mail:stepanov@ukr.net, тел. 068 652 26 62.

Саленко Володимир Дмитрович, кандидат технічних наук, науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1201-6512-1236, salenko@ukr.net, 0938763423. SCOPUS ID 57193059215 (при наявності), індекс DBLP 10 (при наявності), e-mail:stepanov@ukr.net, тел. 068 652 26 62.

Stepanov Sergij, doctor of technical sciences, professor, Chief Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine)

Ukrainets Oleksij, candidate of Technical Sciences, Senior Researcher, Leading Researcher of the Military Institute of Kyiv National Taras Shevchenko University (Kiev, Ukraine)

Salenko Volodymyr, candidate of engineering sciences, Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine).

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

**Київського національного університету імені
Тараса Шевченка**

№ 83

Усі матеріали надруковані в авторській редакції

Підписано до друку 20.09.2024 р.
Авт. друк. арк. 9,25. Формат 60х90/8
Безкоштовно. Замовлення № 3-24.

Надруковано у навчальному тренувальному комплексі ВІКНУ 03189,

Київ, вул. Ю. Здановської, 81

т. 521-32-89