ISSN 2524-0056(Print)
ISSN 2519-481X(Online)

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Виходить 4 рази на рік

№ 74

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 – 2022

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2022. № 74. 172 с.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень та 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 3.02.22р., протокол №11.

Відповідальні за макет:
Ряба Л.О., Солодєєва Л.В.

Адреса редакції: 03189, м. Київ, вул. Ломоносова,81 тел./факс +38 (044) 521 – 33 – 82
Наклад 300 прим.
Ел.адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: http://miljournals.knu.ua/

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ТЕХНІЧНІ НАУКИ
(оформлені за вимогою Web of Science та Scopus)

ЗАГАЛЬНІ ПИТАННЯ

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

INFORMATION TECHNOLOGIES

TECHNICAL SCIENCES
(required by Web of Science and Scopus)

GENERAL QUESTIONS

UDC 531:535

D.Sci. Tech. **Banzak O.V.** (SUITC)
D.Sci. Tech. **Sieliykov O.V.** (KNUCA)
PhD **Gaber A.A.** (SUITC)
Konovalenko O.I. (m/b A 3814)
Vozikova L.M. (SUITC)

DOI: https://doi.org/10.17721/2519-481X/2022/74-01

RESEARCH OF PHYSICAL PROCESSES AND DEVELOPMENT OF METHODS FOR RADIATION MODIFICATION PARAMETERS OF SEMICONDUCTOR OPTOELECTRONICS DEVICES

Operation of solid-state electronics products in the field of ionizing radiation can significantly change their properties, contributing to their premature destruction or loss of technical characteristics necessary for normal operation of the equipment. The changes observed in this case are caused by a number of specific processes discussed above. Distinguish between reversible and irreversible changes.

Irreversible (residual) include radiation changes that remain partially or completely after the termination of exposure. The magnitude of radiation changes is determined by the amount of energy absorbed by materials when interacting with radiation, as well as the rate at which this energy is transferred to them. It depends on the type of radiation and its parameters (energy spectrum, flux density, intensity, etc.), as well as on the nuclear-physical characteristics of materials.

Criteria for the radiation resistance of photodetectors. The criterion for the parametric reliability of photodetectors is formulated on the basis that the object under consideration degrades its parameters gradually, both with an increase in the duration of exposure and the dose of radiation. The purpose of the photodetectors, the imposed restrictions on the criterion of their performance, as well as the physics of the effect of radiation, allow us to consider photodetectors as an object functioning under noise conditions. This allows statistical analysis methods to be applied. With this approach, we can use a well-studied mathematical apparatus for testing statistical hypotheses. Three criteria of radiation resistance of photodetectors are proposed. The first is the signal-to-noise ratio in the interpretation of sufficient statistics, the second is the criterion for the average detection error (Kotelnikov's criterion), and the third is the Bayesian risk criterion. This article examines the physical processes and the development of methods for radiation modification of the parameters of semiconductor optoelectronic devices.

Keywords: solid-state electronics, radiation changes, statistical methods of analysis, photodetectors

Introduction. At present, practically all branches of industry, many branches of science use sources of ionizing radiation (IR). Nuclear power plants, gamma plants of various capacities, flaw detectors, counters and many other equipment are widely used in the defense complex, medicine, agriculture. However, the most important sector of the use of IR in Ukraine after the elimination of nuclear combat potential is nuclear power [1]. The country has five nuclear power plants (NPP) with reactors of two types, which generate about 40% of the country's total electricity [2].

In this regard, the problems of dosimetry, which today have become an independent scientific and technical area of nuclear physics, are acquiring ever increasing importance. Dosimetry, in its essence, solves the problem of linking physical quantities with the expected radiation effects of use IR. The main task of dosimetry - the identification sources of radiation, posing a threat to the environment and humans - today is solved using a variety of technical registration tools with varying degrees of efficiency. A comparative analysis of such means and methods of their application for registration and dosimetry is presented in this section [3]. In addition, the existing variety of terms and values in this industry requires some clarification in order to ensure the reliability of presented research results.

Analysis of previous studies. The level of development and application of radiation 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 of them was marked by the emergence of various devices that register and measure the parameters of ionizing radiation: gas-discharge counters, scintillators, semiconductor detectors, and others. Their appearance and further widespread use was provided in the past by works from Crookes, Rutherford, Geiger and Müller to the works which are closer to us in time Dmitriev A.B., Perelman S.N., Tchaikovsky V.G. and Baranov V.G., Golbek G.R., Nemirovsky B.V., Yakubovich A.L. and many others. The basis for the progress of nuclear instrumentation was the simultaneous development of two areas - nuclear physics research and electronics. However, both directions at that time developed independently, without proper mutual connection.

The advent of modern semiconductor sensors for the first time linked nuclear instrumentation and electronics into a single complex - semiconductor detector. It combines semiconductor primary converter of ionizing radiation (sensor), secondary converter of information from the sensor (electronics) and software for processing this information, interconnected in terms of the problem being solved and parameters. The possibility of appearance such a complex is provided in materials science by the works of Vavilov V.S., Baransky P.I., in applied nuclear physics research - Maksimov M.V., Maslov O.V. and others. In these works, a technique was shown for the selection of semiconductor materials and a design of sensors was proposed, directions for the creation of electronics and computer programs for detectors were determined. This ensured the creation and effective use of semiconductor detectors in dosimetry, radiation control of materials and technological processes of nuclear power plants.

However, the development of nuclear energy, spread nuclear technologies have put forward new requirements for the control and metrology of ionizing radiation. The modern level of nuclear instrumentation cannot fully satisfy them. The solution to this problem can be provided by the development of: methods for choosing the optimal type of semiconductor materials and controlling their properties to create uncooled detectors; sensors with higher resolution; electronics with less noise; computer methods and information processing programs with lower estimated costs; control systems for nuclear materials and the state of NPP protective barriers that meet the requirements of the existing automatic control of radiation safety (ACR).

Main part. The problem of detecting a signal in noise is reduced to a particular algorithm for testing the hypothesis H_I of the presence of a signal in the noise $U_{ш}^{\Sigma}$ against a simple alternative H_0 - only noise $U_{ш}^{0}$ is present.

Under conditions of ionizing radiation, the total output noise $U_{ш}$ is an additive mixture of all noise sources arising in the circuits of photodetectors, which leads to a difference in dispersions $U_{ш}^{\Sigma}$ and $U_{ш}^{0}$. This is due to the influence of radiation, which changes not only the noise level, but also the characteristics of semiconductor devices, which in turn leads to additional noise.

Photodetectors based on $Cd_{1-x}Hg_xTe$ solid solutions (CHT). Photodetectors based on solid solutions have found wide application for the spectrum range of 8-14 μm, which, in contrast to photodetectors based on impurity germanium or silicon, can provide high sensitivity at T = 80 K.

The main parameter of photodetectors is the detectivity at maximum spectral sensitivity $\lambda_{\max}$:

$$D^*_{\lambda_{\max}} = S_i\left(\lambda_{\max}\right)\cdot A^{\frac{1}{2}}\cdot i_{ш}^{-1} \quad , \tag{1}$$

where $S_i\left(\lambda_{\max}\right)$ – is current sensitivity at $\lambda_{\max}$; $i_{ш}$ - noise current in a single frequency band; A - is sensitive surface area.

The maximum achievable value of detectivity is determined by the dominant noise of the photodetector. In ideal photodetectors, the detectivity is limited by radiation fluctuations (LM mode). To ensure LM mode, it is necessary to reduce the level of excess noise to a minimum by improving the technology and generation-recombination noise caused by thermal radiation. The LM mode will be achieved in the case of predominance the generation-recombination noise caused by optical excitation (from the background) over all other noises.

For an *n*-type CHT material with x=0.2 and with an electron density close to its own, the lifetime of charge carriers at T=77 K, and limiting background illumination, it is possible to achieve detectability values

$$D^* = 2.2 \cdot 10^{12} \cdot \eta, \text{ sm·Hz}^{1/2}\text{·Wt}^{-1} \quad , \tag{2}$$

where η - is the quantum efficiency at $\lambda = 10$mkm.

The implementation of photodetectors (PD) based on CHT is associated with the development of three areas: the creation of photoresistors, photodiodes, and MDP-structures. Photodiode radiation receivers are used mainly for receiving short pulses $\tau_{imp} \prec 10^{-9} \div 10^{-8}\ s$, and MDP-structures are used for receiving IR-images in the time delay and accumulation mode (CCD-receivers). The most widespread are photoresistor receivers based on CHT of the electronic type of conductivity (table 1).

Table 1

Parameters of photoresistive receivers based on CHT (T = 77 K)

Spectral range, Δλ, mkm	Photoresistor resistance, R_T, Om	Detectivity, D^*, $\text{sm·Hz}^{1/2}\text{·Wt}^{-1}$	Threshold sensitivity in heterodyne mode, P_{thr}, Wt·Hz^{-1}	Inertia, t, c
9,5 ÷ 12	22 – 110	$(3,9 \div 9) \cdot 10^{10}$	-	$1,6 \cdot 10^{-6}$
10,5	-	$3 \cdot 10^{10}$	-	-
3 ÷ 15	До 10^3	$(0,1 \div 6) \cdot 10^{10}$	-	$4 \cdot 10^{-6}$
8 ÷ 14	-	$5 \cdot 10^{10}$	-	$1 \cdot 10^{-8}$
10,6	200 ÷ 400	-	$7 \cdot 10^{-20}$	$(0,5 \div 2,5) \cdot 10^{-7}$

Model of the mechanism radiation modification photoresistors.

The results of radiation action on photosensitive elements based on this solid solution can be estimated from changes in the photoresponse signal [4-6]. For a photoresistor in idle mode, when the load resistance is much greater than the resistance of photoresistor, and small signals in a semiconductor with an electronic type of conductivity, photoresponse is determined by the formula:

$$\frac{\Delta U}{U} = \frac{\Delta \sigma}{\sigma_T} = \frac{G\left(\tau_n \mu_n + \tau_p \mu_p\right)}{n_T \mu_n} \ , \tag{3}$$

where U - is offset on the photodetector; ΔU - voltage change at the photodetector when it is illuminated; σ_T - dark electrical conductivity of the semiconductor; $\Delta\sigma$ - photoconductivity; G - the rate of generation charge carriers; n_T - is dark concentration of electrons; τ_n, τ_p, μ_n, μ_p - are the lifetime and mobility of electrons and holes, respectively.

For CHT $\mu_n \succ\succ \mu_p$, therefore (3) will take the form:

$$\Delta U = \frac{G\tau U}{n_T} \cdot \tag{4}$$

As follows from (4), the signal taken from the photoresistor is proportional to the bias. This is true for the value $U_n \approx \frac{\ell^2}{\tau\mu_p}$ (ℓ - distance between the contacts), at which the conditions for the passage of minor charge carriers through the photoresistor are realized. At $U \succ\succ U_n$, the signal voltage saturates and does not depend on the offset value:

$$\Delta U = \frac{G\ell^2}{n_T \mu_p} \cdot \tag{5}$$

The lifetime of charge carriers is determined by the recombination mechanism and in narrow-gap semiconductors, which include CHT, depends on the carrier concentration. In this material, the Auger recombination mechanism dominates, and the lifetime is [7, 8]:

$$\tau_{A_0} = 4\tau_i \left(\frac{n_i}{n}\right)^2, \tag{6}$$

where τ_i, n_i - are the lifetime and concentration of charge carriers in the intrinsic material ($Cd_{0,2}Hg_{0,8}Te$ $\tau_i = 3{,}3\cdot 10^{-4}$ s, $n_i = 3\cdot 10^{13}$ sm^{-3} at 80 K); $\tau_{ШР}$ - the actual value of concentration.

In an irradiated material, the lifetime changes:

$$\tau_A = 4\tau_i n_i^2 \left(n_0 + \frac{dn}{dF} F\right)^{-2},$$

where n_0 - is the initial value of carrier concentration in sample; $\frac{dn}{dF}$ - average rate of introduction of carriers during irradiation; F - integral flux of ionizing radiation.

Comparison (4) - (6) shows that of the two operating modes of photoresistor, from the point of view of radiation resistance, the minority carrier transit mode is preferable.

The relative change in voltage across the photoresistor in the latter case is [9]:

$$\frac{\Delta U}{\Delta U_0} = n_0^3 \left(n_0 + \frac{dn}{dF} F\right)^{-3} \cdot \tag{7}$$

When irradiated $n - Cd_{0,2}Hg_{0,8}Te$ ($n_0 = 1\cdot 10^{15}\ sm^{-3}$) by electrons with an energy of 5MeV with an integral flux $F = 1\cdot 10^{14}\ sm^{-2}$, it was found that at 80 K $\frac{dn}{dF}$ =6,3 sm^{-1} [10]. Substituting

these values into (7), we obtain that $\frac{\Delta U}{\Delta U_0} = 0{,}35$, and in the transit mode of minority carriers, signal change under the same conditions is half as much.

In samples $n-Cd_{0,2}Hg_{0,8}Te$ irradiated with fission neutrons at 80 K, lifetime of charge carriers is limited by the simultaneous action of Auger recombination and Shockley-Read recombination mechanisms. The dose dependence of the lifetime $\tau_{ШР}$ during Shockley-Read recombination is determined by a semi-empirical expression:

$$\tau^{-1} = \tau_0^{-1} + K_\tau \cdot F\,, \tag{8}$$

where "0" is an index referring to the value of parameter before irradiation; K_τ - coefficient of radiative change in the lifetime of minor charge carriers.

The relative change in the signal caused by ionizing radiation, taking into account (4), will take the form:

$$\frac{\Delta U}{\Delta U_0} = \tau \cdot n_0 \cdot \tau_0^{-1} \cdot n^{-1}. \tag{9}$$

For the mode of flight of minority carriers at $K_\tau = 3{,}5 \cdot 10^{-9}$ sm^2/neutron.·s, $F = 10^{14}$ sm^2/neutron and $\frac{dn}{dF} = 3$ sm^{-1} experimentally determined during irradiation with fission neutrons, we obtain $\frac{\Delta U}{\Delta U_0} = 0{,}83$ [11].

It should be borne in mind that for the above estimates of changes in the parameters photoresistor, data on changes in the bulk properties of an ideal semiconductor material are used. Any real semiconductor contains impurities and violations of the crystal structure. The general theory describing their influence on the concentration, mobility and lifetime of charge carriers, i.e. on the physical characteristics that determine the main parameters of photoresistors, with the simultaneous introduction of radiation defects, has not yet been created. Therefore, prediction of radiation resistance, taking into account impurities and defects, is possible only for materials in which the nature of impurities (defects), the energy levels created by them, their effect on the physical properties of a substance, and also change in these properties under the action of ionizing radiation have been experimentally established. The complexity of such a task makes it necessary to evaluate the radiation resistance of photodetectors on the basis of statistical methods of analysis.

Radiation control of photoresistors. Irradiation with fast electrons.

The irradiation of these devices with fast electrons $Cd_{0,2}Hg_{0,8}Te$ and the measurement of their parameters were carried out under the conditions described earlier. Photoresistors based on before and after irradiation were studied. In this case, the dark current I_{T_0} and resistance R_{T_0} were considered at the supply voltage U.

Analysis of the data obtained allows us to conclude:

- electron irradiation with doses of 10^{13}-10^{16} sm^{-2} leads to a decrease in dark resistance and an increase in dark current;
- relative change of these parameters is greater with decreasing temperature;
- for irradiation doses greater than 10^{15} sm^{-2}, the rate of relative change in parameters of photoresistors decreases.

The noted changes in the parameters can be explained by the formation of traditional donor-type defects in the material $Cd-Hg-Te$, as a result of which the concentration of free electrons[2,4].

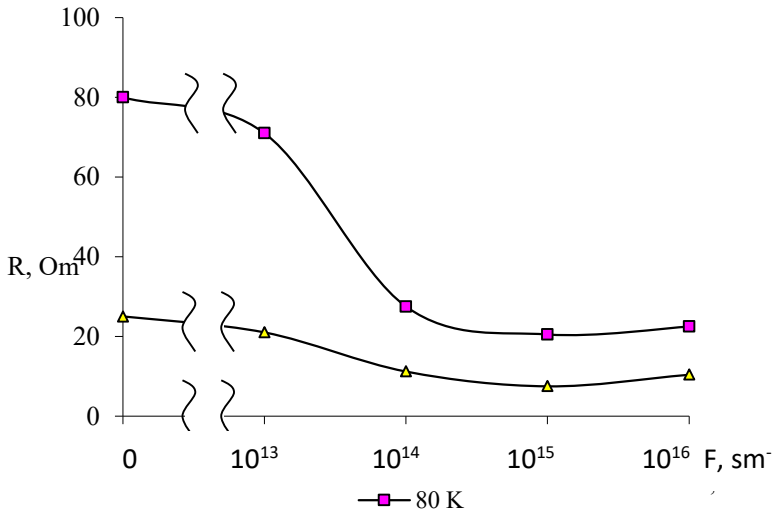

Figura 1 – Dependence of the dark resistance photoresistor on dose of electron irradiation

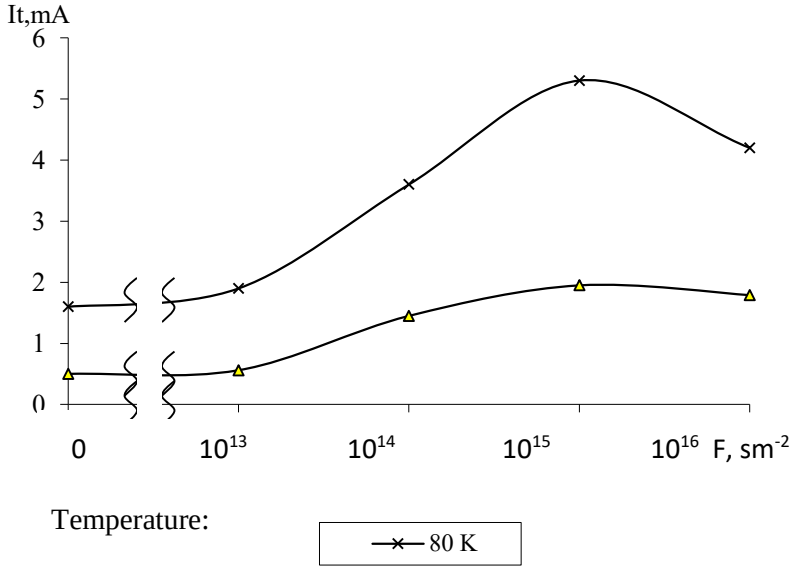

Figura 2 – Dependence of the dark current photoresistors on dose of electron irradiation

The number of such defects is predetermined by the number of mercury vacancies in the interstices of CHT-crystal lattice. Therefore, change in concentration of charge carriers introduced by irradiation, and hence the value of dark resistance, are limited by the concentration of mercury vacancies.

To clarify the mechanisms of degradation properties IR-photoresistors, the influence of ionizing radiation various types on parameters of a single-crystal compound $Cd_{0,2}Hg_{0,8}Te$, on the basis of which they are made, was studied.

Irradiation with gamma quanta.

Features of the photoresistor production technology do not allow achieving full compliance of the parameters of photosensitive elements (dark and light resistance, slope of the lux-ohmic

characteristic, inertia) with the specified values. About 20-30% of the assembled devices do not meet the technical specifications. In this regard, the search for ways to adjust the parameters of devices to these standards is relevant. For this purpose, the effect of gamma irradiation Co^{60} on the main parameters of photoresistors based on CHT was studied. In this case, radiation doping is used as a method for the controlled introduction of defects responsible for the photosensitivity of the material.

Gamma irradiation was chosen by the authors as the most promising for these purposes due to its high penetrating power. This makes it possible to simultaneously irradiate a large number of photoresistors, does not induce residual radiation, and can change the concentration and energy spectrum of local centers. The dose rate of gamma radiation acting on the photoresistors was chosen to be 1000–6000 rad/s (E = 1.7 MeV), and the exponential dose varied from 10^4 to 10^{10} rad. The temperature of the photoresistors during irradiation did not exceed 30^0C, which was achieved by forced air blowing. It was found that the parameters R_T, $R_{св}$, $tg\alpha$, $\tau_н$, τ_{sm} were the most sensitive to gamma radiation.

Lux-ohmic characteristics of photoresistors after gamma irradiation are shown in fig. 2. It can be seen from it that parameters of the photoresistor change even at a dose of Co^{60} rad. Simultaneously with the decrease R_T, there is a decrease $R_{св}$. However, the relative change $\frac{1}{R_{св}}$ in magnitude predominates. This indicates an increase in the photosensitivity of devices as the dose is accumulated [11, 12]. In this case, a non-linear decrease in the relative changes in and occurs R_T and $R_{св}$ a tendency to saturation is observed.

The initial rate of change is proportional to the intensity of gamma irradiation. Its influence on the slope of the lux-ohmic characteristic $tg\alpha$ is described by the formula:

$$tg\alpha = \frac{\ell gR_1 - \ell gR_2}{\ell gE_1 - \ell gE_2}, \qquad (10)$$

where R_1 and R_2 - are the resistances at illumination E_1 and E_2, respectively.

The change in this parameter begins with a dose of $5 \cdot 10^4$ rad. Annealing at a temperature of 40-45 ^{0}C for 40-45 hours leads to (15-20)% restoration of parameters, as well as natural aging within 120-150 hours after the cessation of radiation.

Injection laser and light emitting diodes based on A_3B_5 compounds. The current-voltage characteristic of such devices is the most informative. Its form is determined by such important parameters of the diode as the contact potential difference and the resistance of high-resistance region, which is most sensitive to external influences. The slope of the current-voltage characteristic plotted in coordinates determines the mechanism of charge carrier scattering. By the nature of its change, one can judge the mechanism of effect irradiation on properties of source material and the device itself.

Laser diodes based on indium-gallium-arsenic-phosphorus solid solution are a new type of devices. There is no information in the literature about the effect of irradiation on their properties. In the work of the authors, irradiation with electrons with an energy of 2.4 MeV was carried out with doses from 1013 to 1015 cm-2. Studies have shown that as the dose increases at fixed voltages, the current through the diodes increases.

The following procedure was used to determine the threshold voltages of laser diodes.

On the graph of the dependence of the voltage of the photodiode - the laser radiation receiver - on the voltage of the rectangular pulse generator, we draw two straight lines: the first is tangent at the starting point, and the second coincides with the linear section.

The threshold voltages of the diodes obtained by this method lie in the range from 4.5 to 5.5 V and did not change during electron irradiation with doses from 10^{13} to 10^{15} sm^{-2}.

Thus, based on the results of studying the effect of irradiation with electrons with an energy of 2.4 MeV on the characteristics of laser diodes based on a quaternary solid solution of indium-gallium-

arsenic-phosphorus and LED based on gallium phosphide, the following conclusions can be drawn [13, 14]:

1. Treatment with doses from 10^{13} to 10^{15} sm^{-2} reduces the resistance of the diodes and changes the slope of the current-voltage characteristic (in a semi-logarithmic scale) from 2.49 to 2.11.

2. The threshold voltage of laser radiation generation does not change under electron irradiation with doses from 10^{13} to 10^{15} sm^{-2}.

Conclusions. 1. Irradiation with low doses of electrons leads to the following effects in transistors based on epitaxial silicon layers: there is a tendency to increase the breakdown voltage, shape of breakdown region changes; the gain is reduced by approximately 5-15%.

2. Radiation processing by fast electrons of integrated temperature sensors leads to an increase in the modulus of the voltage temperature coefficient, and, consequently, to an increase in their sensitivity. The technology of radiation processing by fast electrons in order to increase TKU consists in irradiating temperature sensors on the linear electron accelerator ELU-4.

3. The radiation resistance of microassemblies treated with fast neutrons is higher (10^{16} sm^{-2}) compared to their resistance when treated with fast electrons (10^{15} sm^{-2}). The radiation resistance of microassemblies is determined by: a small change in the main parameters (with the exception of U_{cm}) ; changing the on and off currents of the output transistor; a decrease in transfer coefficient of the base current; high radiation resistance of operational amplifiers (op-amps) included in the assembly.

The difference in the radiation resistance of microassemblies when irradiated with fast electrons and fast neutrons is explained by the fact that action of electrons is accompanied by heating of the product, due to their deceleration in the structural elements.

4. Irradiation of photodetectors based on MCT changes their characteristics: threshold sensitivity (to increase it, it is necessary to decrease the concentration of the main charge carriers and increase the quantum efficiency), inertia (to reduce it, it is necessary to reduce the lifetime of charge carriers) and the region of spectral sensitivity of photodetector.

5. Electron irradiation with an energy of 2.4 MeV laser diodes based on a quaternary solid solution of indium-gallium-arsenic-phosphorus and LEDs based on gallium phosphide showed that treatment with doses from 10^{13} at 10^{15} sm^{-2} reduces the resistance of the diodes and changes the slope of current-voltage characteristic (on a semi-log scale) from 2.49 to 2.11. The threshold voltage of laser radiation generation does not change under electron irradiation with doses from 10^{13} до $10^{15} sm^{2}$.

These physical results were unexpected, since it was known that the irradiation of gallium arsenide diode lasers with high-energy electrons leads to a deterioration in their properties, the restoration of which was observed only after prolonged heating to 400-450^{0}C.

REFERENCTS:

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 OV New generation semiconductor detectors for radiation monitoring and dosimetry of ionizing radiation / O.V. Banzak, O.V. Maslov, V.A. Mokritsky. - Monograph. - Odessa, 2013. - Publishing house "VMV". - 220 p.

5. Bouchet J.M. PWR primary flow masurements 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., Maslov O.V., Bansak O.V. Methods and means controls of nuclear materials and state of protective barriers at nuclear power plants // Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. - К .: MIKNU, 2019. - № 63. – С. 66 – 72.

14. Mokritskij V.A., Maslov O.V., Banzak O.V. The detector on basis of CdZnTe-gauge for systems radiating-technological control // Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. - К .: MIKNU, 2018. - № 58. - С. 68-73.

д.т.н., проф. Банзак О.В., д.т.н., проф. Сєлюков О.В.,
к.т.н., доц. Габер А.А., Коноваленко О.І., Возікова Л.М.

ДОСЛІДЖЕННЯ ФІЗИЧНИХ ПРОЦЕСІВ І РОЗРОБКА МЕТОДІВ РАДІАЦІЙНОЇ МОДИФІКАЦІЇ ПАРАМЕТРІВ НАПІВПРОВІДНИКОВИХ ПРИЛАДІВ ОПТОЕЛЕКТРОНІКИ

Експлуатація виробів твердотільної електроніки в полі іонізуючих випромінювань може істотно змінювати їх властивості, сприяючи передчасному руйнуванню або втраті необхідних для нормальної роботи апаратури технічних характеристик. Спостерігаються у своїй зміни або зумовлюються низкою специфічних процесів, розглянутих вище. Розрізняють оборотні та незворотні зміни. До необоротних (залишкових) відносять радіаційні зміни, що зберігаються частково або повністю після припинення опромінення. Величина радіаційних змін визначається кількістю енергії, що поглинається матеріалами при взаємодії з випромінюванням, а також швидкістю, з якою ця енергія передається. Вона залежить від виду випромінювання та його параметрів (енергетичного спектра, щільності потоку, інтенсивності та ін.), а також від ядерно-фізичних характеристик матеріалів. Критерії радіаційної стійкості пристроїв, що фотоприймають. Критерій параметричної надійності пристроїв, що фотоприймають сформульований, виходячи з того, що об'єкт, що розглядається, погіршує свої параметри поступово як при збільшенні тривалості впливу, так і дози випромінювання. Призначення пристроїв, що фотоприймають, обмеження, що накладаються на критерій їх працездатності, а також фізика впливу радіації дозволяють розглядати пристрої, що фотоприймають як об'єкт, що функціонує в умовах шуму. Це дозволяє застосувати статистичні методи аналізу. За такого підходу ми можемо використовувати добре вивчений математичний апарат перевірки статистичних гіпотез.

Пропонуються три критерії радіаційної стійкості фотоприймальних пристроїв. Перший – відношення сигнал/шум у трактуванні достатніх статистик, другий – критерій середньої помилки виявлення (критерій Котельникова) та третій – критерій Байєсовського ризику.

У цій статті розглянуто фізичні процеси та розробку методів радіаційної модифікації параметрів приладів напівпровідникових приладів оптоелектроніки.

Ключові слова: твердотільна електроніка, радіаційні зміни, статистичні методи аналізу, фотоприймальні пристрої.

UDC 681.3(07)

PhD **Tolok I.V.** (MIKNU)
PhD **Banzak G.V.** (SUITC)
PhD **Leschenko O.I.** (SUITC)

DOI: https://doi.org/10.17721/2519-481X/2022/74-02

RELIABILITY MODEL USER INTERFACE

Complex technical objects in modern society are extremely important. Such objects belong to the class of recoverable objects of long-term multiple uses. They tend to be expensive and require significant maintenance costs. To ensure the required level of reliability during their operation, maintenance is usually carried out, the essence of which is the timely preventive replacement of elements that are in a pre-failure state.

The problem is that when developing such facilities, all issues related to maintainability and maintenance should be addressed already at the early stages of designing the facility. If you do not provide in advance the necessary hardware and software for integrated monitoring of the technical condition (TC) of the object, do not develop and "embed" the maintenance technology into the object, then it will not be possible to realize in the future a possible gain in the reliability of object due to maintenance. Since all these issues must be resolved at the stage of creating an object (when the object does not yet exist), mathematical models of the maintenance process are needed, with the help of which it would be possible to calculate the possible gain in the level of reliability of object due to maintenance, to estimate the cost costs required for this. Then, based on such calculations, make a decision on the need for maintenance for this type of objects and, if such a decision is made, develop the structure of the maintenance system, choose the most appropriate maintenance strategy, and determine its optimal parameters.

Key words: maintenance, coefficient of variation, object reliability, components.

Introduction. Under complex technical objects refers to objects consisting of a large number of different types of elements (tens, hundreds of thousands), each of which can be a rather complex technical device. Elements can be electronic, mechanical, electromechanical, hydraulic, etc. The heterogeneity of the elements leads to the fact that different elements are characterized by fundamentally different physical processes (and, consequently, speed) degradation, leading to their failure.

The objects under consideration belong to the class of objects to be repaired for long-term repeated use, and during their operation, maintenance is usually provided to maintain the required level of reliability. By maintenance (MS) is meant "a complex of operations or an operation to maintain the health or performance of an object when used for its intended purpose, simple, stored and transported" [1,2]. Further, only MS will be considered when used as intended.

During operation, an object at any time can be in one of the following states: serviceable, workable, inoperable.

The object can be used for its intended purpose only in good or healthy condition. Restoration of a working or working condition is made at the expense of current repair. MS, as a rule, is carried out only when the object is in working condition. If by the moment of the start of the maintenance (or in the maintenance process) there is a complete failure, then at the beginning the object is restored, and then the maintenance is performed.

The essence of the MS is to prevent some part of the failures due to the replacement of individual elements, cleaning, lubrication, adjustment, etc. (therefore, MS is often called prevention). In modern technical objects, in the overwhelming number of cases, maintenance is reduced to the replacement of elements (liquids, oils, etc.) that are in a pre-order condition.

Analysis of recent research. Currently, there is a decline in the number of scientific publications devoted to the issues of maintenance of complex technical objects. One of the reasons for this, in our opinion, is a sharp increase in the level of integration and reliability of components. Thanks to this, the developers of sophisticated equipment were able to solve the problems of ensuring the required level of reliability without significant maintenance costs (or no maintenance at all).

However, the same reason (high integration and reliability of component elements) opened up the possibility of implementing more and more sophisticated equipment with new functions, which was not possible with the old element base. This again leads objectively to the problems of ensuring reliability and, therefore, the question of the need for maintenance and the choice of the optimal strategy for its implementation becomes again relevant.

Unfortunately, the currently known mathematical models and methods for calculating the optimal parameters of the maintenance processes are not very suitable for application to real technical objects. The main disadvantage of these models is that they either do not take into account the complex structure of the object, or it is possible to take into account only some of the simplest structures [3,4]. In [5,6], a comparative analysis of the problems arising in solving problems of maintenance "by resource" and "by state" was made. An overview of the latest at that time work in the field of maintenance and repair of complex systems. In [7], a theoretical generalization of the well-known mathematical models of MS processes was made. However, these models do not allow to build on their basis suitable for practical use of the methodology.

Main part. With the help of MB, information about a real technical object (composition, structural and reliability structures, data on reliability indicators and cost of elements) is presented, which is then converted to the form required for use in IMS. In IMS, process of operation object is simulated, taking into account the maintenance. As a result of the complex application of MB and ISM, results are obtained for a specific type of object, the characteristics of which are specified in the initial data.

MB is developed using well-known concepts and methods of probability theory, reliability theory, graph theory. ISM is based on the application of the statistical modeling method (Monte Carlo method). The use of any analytical method turned out to be impossible due to the complexity of the process being modeled.

MB is implemented in such a way that when the software is launched, all data structures used in the model are immediately (automatically) created in the PC RAM and become available for other models. At the same time, reliability indicators of object and all its elements are immediately formed.

In the "Database" mode, it is possible to create a database, correct previously entered information. The PC screen in this mode is shown in fig. one.

The tree of the constructive structure of object is displayed on the left side of screen. In this tree, you can collapse or expand the internal structure of any of the elements. When you select (by mouse click) any of the elements in this tree, the tables on the right display information about the elements that make up selected element. The upper table displays data on composite structural elements that make up the selected element. The lower table displays the data on IDI that are directly included in the selected element. You can edit data in these tables.

At the bottom left (under tree) a panel with data is displayed:

- mean time to failure of the selected element (h);
- cost of the element (c.u.);
- number of structural elements included in the selected element;
- total number of elements-INR in the selected element.

At bottom of screen (below tables) a histogram of *DN*-distribution density of the selected element is displayed.

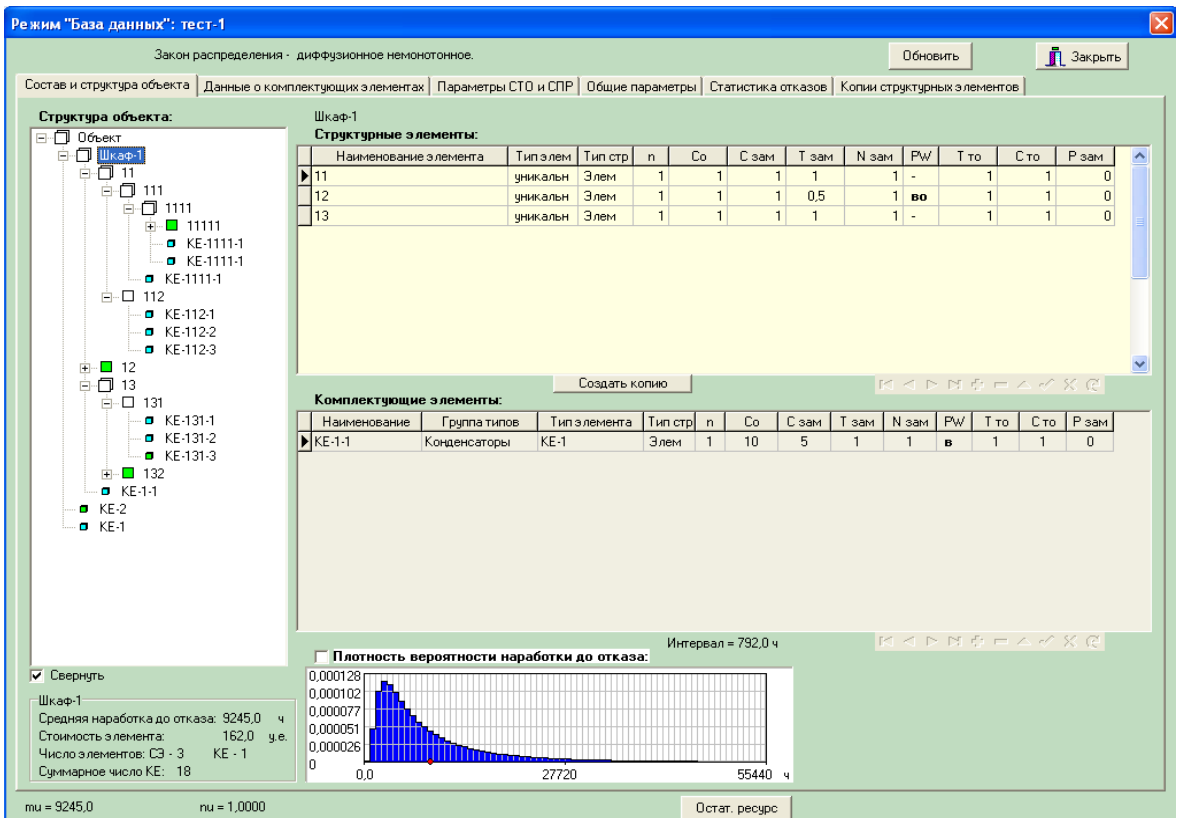

Figura 1 – View of the PC screen in the “Database” mode

To test and study the developed models and methods, test objects with different structures and reliability were used. The characteristics of test objects are selected in such a way as to cover all typical cases of possible real objects encountered in practice. With help of test objects, the following sections demonstrate the features of application developed models and their capabilities. This section presents the main characteristics of test objects, as well as the simulation results obtained for them using MB software.

The Test-1 object is an example of the simplest object that has a consistent reliability structure and a constructive structure that has 6 levels of nesting (Fig. 2). It consists of 20 INR elements that are part of other structural elements of higher levels. INR elements are indicated by circles. All INR have the same reliability characteristics: $T_{ср}$ = 20000 h; ν = 1. The elements included in the set $E_{в}$ are hatched.

The Test-2 facility is an example of a low reliability facility that uses redundancy to improve reliability. The constructive structure of the object is shown in fig. 3. Three least reliable elements have a reserve: 11 (n=3), 12 (n=3) and 131 (n=2). All other elements are consistent (in the sense of reliability) of all the elements included in them. The total number of INR is 900. The elements included in set of recoverable elements are also marked with hatching.

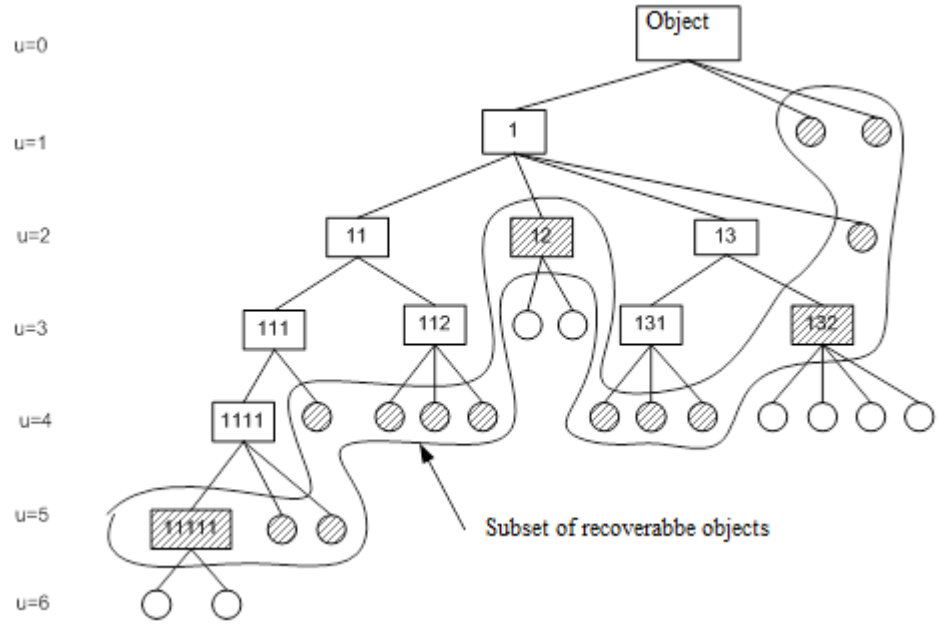

Figura 2 – Constructive structure of object Test-1

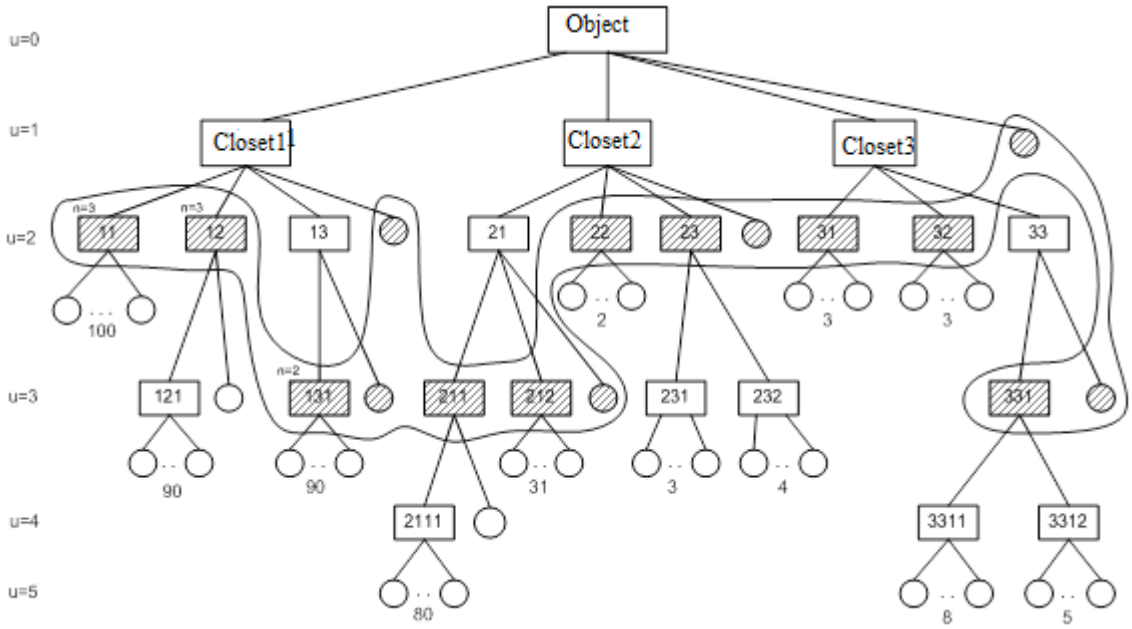

Figura 3 – Constructive structure of the object Test-2

Objects Test-3 and Test-4 are examples of objects that have a single-level constructive structure (Fig. 4). The number of all elements is 50. Elements of objects differ significantly in terms of their reliability. The object Test-3 is an example of an object with a high level of reliability, the object Test-4 is an example of an object with low reliability. Since the structural structure is single-level, all elements are INR, and all of them are recoverable.

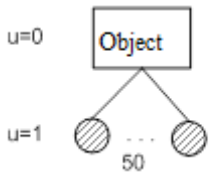

Figura 4 – Constructive structure of objects Test-3 and Test-4

For each of the test objects, a separate database was created, into which the necessary information about the object was entered. For all INR, the coefficient of variation is set to same, equal to 1.

Table 1 presents the main characteristics of test objects.

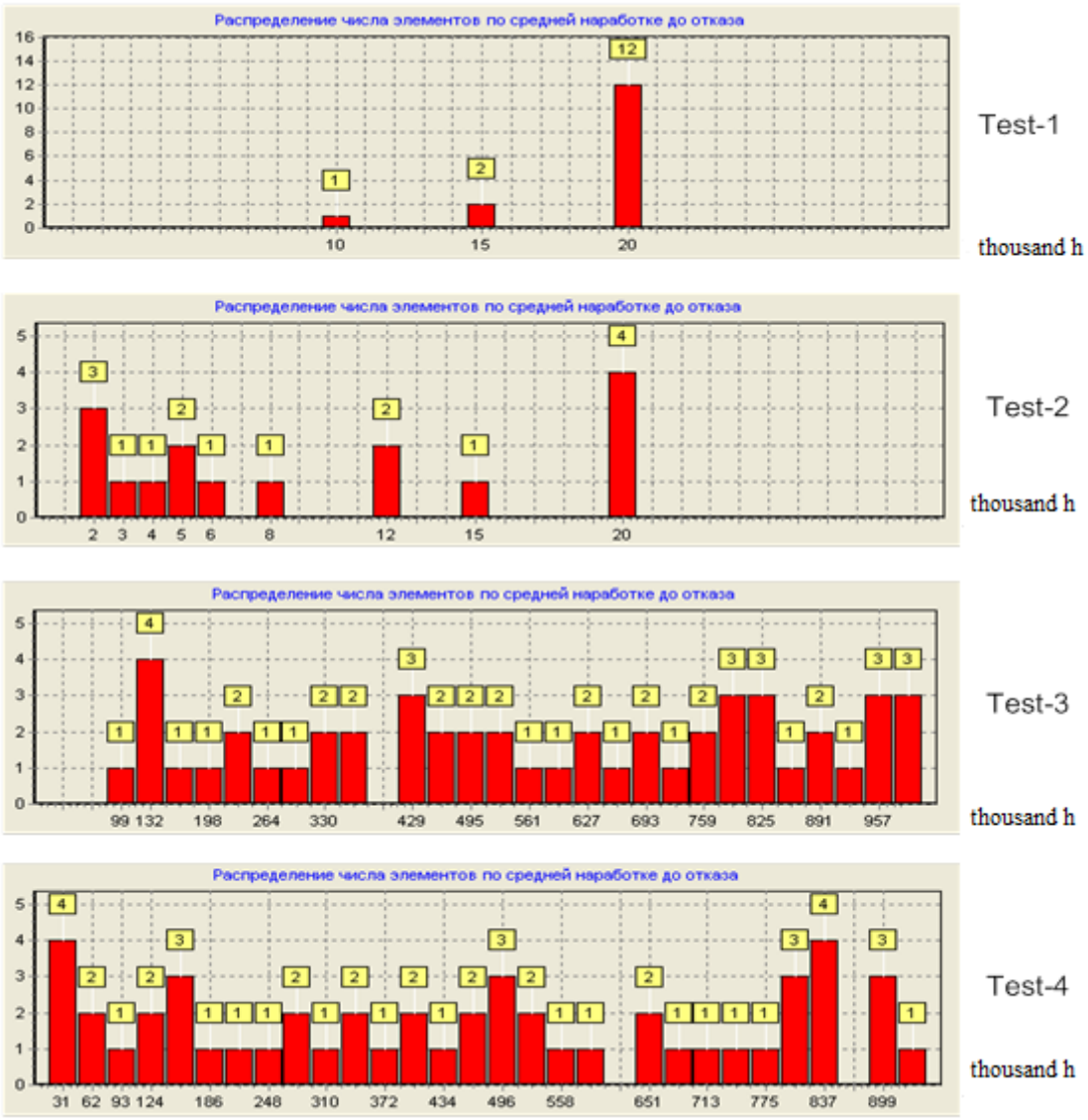

Figura 5 – Distribution histograms of average time to failure restored elements of test objects

Table 1

Characteristics of test objects

Object	Number of INR	Number of elements to be restored	Mean time to failure, h	Coefficient of variation
Test-1	20	15	4472,1	1,0
Test-2	900	16	745,8	0,726
Test-3	50	50	29930,7	1,0
Test-4	50	50	1783,2	1,0

The values of the reliability indicators given in table (mean time to failure and coefficient of variation) are formed automatically when DB program is launched and displayed on PC screen (Fig. 1). For object Test-2, the resulting coefficient of variation is not equal to 1 due to the presence of redundant groups elements in the object.

The most important characteristic of object, which affects the operational indicators of reliability and cost of the object, is distribution of reliability indicators object by its elements. On fig. 5 shows the distribution histograms of the mean time to failure elements of test objects. Grouping intervals are plotted horizontally, and the number of elements in the intervals vertically.

The histograms shown in the figures were formed using the model software in the "Database" mode.

Conclusions

1. The reliability model (RM) makes it possible to obtain estimates of the reliability indicators (RI) of individual structural elements and the object as a whole based on information about the RI of the elements of the lower structural level. The RM represents the hierarchical constructive structure of object. Structural elements of a certain *u*-th structural level are a sequential (in terms of reliability) connection of the elements of (u+1)-th level included in it. Separate structural elements can be a redundant group (parallel connection) of the same type of elements. Thus, with the help of RM, representation of a hierarchical structural structure is combined with an arbitrary serial-parallel reliability structure of an object, which is an acceptable representation for most technical objects encountered in practice.

2. *DN*-distribution is used as a failure model for all elements and the object as a whole. *DN* - distribution is considered to be an adequate model of gradual failures both for electronic products and for various mechanical units and elements. An important advantage of *DN*-distribution is also that its form is preserved during transformations of the reliability structure of the system. It is this feature of *DN*- distribution that made it possible to apply it to a system that has a hierarchical structure.

3. The software implementation of RM was developed in the Delphi programming system. The hierarchical constructive structure of an object is programmatically represented using list data structures (TList lists are used). List elements are objects (instances of Delphi classes) representing individual structural elements of a technical object. Such objects encapsulate all the necessary data related to individual structural elements, including the parameters of *DN*-distributions of the time of failure.

Information about the composition, structure and reliability indicators of the elements of the object is stored in the database of the model built using tables of the InterBase DBMS format.

REFERENCES:

1. Forecasting to reliability complex object radio-electronic texnology and optimization parameter their technical usage with use the simulation statistical models: [monography] in English / Sergey Lenkov, Konstantin Borjak, Gennady Banzak, Vadim Braun, ets.; under edition S.V. Lenkov. – Odessa: Publishing house "VMV", 2014. – 252 p.

2. Jason Brown, Lucas Mol On the roots of all-terminal reliability polynomials / Discrete Mathematics, Volume 340, Issue6, June 2017, pages 1287-1299.

3. Lirong Cui, Yan Li, Jingyuan Shen, Cong Lin Reliability for discrete state systems with cyclic missions periods / Applied Mathematical Modtlling, Volumt 40, Issues 23-24, December 2016, Pages 10783-10799/

4. Iris Tien, Armen Der Kiureghian Algorithms for Bayesian network modeling and reliability assessment of infrastructure systems / Reability Engineering & System Safety, Volume 156, December 2016, Pages 134-147.

5. Volokh O.P. Methods of substantiation rational values operiodicity of maintenance of machines of engineering armament during operation // Collection of scientific works of Military Institute of Taras Shevchenko National University of Kyiv, 2005. – P. 29-32.

6. Boryak K.F Faultlessness model of a complex recoverable object of electronic equipment // Collection of scientific works of Military Institute of Taras Shevchenko National University of Kyiv: 2009. - № 21. – P.33-41.

7. Reliability and efficiency in technology. Directory. Vol.2. Mathematical methods in the theory of

reliability and efficiency / Ed. B.V. Gnedenko. M .: Mechanical Engineering, 1988. – 280 p.

8. Computational methods of research and design of complex systems. Mikhalevich V.S., Volkovich V.L. - M .: Science, 1982. 286 s.

9. Braun V.O., Boryak K.F., Lantvoyt O.B., Tsytsarev V.N. Modeling of maintenance processes of complex reconstructed objects of radio-electronic equipment // News of the Engineering Academy of Ukraine.- K., 2008. - №1. – P. 47 – 52.

10. Boryak K.F. Research of the process of maintenance of complex renewable objects of electronic equipment with the help of simulation statistical model // Bulletin of the Engineering Academy of Ukraine. - K., 2008. - №2. – P.85 – 91.

11. Banzak H.V. Reliability database of complex objects of radio-electronic equipment / H.V.Banzak, K.F.Boryak, V.N.TSytsarev // Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv. – 2010. – № 27. – P.89 – 97.

12. Banzak O.V. Research processes of gamma radiation detector for developing a portable digital spectrometer / O.V. Sieliykov, M.V. Olenev, S.V. Dobrovolskaya, O.I. Konovalenko // Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv. - 2020. - № 69. - P.5 - 13.

13. Banzak H.V. Mathematical model of the “on condition” maintenance process / O. V. Banzak, L. M. Vozikova // The 4th International scientific and practical conference “Scientific achievements of modern society” (December 4-6, 2019) Cognum Publishing House, Liverpool, United Kingdom. 2019. P. 1073 – 1079.

14. Banzak H.V. Development of the failure-free model of a complex technical non-restorable object / O. V. Banzak, O. I. Leschenko // The 3rd International scientific and practical conference “Perspectives of world science and education” (November 27-29, 2019) CPN Publishing Group, Osaka, Japan. 2019. P. 443-450.

к.пед.н., доц. Толок І.В., к.т.н., доц. Банзак Г.В., к.т.н., доц. Лещенко О.І.

ІНТЕРФЕЙС, ЩО ВИКОРИСТОВУЄТЬСЯ В МОДЕЛІ БЕЗВІДМОВНОСТІ

Складні технічні об'єкти у суспільстві мають виключно важливе значення. Такі об'єкти належать до класу об'єктів, що відновлюються тривалого багаторазового застосування. Вони, як правило, є дорогими та потребують значних витрат на їх експлуатацію. Для забезпечення необхідного рівня безвідмовності в процесі їх експлуатації зазвичай проводиться технічне обслуговування (ТО), суть якого полягає у своєчасній запобіжній заміні елементів, що знаходяться в стані перед відмовою.

Проблема полягає в тому, що при розробці таких об'єктів усі питання, пов'язані з ремонтопридатністю та технічним обслуговуванням, повинні вирішуватися вже на ранніх етапах проектування об'єкта. Якщо не передбачити заздалегідь необхідні апаратні та програмні засоби вбудованого контролю технічного стану (ТС) об'єкта, не розробити і не вбудувати в об'єкт технологію проведення ТО, то реалізувати в майбутньому можливий виграш у безвідмовності об'єкта за рахунок проведення ТО не вдасться. Оскільки всі ці питання повинні вирішуватися на етапі створення об'єкта (коли об'єкта ще немає), необхідні математичні моделі процесу ТО, за допомогою яких можна було б прорахувати можливий виграш у рівні безвідмовності об'єкта за рахунок проведення ТО, оцінити вартісні витрати. Потім на підставі таких розрахунків прийняти рішення про необхідність проведення ТО для даного типу об'єктів і, якщо таке рішення прийнято, розробити структуру системи ТО, вибрати найпідходящу стратегію, визначити її оптимальні параметри.

Ключові слова: технічне обслуговування, коефіцієнт варіації, безвідмовність об'єкта, комплектуючі елементи

УДК 621.396.967

д.фіз.-мат.н., проф. **Ільченко В.В.** (КНУ)
к.військ.н., ст.досл. **Нікіфоров М.М.** (ВІКНУ)
д.фіз.-мат.н., с.н.с. **Мостовой В.С.** (ВІКНУ)
к.військ.н, с.н.с. **Попков Б.О.** (ВІКНУ)
к.т.н., ст.досл. **Лоза В.М.** (ВІКНУ)
к.т.н., с.н.с. **Кульський О.Л.** (ІВТ КНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-03

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СЕЙСМОАКУСТИЧНОЇ ЛОКАЦІЇ ДЛЯ ВИЗНАЧЕННЯ РУХОМИХ ОБ'ЄКТІВ

Робота пов'язана з дослідження поверхових хвиль в рішенні задач сейсмоакустичної локації під час переміщення рухомих об'єктів, та в оцінюванні точності визначення координат рухомих об'єктів різного походження. В розв'язанні зворотних задач сейсмоакустичної локації досліджуються поверхні хвилі, які виникають на поверхні Землі під час руху об'єкту що переміщується. Точність розв'язку оберненої задачі безпосередньо залежить від помилок це: визначення часу вступу сейсмічної акустичної хвилі, швидкісної характеристики середовища, шумів різного походження, вибору геометрії розстановки датчиків.

Обґрунтована необхідність в дослідженні поверхневих хвиль, а саме Хвиль Релея і хвиль Лява, тому що вони поширюються по поверхні Землі. Площина коливань релеєвських хвиль вертикальна до поверхні Землі та напрямку поширення, а хвилі Лява мають горизонтальну площину коливань. В якості однієї з розглядаємих задача сейсмоакустичної локації за джерело енергії рухомого об'єкту ми приймаємо сейсмічну енергію, яка виникає під час крокування людини. Крокування людини є періодичним. Воно збуджує імпульси зміщення у геологічному середовищі. За відомим коефіцієнтом жорсткості середовища можна визначити, яким буде максимальне відхилення сейсмоприймача.

В роботі досліджені поверхові хвилі, Релея та Лява в рішенні задач сейсмоакустичної локації під час переміщення людини, та визначені фактори що впливають на точності визначення координат рухомого об'єкту. З погляду використання поверхневих хвиль для вирішення задач сейсмоакустичної локації для визначення рухомих об'єктів вони мають такі переваги: енергія цих хвиль не зникає у глибині Землі, а поширюється під її поверхнею; на їх утворення йде більш ніж 60 % енергії джерела, а на утворення глибинних хвиль тільки 8 %, то такі хвилі мають набагато більшу енергію;

З цього зроблено висновок, що навіть за незначних енергій джерела збудження поверхові хвилі можуть бути використані для рішення задач сейсмоакустичної локації під час переміщення рухомих об'єктів та в оцінюванні точності визначення координат цих об'єктів.

Ключові слова: поверхові хвилі, сейсмоакустична локація, рухомий об'єкт, сейсмоприймач.

Вступ. З початком військових дій в Україні різко зросла загроза тероризму. Ця загроза стосується як великих підприємств, так і тих, що займаються забезпеченням життєдіяльності людей (ТЕЦ, електростанції, зокрема атомні, газові трубопроводи та розподільні пункти тощо). На сьогодні криза з мігрантами на кордоні Білорусі та Польщі стає гострішою з дня у день, що приводить до зростання загрози несанкціонованого перетину кордону України. На певних ділянках Україна почала впорядковувати свій кордон так, щоб ускладнити його перехід як окремим особам, так і цілим групам порушників. Тому актуальним є створення таких систем охоронної сигналізації, які можуть працювати цілодобово, в автоматичному режимі, передаючи інформацію про координати порушника до єдиного центру.

Аналіз останніх досліджень, виділення не вирішених раніше частин проблеми. Одним із актуальних напрямків розвитку інтелектуальних сейсмічних систем охорони периметра є підвищення достовірності виявлення та класифікації типу порушника (людина, група людей, наземна техніка) в умовах впливу численних завадових факторів природно-кліматичного, біологічного та техногенного характеру [1].

При русі людини чи техніки з'являються сейсмічні хвилі, які можна умовно розділити на дві складові – вертикальну та горизонтальну. Горизонтальна сейсмічна хвиля (поверхнева хвиля, релеївська хвиля) поширюється вздовж межі розділу ґрунту та повітря. Саме вона реєструється сейсмічними сенсорами і надалі обробляється. Поширення хвилі вздовж межі розділу середовищ обумовлює її характеристики, які залежать від багатьох факторів: виду ґрунту та його стану, анізотропії, стану підстилаючої поверхні та інших факторів. При аналізі таких сигналів необхідно враховувати наявність природних мікросейсмів (будівництво, дерева, ЛЕП, дороги). Таким чином, корисний сигнал від порушника виникає в умовах численних завадових факторів [2, 3]. Причому діапазони основних характеристик корисних сигналів та перешкод, як правило, перекриваються.

Сейсмічні сигнали містять інформацію про факт переміщення, про місцезнаходження об'єкта, що рухається, про його тип. Виходячи з цього, обробка сейсмічних сигналів має бути спрямована на вирішення задач виявлення об'єкта, що рухається, визначення його типу (класифікація), поточну оцінку його координат. Істотне значення мають вимоги обробки сигналів у реальному часі та малого енергоспоживання, що забезпечує значний час роботи в автономному режимі, а також високий рівень сигналів, що заважають, обумовлених присутністю сейсмічного фону [4-7].

Питання дослідження проблем геофізичного моніторингу, сейсмоакустичної локації, визначення просторових координат і потужності джерел сейсмоакустичних хвиль розглядалися в наукових працях: Дудкін, С.С. Звежинський, В.А. Іванов, І.М. Крюков, Є.С. Нежевенко, М.А. Райфельд, А.А. Спектор, Г.К. Чистова, Цибульчіка Г.М., Романова В.Г., Яновська Т.Б., Dziewonski AM, An-derson DI, Nolet G . G.L. Goodman, R.A. Gramann, Z. Liang, A. Pakhomov, L. Peck, A. Sicignano, G. Succi,. та ін.

У доступних опублікованих дослідженнях науковців не достатньо зверталась увага дослідженню питань в оцінюванні точності визначення координат рухомих об’єктів різного походження до розв'язання оберненої задачі сейсмоакустичної локації. Крім того, не завжди враховується вимога стабілізації ймовірності хибної тривоги, а також той факт, що системи охорони відносяться до систем реального часу, де затримки у прийнятті рішення неприпустимі. Точність розв'язку оберненої задачі безпосередньо залежить від помилок це: визначення часу вступу сейсмічної акустичної хвилі, швидкісної характеристики середовища, шумів різного походження, вибору геометрії розстановки датчиків. З результатів аналізу опублікованих робіт слід, що практично невивченим є потенційно більш точний підхід до вирішення завдання визначення моментів вступу хвиль із застосуванням методів комбінаторної оптимізації.

Мета статті. Дослідження поверхових хвиль в рішенні задач сейсмоакустичної локації під час переміщення рухомих об’єктів та в оцінюванні точності визначення координат рухомих об’єктів різного походження.

Виклад основного матеріалу. Сьогодні у системах охоронної сигналізації використовують сейсмоакустичні датчики, які встановлюють на поверхні Землі. Сучасні датчики можуть працювати цілодобово, в автоматичному режимі. В розв'язанні зворотних задач сейсмоакустичної локації в роботі пропонується дослідити поверхні хвилі, які виникають на поверхні Землі під час крокування людини та переміщення автомобільного транспорту.

Є чотири типи сейсмічних хвиль: первинні хвилі (primary waves), вторинні хвилі (secondary waves), хвилі Релея та хвилі Лява. Перші два типи ще називають глибинними, тому що вони проникають у глибини Землі. Хвилі Релея і хвилі Лява ще називають поверхневими хвилями тому, що вони поширюються по поверхні Землі. Теория распространения сейсмических волн в реальных средах базируется, в основном, на линейной теории упругости. Для упругой среды или любой среды при нагрузках, меньших предела упругости, справедлив закон Гука, устанавливающий прямо пропорциональную зависимость между нагрузкой и деформацией.

Площина коливань релеєвських хвиль вертикальна до поверхні Землі та напрямку поширення, а хвилі Лява мають горизонтальну площину коливань. Швидкості S-хвиль та P-хвиль зв'язані таким співвідношенням [1,2]:

$$\gamma = \frac{V_S}{V_P} = \sqrt{\frac{1-2_V}{2(1-V)}} \quad , \tag{1}$$

де V_S −швидкість S-хвилі; V_P- швидкість P-хвилі; γ -коефіцієнт Пуансона.

Знаючи V_S та γ, легко визначити коефіцієнт Пуансона та швидкість хвиль Релея:

$$V_P = \frac{0{,}87+1{,}12v}{1+v} \cdot V_S \, , \tag{2}$$

де V_P-швидкість хвиль Релея.

P-хвилі та S-хвилі є об'ємними. Їх енергія поширюється сферично. Концентрація цієї енергії залежно від відстані r до джерела через геометричне розходження буде зменшуватися відповідно до $1/4\pi r^2$. Крім того, енергія хвиль буде втрачатися на тертя через неідеальну пружність середовища. Таке ослаблення можна виразити множником $e^{-2\alpha r}$. Отже, енергія об'ємної сейсмічної хвилі в геологічному середовищі одночасно розсіюється внаслідок геометричного розходження і поглинається через неідеальну пружність. Залежність цієї енергії від відстані до джерела дорівнюватиме:

$$E(r) = \frac{E_0}{2\pi \cdot r} \cdot e^{-2\alpha r} \, . \tag{3}$$

Хвиля Релея пов'язана з вільною поверхнею і є результатом накладання поздовжніх і поперечних хвиль SH. Частинки середовища у хвилі рухаються по еліптичних орбітах у вертикальній площині, паралельній поширенню хвилі. Вертикальна вісь еліпса приблизно 1,5 разу перевищує горизонтальну. Швидкість поширення хвилі Релея \/ R змінюється від 0,874 до 0,956 значення Vs, що наданні в табл. 1.

Таблиця 1

Ґрунти	Vp	Vs	Vp/Vs	Діапазон частот
Ліси та лесоподібні суглинки	0,4 - 0,5	0,32 - 0,5	1,25 - 1,0	Сейсмічний
	0,41 - 9,5	-	-	Ультразвуковий
Суглинки морені	3,72 - 4,87	-	-	-"-
Супесь	0,48 - 0,76	0,62 - 0,65	0,77 - 1,17	Сейсмічний
Суглинки покривні	0,66 - 4,87	-	-	Ультразвуковий
Глини	0,14 - 0,64	0,28 - 0,49	0,5 - 1,3	Сейсмічний
	1,15 - 4,25	-	-	Ультразвуковий
Водо насичені глини	0,02 - 0,06	0,08 - 0.22	0,36 - 0,38	Сейсмічний

При шаруватому характері середовища у верхній частині розрізу утворюється так звана псевдо-релеївська хвиля подібна до хвилі Релея в однорідному середовищі. Швидкість псевдо-релеївської хвилі залежить від її довжини R, тобто. має місце дисперсія швидкості.

Останнє спостерігається за умови, що R > Δ h, де Δ h - потужність окремого шару ґрунту.

Хвиля Лява утворюється тільки в шарі (або пачці шарів) зі зниженою швидкістю поперечних хвиль VS1, під товщею товщою більш високошвидкісних порід VS2.

Хвиля Лява є інтерференційною хвилею типу SH та поляризована горизонтально. Швидкість поширення хвиль Лява VL залежить від частоти коливань та змінюється в межах

$$V_{S1} < V_L < V_{S2}. \tag{4}$$

У ряді випадків на межі середовищ утворюються обмінні хвилі (відбиті та заломлені), пов'язані зі зміною типу хвилі.

На вільній поверхні шаруватого середовища можуть реєструватися такі типи хвиль:

поздовжні - прямі, відбиті і заломлені (від різних кордонів), і навіть різні види багаторазово відбитих і заломлених хвиль;

поперечні - тих самих класів, що поздовжні;

обмінні - відбиті, заломлені та різні комбінації відбито-заломлених хвиль;

поверхневі хвилі Релея та Лява [1,2].

За джерело енергії рухомого об'єкту ми приймаємо сейсмічну енергію, яка виникає під час крокування людини. Під час кожного кроку центр мас людини переміщається по циклоїді [4], коливаючись відносно середньої лінії на ± 4 см. Отже, загальна висота піднімання 8 см. Коли центр мас у найвищій точці, то його потенціальна енергія є найбільшою. Під час кожного кроку ця енергія передається землі, в результаті чого виникають як об'ємні, так і поверхневі сейсмічні хвилі.

Енергію хвиль Релея E_0, які виникають під час крокування людини, можна записати

$$E_0 = (m_л g H) \cdot k, \tag{5}$$

де $m_л$ –маса людини $m_л$=80 *кг;* $g -$ прискорення вільного падіння; -висота $H = 0{,}08$ м; k- емпіричний коефіцієнт, що враховує, яка частина енергії кроку переходить у енергію хвиль Релея. З глибиною енергія хвилі Релея зменшується експоненціальне і на відстані довжини хвилі λ у 10 разів менша, ніж на поверхні. Для визначення коефіцієнта згасання енергії хвиль з глибиною запишемо

$$E_\lambda = E_0 \cdot e^{\alpha_\lambda \lambda} \ , \tag{6}$$

де E_λ– енергія хвиль Релея на глибині λ; α_λ – коефіцієнт згасання хвиль з глибиною. Визначено відношенням

$$\frac{E_\lambda}{E_0} = \frac{E_0 \cdot e^{\alpha_\lambda \lambda}}{E_0} = 0{,}1 \ . \tag{7}$$

Для глини [1] λ = 190 м. З (7) визначимо, α_λ = –0,012.

Фронти хвилі Релея поширюються квазі-циліндрично. Енергія цих хвиль зменшується як з глибиною, так і зі зростанням радіуса поширення по поверхні. Вісь циліндричного фронту перпендикулярна до поверхні й розміщена там, де і джерело. Знаючи коефіцієнт згасання енергії з глибиною, визначимо середнє значення енергії $E_{ср}$на глибині осі від 0,4 до 0,5 м. На цій глибині буде встановлено сейсмоприймач. Він займає об'єм куба з розміром ребра 0,1 м:

$$E_{ср} = \frac{E_0}{0{,}1} \int_{0{,}4}^{0{,}5} e^{-\alpha_\lambda z} dz, \tag{8}$$

де z- глибина.

Енергія від джерела, падає на площу S де розташований сейсмоприймач. З урахуванням коефіцієнта поглинання α та відстані до сейсмоприймача x енергія, яка доходить до сейсмоприймача E_{sp}, дорівнюватиме

$$E_{sp}(x) = \frac{E_{ср} \cdot e^{-2\alpha \cdot x}}{10 \cdot s} = \frac{E_{ср} \cdot e^{-2\alpha \cdot x}}{10 \cdot 2\pi \cdot x}, \tag{9}$$

Оскільки x ми підставляємо у метрах, а α у м$^{-1}$, то для того, щоб визначити, скільки енергії падає на грань куба розміром 0,1·0,1 м, необхідно енергію, що падає на площу циліндра S, зменшити у десять разів (рис. 1).

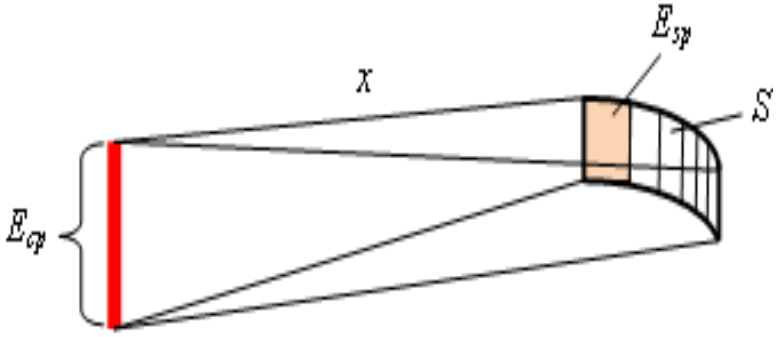

Рисунок 1 – Циліндричний розподіл енергії хвиль Релея по глибині

У хвилях Релея коливання здійснюються у вертикальній площині перпендикулярно до напрямку променя [1,2]. Коли до куба, де в геологічному середовищі розміщено сейсмоприймач, доходить енергія E_{sp}, то під час проходження хвиль ця енергія почергово перетворюється з потенціальної на кінетичну. Для того, щоб знайти максимальну швидкість переміщення заданого об'єму геологічного матеріалу у вертикальній площині, необхідно записати

$$V_m(x) = \sqrt{\frac{2E_k(x)}{\text{м}}}\ , \tag{10}$$

де V_m- максимальна швидкість коливань геологічного матеріалу; м – маса геологічного матеріалу; E_k –кінетична енергія, якої набуде певний об'єм геологічного матеріалу, $E_k = E_{sp}$.

Знаючи максимальну швидкість матеріалу та частоту кроків f, можна визначити, як змінюється швидкість матеріалу $V(t)$ у часі

$$V(t) = V_m(x) \cdot \sin(2\pi f \cdot t)\ , \tag{11}$$

У нашому випадку $f = 2$Гц. Середнє значення швидкості за чверть періоду T дорівнюватиме

$$V_{cer}(x) = \frac{4}{T}\int_0^{T/4} \mathrm{V_m(x)} \cdot \sin(2\pi \mathrm{f} \cdot \mathrm{t})\mathrm{dt}\ . \tag{12}$$

Для потенціальної енергії певного об'єму геологічного матеріалу визначимо:

$$E_p(x) = K \cdot z_m^2(x)\ , \tag{13}$$

де K – коефіцієнт жорсткості середовища, H/m; z_m – максимальне вертикальне зміщення геологічного матеріалу в місці встановлення сейсмоприймача.

Проінтегрувавши (11) за половину періоду, можна визначити максимальне зміщення z_m

$$z_m(x) = \int_0^{T/2} V_m(x) \cdot \sin(2\pi f \cdot t)dt\ , \tag{14}$$

Підставивши z_m у (13), визначимо коефіцієнт жорсткості середовища K

$$K = \frac{E_p(x)}{z_m^2(x)}\quad . \tag{15}$$

За відомим коефіцієнтом жорсткості середовища можна визначити, яким буде максимальне відхилення сейсмоприймача, розміщеного у геологічному середовищі на глибині від 0,4 до 0,5 м у кубі з розміром ребра 0,1 м, залежно від відстані x від джерела сейсмічних коливань

$$z_m(x) = \sqrt{\frac{E_p(x)}{K}}\,. \tag{16}$$

Напруга вихідного сигналу існуючих сейсмоприймачів є функцією їх швидкості, а не переміщення (амплітуди коливань). Тому на значення вихідного сигналу впливатиме не тільки амплітуда коливань, а і їх частота, що створюватиме неоднозначність вихідного сигналу. За чутливості від 0,3 до 0,7 $В/мс^{-1}$ [2, 4] та зміщення геологічного середовища на $1-10^{-7}$м вихідний сигнал такого сейсмоприймача матиме значення від 0,4 до 0,9 мкВ. Виділити такий сигнал на фоні шумів дуже важко.

При побудові характеристик виявлення об'єктів з імпульсним впливом на ґрунт (людина, група людей, тварини) необхідно враховувати, що сигнали цих об'єктів мають імпульсний характер: на аналізованому інтервалі сигнал що спостерігається змінює свої властивості і є або суміш корисного сигналу з сейсмічним фоном, або тільки сейсмічний фон. З погляду використання поверхневих хвиль для вирішення задач систем охоронної сигналізації вони мають такі переваги [2]:

1. Енергія цих хвиль не зникає у глибині Землі, а поширюється під її поверхнею;
2. Оскільки на їх утворення йде більш ніж 60 % енергії джерела, а на утворення глибинних хвиль тільки 8 %, то такі хвилі мають набагато більшу енергію;
3. Зі зростанням відстані r від джерела їх енергія зменшується пропорційне до 1/r, а не до 1/r2 .

За даними з [8] для рихлих осадових порід (глина) коефіцієнт поглинання може мати значення від 10^{-3} $1м^{-1}$ до $0{,}5\,м^{-1}$. Крокування людини є періодичним. Воно збуджує імпульси зміщення у геологічному середовищі. Ці імпульси можна розкласти у спектр частот. Оскільки перша гармоніка такого спектра має найбільшу енергію, то для оцінки відстані зроблено допущення, що саме ця гармоніка несе всю енергію спектра. Також у літературних джерелах [2, 9, 10], вказано, що від 60 до 65 відсотків енергії джерела забирають поверхневі хвилі, однак ніде не вдалося знайти розподілу енергії між цими хвилями. Тому зроблено допущення, що у малопотужних джерелах поверхневі хвилі забирають 20 % відсотків енергії і ця енергія розподіляється між хвилями Релея та хвилями Лява порівну.

З метою визначення характеристик сигналу більш доцільно розглянуту наступну математичну модель [11, 12] з значення критерію у точці глобального мінімуму. Фізично змістовну цінність мають перш за все значення частот і логарифмічних декрементів осциляторів моделі зареєстрованого сигналу. Фізичні уявлення про природу і характер осциляцій корисного сигналу і облік многомодальним його спектра, дозволяють висунути гіпотезу про можливість моделювати його суперпозицією осциляторів з демпфуванням. В цьому випадку сигнал в фіксованій точці реєстрації можна представити в вигляді:

$$y_k(t) = \sum_{s=1}^{S} A_{ks}\,\exp\{-\alpha_{ks}t\}\sin(\omega_{ks}\,t + \Psi_{ks}) + n_k(t)\,. \tag{17}$$

Тут k - номер сенсора, який реєструє коливання, K - кількість сенсорів, в нашому випадку K =2, (k =1 у вертикальній площині і k = 2 у горизонтальній площині). $A_{ks}, \alpha_{ks}, \omega_{ks}, \psi_{ks}$ - вільні параметри моделі, $n_k(t)$ - адитивний шум у вимірах k-го сенсора. S - безліч розглянутих однотипних підмоделей, суперпозиція яких моделює процес, $y_k(t)$, $s \in S$.

Завдання полягає в оптимальному визначенні вільних параметрів моделі. Критерієм оптимальності вибирається ступінь близькості моделі до даних що досліджуються в обраній метриці.

У метриці L_2 критерій являє собою функціонал для кожної з компонент виду:

$$F_k(\Pi_k) = \left\| \left(\sum_{s=1}^{S} A_{ks}\, ekp\{\alpha_{ks} t\} \sin\left(\omega_{ks}(t - \psi_{"ks"})\right) \right) - y_k(t) \right\| L_2;\ k = \overline{1,K} \quad . \qquad (18)$$

Оптимальне рішення – це точка глобального мінімуму функціоналу (18). Глобальний екстремум знаходився на множині локальних, які обчислювалися на околиці «викинутих» шляхом Монте-Карло, за апріорними розподілами, параметрів.

Існування рішення (18) приведено в [14], а саме рішення надано в [15]. Фізично змістовну цінність мають насамперед значення частот та логарифмічного декременту об'єкта дослідження. Особливо важливі останні. Для наведеного на рис. 3, сингала при вирішенні задачі (18) вектор логарифмічних декремент має значення {0.194, 0.115, 0.675}, а вектор частот {0.559, 0.783, 2.015}. Вектор значень частот надано в Герцах, а логарифмічний декремент в безрозмірних одинцях. Розглянемо модель (17) =3.

На рис. 2 представлена модель (17) (крива червоного кольору, більш згладжена крива) і сигнал, (крива синього кольру).

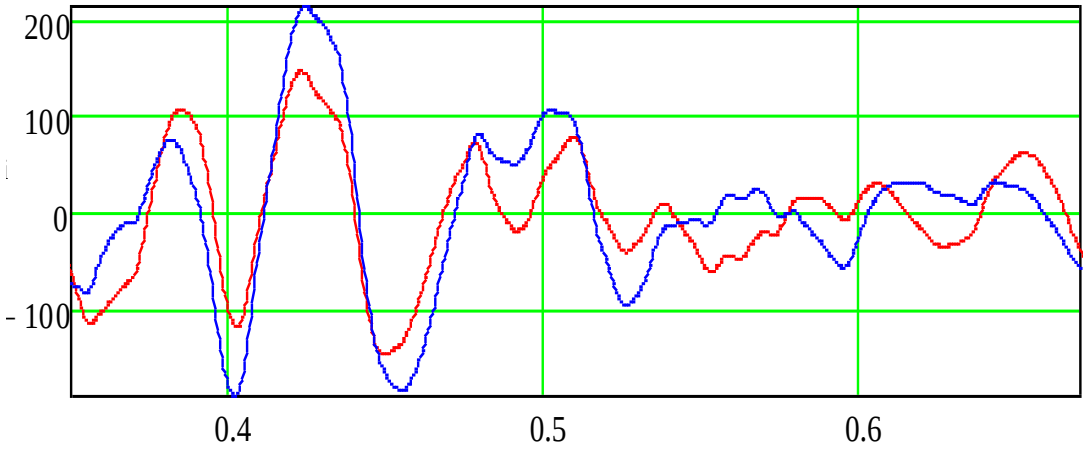

Рисунок 2 – модель (17) (крива червоного кольору, більш згладжена крива) і сигнал, (крива синього кольору)

Таким чином представляється моделі з дванадцятьма вільними параметрами. Оцінкою якості моделі є значення критерію у точці глобального мінімуму. Фізично змістовну цінність мають перш за все значення частот і логарифмічних декрементів осциляторів моделі зареєстрованого сигналу .

Знаючи поріг чутливості, за поданими вище математичними моделями з урахуванням всіх допущень можна оцінити відстань, з якої ємнісний сейсмоприймач з чутливістю 1Гц/1.2·10^{-7} м відчує сейсмічні хвилі, збуджені крокуванням людини.

За відсутності об'єкта, що рухається, на виході сейсмічного сенсора присутні випадкові сигнали (сейсмічні шуми), які накладаються на квазіперіодичні імпульсні сигнали, що виникають під час руху людини. Збільшення та спад амплітуди огинальної послідовності імпульсів у міру наближення людини до сенсора та при віддаленні від нього здійснюються за законом, близькому до експонентного. Швидкість наростання та зменшення сейсмічного сигналу, що виникає при русі наземної техніки, набагато повільніше, ніж під час руху людини чи групи людей. У цьому корисний сигнал характеризується відсутністю яскраво вираженої періодичності. Спектр сигналу визначається типом об'єкта, швидкістю руху, відстанню між об'єктом, що рухається, і місцем установки сейсмічного сенсора, зоною виявлення (чутливістю) сейсмоприймача [4, 13]. Спектральні складові сигналу в діапазоні частот від 0 до

80 Гц обумовлені впливом на ґрунт поодинокого порушника. При русі групи людей спектр сигналу сейсмічного сенсора розширюється високочастотну область. Спектр сигналу, спричиненого рухом наземної техніки, що перекриває всю область корисних сигналів без характерних максимумів. Спектральні складові понад 200–300 Гц. практично мало розрізняються і натомість природних мікросейсмів, оскільки при поверхневий шар ґрунту грає роль фільтра низьких частот, тобто. сильніше поглинає високі частоти.

Аналіз характеристик сейсмічних сигналів дозволяє визначити ознаковий простір для класифікації об'єктів, що рухаються. Для розпізнавання класів об'єктів – людина, група людей, легковий автомобіль – доцільно використати спектральний опис у частотному діапазоні до 300 Гц. і характеристики періодичності сигналу – кількісну оцінку та значення періоду проходження імпульсів сейсмічних сигналів, що фіксуються при русі людини в зоні виявлення.

Висновки

1. Досліджені поверхові хвилі, Релея та Лява в рішенні задач сейсмоакустичної локації, під час переміщення людини, та визначені фактори що впливають на вирішення задачі виявлення сигналу на фоні мікросейсмічного шуму.

2. Визначено що навіть за незначних енергій джерела збудження, поверхові хвилі можуть поширюватися на значно більші відстані, та можуть бути використані для рішення задач сейсмоакустичної локації під час переміщення рухомих об’єктів та в оцінюванні точності визначення координат цих об’єктів.

3. Запропоновано, з метою визначення координат та характеристик сигналу розглянути математичну модель з визначення критерію у точці глобального мінімуму.

4. Обробка даних моніторингу об'єкта зі змінними характеристиками за запропонованим алгоритмом дозволила виявити інформативні параметри, які характеризують специфіку об’єкта дослідження, що відображено в просторі вільних параметрів моделі.

ЛІТЕРАТУРА:

1. Манштейн А. К. Малоглубинная геофизика: пособие по спецкурсу. – Новосибирск: Новосибирский государственный университет, 2002. –135 с.

2. Рак В.С. Про використання сейсмічних хвиль Релея в системах безпеки. Національний університет “Львівська політехніка”. Вимірювальна техніка та метрологія, № 76, 2015 р. С 156–161.

3. Онуфриев Н.В., А.В. Скридловский, В.В. Матвеев. Уточнение статистических моделей биологических объектов для сейсмического принципа обнаружения // Радиотехника, 2011. - №2. -С. 101 - 104.

4. Райфельд М.А., Коробов В.В., Мартухович И.О., Сосновский А.В. Квазиоптимальный алгоритм классификации «одиночный человек, группа людей» в сейсмической системе охраны периметров. Радиотехника, 2012. - №1. - С. 17 - 19.

5. Нікіфоров М.М., Пампуха І.В., Щербіна С.В., Шевцов А.Г., Лоза В.М. Особливості використання автоматизованого сейсмоакустичного комплексу за допомогою комбінованого способу виявлення об’єктів. Геофізичний журнал. Інституту геофізики ім. С. І. Субботіна НАН України. 2018, №6, т. 40, С.150-158.

6. Дудкин В.А.,. Вольсков А.А. Методы определения пеленга объекта, основанные на измерении временных задержек сейсмических сигналов. Современные технологии безопасности, 2010. – №1.— С. 28-30.

7. Фальшинский В.В. Паралельная обработка данных многокомпонентных сейсмических наблюдений // Кибернетика и системный анализ. – 2011. – № 2. – С 181–186.

8. Табулевич В.Н. Об определении положения источника возбуждения микросейсмических колебаний. Изв. АН СССР, сер. Физика Земли. 1977. № 5. С.89-92.

9. Кугаенко Ю.А, Салтыков В.А., Синицин В.И., Чебров В.Н. Локация источников сейсмического шума, связанного с проявлением гидротермальной активности, методом эмиссионной томографии // Физика земли. 2004. № 2. С.66-81.

10. Гуляев В.Т., Кузнецов В.В., Плоткин В.В., Хомутов С.Ю. Генерация и распространение инфразвука в атмосфере при работе мощных сейсмовибраторов. // Изв. АН СССР: Физика атмосферы и океана. – 2001. – Т.37, №3. – С.303-312

11. Andreev P.R., Grigoruk A.P., Shorokhov M.N.. Systems for reception and recording of vibroseismic signals. // Bull. Nov. Comp. Center, Math. Model. in Geoph., v. 7 (2002), p.1–11.

12. Mostovoy V. S., Mostovyi S. V. Mathematical model of seismic signal, as a flow of physically non realizable single seismic waves // Geophysical Journal– 2016. Vol. 38, № 5, p. 166-169. http://journals.uran.ua/geofizicheskiy/article/view/107830.

13. Авроров С.А., Хайретдинов М.С. Распределенная обработка данных в мониторинговых системах и сетях// Научный вестник НГТУ. – 2010. – №1. – С.1-11.

14. Мостовой В.С., Мостовой С.В. О корректности задачи нелинейной регрессиипри мониторинге природных и рукотворных объектах. Геофиз. журн. – 2012. – 34, № 2. – С. 140-143.

15. Мостовой В.С. Оптимальное обнаружение сигналов на фоне микросейсмического шума. Доп. НАН Украины. – 2008. – № 1. – С. 106-110.

REFERENCES:

1. Manshtejn A. K. (2002) *Maloghlubynnaja gheofyzyka*. [Shallow geophysics] posobye po speckursu. – Novosybyrsk: Novosybyrskyj ghosudarstvennыj unyversytet, 135 p.

2. Rak V.S. (2015) *Pro vykorystannja sejsmichnykh khvylj Releja v systemakh bezpeky*. [On the use of Rayleigh seismic waves in security systems. On the use of Rayleigh seismic waves in security systems.] Nacionaljnyj universytet “Ljvivsjka politekhnika”. Vymirjuvaljna tekhnika ta metrologhija, No.76, p.p. 156–161.

3. Onufryev N.V., A.B. Skrydlovskyj, V.V. Matveev. (2011) *Utochnenye statystycheskykh modelej byologhycheskykh obъektov dlja sejsmycheskogho pryncypa obnaruzhenyja* [Clarification of statistical models of biological objects for the seismic detection principle] Radyotekhnyka, No.2. p.p. 101 - 104.

4. Rajfeljd M.A., Korobov V.V., Martukhovych Y.O., Sosnovskyj A.B. (2012) *Kvazyoptymaljnыj alghorytm klassyfykacyy «odynochnыj chelovek, ghruppa ljudej» v sejsmycheskoj systeme okhranы perymetrov.* [Quasi-optimal algorithm for classification "single person, group of people" in the seismic system of perimeter protection.] adyotekhnyka, No.1. p.p. 17 - 19.

5. Nikiforov M.M., Pampukha I.V., Shherbina S.V., Shevcov A.Gh., Loza V.M. (2018) *Osoblyvosti vykorystannja avtomatyzovanogho sejsmoakustychnogho kompleksu za dopomoghoju kombinovanogho sposobu vyjavlennja ob'jektiv.* [Features of using an automated seismic acoustic complex using a combined method of object detection.] Gheofizychnyj zhurnal. Instytutu gheofizyky im. S. I. Subbotina NAN Ukrajiny. No 6, T. 40 pp.150-158.

6. Dudkyn V.A., Voljskov A.A. (2010) *Metodы opredelenyja pelengha obъekta, osnovannыe na yzmerenyy vremennыkh zaderzhek sejsmycheskykh syghnalov.* [Methods for determining the bearing of an object based on the measurement of time delays of seismic signals.] Sovremennыe tekhnologhyy bezopasnosty, No.1, p.p. 28-30.

7. Faljshynskyj V. V. (2011) *Paraleljnaja obrabotka dannыkh mnoghokomponentnыkh sejsmycheskykh nabljudenyj* [Parallel data processing of multicomponent seismic observations.] Kybernetyka y systemnыj analyz. No. 2, p.p. 181–186.

8. Tabulevych V.N. (1977) *Ob opredelenyy polozhenyja ystochnyka vozbuzhdenyja mykrosejsmycheskykh kolebanyj*. [On determining the position of the source of excitation of microseismic oscillations.] Yzv. AN SSSR, ser. Fyzyka Zemly. No. 5, p.p.89-92.

9. Kughaenko Ju.A, Saltыkov V.A., Synycyn V.Y., Chebrov V.N.. (2004) *Lokacyja ystochnykov sejsmycheskogho shuma, svjazannogho s projavlenyem ghydrotermaljnoj aktyvnosty, metodom эtyssyonnoj tomoghrafyy* [Location of sources of seismic noise associated with the manifestation of hydrothermal activity, the method of emission tomography] Fyzyka zemly. No. 2, p.p. 66-81.

10.Ghuljaev V.T., Kuznecov V.V., Plotkyn V.V., Khomutov S.Ju. (2001) *Gheneracyja y rasprostranenye ynfrazvuka v atmosfere pry rabote moshhnыkh sejsmovybratorov.* [Generation and propagation of infrasound in the atmosphere during the operation of powerful seismic vibrators.] Yzv. AN SSSR: Fyzyka atmosferы y okeana. T.37, No. 3, p.p.303-312.

11.Andreev P.R., Grigoruk A.P., Shorokhov M.N. (2002) *Systems for reception and recording of vibroseismic signals.* [Reception and recording systems of vibroseismic signals.] Bull. Nov. Comp. Center, Math. Model. in Geoph., No. 7, p.p. 1–11.

12.Mostovoy V. S., Mostovyi S. V. Mathematical model of seismic signal, as a flow of physically non realizable single seismic waves // Geophysical Journal– 2016. Vol. 38, no. 5, p.p. 166-169. http://journals.uran.ua/geofizicheskiy/article/view/107830.

13. Avrorov S.A., Khajretdynov M.S. (2010) *Raspredelennaja obrabotka dannыkh v monytorynghovыkh systemakh y setjakh*. [Distributed data processing in monitoring systems and networks] Nauchnыj vestnyk NGhTU. n.1, p.p.1-11.

14. Mostovoj V.S., Mostovoj S.V. (2012) *O korrektnosty zadachy nelynejnoj reghressyypry monytorynghe pryrodnыkh y rukotvornыkh obъektakh*. [On the correctness of the problem of nonlinear regression in monitoring natural and man-made objects.] Gheofyz. zhurn. 34, No. 2. – p.p. 140-143.

15. Mostovoj V.S. (2008) *Optymaljnoe obnaruzhenye syghnalov na fone mykrosejsmycheskogho shuma.* [Optimal signal detection against a background of microseismic noise.] Dop. NAN Ukraynы. No. 1. p.p. 106-110.

Dr. Sci. in physical and mathematical Ilchenko V.V.,
PhD Nikiforov M.M., PhD Mostovoy V.S., PhD Popkov B.O., PhD Loza V.M.

PECULIARITIES OF APPLICATION OF SEISMOACOUSTIC LOCATION FOR DETERMINATION OF MOVING OBJECTS

The work is related to the study of surface waves in solving seismic acoustic location problems during the movement of moving objects, and in assessing the accuracy of determining the coordinates of moving objects of different origins. In solving the inverse problems of seismic acoustic location, the surfaces of the wave that occur on the Earth's surface during the movement of a moving object are studied. The accuracy of the solution of the inverse problem directly depends on the errors: determination of the time of entry of the seismic acoustic wave, the velocity characteristics of the environment, noise of various origins, the choice of the geometry of the location of sensors.

The need to study surface waves, namely Rayleigh Waves and Lion Waves, is justified because they propagate on the Earth's surface. The plane of oscillation of Rayleigh waves is vertical to the Earth's surface and direction of propagation, and Lev waves have a horizontal plane of oscillation. As one of the considered problems of seismic acoustic location as a source of energy of a moving object, we take seismic energy, which occurs during human walking. Human walking is periodic. It excites impulses of displacement in the geological environment. According to the known coefficient of rigidity of the medium, it is possible to determine what will be the maximum deviation of the seismic receiver.

The paper investigates surface waves, Rayleigh and Lev in solving seismic acoustic location problems during human movement, and identifies factors that affect the accuracy of determining the coordinates of a moving object. In terms of using surface waves to solve seismic location problems to identify moving objects, they have the following advantages: the energy of these waves does not disappear deep into the Earth, but propagates below its surface; their formation takes more than 60% of the energy of the source, and the formation of deep waves only 8%, such waves have much more energy;

From this it can be concluded that even at low energies of the excitation source surface waves can be used to solve seismic location problems during the movement of moving objects and to assess the accuracy of determining the coordinates of these objects.

Keywords: surface waves, seismic location, moving object, seismic receiver.

УДК 681.1

к.т.н., ст.досл. **Лєнков Є.С.** (ЦНДІ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-04

РОЗРОБКА МЕТОДІВ МОДЕЛЮВАННЯ СКЛАДУ ТА РЕСУРСУ УГРУПУВАННЯ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ ДЛЯ КОРИСТУВАЧА

Для створення користувальницької моделі угрупування озброєння і військової техніки пропонується в бази даних моделей ввести реальні дані про реально існуючі об'єкти, що входять до складу цього угрупування. Технологія створення користувальницького угрупування ні чим не відрізняється від технології створення нового угрупування розглянутої раніше. Фактично модель угруповання, що призначена для користувача спочатку створюється просто як нове угруповання, при цьому в базу даних повинні бути введені всі нормативні параметри ресурсу усіх об'єктів точно так, як це робиться для віртуального угрупування. Відмінності починаються тільки після збереження угрупування в базі даних моделі. Після збереження нового угрупування можна працювати як з віртуальним угрупуванням, генеруючи і зберігаючи її різні варіанти, або зберегти її як призначену для користувача угруповання. В останньому випадку з угрупуванням вже не можна експериментувати (створювати для неї будь-яку кількість варіантів і досліджувати їх), а можна тільки виробляти прогнозні і планові розрахунки точно так же, як це можна робити для збережених варіантів віртуальних угрупувань.

У режимі моделювання робота з угрупуванням користувача нічим не відрізняється від роботи з віртуальними угрупуваннями. Відмінність полягає лише в тому, що потрібно вибирати не з двох режимів прогнозування, а з чотирьох: нормативне планування та планування користувача як з умовами постачання нових об`єків так і без них.

В статті проведено дослідження модельних угрупувань об`єктів озброєння і військової техніки старих, нових та урівноважених з урахуванням поставок нових зразків. Процедура моделювання у режимі користувача угрупування включає моделювання процесів витрачання та поповнення ресурсу з метою отримання необхідного графіку та редагування даних про усі об`єкти угрупування; редагуванню плану ремонтів та поставок нових об`єктів. Проведено моделювання в режимі нормативного планування для об`єктів умовних типів Тіп-0 та Тіп-1. Це моделювання показало, що перший ремонт планується 01.2023 та списання 03.2031. Аналогічні результати отримані для умов з поставкою нових об`єктів. Підтверджено на практиці достатньо значну ефективність розробленої методики дослідження моделей угрупування озброєння і військової техніки для користування.

Ключові слова: база даних моделей, користувальницьке угрупування, нормативні параметри ресурсу, нормативне планування.

Вступ та аналіз останніх досліджень. Автором зроблено аналіз досліджень в галузі прогнозування процесів витрачання та поповнення ресурсу обєктів озброєння і військової техніки (ОВТ) та їх угрупувань. Так, в даній предметній області багато років працювали і працюють наступні вчені Барзиловіч Є.Ю., Боряк К.Ф., Гніденко Б.В., Каштанов В.О., Коваленко І.Н., Креденцер Б.П., Ланєцький Б.М., Лєнков С.В., Лук`янчук О.О., Сєлюков О.В., Стрельников В.П., Толок І.В., Ушаков І.О., Федухін А.В., Цицарєв В.Н., Шишанов М.О., а також деяких закордонних вчених: Yu Zhou, Gang Kou, Hui Xiao, Yi Peng, Fawaz E.Alsaadi, . K.Chaabane, A.Khatab,C.Diallo, E.-H.Aghezzaf, U.Venkatadri, Fabian Biebl, Robert Glawar, Anahid Jalali, Fazel Ansari, Bernhard Haslhofer, Peter deBoer, Wilfried Sihn, Rui Zheng, Bingkun Chen, LiudongGu, Duc-HanhDinh, PhucDo, Benoit Iung.

В роботі [1] автором надано аналіз його наробок та зроблено висновок, що доволі детально та повно вивчалась та розв`язувалась поставлена задача ще в часи колишнього СРСР, оскільки вона була спрямована на підвищення боєготовності радянської ретро військової техніки. Наукових робіт, що розв`язують проблему прогнозування складу та ресурсу угрупування об`єктів військової техніки та аналіз його варіантів комплексно, в повній мірі сьогодні фактично не існує. Це обумовлює необхідність розв`язання наукової задачі

прогнозування складу та ресурсу угрупування об`єктів військової техніки і аналізу його варіантів.

Через наведене автор значну увагу приділяє розробці методів і засобів підтримання боєготовності Збройних Сил України через підтримання технічного ресурсу як окремих ОВТ так і їх угрупувань. Розглядання питання аналізу витрачання та поповнення ресурсу присвячена велика кількість досліджень, в яких брав участь автор [2-14].

В наведених публікаціях вирішена значна кількість основних аспектів зазначеної проблеми. Особливе місце серед них має робота [4], це монографія у співавторстві на мові Євросоюзу, де розглянуті питання ресурсу складної техніки. Монографія, до речі, проіндексована і стоїть на перших шпальтах фірми Amazon. Достатньо завершеними роботами є [3,5-7,9-11], що видані в редакціях Харківського національного університету Повітряних Сил України та НДІ МВСУ.

Разом з тим до конкретної мети цієї статті максимально наблизила робота [1] та стаття, що видається найближчим часом у Національній Академії Державної прикордонного служби України. Так в них розроблено прогнозування складу та ресурсу угрупування об`єктів військової техніки та аналіз його варіантів та дослідження модельних угрупувань об`єктів озброєння і військової техніки старих, нових та урівноважених з урахуванням поставок нових зразків.

Дійсна стаття у розвиток цих питань присвячена дослідження користувача моделей угрупувань озброєння і військової техніки.

Основна частина роботи. До сих пір ми розглядали приклади моделювання для так званих «віртуальних» угрупувань, тобто угрупувань, склад яких генерувався штучно відповідно заданими користувачем параметрами. Зараз розглядається приклад створення «користувальницького» угрупування, конкретний склад якої визначається користувачем. Якщо віртуальні угрупування створюються з метою дослідження впливу тих чи інших параметрів угрупування на характер протікання в них процес витрачання та поповнення ресурсу (ПВПР) в майбутньому, то призначені для користувача методики визначає, що угрупування створюються з метою вирішення практичних задач планування технічної експлуатації в реальних угрупуваннях.

Створення моделі угрупування ОВТ для користувача. Для створення користувальницької моделі угрупування ОВТ необхідно в базі даних (БД) моделі ввести реальні дані про реально існуючі об'єкти, що входять до складу цього угрупування.

Технологія створення користувальницького угрупування ні чим не відрізняється від технології створення нового угрупування [1] розглянутої вище. Угруповання призначене для користувача спочатку створюється просто як нове угруповання, при цьому в базу даних повинні бути введені всі нормативні параметри ресурсу об'єктів (параметри $\mathbf{P}^{\text{н}}_{\text{рес}i}$) точно так же, як це робилося для віртуального угрупування. Відмінності починаються тільки після збереження угрупування в БД моделі. Після збереження нового угрупування (після того, як її ім'я з'явилося в списку **Збережені угрупування**) далі з нею можна працювати як з віртуальним угрупуванням, генеруючи і зберігаючи її різні варіанти, або зберегти її в БД як призначену для користувача угруповання. В останньому випадку з угрупуванням вже не можна експериментувати (створювати для неї будь-яку кількість варіантів і досліджувати їх), а можна тільки виробляти прогнозні і планові розрахунки точно так же, як це можна робити для збережених варіантів віртуальних угрупувань.

Для створення користувальницького угрупування потрібно в списку **Збережені угруповання** виділити ім'я угрупування, яку ми хочемо зробити для користувача, і після цього натиснути кнопку «Зберегти як угрупування користувача». Після цього в списку збережених угрупувань з'явиться її ім'я зі значком «(п)», а в списку варіантів угрупувань (список праворуч) з'являться варіанти (реалізації), що відповідають кожному окремому типу об'єктів користувальницького угрупування. На рис. 1 показана форма екрану ПК в стані після того, як угрупування якогось типу ААА була збережена як угрупування користувача. У **списку**

Збережені варіанти з'явилися три записи, що відповідає трьом типам об'єктів, які були визначені раніше для угрупування якогось типу AAA (яку ми використовуємо в розглянутих прикладах як тестову угрупування). Імена варіантів формуються автоматично за правилом, яке ми пояснювали раніше. Імена ці в будь-який час можуть бути змінені користувачем на будь-які інші, зручні і звичні для користувача. Для цього потрібно вибрати в списку потрібний варіант і в який з'явився вище (над списком) поле редагування ввести нове найменування.

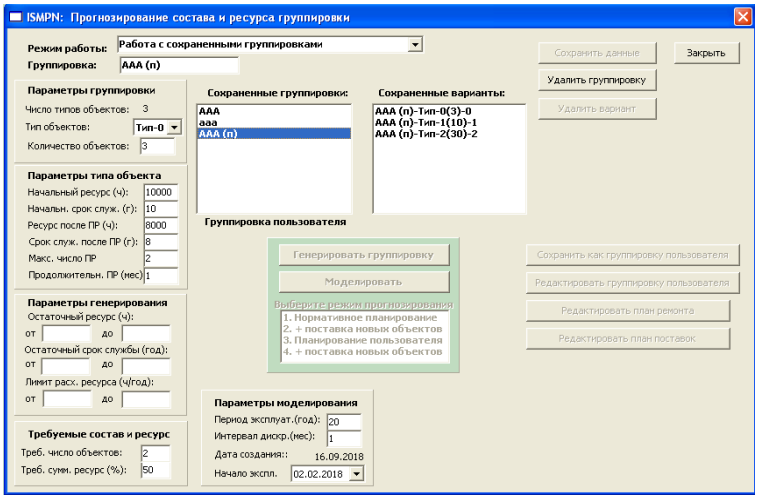

Рисунок 1 – Вигляд екрану ПК після збереження угрупування AAA як угрупування користувача

Моделювання в режимі користувача угрупування. Подальша робота з угрупуванням користувача можлива тільки після того, як буде обраний (клацанням миші) її конкретний варіант в списку збережених варіантів (рис. 2). У цьому стані можливі наступні подальші дії:

- моделювать ПВПР з метою отримання графіків $\overline{R}_{\Sigma i}(t)$ та $\overline{N}_{\Sigma_i}(t)$ (нажать кнопку «Моделювать»);

- редагувати дані про об'єкти угрупування (кнопка «Редагувати угрупування користувача»);

- редагувати призначені для користувача плани ремонту (кнопка «Редагувати план ремонту»);

- редагувати користувальницький план поставок (кнопка «Редагувати план поставок»).

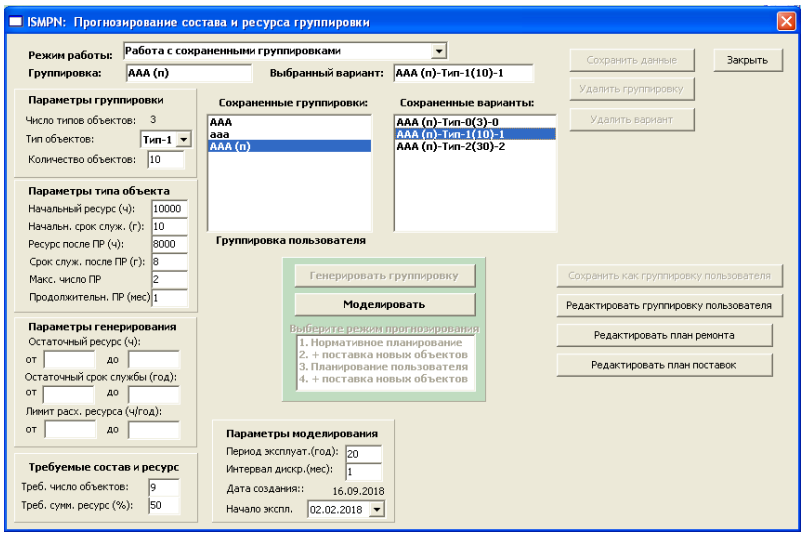

Рисунок 2 – Робота з варіантом угрупування користувача

У режимі моделювання (після натискання кнопки «Моделювати») робота з угрупуванням користувача нічим не відрізняється від роботи з віртуальними угрупуваннями (методику та приклади ми розглянули вище). Відмінність полягає лише в тому, що після натискання кнопки «Моделювати» є можливість вибирати не з двох режимів прогнозування, а з чотирьох, як це показано на рис. 3.

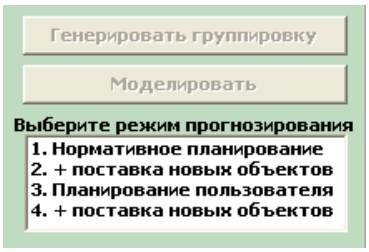

Рисунок 3 – Список вибору режимів прогнозування

Перші два режими повністю аналогічні розглянутим раніше режимам. Відмінністю в їх застосуванні до угрупування користувача полягає тільки в тому, що при моделюванні початковий стан об'єктів та інтенсивності витрачання ресурсу задаються користувачем (а не генеруються, як це робиться в разі віртуальної угрупування). Планові терміни ремонту і списання об'єктів визначаються автоматично (є результатом моделювання) відповідно до заданих для даного типу об'єктів нормативами заповнення ресурсу. Режими планування користувача (режими 3 і 4) відрізняються від відповідних режимів 1 і 2 тим, що користувачем задається не тільки початковий стан об'єктів, але також і заплановані ним терміни відправки в ремонт і списання об'єктів, які також зберігаються в БД. Тому перш ніж здійснювати моделювання для користувальницької угрупування, спочатку слід перевірити (або ввести і зберегти в БД, якщо моделювання проводиться вперше) вихідні дані, що представляють угрупування користувача.

Для цього потрібно натиснути кнопку «Редагувати угруповання користування користувача» (рис. 2). При її натисканні відкриється форма, вид якої показаний на рис. 4. На формі відображається таблиця з даними, відповідними станом об'єктів користувальницького угрупування.

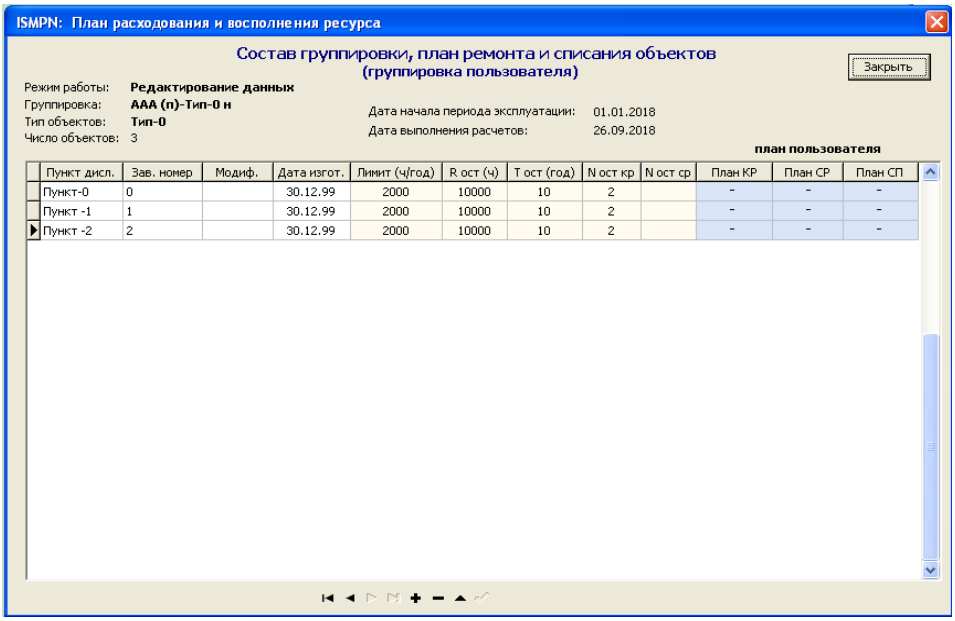

Рисунок 4 – Вигляд екрану ПК в режимі редагування угрупування користувача

Спочатку (після створення угрупування користувача) в таблиці можуть бути випадкові дані. З метою демонстрації роботи програми і одночасно перевірки правильності алгоритмів моделювання введемо для об'єктів Тіп-0 (для угрупування «ААА (п) Тип-0 н») такі дані, однакові для всіх 3-х об'єктів:

L_{ij} = 2000 год/рік – річний ліміт витрати ресурсу;

$R_{ij}(t_0)$ = 10000 год – залишковий ресурс;

$T_{ij}(t_0)$ = 10 років – залишковий термін служби;

$N_{ij}(t_0) = 2$ – залишкове число планових ремонтів (на рис. 4 ці дані вже введені).

Закриємо форму з даними і зробимо моделювання в режимі **Нормативного планування**. В результаті моделювання отримаємо графіки, показані на рис. 5.

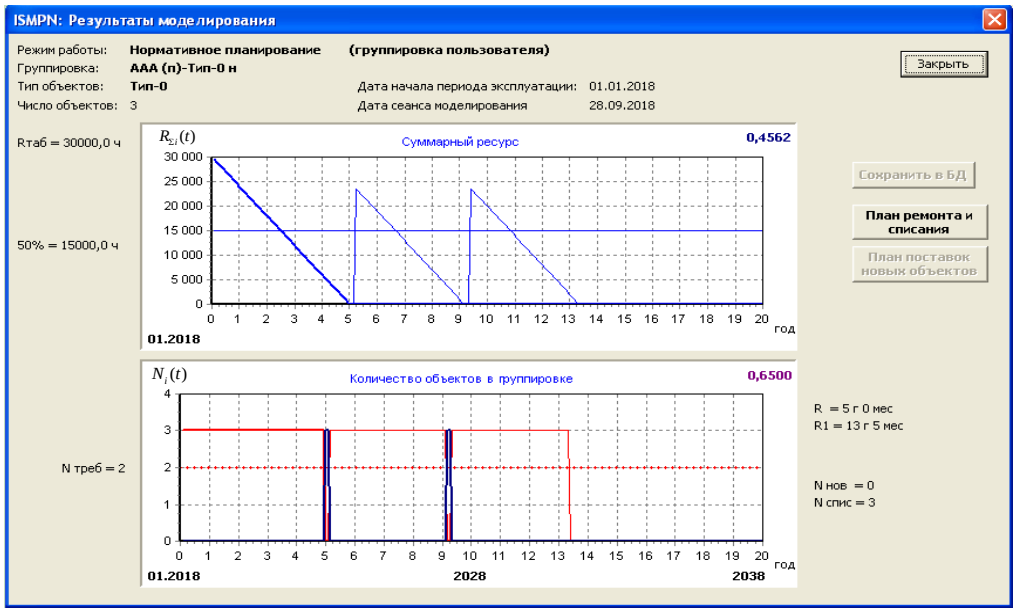

Рисунок 5 – Результати моделювання в режимі **Нормативне планування** (Угруповання користувача, об'єкти **Тіп-0,** тестові дані)

Всі три об'єкти одночасно відправляються в ремонт (01.2023 р - перший ремонт) і одночасно списуються (03.2031 р). Неважко бачити, що отримані результати точно відповідають очікуваним (розрахунковим). Розрахувати нормативні терміни ремонту і списання об'єктів в даному випадку можна наступним чином:

- дата 1-го ремонту:

$$D_{\text{кр1}ij} = D_0 + \frac{R_{ij}(t_0)}{L_{ij}} = 01.2018 + \frac{10000\text{год}}{2000\ \text{год/рік}} = 01.2018 + 5\ \text{років} = 01.2023\ \text{р},$$

де $D_{\text{кр1}\,ij}$ – дата 1-го КР *ij*-го об`єкту; $D_0$ – дата початку інтервалу прогнозування (в нашому прикладі $D_0 = 01.2018$ г ); $R_{ij}(t_0)$ – остаточний ресурс *ij*-го об'єкта на початку інтервалу прогнозування (в момент часу $t_0$ , ототожнюється з датою $D_0$ ); $L_{ij}$ – річний ліміт витрати ресурсу *ij*-го об`єкту; *ij*-й об'єкт в розглянутому прикладі - це *i*-й об`єкт типу **Тіп-0**;

- дата 2-го ремонту:

$$D_{\text{кр2}y} = D_{\text{кр1}y} + \frac{R_j^{\text{н1}}}{L_y} = 01.2023 + \frac{8000\text{год}}{2000\text{год/рік}} = 01.2023 + 4\ \text{роки} + 2\ \text{місяці} = 03.2027\text{р},$$

де $D_{\text{кр2 }ij}$ – дата 2-го КР ij-го об`єкту; $R_j^{\text{н1}}$ – величина ресурсу, що заповнюється після проведення капітального ремонту:

- дата списання:

$$D_{\text{сп}ij} = D_{\text{кр2}ij} + \frac{R_j^{\text{н1}}}{L_{ij}} = 03.2027 + \frac{8000 \text{ год}}{2000 \text{ год/рік}} = 03.2027 + 4 \text{ роки} = 03.2031 \text{ р.}$$

При натисканні кнопки «План ремонту та списання» відкриєтья форма з одержаним нормативним планом (рис. 6). Переконуємось, що одержані в результаті моделювання дані – планові строки ремонту та списання об`єктів **Тіп-0** точно відповідають наведеним вище розрахунковим даним. Це підтверджує правильність реалізації алгоритмів моделювання.

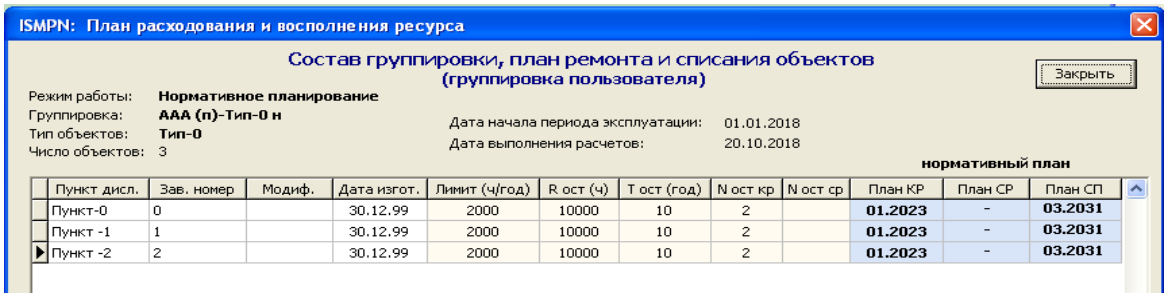

Рисунок 6 – Склад угрупування користувача та одержані для неї нормативні планові строки ремонту та списання об`єктів

Тепер для цього ж угрупування (для об'єктів Тіп-0) зробимо моделювання в режимі **Нормативне планування + поставка нових об'єктів**. Результати моделювання в цьому режимі представлені графіками на рис. 7. Аналіз графіків дозволяє простежити послідовність подій, що відбуваються. У момент часу відправки в 1-й ремонт одночасно 3 об'єктів (01.2023) відбувається поставка 2 нових об'єктів, так як необхідне число об'єктів типу Тіп-0 у вихідних даних задано рівним 2. Двох нових об'єктів, що надійшли в угруповання 01.2023 р, виявляється досить аж до моменту часу одночасного списання старих об'єктів 03.2031 р У цей час ще залишаються працездатними 2 нових об'єкти, раніше надійшли в угруповання. Їх необхідно відправляти в 1-й плановий ремонт 12.2022 р При відправці їх в ремонт порушується необхідний склад угрупування. Для недопущення цього в угрупування необхідно поставити 12.2022 ще два нових об'єкти (сумарне число всіх нових об'єктів, що надійшли в угрупування, стає рівним 4). Після списання двох нових об'єктів, першими надійшли в угрупування (02.2036) ситуація повторюється - через деякий час знову потрібно відправити в ремонт 2 об'єкти і, отже, знову потрібно поставити в угрупування ще 2 нових об'єкти (07.2036). Всі описувані події легко простежуються по рис.7.

Якщо тепер натиснути кнопку «План поставок нових об'єктів», відобразиться форма, вид якої показаний на рис. 8. У розглянутому прикладі на заданому інтервалі експлуатації планується надходження 6 нових об'єктів. Всі нові об'єкти пронумеровані в порядку їх надходження в угрупування.

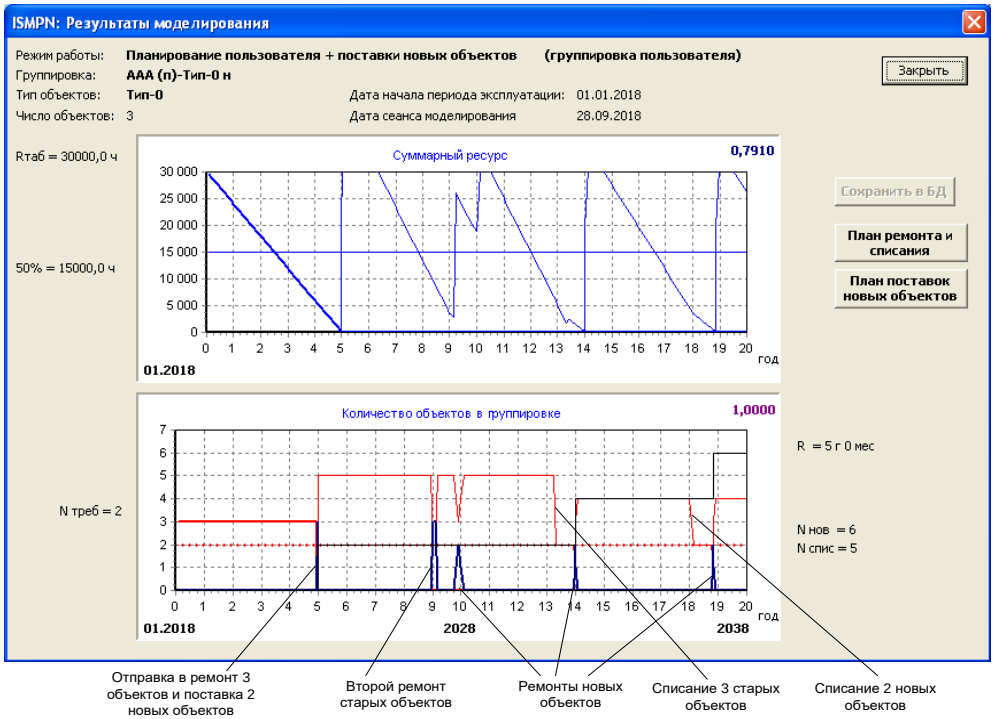

Рисунок 7 – Результати моделювання в режимі **Нормативне планування + поставка нових об'єктів** (угрупування користувача, об'єкти Тіп-0, тестові дані)

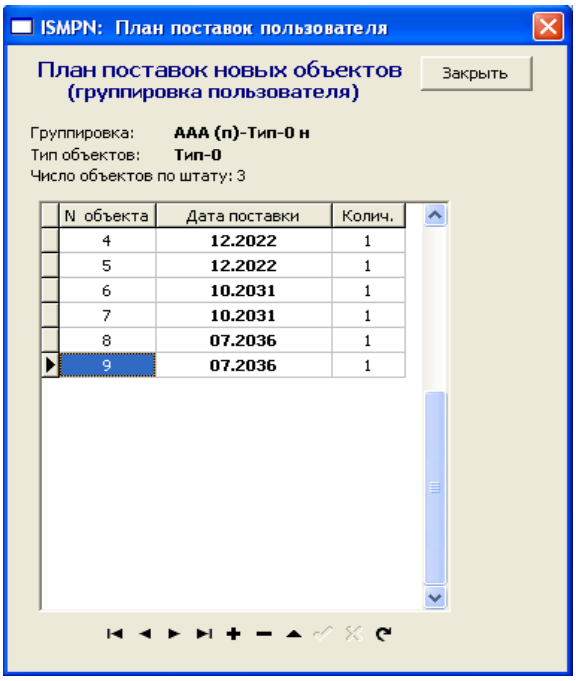

Рисунок 8 – План поставок нових об'єктів (угрупування користувача)

Якщо тепер отримані нормативні значення планових термінів введемо у шпальтах таблиці рис. 4 в якості планових термінів користувача (тобто план користувача зробимо збігається з нормативним планом) і зробимо моделювання в режимі **Планування користувача**, то отримаємо результати, точно збігаються з результатами, отриманими в режимі **Нормативне планування** (рис. 5). Для економії місця ми їх наново не показуємо. Цей результат свідчить про правильність реалізації алгоритмів моделювання в режимі **Планування користувача**.

Тепер відкриємо режим редагування угруповання користувача (шляхом натискання відповідної кнопки) і введемо дані для об'єктів типу Тип-1, показані на рис. 9. Всі цифрові значення параметрів об'єктів задані довільно і є чисто ілюстративними в рамках розглянутого прикладу. Після введення цих даних зробимо моделювання в режимі **Планування користувача**. В результаті моделювання для об'єктів Тіп-1 отримаємо графіки функцій $R_{\Sigma\,\text{тип}-1}(t)$, $N_{\text{тип}-1}(t)$ та $N_{\text{р тип-1}}(t)$, показані на рис. 10.

Пункт дисл.	Зав. номер	Модиф.	Дата изгот.	Лимит (ч/год)	R ост (ч)	T ост (год)	N ост кр	N ост ср	План КР	План СР	План СП
Пункт-0	0		30.12.99	1500	10000	12	2		01.03.21	-	01.01.28
Пункт-1	1		30.12.99	1500	10000	12	2		01.06.21	-	01.01.29
Пункт-2	2		30.12.99	1500	10000	12	2		01.08.21	-	01.01.30
Пункт-3	3		30.12.99	1500	10000	12	2		01.01.22	-	01.06.30
Пункт-4	4		30.12.99	1500	10000	12	2		01.05.22	-	01.01.31
Пункт-5	5		30.12.99	1500	10000	12	2		01.05.22	-	01.05.31
Пункт-6	6		30.12.99	1500	10000	12	2		01.09.22	-	01.06.31
Пункт-7	7		30.12.99	1500	10000	12	2		01.01.23	-	01.01.32
Пункт-8	8		30.12.99	1500	10000	12	2		01.01.23	-	01.06.32
Пункт-9	9		30.12.99	1500	10000	12	2		01.07.23	-	01.01.34

Рисунок 9 – Вихідні дані для моделювання в режимі **Планування користувача** (Об'єкти Тіп-1, дані користувача)

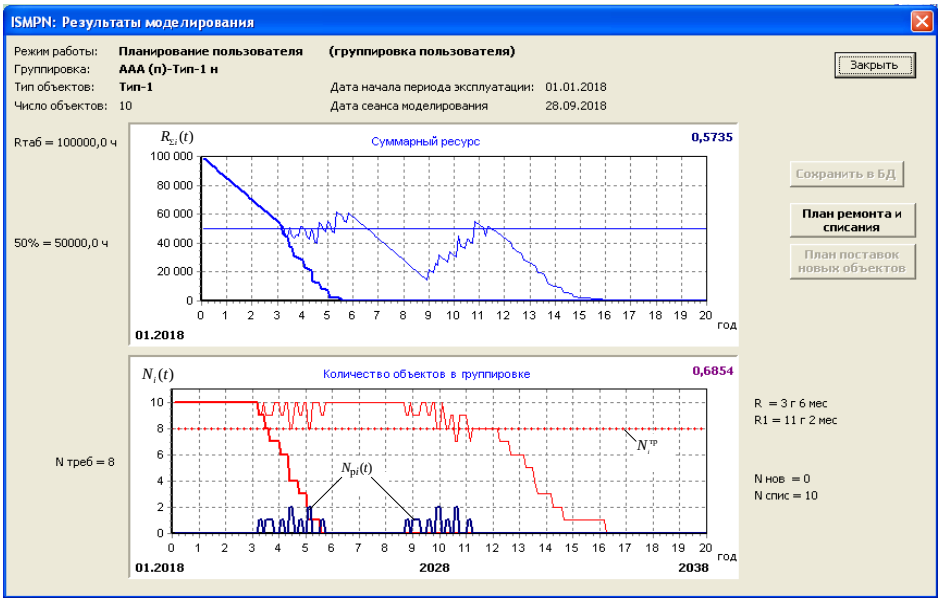

Рисунок 10 – Результати моделювання в режимі **Планування користувача** для об'єктів Тіп-1 (для вихідних даних, показаних на рис. 7)

Для цих же вихідних даних зробимо моделювання в режимі **Планування користувача + поставки нових об'єктів.** Необхідна кількість об'єктів поставимо рівним $N^{\text{тр}}_{\text{тип-1}}$. Отримані в результаті моделювання відповідні графіки наведені на рис. 11.

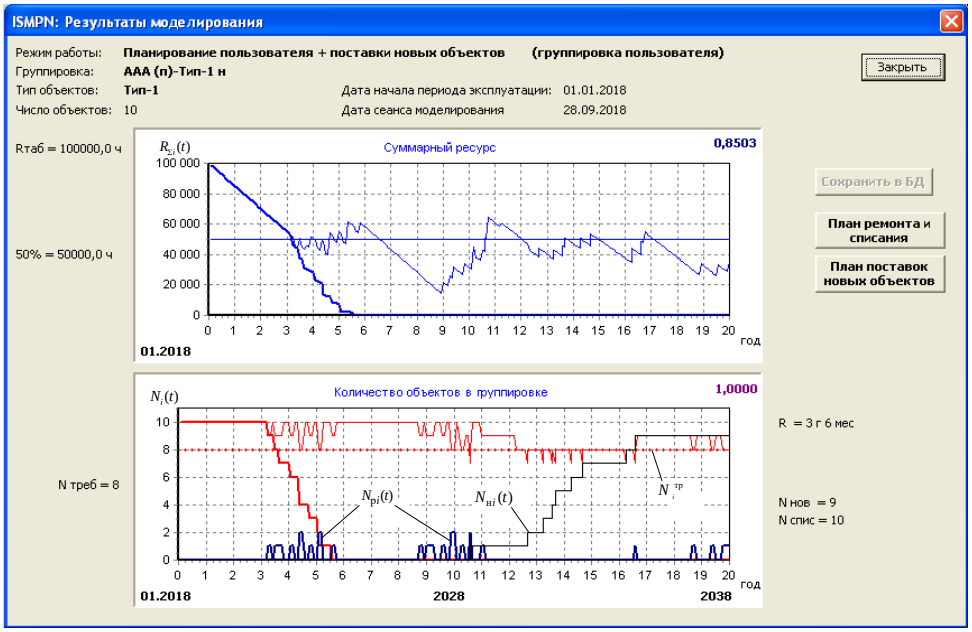

Рисунок 11 – Результати моделювання в режимі **Планування користувача + поставки нових об'єктів** (об'єкти типу Тип-1)

Висновки

1. В статті представлені основні результати розробки методів та дослідження моделей створення угрупування озброєння і військової техніки для користувача, що є розвитком розробок прогнозування складу та ресурсу угрупування об`єктів військової техніки та аналізу його варіантів та дослідження модельних угрупувань об`єктів озброєння і військової техніки старих, нових та урівноважених з урахуванням поставок нових зразків.

2. Процедура моделювання у режимі користувача угрупування включає моделювання ПВПР з метою отримання відповідного графіку та редагування даних про об`єкти угрупування; редагуванню плану ремонтів та поставок нових об`єктів.

3. Проведено моделювання в режимі нормативного планування для об`єктів умовних типів Тіп-0 та Тіп-1. Це моделювання показало, що перший ремонт планується 01.2023 та списання 03.2031; з поставкою нових об`єктів відповідно 02.2036 та 07.2036.

4. Підтверджено на практиці достатньо значну ефективність розробленої методики дослідження моделей угрупування озброєння і військової техніки для користувача.

ЛІТЕРАТУРА:

1. Лєнков Є.С. Прогнозування складу та ресурсу угрупування об`єктів військової техніки, аналіз його варіантів кроків управління підрозділами // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2021. – № 73. – С. 39 – 51.

2. Жиров Г.Б., Лєнков Є.С., Толок І.В. Алгоритмічна модель адаптивного технічного обслуговування за станом озброєння і військової техніки // Збірник праць Національної академії Державної прикордонної служби України імені Б. Хмельницького. Серія: військові та технічні науки. – Хмельницький, 2017 – № 1(71). С.368 – 378.

3. Жиров Г.Б., Лєнков Є.С., Бондаренко Т.В. Алгоритмічна модель процесу технічного обслуговування за станом з постійною періодичністю контролю // Журнал «Сучасна спеціальна техніка». – Київ, 2017. – №1(45). - С. 26 – 29.

4. Forecasting reliability of complex technology objects. Parameters optimization of their technical exploitation: [monography] in English / Sergey Lenkov, Igor Tolok, Vadim Tsitsarev, Genadiy Zhyrov, Evgen Lenkov, Yurii Khlaponin, Bohdan Borowik; under edition S.V. Lenkov. – Poland: Publishing house «Bielsko-Biala», 2018. – 253 p.

5. Ленков Е.С., Жиров Г.Б., Бондаренко Т.В. Формализованная математическая модель процесса адаптивного технического обслуживания по состоянию сложной радиоэлектронной техники // Журнал «Інформатика та математичні методи в моделюванні». – Одеса, 2016. –Т.6., №4. - С.365 – 371.

6. S. Lenkov, G. Zhyrov, D. Zaytsev, I. Tolok, E. Lenkov, T. Bondarenko, Y. Gunchenko, V. Zagrebnyuk, O. Antonenko/ Features of modeling failures of recoverable complex technical objects with a hierarchical constructive structure // Восточно-европейский журнал передовых технологий.- №4. – 2017. – С. 34 – 42.

7. Лєнков С.В., Сєлюков О.В., Толок І.І., Лєнков Є.С., Бондаренко Т.В. Математична модель процесів витрачання та поповнення ресурсу угруповання складних технічних об'єктів // Журнал «Наука і техніка Повітряних Сил ЗСУ» - Харків, – 2018. – №. 2 (31)– С. 174 – 181.

8. Lenkov E.S. The option for calculating the indicators of the needlessness of the unbelievable complex object of technique // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2018. – № 59. – С.56 – 61.

9. Ленков С.В., Жиров Г.Б., Толок И.В., Ленков Е.С. Имитационная статистическая модель процесса технического обслуживания и ремонта группировки сложных технических объектов // Журнал сучасна спеціальна техніка. – К., №1(52). – С. 49 – 57.

10. Лєнков Є.С., Толок І.В. Прогнозування складу і ресурсу угрупувань технічних об'єктів // Науковий журнал «Системи озброєння і військова техніка», Харків, 2018. – №3(55). – С. 78 – 84.

11. Лєнков С.В., Толок І.В., Лєнков Є.С., Цицарєв В.М. Програмне забезпечення моделювання процесів витрачання і поповнення ресурсу угрупувань технічних об’єктів // Журнал «Наука і техніка Повітряних Сил ЗСУ. - Харків, – 2018. – Вип.3(32). – С. – 120 – 126.

13. Lienkov S. V. Zhirov H. B. Tolok I. V. Lienkov Ye. S. // Simulation model of the adaptive maintenance procedure of complex radioelectronic facilities 2313-688X Radio Electronics, Computer Science, Control. ISSN: 1607-3274. 2020. № 1. – P63-74. DOI 10.15588/1607-3274-2020-1-7.

14. Tolok I.V., Banzak G.V., Lienkov Ye.S., Vozikova L.M. Comparative study of different maintenance strategies // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2020. – № 68. – С.14 – 22.

REFERENCES:

1. Lenkov Je.S. (2021), Prognozuvannja skladu ta resursu ugrupuvannja ob`jektiv vijs'kovoi' tehniky, analiz jogo variantiv krokiv upravlinnja pidrozdilamy, Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, Kyiv, no. 73, pp. 39 – 51.

2. Zhyrov G.B., Lenkov Je.S. and Tolok I.V. (2017), Algorytmichna model' adaptyvnogo tehnichnogo obslugovuvannja za stanom ozbrojennja i vijs'kovoi' tehniky. Zbirnyk prac' Nacional'noi' akademii' Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny imeni B. Hmel'nyc'kogo. Serija: vijs'kovi ta tehnichni nauky. – Hmel'nyc'kyj, no. 1(71), pp.368 – 378.

3. Zhyrov G.B., Lenkov Je.S. and Bondarenko T.V. (2017), Algorytmichna model' procesu tehnichnogo obslugovuvannja za stanom z postijnoju periodychnistju kontrolju. Zhurnal «Suchasna special'na tehnika». Kyi'v, no. 1(45), pp. 26 – 29.

4. Forecasting reliability of complex technology objects. Parameters optimization of their technical exploitation: [monography] in English / Sergey Lenkov, Igor Tolok, Vadim Tsitsarev, Genadiy Zhyrov, Evgen Lenkov, Yurii Khlaponin, Bohdan Borowik; under edition S.V. Lenkov. – Poland: Publishing house «Bielsko-Biala», 2018. – 253 p.

5. Lenkov E.S., Zhyrov G.B. and Bondarenko T.V. (2016), Formalyzovannaja matematycheskaja model' processa adaptyvnogo tehnycheskogo obsluzhyvanyja po sostojanyju slozhnoj radyoэlektronnoj tehnyky, Zhurnal «Informatyka ta matematychni metody v modeljuvanni». Odesa, Vol .6., no. 4, pp. 365 – 371.

6. S. Lienkov, G. Zhyrov, D. Zaytsev, I. Tolok, E. Lenkov, T. Bondarenko, Y. Gunchenko, V. Zagrebnyuk and O. Antonenko (2017), Features of modeling failures of recoverable complex technical objects with a hierarchical constructive structure. Eastern European Journal of Advanced Technology, no. 4, pp. 34 – 42.

7. Lienkov S.V., Sjeljukov O.V., Tolok I.I., Ljenkov Je.S. and Bondarenko T.V. (2018), Matematychna model' procesiv vytrachannja ta popovnennja resursu ugrupovannja skladnyh tehnichnyh ob'jektiv. Nauka i tehnika Povitrjanyh Syl ZSU. Harkiv, no. 2 (31), pp. 174 – 181.

8. Lenkov E.S. (2018), The option for calculating the indicators of the needlessness of the unbelievable complex object of technique. Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka. Kyi'v, no. 59, pp.56 – 61.

9. Lienkov S.V., Zhyrov G.B., Tolok Y.V. and Lenkov E.S. (2018), Imitacionnaja statisticheskaja model' processa tehnicheskogo obsluzhivanija remonta gruppirovki slozhnyh tehnicheskih ob#ektov. Zhurnal suchasna special'na tehnika // Zhurnal suchasna special'na tehnika. Kyi'v, no 1(52), pp. 49 – 57.

10. Lenkov Є.S., Tolok I.V. (2018), Prognozuvannja skladu i resursu ugrupuvan' tehnichnih ob'єktiv. Naukovij zhurnal «Sistemi ozbroєnnja i vijs'kova tehnika», Harkiv, no 3(55), pp. 78 – 84.

11. Lienkov S.V., Tolok I.V., Lenkov Є.S. and Cicarev V.M. (2018), Programne zabezpechennja modeljuvannja procesiv vitrachannja i popovnennja resursu ugrupuvan' tehnichnih ob'єktiv. Nauka i tehnika Povitrjanih Sil ZSU. Harkiv, Vip.3(32), pp. 120 – 126.

13. Lienkov S.V. Zhirov H.B. Tolok I.V. Lienkov Ye.S. // Simulation model of the adaptive maintenance procedure of complex radioelectronic facilities 2313-688X Radio Electronics, Computer Science, Control. ISSN: 1607-3274. 2020. № 1. – P63-74. DOI 10.15588/1607-3274-2020-1-7.

14. Tolok I.V., Banzak G.V., Lenkov Ye.S., Vozikova L.M. Comparative study of different maintenance strategies Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv. – K., 2020. No. 68, pp.14 – 22.

PhD Lenkov E.S.

DEVELOPMENT OF WAREHOUSE AND RESOURCE MODELING METHODS WEAPONS AND MILITARY EQUIPMENT GROUP FOR USER

For creation a custom model of the group of armaments and military equipment, it's proposed to enter real data on the existing objects, that are part of this group in the database of models. The technology of creating a custom grouping is no different from the technology of creating a new grouping discussed earlier. In fact, the user grouping model is initially created simply as a new grouping, and all regulatory resource parameters of all objects must be entered into the database exactly as it's done for a virtual grouping. Differences begin only after saving the grouping in the model database. After saving a new group, you can work as a virtual group, generating and saving its various variants, or save it as a custom group. In the latter case, you can no longer experiment with the group (create any number of options for it and explore them), but can only make forecast and planned calculations in the same way as you can for saved versions of virtual groups.

In simulation mode, working with a group of users is no different from working with virtual groups. The only difference is that you need to choose not from two forecasting modes, but from four: regulatory planning and user planning, both with the conditions of delivery of new facilities and without them.

In the article the research of model groupings of objects of armaments and military equipment of old, new and balanced taking into account deliveries of new samples is carried out. The modeling procedure in the group user mode includes modeling the processes of spending and replenishing the resource in order to obtain the necessary schedule and edit data on all objects of the group; editing the plan of repairs and deliveries of new objects. The modeling in the mode of normative planning for objects of conditional types Tin-0 and Tin-1 is carried out. This simulation showed that the first repair is planned for 01.2023 and write-off on 03.2031. The similar results were obtained for the conditions with the delivery of new facilities. The rather significant efficiency of the developed methodology of the research models of armaments and military equipment grouping for using is confirmed in practice.

Keywords: models database, user grouping, normative parameters of resource, normative planning.

УДК 351.864

д.т.н., проф. **Харченко О.В.** (ДНДІА)
д.т.н., проф. **Зіатдінов Ю.К.** (ДНДІА)
д.т.н., с.н.с. **Мавренков О.Є.** (ДНДІА)

DOI: https://doi.org/10.17721/2519-481X/2022/74-05

МЕТОДИКА ОПЕРАТИВНОГО РОЗРАХУНКУ ТЕХНІЧНОГО РІВНЯ КЕРОВАНИХ АВІАЦІЙНИХ ЗАСОБІВ УРАЖЕННЯ

Актуальність проблематики кількісного оцінювання технічної досконалості авіаційних засобів ураження обумовлюється, насамперед, завданням порівняння альтернативних їх зразків та вибору кращих варіантів при розробленні або закупівлі для потреб Збройних Сил України.

Аналіз практичного застосування відомих методів теорії прийняття рішень показує, що вони власне не вирішують задачу отримання оцінки технічного рівня виробу у кількісному вимірі, а лише дозволяють побудувати певний пріоритетний ряд оцінюваних виробів у порядку збільшення / зменшення їх технічного рівня, що не дозволяє наочно оцінити (порівняти) величину (ступінь) зміни рівня технічної досконалості одного виробу по відношенню до іншого.

В цьому сенсі кваліметрічні методи дозволяють здійснювати кількісне оцінювання технічного рівня (якості) виробів по відношенню до базового (еталонного) зразка, що обумовлює зручність їх застосування для вирішення задач вибору. Але використання методичного апарату кваліметрії в кожному конкретному випадку потребує його адаптації з урахуванням особливостей оцінюваного виробу в частині обґрунтування його визначальних показників технічної досконалості та визначення їх відносної важливості.

У статті представлено результати дослідження авторів з розроблення методики оцінювання технічного рівня (якості) керованих авіаційних засобів ураження як складової системи підтримки рішень з розроблення / закупівлі зразків озброєння та військової техніки для потреб Збройних Сил України. В основу розробленої методики покладається кваліметрічний комплексний метод оцінювання якості складних технічних систем, заснований на співвідношенні визначальних показників технічної досконалості оцінюваного та базового (еталонного) виробів з урахуванням відносної важливості (вагомості) таких показників. Представлена методика дозволяє оперативно (з мінімальними витратами часу в порівнянні з процедурами експертного оцінювання) проводити розрахунки технічного рівня авіаційних засобів ураження з метою їх порівняння (вибору).

Ключові слова: авіаційні засоби ураження, складна технічна система, технічний рівень, показники технічної досконалості, тактико-технічні характеристики, коефіцієнт вагомості.

Вступ. На сьогодні в Збройних Силах України гостро постала проблема технічного оновлення авіаційних засобів ураження (АЗУ). Розв'язання цієї проблеми можливо шляхом розроблення нових перспективних зразків, модернізації існуючих та / або закупівлі зразків за імпортом, що в свою чергу породжує задачу вибору раціональних варіантів рішень. Одним з визначальних показників такого вибору є технічний рівень зразка АЗУ.

Власне оцінювання технічного рівня (якості) зразків озброєння та військової техніки (ОВТ) є одним з ключових етапів у системі прийняття рішення на їх розроблення (закупівлю), вибір кращих (раціональних) їх варіантів, впровадження оптимальних технічних рішень з їх створення та модернізації тощо.

Аналіз останніх досліджень і публікацій. Як відомо, теорія та практика оцінювання якості товарів і послуг використовує аналітичні (математичні) та експертні методи. Серед аналітичних (математичних) методів широке застосування для оцінювання технічного рівня виробів (систем, пристроїв тощо) поряд з "класичними" кваліметрічними методами знайшли й окремі методи теорії прийняття рішень, наприклад, метод простого адитивного зважування, метод ідеальної точки, метод ЕЛЕКТРА, метод аналізу ієрархій [1-6].

Однак аналіз практичного застосування зазначених методів теорії прийняття рішень показує, що вони власне не вирішують задачу отримання оцінки технічного рівня виробу у кількісному вимірі, проте дозволяють побудувати певний пріоритетний ряд оцінюваних

виробів у порядку збільшення / зменшення їх технічного рівня, що не дозволяє наочно оцінити (порівняти) величину (ступінь) зміни рівня технічної досконалості одного виробу по відношенню до іншого.

Кваліметрічні ж методи дозволяють здійснювати кількісне оцінювання технічного рівня (якості) виробів по відношенню до базового (еталонного) зразка. Застосування таких методів для оцінювання технічного рівня складних технічних систем (СТС), до яких належать і керовані АЗУ, показує, що найбільш доцільним для зазначеної задачі є комплексний метод оцінювання якості, який дозволяє врахувати не тільки потрібну множину показників технічної досконалості (ПТД), що описують СТС, а й складну ієрархічну їх побудову [7-13].

Авторами пропонується методика оперативного розрахунку технічного рівня керованих авіаційних засобів ураження, заснована на кваліметрічному комплексному методі оцінювання якості СТС. Термін "оперативний" тут використовується у розумінні мінімуму потрібних трудовитрат (часу) для здійснення процедури оцінювання технічного рівня.

Основний матеріал дослідження. Загальноприйнятим показником оцінювання технічного рівня СТС є коефіцієнт технічного рівня (КТР). Математичний апарат розрахунку КТР засновується на співставленні (співвідношенні) визначальних ПТД оцінюваного та базового зразків, як правило, з урахуванням відносної важливості функціональних підсистем та показників [7-12].

Власне розрахунок КТР АЗУ виконується за формулою:

$$K_{TP} = \sum_{k=1}^{M} \sum_{ki=1}^{N_k} \delta_k \gamma_{ki} \frac{\overline{\chi}_{ki}}{\overline{\chi}_{ki}^{баз}},$$

де δ_k – коефіцієнт вагомості k-ої функціональної підсистеми зразка АЗУ, який оцінюється, такий, що $\sum_{k=1}^{M} \delta_k = 1$;

γ_{ki} – коефіцієнт вагомості і-го ПТД (ТТХ) k-ої функціональної підсистеми зразка АЗУ, який оцінюється, такий, що $\sum_{ki=1}^{N_k} \gamma_{ki} = 1$;

M – кількість функціональних підсистем оцінюваного зразка АЗУ;

N_k – кількість визначальних ПТД (ТТХ) k-ої функціональної підсистеми оцінюваного зразка АЗУ;

$\overline{\chi}_{ki}, \overline{\chi}_{ki}^{баз}$ – приведені значення і-го ПТД (ТТХ) k-ої функціональної підсистеми оцінюваного та базового зразка АЗУ, відповідно, такі, що:

$$\overline{\chi}_{ki}(\overline{\chi}_{ki}^{баз}) = \begin{cases} X_{ki}(X_{ki}^{баз}) & \text{, якщо збільшення і-го ПТД (ТТХ) k-ої функціональної підсистеми зразка АЗУ відповідає збільшенню його технічної досконалості;} \\ \frac{1}{X_{ki}}(\frac{1}{X_{ki}^{баз}}) & \text{, якщо збільшення і-го ПТД (ТТХ) k-ої функціональної підсистеми зразка АЗУ відповідає зменшенню його технічної досконалості.} \end{cases}$$

$X_{ki}, X_{ki}^{баз}$ – натуральні значення і-го ПТД (ТТХ) k-ої функціональної підсистеми оцінюваного та базового зразків АЗУ, відповідно.

Структурну блок-схему методики розрахунку КТР АЗУ наведено на рис. 1.

На першому етапі процесу оцінювання КТР здійснюється формування масиву вихідних даних, необхідних для проведення розрахунків, а саме визначаються зразок АЗУ, який підлягає оцінюванню, та зразок-аналог, який буде прийнятий за базовий, та, за необхідності,

виконується адаптація математичного апарату кваліметрічної оцінки якості складних технічних систем до конкретного об’єкту оцінки.

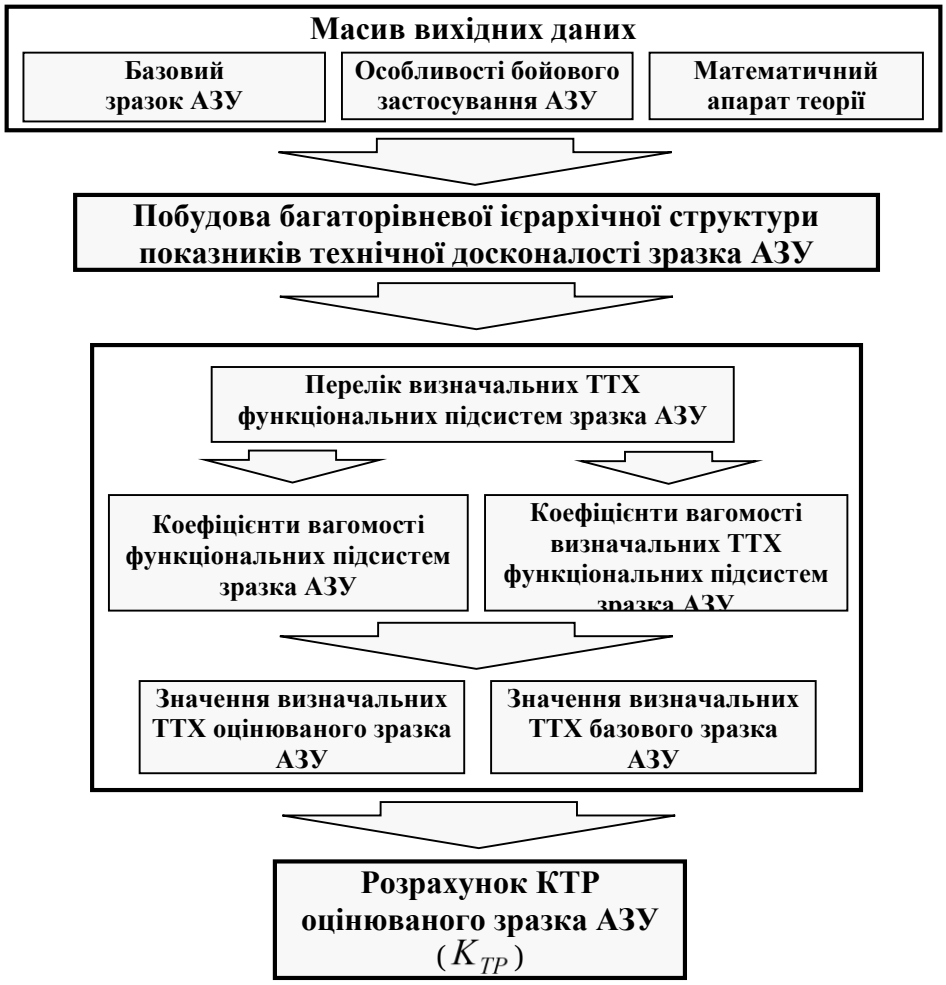

Рисунок 1 – Блок-схема методики розрахунку КТР зразка АЗУ

На другому етапі здійснюється формування структури оцінюваних ПТД (ТТХ, параметрів), а саме виконується побудова багаторівневої ієрархічної структури показників технічної досконалості зразка АЗУ та визначаються його основні функціональні підсистеми, їх визначальні ТТХ (ПТД), напрями впливу кожної ТТХ (ПТД) на технічну досконалість зразка, значення (кількісні та / або якісні) ТТХ (ПТД) оцінюваного та базового зразків.

На третьому етапі визначаються коефіцієнти вагомості функціональних підсистем зразка АЗУ та їх ТТХ (ПТД). На цьому етапі встановлюється відносна важливість кожної з функціональних підсистем та відносна важливість кожної ТТХ (ПТД) у окремій функціональній підсистемі з точки зору ефективного ураження об’єктів противника. З цією метою використовується метод парних порівнянь [14].

На останньому етапі виконується розрахунок КТР зразка АЗУ, що оцінюється, за формулою (1) та здійснюється аналіз отриманих результатів.

Програмна реалізація математичного апарату методики розрахунку КТР зразка АЗУ може бути впроваджена у середовищі табличного редактору Excel програмного пакету Microsoft Office.

Представлену методику апробовано в рамках досліджень щодо порівняльного аналізу керованих АЗУ, що стоять на озброєння Збройних Сил України та закордонних аналогів. Результати оцінювання технічного рівня зазначених АЗУ наведено в табл. 1 – 4.

Таблиця 1

Вхідні дані та результати розрахунку коефіцієнтів технічного рівня керованих ракет класу "повітря - повітря" малої дальності

№ п/п	Найменування функціональних підсистем та їх основних характеристик (показників)	Коефіцієнт вагомості	Найменування ракети								
			Р-60М	Р-73	AIM-9X Sidewinder	AIM-132 ASRAAM	A-DARTER	IRIS-T	AIM-7E Sidewinder	R.550 Magic-2	PYTHON-5
1.	**БОЙОВА**	**0,354**									
1.1	Ймовірність ураження цілі	0,34	0,5	0,6	0,75	0,7	0,6	0,7	0,5	0,7	0,75
1.2	Уражаючий фактор, од.	0,33	0,078	0,067	0,119	0,080	0,191	0,131	0,195	0,133	0,194
1.3	Максимальна дальність пуску, м	0,33	10	20	35	18	20	25	12	10	15
2.	**ТАКТИЧНА**	**0,343**									
2.1	Ступінь автономності[1]	0,34	3	3	3	3	3	3	1	3	3
2.2	Швидкість на траєкторії (число Маха)	0,33	2,0	2,02	2,5	3,5	2,0	3,0	2,0	2,7	2,5
2.3	Можливість захвату цілі на траєкторії[2]	0,33	1	1	2	1	1	1	1	1	2
3.	**ВИЖИВАНОСТІ**	**0,303**									
3.1	Величина ЕПР, кв.м.	0,33	0,097	0,263	0,147	0,251	0,258	0,152	0,460	0,221	0,214
3.2	Можливість скритності дії системи наведення[3]	0,34	2	2	2	2	2	2	1	2	2
3.3	Максимальне перевантаження цілі, од.	0,33	10	12	15	10	12	12	10	15	15
Коефіцієнт технічного рівня			0,91	1,0	1,39	1,09	1,22	1,28	0,91	1,15	1,40

Примітки.

[1] – «1» – принцип «пустив – супроводжую до влучення у ціль», «2» – принцип «пустив – супроводжую до захвату цілі ракетою», «3» – принцип «пустив – забув»; [2] – «1» – ні, «2» – так; [3] – «1» – ні, «2» – так.

Таблиця 2

Вхідні дані та результати розрахунку коефіцієнтів технічного рівня керованих ракет класу "повітря - повітря" середньої та великої дальності

№ п/п	Найменування функціональних підсистем та їх основних характеристик (показників)	Коефіцієнт вагомості	Найменування ракети										
			Р-27Т	Р-27ЭТ	Р-27Р	Р-27ЭР	MICA IR	AIM-120C AMRAAM	MICA EM	Meteor	PBB-AE	AIM-7M Sparrow	AIM-120A AMRAAM
1.	**БОЙОВА**	**0,354**											
1.1	Ймовірність ураження цілі	0,34	0,7	0,7	0,6	0,6	0,7	0,8	0,8	0.8	0,8	0.6	0,8
1.2	Уражаючий фактор, од.	0,33	0,159	0,114	0,154	0,111	0,107	0,124	0,109	0,156	0,120	0,195	0,149
1.4	Максимальна дальність пуску, м	0,33	50	84	60	93	60	120	50	100	100	100	70
2.	**ТАКТИЧНА**	**0,343**											
2.1	Ступінь автономності[1]	0,25	3	3	1	1	3	3	3	3	3	1	3
2.2	Швидкість на траєкторії число Маха)	0,25	2,8	2,8	2,8	2,8	4,0	4,0	4,0	4,0	4,0	2,5	4,0
2.3	Можливість захвату цілі на траєкторії[2]	0,25	1	1	1	1	1	2	2	1	2	1	2
2.4	Можливість пере націлювання[3]	0,25	1	1	2	2	1	2	2	1	2	1	2
3.	**ВИЖИВАНОСТІ**	**0,303**											
3.1	Величина ЕПР, кв.м.	0,33	0,630	0,746	0,678	0,794	0,265	0,364	0,265	0,363	0,454	0,456	0,364
3.2	Можливість скритності дії системи наведення[4]	0,34	2	2	1	1	2	2	2	2	2	1	2
3.3	Максимальне перевантаження цілі, од.	0,33	8,0	8,0	8,0	8,0	10,0	12,0	10,0	15,0	12,0	8,0	10,0
Коефіцієнт технічного рівня			1,33	1,42	1,0	1,05	1,46	1,76	1,57	1,69	1,71	1,10	1,64

Примітки.

[1] – «1» – принцип «пустив – супроводжую до влучення у ціль», «2» – принцип «пустив – супроводжую до захвату цілі ракетою», «3» – принцип «пустив – забув»; [2] – «1» – ні, «2» – так; [3] – «1» – ні, «2» – так; [4] – «1» – ні, «2» – так.

Таблиця 3

Вхідні дані та результати розрахунку коефіцієнтів технічного рівня керованих ракет класу "повітря - поверхня"

№ п/п	Найменування функціональних підсистем та їх основних характеристик (показників)	Коефіцієнт вагомості	Найменування ракети										
			С-25Л	Х-25МЛ	Х-29Л	Х-29Т	Х-59	AGM-65E Maverick	AJ.168 Martel	AGM-65F Maverick	AGM-142E Рерчк-2	AGM-65H Maverick	AS.30AL
1.	**БОЙОВА**	**0,354**											
1.1	Точність наведення (кругове ймовірне відхилення), м	0,2	6,0	5,8	5,75	2,9	4,0	2,5	3,0	2,5	4,0	2,5	1,0
1.2	Уражаючий фактор, од.	0,2	0,379	0,406	0,482	0,473	0,187	0,472	0,273	0,424	0,250	0,469	0,481
1.3	Швидкість на траєкторії, м/с	0,2	500	420	350	350	350	320	400	320	420	320	472
1.4	Максимальна дальність пуску, км	0,2	7	7	7	13	40	27	45	27	150	30	13
1.5	Мінімальна дальність пуску, км	0,2	3	3	3	3	13	5	15	5	20	5	3
2.	**ТАКТИЧНА**	**0,343**											
2.1	Ступінь автономності[1]	0,25	1	1	1	2	3	1	2	3	2	3	1
2.2	Ступінь цілодобовості та всепогодності[2]	0,25	1	1	1	2	2	1	2	3	2	3	1
2.3	Можливість застосування по рухомим цілям[3]	0,25	1	1	1	2	2	1	2	1	1	2	1
2,4	Можливість перенацілювання[5]	0,25	1	1	1	2	2	1	2	1	2	1	1
3.	**ВИЖИВАНОСТІ**	**0,303**											
3.1	Величина ЕПР, кв.м.	0,33	1,380	0,848	1,758	1,758	2,435	0,728	1,945	0,728	4,284	0,728	1,344
3.2	Можливість скритності дії системи наведення[6]	0,34	1	1	1	2	2	1	2	2	2	1	1
3.4	Наявність горизонтальної ділянки польоту при підході до цілі[7]	0,33	1	1	1	1	2	1	1	1	2	1	1
Коефіцієнт технічного рівня			0,81	0,80	0,80	1,0	1,14	1,02	1,07	1,20	1,57	1,21	1,04

Примітки.

[1] – «1» – принцип «пустив – супроводжую до влучення у ціль», «2» – принцип «пустив – супроводжую до захвату цілі ракетою», «3» – принцип «пустив – забув»; [2] – «1» – вдень в ПМУ, «2» – вдень і вночі в простих метеоумовах, «3» – вдень і вночі в простих і складних метеоумовах; [3, 4, 5, 6, 7] – «1» – ні, «2» – так.

Таблиця 4

Вхідні дані та результати розрахунку коефіцієнтів технічного рівня керованих / коригованих авіаційних бомб

№ п/п	Найменування функціональних підсистем та їх основних характеристик (показників)	Коефіцієнт вагомості	Найменування авіаційної бомби										
			КАБ-500Л	КАБ-500Кр	КАБ-1500Л-Ф	КАБ-1500Кр	GBU-10 Paveway II	GBU-12 Paveway II	GBU-15 (V)2/B	GBU-35 JDAM	GBU-38 JDAM	BLG 1000 Arcole	Opher Mk.82
1.	**БОЙОВА**	**0,354**											
1.1	Точність наведення (кругове ймовірне відхилення), м	0,34	10	4	10	5	9	9	4	10	10	2	1,5
1.2	Маса бойової частини, кг	0,33	360	380	1180	1075	429	100	930	202	100	500	100
1.3	Максимальна дальність скидання, км	0,33	9	9	10	10	15	10	24	24	16	10	15
2.	**ТАКТИЧНА**	**0,343**											
2.1	Ступінь автономності[1]	0,25	1	3	1	3	1	1	3	3	3	1	3
2.2	Ступінь цілодобовості та всепогодності[2]	0,25	1	1	1	1	1	1	2	3	3	1	1
2.3	Можливість застосування по рухомим цілям[3]	0,25	1	1	1	1	2	1	2	1	1	1	2
2,4	Можливість перенацілювання[4]	0,25	1	1	1	1	1	1	2	1	1	1	2
3.	**ВИЖИВАНОСТІ**	**0,303**											
3.1	Величина ЕПР, кв.м.	0,50	0,38	0,29	1,16	1,16	0,72	0,20	0,65	0,31	0,14	2,87	0,21
3.2	Можливість скритності дії системи наведення[5]	0,50	1	2	1	2	1	1	2	2	2	1	2
Коефіцієнт технічного рівня			0,75	1,0	0,94	1,08	0,89	0,86	1,54	1,23	1,27	0,90	1,42

Примітки.

[1] – «1» – принцип «пустив – супроводжую до влучення у ціль», «2» – принцип «пустив – супроводжую до захвату цілі», «3» – принцип «пустив – забув»; [2] – «1» – вдень в ПМУ, «2» – вдень і вночі в простих метеоумовах, «3» – вдень і вночі в простих і складних метеоумовах; [3, 4, 5] – «1» – ні, «2» – так.

Висновки. За результатами розрахунку КТР АТР класу "повітря-повітря" малої дальності (див. табл. 1) найбільш досконалим з військово-технічної точки зору є авіаційні ракети AIM-9X Sidewinder та PYTHON-5.

Ці авіаційні ракети на 40 - 50 % технічно досконаліші за ракети типу Р-60 і Р-73, що, насамперед, обумовлюється досконалими алгоритмами оброблення сигналів цілі в інфрачервоному діапазоні довжин хвиль і можливістю захвату цілі на траєкторії польоту ракети, що забезпечує високу ймовірність ураження цілі,

За результатами розрахунку КТР АТР класу "повітря-повітря" середньої / великої дальності (див. табл. 2) найбільш досконалим з військово-технічної точки зору є авіаційна ракета AIM-120A(C) AMRAAM та РВВ-АЕ.

Технічна досконаліть цих авіаційних ракет, насамперед, обумовлюється ступенем автономності наведення ракети, великою дальністю пуску, швидкістю на траєкторії польоту та маневровими характеристиками ракети.

За результатами розрахунку КТР АТР класу "повітря-поверхня" (див. табл. 3) найбільш досконалим з військово-технічної точки зору є ізраїльсько-турецька авіаційна ракета AGM-142E Popoye-2.

Технічна досконаліть цієї авіаційної ракети, насамперед, обумовлюється великою дальністю пуску, наявністю горизонтальної ділянки польоту при підході до цілі, можливістю перенацілювання ракети після її відділення від носія.

За результатами розрахунку КТР КАБ (див. табл. 4) найбільш досконалим з військово-технічної точки зору є КАБ американського виробництва GBU-15(V)2/B.

Технічна досконаліть КАБ GBU-15(V)2/B, насамперед, обумовлюється високою точністю тепловізійної системи самонаведення, високим уражаючим фактором за рахунок значної маси бойової частини, порівняно великою дальністю скидання з носія, можливістю застосування по рухомим цілям та перенацілювання після відділення від носія.

Таким чином, представлена методика дозволяє оперативно (з мінімальними витратами часу в порівнянні з процедурами експертного оцінювання) провести розрахунки технічного рівня АЗУ з метою їх порівняння (вибору). Доцільність її використання бачиться як складової системи підтримки прийняття рішень з розроблення / закупівлі зразків ОВТ для потреб Збройних Сил України.

Перспективи подальших досліджень бачаться авторами у розробленні (удосконаленні) кваліметрічних моделей оцінювання технічного рівня інших зразків авіаційної техніки, зокрема, багатофункціональних винищувачів, ударних, протичовневих і пошуково-рятувальних вертольотів, безпілотних авіаційних комплексів різного цільового призначення.

ЛІТЕРАТУРА:

1. Han-Lin Li. Solving Discrete Multicriteria Decision ProbIems Based оп Logic-Based Decision Support Systems. – North-Holland: Decision Support Systems, 1987. Vol. 3(1). – P.101-119.

2. Руа Б. Классификация и выбор при наличии нескольких критериев // Вопросы анализа и процедуры принятия решений. – М.: Мир, 1976. – С. 80-107.

3. C. Hwang, K. Yoon. Multiple Attribute Decision Making – Springer-Verlag, 1981.

4. T. Saaty. Decision making with the analytic hierarchy process, Int. J. Services Sciences, Vol. 1, No. 1, 2008.

5. T. Saaty, L. Vargas (2001) Models, Methods, Concepts & Applications of the Analytic Hierarchy Process, Kluwer Academic, 346 p..

6. Семенов С.С., Харчев В.Н., Иоффин А.И. Оценка технического уровня образцов вооружения и военной техники. М.: Радио и связь, 2004 – 552 с.

7. Azgaldov, G.G. and Kostin, A.V. (2011), "Applied Qualimetry: its Origins, Errors and Misconceptions", Benchmarking: An International Journal, Vol. 18 Iss: 3, pp.428 – 444.

8. Азгальдов Г.Г. Теория и практика оценки качества товаров / Азгальдов Г.Г. – М.: Экономика, 1982.– 258с.

9. Гличев А.В. Прикладные вопросы квалиметрии / Гличев А.В. – М.: Изд. стандартов, 1983. – 135с.

10. Азгальдов Г.Г. Количественная оценка качества продукции. Основы квалиметрии / Азгальдов Г.Г. – М.: Знание, 1986. – 252 с.

11. Азгальдов Г. Г. Метрология и квалиметрия: вопросы идентификации / Г. Г Азгальдов, А. В. Костин // Мир измерений, 2010. – № 1. – С. 4–7.

12. В. Куц, П. Столярчук, В. Друзюк. Квалиметрия. Львов, Украина: Изд. Дом Львовский Политех. Нац. ун., 2012

13. Самков О.В., Мавренков О.Є. До порівняльної оцінки військових літаків // Зб. наук. праць. – К.: КІ ВПС, 1999. – Вип. 6. – С. 135-140

14. Дэвид Г. Метод парных сравнений / Перевод с английского Н. Космарской и Д. Шмерлинга. Под ред. Ю. Адлера. – М.: Статистика, 1978. – 144 с.

REFERENCES:

1. Han-Lin Li (1987). "Solving Discrete Multicriteria Decision ProbIems Based оп Logic-Based Decision Support Systems". / North-Holland: Decision Support Systems, Vol. 3(1). – pp.101-119.

2. Rua, B. (1976) "Classification and selection in the presence of several criteria" / Analysis issues and decision-making procedures, pp. 80-107.

3. Hwang, C. and Yoon, K. (1981). Multiple Attribute Decision Making – Springer-Verlag.

4. Saaty, T. (2008). "Decision making with the analytic hierarchy process", Int. J. Services Sciences, Vol. 1, No. 1.

5. Saaty, T. and Vargas, L. (2001) Models, Methods, Concepts & Applications of the Analytic Hierarchy Process, Kluwer Academic, 346 p..

6. Semenov, S.S., Kharchev, V.N. and Ioffin, A.I. (2004). Ocenka tekhnycheskogho urovnja obrazcov vooruzhenyja y voennoj tekhnyky [Assessment of the technical level of weapons and military equipment]. Moscow: Radio and communications – 552 p.

7. Azgaldov, G.G. and Kostin, A.V. (2011), "Applied Qualimetry: its Origins, Errors and Misconceptions", Benchmarking: An International Journal, Vol. 18 Iss: 3, pp.428 – 444.

8. Azgaldov G.G. (1982). Teoryja y praktyka ocenky kachestva tovarov [Theory and practice of assessing the quality of goods]. Moscow: Economy, 258 p.

9. Glichev A.V. (1983). Prikladnye voprosy kvalimetrii [Applied questions of qualimetry]. Moscow: Standards Publishing House, 135 p.

10. Azgaldov G.G. (1986) Kolichestvennaya ocenka kachestva produkcii. Osnovy kvalimetrii [Quantification of product quality. Fundamentals of qualimetry]. Moscow: Knowledge, 252 p.

11. Azgaldov, G.G. and Kostin, A.V. (2010). "Metodologia i kvalimetria: voprosi identifikacii" [Metrology and qualimetry: issues of identification] / The world of measurements, No 1, pp. 4–7.

12. Kuc, V., Stoliarchuk, P. and Druzuk, V. (2012) Kvalimetria [Qualimetry]. Lvov: Publishing house Lviv Polytechnic National University.

13. Samkov, O.V. and Mavrenkov, O.Ye. (1999) "Do porivnjaljnoji ocinky vijsjkovykh litakiv" [To the comparative assessment of military aircraft] / Zbirnik naukovih prac KIVPS, Vol.. 6, pp. 135-140

14. Devid, G. (1978) Pairwise Comparison Method. Moscow: Statistics, 144 p.

Doct. of Sc. Kharchenko O.V., Doct. of Sc. Ziatdinov Yu.K., Doct. of Sc. Mavrenkov O.Ye.

METHODS OF OPERATIONAL CALCULATION OF TECHNICAL LEVEL OF CONTROLLED AVIATION VEHICLES

The urgency of the issue of quantitative assessment of technical perfection of aircraft weapons is determined primarily by the task of comparing alternative models and choosing the best options when developing or purchasing for the needs of the Armed Forces of Ukraine.

Analysis of the practical application of known methods of decision theory shows that they do not actually solve the problem of estimating the technical level of the product in quantitative terms, but only allow to build a certain priority series of evaluated products in order of increasing / decreasing their technical level.) the magnitude (degree) of change in the level of technical excellence of one product in relation to another.

In this sense, qualimetric methods allow for quantitative assessment of the technical level (quality) of products in relation to the basic (reference) sample, which determines the convenience of their use to solve problems of choice. But the use of the methodological apparatus of qualimetry in each case requires its adaptation taking into account the characteristics of the evaluated product in terms of substantiation of its defining indicators of technical excellence and determining their relative importance.

The article presents the results of the authors' research on the development of methods for assessing the technical level (quality) of guided aircraft as part of the support system for decisions on the development / purchase of samples of weapons and military equipment for the Armed Forces of Ukraine. The developed methodology is based on a qualimetric complex method of quality assessment of complex technical systems, based on the ratio of determinants of technical excellence of the evaluated and basic (reference) products, taking into account the relative importance (weight) of such indicators. The presented technique allows you to quickly (with minimal time compared to expert evaluation procedures) to calculate the technical level of aircraft damage in order to compare (select).

Keywords: aircraft means of destruction, complex technical system, technical level, indicators of technical perfection, tactical and technical characteristics, weighting factor.

УДК 006.013

Вдовенко С.Г. (НУОУ)
к.н.держ.упр. **Живило Є.О.** (НУОУ)
Черноног О.О. (МОУ)
Докіль В.М. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-06

АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРОБОРОНИ. НОРМАТИВНО-ПРАВОВІ АСПЕКТИ

Актуальність данної роботи обумовлена одним із пріоритетів системи національної безпеки України по виконанню функцій і завдань сил оборони України в умовах деструктивної активності на кібербезпекове середовище держави.

Сучасний розвиток інформаційних і кібертехнологій та глобальна інформатизація у світі призвели до того, що інформаційна та кіберсфери стали об'єктом різноманітних деструктивних впливів на усі сфери діяльності суспільства через кіберпростір, який доповнив існуючі, а саме сухопутний, морський, повітряний, космічний, та став сферою конфліктів і можливих бойових дій.

Держави, в залежності від ступеню їх розвитку, по різному будують системи (моделі) захисту своїх інформаційних, телекомунікаційних інфрастуктур, визначають порядок використання технологічних процесів, які циркулюють в зазначених системах та здійснюють захист об'єктів критичної інфраструктури від кіберзагроз, визначають функції, напрями та способи дій у кіберпросторі. На сьогодні в світі більш ніж 60 держав відкрито або/та приховано провадять діяльність щодо підвищення рівня функціональності національних систем кібербезпеки та кібероборони. Йде створення національних та коаліційних кіберсил, визначаються їх функції, завдання, формуються зміст та порядок діяльності, склад, алгоритми підготовки підрозділів, військових і цивільних фахівців, розробляються стратегії, вдосконалюється нормативно-правова база, апаратно-програмні комплекси, спеціальне-програмне забезпечення для кібероборони та тактики їх застосування.

В цілому, розвиток та широке впровадження систем і комплексів зв'язку з використанням інноваційних інформаційних та телекомунікаційних технологій в системах військового призначення відбувається у відповідності до міжнародних правил ведення кібервійн на зразок Женевської конвенції. При цьому основними принципами формування систем кібербезпеки і кібероборони провідних країн світу є науково обґрунтовано законодавче, нормативно-правове, дефініційно-термінологічне супроводження. За цих умов трансформування нормативно-правової бази відбувається з врахуванням постійної мілітарізації національних сегментів кіберпростору з врахуванням критеріїв (індикаторів) загроз у сфері кібербезпеки та кібероборони провідних держав, рівня готовності систем та набуття відповідних спроможностей, тощо.

Для вирішення завдань, щодо врегулювання та імплементації норм та правил міжнародних організацій сфери кібербезпеки та кібероборони пропонується провести аналіз чинних положень (аксіоматик) існуючої законодавчої, державної та відомчої нормативно-правової бази, а також нормативно-правового поля міжнародних організацій (Європейский Союз, НАТО, ITU) щодо забезпечення кібербезпеки.

Ключові слова: кіберпростір, кібербезпека, кібероборона, закон України, нормативно – правова база, нормативно-правовий акт, об'єкт критичної інформаційної інфраструктури.

Вступ та постановка задачі. Вимогами рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про невідкладні заходи з кібероборони держави", введеного в дію Указом Президента України від 26 серпня 2021 р. № 446 та у відповідності до вимог схваленого на засіданні Кабінету Міністрів України Плану організації виконання рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про невідкладні заходи з кібероборони держави", введеного в дію Указом Президента України від 26 серпня 2021 р. №

446 передбачено нормативне визначення та включення до системи операцій Збройних Сил України (далі – ЗС України) сучасних форм і способів дій військ (сил) у кіберпросторі та через кіберпростір, ведення ними кібероборони.

У цьому контексті вбачається, що система кібероборони буде орієнтована на набуття необхідних спроможностей суб'єктами підготовки та здійснення заходів кібероборони, створення і розвиток сил, засобів та інструментів протиборства в кіберпросторі та через кіберпростір, які забезпечать створення необхідного потенціалу сил оборони для відбиття воєнної агресії в кіберпросторі.

За цих умов постає доволі суттєва проблема, щодо вдосконалення державних механізмів регулювання проведення узгоджених дій силами оборони зі здійснення цифрової трансформації, впровадження сучасних технологій автоматизації управління військами та зброєю, моніторингу, аналізу інформації, моделювання, експертних систем, спеціального програмного забезпечення та інформаційних систем.

Також, доволі змістовним питанням постає розробка нового, трансформація та вдосконалення існуючого нормативно-правового поля щодо формування та використання єдиного інформаційного середовища сил оборони шляхом застосування єдиних стандартів, протоколів, архітектур (проектних рішень), надання необхідних сервісів та повноцінного використання інформаційних ресурсів, спрямованих на ефективне застосування сил оборони під час проведення операцій сил оборони (операцій об'єднаних сил).

Запровадження системної, нормативно врегульованої взаємодії складових сил оборони в подальшому надасть їм змоги досягти військових критеріїв сумісності, необхідних для інтеграції України в євроатлантичні та європейські безпекові структури, здійснити взаємодію та співробітництво зі збройними силами держав - членів НАТО та держав - партнерів НАТО.

Отже, удосконалення існуючої нормативно-правової бази (далі – НПБ), підготовка проектів нормативно-правових актів (далі – НПА), нормативне врегулювання питань з реалізації заходів, що забезпечують якісне проведення розрахунків потреб з обсягу матеріально-технічних та фінансових ресурсів, необхідних для створення і забезпечення належного функціонування кібервійськ, комплектування особовим складом кібервійськ з урахуванням оптимального співвідношення військовослужбовців, працівників Міністерства оборони України (далі – МО України), а також зарахованих у запас, резервістів та інших категорій осіб є важливим практичним та науковим завданням.

Аналіз останніх досліджень. Аналіз існуючої НПБ щодо створення та функціонування системи кібербезпеки та кібероборони (далі – КБ та КО) в інформаційно-телекомунікаційних системах військового призначення (далі – ІТС ВП) свідчить про те, що Національна система кібербезпеки, одним із трьох завдань якої є кіберзахист державного інформаційного ресурсу**,** створюється і розвивається відповідно до Конституції України, законів України (далі – ЗУ) та інших НПА, що регулюють суспільні відносини у сфері національної безпеки, оборони, інформаційної та кібербезпеки і захисту інформації. Виходячи з цього, системи кіберзахисту в ІТС ВП також створюються та функціонують відповідно до вимог законів та НПА України, а саме:

Законів України: "Про національну безпеку України" [4]; "Про основні засади забезпечення кібербезпеки України" [5]; "Про захист інформації в інформаційно-телекомунікаційних системах" [6]; "Про розвідку" [7]; "Про електронні довірчі послуги" [8]; "Про Національну програму інформатизації" [9]; "Про ратифікацію Конвенції про кіберзлочинність" [10]; "Про Державну службу спеціального зв'язку та захисту інформації України" [11]; "Про державну таємницю" [12]; "Про доступ до публічної інформації" [13]; "Про захист персональних даних" [14]; "Про оборону України" [15]; "Про інформацію" [16]; "Про Збройні Сили України" [17].

Документів довгострокового та оборонного планування України: Стратегія національної безпеки України [18]; Стратегія кібербезпеки України [2]; Стратегія воєнної безпеки України [19]; Стратегічний оборонний бюлетень України (далі – СОБ) [20]; Питання

Апарату Ради національної безпеки і оборони України, Про Національний координаційний центр кібербезпеки [21]; Стратегія інформаційної безпеки України [22].

Нормативних документів міжнародних організацій, згода на використання яких надана Верховною Радою України. Зокрема, рекомендації Міжнародного союзу електрозв'язку (далі – ITU), міжнародні стандарти з інформаційної безпеки ISO/IEC 27000 та інші [25-29]. З урахуванням того, що проблема кібербезпеки носить глобальний характер, позиція міжнародних організацій є важливою. Глобальна програма програми кібербезпеки Міжнародного союзу електрозв'язку [29] включає п'ять стратегічних напрямів та сім стратегічних цілей, що їх слід враховувати при створенні систем кіберобезпеки ІТС, в т.ч. військового призначення. Причому вимога щодо уніфікації глобального законодавства у сфері кібербезпеки, сумісного з діючими національними та регіональними нормами законодавства, розглядається як головна стратегічна ціль [29, 30, 42].

Аналіз існуючих ЗУ та інших НПА України, ЄС, НАТО, провідних країн світу, зокрема США, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області декількох десятків понять, що складають базовий термінологічний набір терміносистеми сфери КБ та КО, зокрема таких як: "кібербезпека", "кіберзахист", "кіберзброя" "кібероборона", "кіберпростір", "кібертероризм" тощо [42].

Так, ITU [27, 28] визначає що кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Загальні завдання безпеки у кіберсередовищі включають забезпечення доступності, цілісності, конфіденційності інформації**.** Українське ж законодавство [6] комплекс цих заходів однозначно визначає як – технічний захист інформації [30, 42].

Нормативно-правових актів МО України та ЗС України, більшість з яких має обмеження доступу, видаються відповідно до вимог ЗУ, підзаконних актів державних органів, уповноважених у сферах телекомунікації, інформатизації, захисту інформації тощо, частина з яких також не є відкритою інформацією відповідно до вимог ЗУ [12, 13, 16]. Разом з тим, спираючись на [13, 16], є можливим й доцільним цитування в частині кіберзахисту ІТС військового призначення, окремих положень та завдань з НПА МО України і ЗС України, які не є інформацією з обмеженим доступом. Так, визначено, що функціональна складова кіберзахисту включає системи на [54]:

запобігання (англійською мовою – "Prevention") – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них;

захисту (англійською мовою – "Protection") – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу в інтересах всебічного та стійкого забезпечення у кіберпросторі процесів управління власними військами;

попередження (англійською мовою – "Mitigation") – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) у разі безпосередньої загрози проведення кібератак;

реагування (англійською мовою – "Response") – заходи комплексного реагування на вплив противника, у тому числі заходи захисту власної інфраструктури, особового складу, ресурсів тощо від впливу противника;

відновлення (англійською мовою – "Recovery") – заходи, направлені на відновлення інформаційної та іншої інфраструктури, яка стала об'єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Відповідним органом військового управління (далі – ОВУ), що керує військовими організаційними структурами, які уповноважені на виконання вищезазначених функцій, визначені завдання щодо:

співпраці (реалізації спільних проектів та заходів, підтримання взаємодії) у межах повноважень з суб'єктами забезпечення воєнної безпеки та кібербезпеки держави, а також з НАТО, Європейським Союзом, державами-партнерами в частині спільного виконання завдань кібероборони;

реагування (практичного виконання необхідних заходів) на поточні загрози кібербезпеці у воєнній сфері шляхом їх попередження, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу;

здійснення кіберзахисту власної інформаційної інфраструктури (засобів рухомого зв'язку як апаратної, так і контентної складових, додатків та сервісів зв'язку, інших інформаційно-комунікаційних систем та об'єктів інформаційної діяльності суб'єктів оборони держави) від кібератак та кібервпливу противника, що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю, інші дії в кіберпросторі тощо.

Виклад основного матеріалу. Формування НПБ в сфері КБ та КО останніми роками здійснювалося та здійснюється під впливом певних історичних, воєнно-наукових, зовнішньо-політичних та інших причин та обставин з елементами жорсткої нормативно-правової легітимізації дефініцій (термінів), що запропоновані та втілені в обіг на рівні емоційних та емпіричних логічних операцій окремих виконавців (авторів), без необхідного наукового супроводження [30]. Так, наприклад, на формування НПБ системи нормативних документів системи технічного захисту інформації значною мірою вплинули, та й досі впливають норми й правила, у т.ч. з обмеженням доступу, започатковані та встановлені Державною технічною комісією СРСР (Гостехкомиссия СССР). Разом з тим, слід відмітити, що цей процес є результатом всесвітньо визнаних наукових робіт С.Соболева, А.Кітова, О.Ляпунова, В.Глушкова, зокрема [31, 32], які разом склали основи методології сучасної кібернетики, а надалі й кібербезпеки, як галузі знань про забезпечення захищеності процесів управління в усіх сферах (технічній, соціальній, соціотехнічній, економічній тощо) від різноманітних кіберзагроз різної природи та для забезпечення його ефективності.

Формування сучасної НПБ системи КБ та КО відбувається з урахуванням норм міжнародного права, стандартів та директив ЄС та НАТО, що зафіковано у Законах та НПБ України [2, 5, 10, 20].

З огляду перманентності законодавчого, нормативно-правового, дефініційно-термінологічного супроводження системи КБ та КО України вважається за доцільне надати коротку історичну довідку щодо законодавчого забезпечення дій у кіберпросторі.

До 2007 року в Україні, в т.ч. стосовно кримінальної відповідальності законодавчо розглядалися лише питання пов'язані з терміном комп'ютерні загрози. Вперше, у 2003 р. в ЗУ "Про основи національної безпеки України" [37] одними з потенційних загроз національній безпеці України визнані комп'ютерна злочинність та комп'ютерний тероризм, але зазначені дефініції не розкриті.

Вперше термін кібербезпека використано в 2007 р. у Стратегії національної безпеки України [34] визнаючи за пріоритетне завдання створення національної системи кібербезпеки, але лише в контексті необхідності розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність. Конвенцію ратифіковано ЗУ [10] із застереженнями і заявами. Конвенція наголошує на необхідності зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладання домовленостей щодо швидкого і надійного міжнародного співробітництва.

До 2012 р. в Україні використовували термін кібербезпека без розкриття його змісту [35].

У 2013 р. законопроєкт № 2483 [36], що був відкликаний 27.02.2014, передбачав з порушенням принципів однозначності, точності та відсутності синонімів, визначення дефініцій з подвійним дефінієндумом: кібернетична безпека (кібербезпека), кібернетичний простір (кіберпростір). Це започаткувало безсистемність вжитку цих та інших термінів не лише у наукових працях, але й в ЗУ [5] та НПБ державного та відомчого рівнів. Що призводить до викривлень у становленні теорії предмету кібербезпеки, неадекватності НПБ цієї галузі, і, як наслідок, до хаотичності у практичних діях.

У 2015 р. на державному рівні [37, 38] наголошено на уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів та визначено шляхи досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони, зокрема щодо систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки державних інформаційних ресурсів, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС.

У 2016 р. введена в дію Стратегія кібербезпеки України [39], яка системно базувалася на положеннях Конвенції про кіберзлочинність, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України [40] та стала першим офіційнм документом, який визначив дефініцію кібербезпека як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. Стратегія [39] визначила МО України та ГШ ЗС України завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони) та кіберзахисту власної інформаційної інфраструктури. Вона передбачала гармонізацію нормативних документів України у сфері кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО. За результатами експертних оцінок, стан реалізації Стратегії за визначеними показниками не перевищує 40 %, а саме:

не розроблені індикатори виконання Стратегії кібербезпеки України;
не вирішені питання оперативного обміну інформацією про кіберзагрози;
не сформовано перелік об'єктів критичної інформаційної інфраструктури;
недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки;
не створена ефективна система підготовки кадрів;
не створено дієву модель державно-приватного партнерства;
кібернавчання проводились епізодично.

У 2017 р. Указом Президента України [41] було визначено завдання щодо невідкладного забезпечення підготовки законодавчих пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та вкотре, з 2005 р., наголошено на необхідності імплементації в Україні положень Конвенції про кіберзлочинність. Еволюцію НПА України стосовно підходів щодо дій в кіберпросторі наведено в таблиці.

У цьому ж 2017 р. ЗУ "Про основні засади забезпечення кібербезпеки України" [5] було визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Законом [5] також визначені базові терміни у сфері кібербезпекі, зокрема такі, що впливають на виконання завдання щодо формалізації опису стану кібербезпеки та процесів кіберзахисту в ІТС ВП: індикатори кіберзагроз; інформація про інцидент кібербезпеки; інцидент кібербезпеки (кіберінцидент); кібератака; кібербезпека; кіберзагроза; кіберзахист; кіберзлочин (комп'ютерний злочин); кіберзлочинність; кібероборона; кіберпростір; кіберрозвідка; кібертероризм; кібершпигунство; критична інформаційна інфраструктура;

критично важливі об’єкти інфраструктури (об’єкти критичної інфраструктури); національна телекомунікаційна мережа; національні електронні інформаційні ресурси (національні інформаційні ресурси); об’єкт критичної інформаційної інфраструктури; система управління технологічними процесами (технологічна система); системи електронних комунікацій (комунікаційні системи).

Таблиця 1

Еволюція НПА України стосовно підходів щодо дій в кіберпросторі

Термін	Закон, нормативно-правовий акт	Короткий зміст, особливості
19.06.2003	Закон України “Про основи національної безпеки України” № 964-IV від 19.06.2003	Одними з потенційних загроз національній безпеці України визнані комп’ютерна злочинність та комп’ютерний тероризм
07.09.2005	Закон України “Про ратифікацію Конвенції про кіберзлочинність” від 07.09.2005 № 2824-IV	Ратифіковано із застереженнями і заявами
12.02.2007	Стратегія національної безпеки України від 12 лютого 2007 № 105/2007	Вперше використано термін кібербезпека. Наголошено про необхідність гармонізації національних стандартів та технічних регламентів згідно з Конвенцією про кіберзлочинність
2013	Проект Закону України “Про внесення змін до Закону України про основи національної безпеки України щодо кібернетичної безпеки України” (№ 2483 від 07.03.2013)	Запропоновані визначення: кібербезпека (кібернетична безпека), кіберпростір (кібернетичний простір). Проект відкликано 27.02.2014
26.05.2015	Стратегія національної безпеки України, Указ Президента України від 26 травня 2015 року № 287 “Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”	1. Наголошено на уразливості об’єктів критичної інфраструктури, державних інформаційних ресурсів; 2. Визначено завдання щодо удосконалення систем забезпечення інформаційної і кібербезпеки, захисту інформації та безпеки інформаційних ресурсів
14.03.2016	Концепція розвитку сектору безпеки і оборони України, Указ Президента України від 14.03.2016 № 92/2016	Визначено завдання щодо удосконалення систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів
15.03.2016	Стратегія кібербезпеки України. Указ Президента України 15 березня 2016 року № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”	1. Наведено визначення кібербезпека України; 2. Кіберпростір визнано сферою ведення бойових дій; 3. МО України, ГШ ЗС України визначено завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони) та кіберзахисту власної інформаційної інфраструктури; 4. Визначено пріоритетні заходи у сфері забезпечення кібербезпеки сектору безпеки і оборони:

Термін	Закон, нормативно-правовий акт	Короткий зміст, особливості
		а) створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист); б) розвиток підрозділів кібербезпеки та кіберзахисту ЗС України
13.02.2017	Указ Президента України від 13 лютого 2017 року №32/2017 Про затвердження Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації"	Визначено конкретні завдання щодо: невідкладної підготовки законодавчих пропозицій стосовно: а) імплементації положень Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересни 2005 року № 2824-IV; б) визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення вимог щодо кіберзахисту

Термінологічну базу Закону [5] необхідно визнати принципово недосконалою, що перешкоджає змістовно розглядати практично значну кількість його положень. Жорстка нормативно-правова легітимізація наведених термінів та їх дефініцій за умов недотримання в термінографії сфери кібербезпеки принципів однозначності, точності та відсутності синонімів закладає перше протиріччя, що вимагає наукового та правового розв'язання задачі щодо стандартизації та гармонізаціїї в нормативно-правовому полі України дефініцій термінологічних систем сфери КБ та КО. Шляхи її вирішення запропоновані в НДР "Дефініція" [42].

Встановлено, що національна система кібербезпеки включає в тому числі й оборонні заходи, також визначено МО України та ГШ ЗС України завдання щодо підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); передбачено військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, зазначено про забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану. Розвідувальним органам України визначені завдання із здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інші події і обставини, що стосуються сфери кібербезпеки [3].

З огляду на актуальність цієї проблематики стосовно обґрунтування пропозицій щодо формалізації процесів кіберзахисту в ІТС ВП, між Законами [5] та [6, 15] закладено друге протиріччя, що підлягає розв'язанню. Воно полягає в штучному звуженні спектру завдань, що вирішуються ІТС військового призначення за рахунок виключення зі сфери діяльності Закону

[5] комунікаційних та технологічних систем, призначених для оброблення інформації, що містить державну таємницю.

Так, ЗУ [5] визначаючи МО України, ЗС України та розвідувальним органам завдання щодо кібероборони та кіберрозвідки зазначає, що його дія не поширюється на:

1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

Разом з тим, ЗУ [6] встановлює умови та обмеження щодо поводження з державними інформаційними ресурсами або інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом, зокрема ЗУ "Про державну таємницю" [12], яким визначається, що інформація у сфері оборони визначеним порядком та за відповідними процедурами може бути віднесена до державної таємниці. ЗУ [15, 17] встановлюють норму, щодо дотримання вимог законодавства України [12] в ході вирішення завдань підготовки держави до оборони та виконання завдань передбачених ст. 17 Конституції України.

У 2018 р. ЗУ "Про національну безпеку України" [4] кібербезпека України віднесена до сфери національної безпеки і оборони, визначена роль Стратегії національної безпеки України, Стратегії кібербезпеки України, Стратегії воєнної безпеки України, Національної розвідувальної програми у формуванні засад національній безпеки України. Так, Стратегія кібербезпеки [39] визначається як основа для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України. ЗУ [4] огляд стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури, що є основою для розроблення Стратегії кібербезпеки, включено до питань Комплексного огляду сектору безпеки і оборони.

Кабінету Міністрів України встановлено завдання щодо визначення порядку проведення:

огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом – Державною службою спеціального зв'язку та захисту інформації України;

оборонного огляду, що є основою для розроблення Стратегії воєнної безпеки – МО України. Стратегіія воєнної безпеки, в свою чергу, є основою для розроблення Стратегічного оборонного бюлетеня України [4].

Крім того, Законом [4] покладені завдання щодо:

формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом – на Державну службу спеціального зв'язку та захисту інформації України;

забезпечення контррозвідувального захисту кібербезпеки – на Службу безпеки України.

Чим закладено третє протиріччя між ЗУ [4] та ЗУ "Про контррозвідувальну діяльність" [43], яке не визначає завдання щодо ведення контррозвідувальної діяльності в кіберпросторі. Розв'язання протиріччя є можливим у ході реформування Служби безпеки України з прийняттям Стратегії забезпечення державної безпеки України, відповідного Закону та подальшим внормуванням контррозвідувальної діяльності.

У 2019 р. Постановою Кабінету Міністрів України [24] затверджені загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, обов'язок та відповідальність за впровадження якого покладається на керівника об'єкту критичної інфраструктури (далі – ОКІ) на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури (далі – ОКІІ) ОКІ. Визначено, що кібербезпека ОКІ забезпечується шляхом впровадження на ОКІ ОКІІ кіберзахисту або системи інформаційної безпеки з підтвердженою відповідністю. Наведена дефініція Система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на ОКІ ОКІІ з метою

запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів.

Постанова [24] визначає організаційно-методологічні, технічні та технологічні умови кіберзахисту ОКІ, які впроваджуються на ОКІ ОКІІ та повинні забезпечувати:

формування на ОКІ загальної політики інформаційної безпеки;

управління доступом користувачів та адміністраторів до об'єктів захисту ОКІІ ОКІ;

ідентифікацію та автентифікацію користувачів та адміністраторів ОКІІ ОКІ;

реєстрацію подій компонентами ОКІІ ОКІ та їх періодичний аудит;

мережевий захист компонентів та інформаційних ресурсів ОКІІ ОКІ;

доступність та відмовостійкість компонентів та інформаційних ресурсів ОКІІ ОКІ;

визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ ОКІ;

визначення умов використання програмного та апаратного забезпечення ОКІІ ОКІ;

визначення умов розміщення компонентів ОКІІ ОКІ.

Постановою [24] визначені базові функції захисту, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) ОКІІ ОКІ, зокрема такі:

захист від атак "нульового дня" (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

фільтрація трафіку та розмежування доступу між мережею об'єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. блокування трафіку та з'єднань, які не відповідають визначеним критеріям;

фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

захист від атак типу "відмова в обслуговуванні";

захист від несанкціонованого доступу через Інтернет;

балансування навантаження;

маскування структури і мережевих адрес мережі;

завершення з'єднання з вузлом уразі атаки;

здійснення реєстрації збереження в електронних журналах та захист від модифікації інформації про події, що мають відношення до безпеки.

До останніх віднесено наступні події:

доступ та дії з інформацією, яка зберігається та обробляється на ОКІІ ОКІ, а також з налаштуваннями програмного та апаратного забезпечення ОКІІ ОКІ, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

реєстрація подій, пов'язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів об'єкта;

вхід/вихід користувачів та адміністраторів в/із компонентів об'єкта;

невдалі спроби входу користувачів та адміністраторів на ОКІІ ОКІ та перевищення граничної кількості спроб введення пароля;

реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах об'єкта;

зміна пароля користувача в компонентах об'єкта;

реєстрація подій, пов'язаних із зміною конфігураційних налаштувань компонентів об'єкта;

спроби здійснення несанкціонованого доступу до ресурсів ОКІІ ОКІ;

негативні результати перевірок цілісності даних та програмного і апаратного забезпечення ОКІІ ОКІ;

всі дії адміністратора з журналами реєстрації подій компонентів об'єкта та налаштування ним параметрів реєстрації.

Четверте протиріччя закладено між ЗУ "Про основні засади забезпечення кібербезпеки України" [5] та іншими НПА внаслідок вищезгаданих причин, та полягає у тому, що ОВУ, військові частини, установи, організації МО України та ЗС України, а також угруповання військ до ОКІ не віднесені. Так, в Україні дефініція критична інфраструктура законодавчо не визначена. ЗУ [5] визначає синонімічно, що критично важливі об'єкти інфраструктури (об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. Також визначається, що об'єкт критичної інформаційної інфраструктури є об'єктом кіберзахисту (запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідація їх наслідків, відновлення функціонування).

Це протиріччя може бути частково вирішене з прийняттям Закону на основі проекту ЗУ "Про критичну інфраструктуру та її захист" [44], робота над яким триває з 2019 р. Проєкт розглядає критичну інфраструктуру, як сукупність об'єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам; та об'єкт критичної інфраструктури, як визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєво важливих національних інтересів. Законопроєкт [44] пропонує визначити суб'єктність питань захисту КІ та критерії віднесення підприємств, установ та організацій незалежно від форми власності до ОКІ, які дещо відмінні від [5]. Так, до суб'єктів державної системи захисту критичної інфраструктури пропонується віднести також ЗС України, інші військові формування, утворені відповідно до ЗУ, правоохоронні та розвідувальні органи. До ОКІ, відповідно до визначених критеріїв, арсенали, бази та склади та інші об'єкти ЗС України, де знаходяться або зберігаються озброєння, військова техніка, матеріально-технічні засоби, здійснюється підготовка і застосування військ (сил).

Завдання покладені на МО України щодо вирішення деяких з цих питань визначені законопроектом [44]. До прийняття встановленим порядком Закону на основі законопроекту [44], відповідно до нормативно-правових актів [45] важливі об'єкти ЗС України можуть розглядатися лише як військові об'єкти, що є цілями для нападу, об'єктами терористичних посягань. Це може вплинути на повноту та об'єктивність формального опису стану кібербезпеки та процесів кіберзахисту в ІТС ВП, оскільки є нормативно-правовою підставою для формування моделі загроз та моделі порушника для ІТС та її підсистем.

У 2020 р. відповідно до вимог ЗУ "Про національну безпеку України" [4] прийнята Стратегія національної безпеки України [18], яка є основою для розроблення ряду документів щодо планування у сферах національної безпеки і оборони, що визначатимуть шляхи та інструменти її реалізації, зокрема таких, що на сьогодні діють, або розробляються: Стратегія кібербезпеки України [2]; Стратегія воєнної безпеки України [19]; Стратегія інформаційної безпеки; Стратегія забезпечення державної безпеки; Національна розвідувальна програма.

Для системного захисту України від загроз національній безпеці Стратегія [18] акцентує увагу на необхідності розвитку сектору безпеки і оборони зі стратегічною метою завершення

створення національної системи кібербезпеки, формування сучасних спроможностей суб'єктів забезпечення кібербезпеки і кібероборони та зміцнення системи їх координації.

Отже, враховуючи зазначене вище слід відмітити, що НПБ сфери КБ та КО в Україні ще не сформована. Враховуючи ієрархію існуючої НПБ на рисунку нижче наведено модель формування НПБ України, МО України та ЗС України сфери КБ та КО станом на 2021 рік.

Рисунок 1 – Модель формування нормативно правової бази України, МО України та ЗС України сфери КБ та КО

У 2021 р. прийнято низку логічно взаємопов'язаних (рис. 1) документів оборонного та довгостроковго планування, зокрема, Стратегія воєнної безпеки [19] та Національну розвідувальну програму, які поряд зі Стратегією кібербезпеки [2] мають бути основою для відпрацювання Стратегічного оборонного бюлетеня (далі – СОБ) [46]. Разом з тим, Стратегією [19] цілі та приорітети у сфері КБ та КО не визначені. Натомість, у СОБ [46] кіберзагрози воєнного характеру розглядаються як реальні та потенційні кіберзагрози національним інтересам у воєнній сфері та визначено стратегічні цілі щодо кібероборони, зокрема щодо захисту інформації та кіберзахисту інформаційної інфраструктури.

Із затвердженям у 2021р. Стратегії кібербезпеки України [2] втратила чинність Стратегя кібербезпеки 2016 р. [39]. Ряд її засад, стратегічних цілей та завдань, з урахуванням значного відсотка її не виконання, враховано в новій Стратегії [2], яка на відміну від попередньої, забезпечення кібербезпеки визначає одним із пріоритетів у системі національної безпеки України. Стратегія [2] враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегії кібербезпеки окремих держав-членів ЄС та держав-членів НАТО, зокрема в черговий раз окреслює завдання щодо завершення імплементації в законодавство України положень Конвенції про кіберзлочинність.

Вона визначає загрози кібербезпеці України, серед яких:

гібридна агресія Російської Федерації проти України у кіберпросторі із застосуванням кіберзброї;

організовані та спонсоровані урядами інших держав кібератаки;

використання терористичними організаціями кіберпростору для вчинення актів кібертероризму.

Серед передумов загрозам кібербезпеці України, що можуть вплинути на хід та результати обґрунтування пропозицій щодо формалізації процесів кіберзахисту в ІТС ВП розглядаються:

висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій, що підвищує ступінь уразливості інформаційної інфраструктури та звужує спроможності протидії кіберзагрозам;

недосконаліть НПБ у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства;

невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів, в яких обробляється значна частина інформації з обмеженим доступом;

відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави;

недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту;

відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки;

відсутність належного контролю за кіберзахистом;

низький рівень правової відповідальності за порушення вимог законодавства у сфері кібербезпеки.

Серед стратегічних цілей необхідним для формування потенціалу стримування кіберзагроз та набуття кіберстійкості в Стратегії [2] визначені:

формування належної правової, організаційної, технологічної моделі функціонування та застосування підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі;

формування системи ефективної протидії розвідувально-підривній діяльності у кіберпросторі, кібертероризму та кіберзлочинності;

забезпечення кіберстійкості шляхом створення національної системи управління кіберінцидентами та забезпечення постійної готовності до реальних та потенційних кіберзагроз, здатності виявленя та усуненя передумов до їх виникнення;

спрямування відносин з міжнародними партнерами на обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками;

координація спільних дій заінтересованих сторін під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів та подолання надзвичайних (кризових) ситуацій у кіберпросторі,

створення умов для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки.

Відповідно ЗУ [5] національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів розвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Серед основних суб'єктів національної системи кібербезпеки визначені МО України та ГШ ЗС України, розвідувальні органи.

СОБ прийнятий у 2021 р. [46] на підставі Стратегії кібербезпеки [37] формує стратегічні цілі розвитку сил оборони на період до 2025 року, спрямовує діяльність державних органів й сил безпеки і оборони на досягнення такого рівня оперативних, бойових і спеціальних спроможностей, які забезпечать здатність ведення узгодженого протиборства в усіх сферах ведення бойових дій, у т.ч. - в кіберпросторі, зосереджуючи увагу на досягненні визначеного

рівня спроможностей в інформаційних технологіях, у т. ч. електронних комунікаціях, визначає завдання та заходи для їх досягнення.

Це вкотре підкреслює існування п'ятого протиріччя, яке полягає у відмінностях термінологічних систем сфер КБ та КО міжнародного співтовариства, зокрема ЄС та НАТО й України, має історичні та науково-термінологічні коріння та є невирішеним протягом десятиліть.

Відмінності еволюційно сформувалися внаслідок особливостей розвитку науки і техніки в умовах геополітичних подій XX століття та суттєво ускладненюють практичне застосування термінів сфери КБ та КО щодо спільних заходів із забезпечення безпеки кіберпростору та дій у кіберпросторі.

Зокрема, суттєвою відмінністю є, наприклад те, що за кордоном кіберпростір розглядається як сфера діяльності складних технічних систем, а в Україні – складних соціотехнічних систем [30, 42, 47]. Інша відмінність полягає в підходах щодо формування критеріїв віднесення об'єктів до критичної інфраструктури в Україні та ЄС і державах-членах НАТО. На відміну від ЗУ [5] ЄС та США визначають ОКІ як системи, їх частини або об'єкти розташовані в державах-членах, які мають важливе значення для підтримки життєво важливих соціальних функцій. Пошкодження, руйнування або порушення яких в результаті стихійних лих, тероризму, злочинної діяльності або зловмисної поведінки, може істотно негативно вплинути на безпеку ЄС, здоров'я і захищеність економічного та соціального добробуту населення держави-члена, через неспроможність такої інфраструктури підтримувати згадані функції. Загальна методологія із захисту ОКІ рекомендує посилити увагу на технологічних й інформаційних елементах захисту об'єктів КІ, припинення функціонування яких матиме транскордонний вплив. [48 - 50].

Дане, п'яте , протиріччя не можливо вирішити директивним шляхом, як то визначено в Законі [5] щодо вищого пріоритету міжнародних договорів в сфері КБ та КО над НПБ України. Шляхи його вирішення мають бути вирішені в ході науково обґрунтованої імплементації (адаптації) нормативно-правових вимог та термінологічних систем ITU, ЄС, НАТО до НПБ України, як то передбачено, наприклад у законопроекті [42].

СОБ [46] пропонує до вжитку ряд нових дефініцій, зокрема таких, як: воєнна агресія в кіберпросторі, дії в кіберпросторі, єдине розвідувально-інформаційне середовище, кіберзагрози воєнного характеру, кіберборотьба, кібердії, кібердорозвідка, кіберзброя, кіберінфраструктура, оперативне обладнання території. Зазначене також має безпосереднє відношення до п'ятого протиріччя, оскільки в СОБ [46] визначено захід 5.6.9. Розширення військової співпраці з НАТО щодо забезпечення безпеки кіберпростору та спільних дій у кіберпросторі, що неможливо вирішити без гармонізації термінологічних баз систем КБ та КО України та НАТО.

Окремо слід розглянути положення законів України, що встановлюють відповідальність за злочини та правопорушення у кіберпросторі, не врахування яких може вплинути на повноту та об'єктивність формального опису стану кібербезпеки та процесів кіберзахисту в ІТС військового призначення, оскільки такі є нормативно-правовою підставою для формулювання опису окремих ситуацій, пов'язаних з ліквідацією наслідків порушення сталої роботи ІТС в результаті кібервпливу на них.

Чинний Кримінальний кодекс (далі - КК) України [51] встановлює (відповідно до Розділу (XVI) відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361-363). розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" Особливої частини КК містить шість статей:

1. ст. 361 КК - несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

2. ст. 361[1] КК - створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

3. ст. 361² КК - несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

4. ст. 362 - несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

5. ст. 363 КК - порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

6. ст. 363¹ КК - перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Кодексом України про адміністративні правопорушення (далі - КУпАП) [52] (ст. 212-6) передбачена адміністративна відповідальність за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем. Визначається відповідальність за таки правопорушення:

здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах;

здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, призначених для зберігання та обробки інформації з обмеженим доступом;

незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі;

безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі;

незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі.

КК та КУпАП України не встановлюють відповідальності за діяльність, неналежну діяльність або бездіяльність, яка класифікується як кіберзлочини, кібершпигунство, кібертероризм, кібердиверсії, кіберпроступки, а також призвела до шкідливих наслідків різного ступеню, пов'язаних із порушенням сталої роботи ІТС, комп'ютерних систем, цілісності, конфіденційності, доступності інформації внаслідок кібердій.

У 2017 р. Указом Президента України [42] було визначено завдання щодо забезпечення підготовки законодавчих пропозицій щодо посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в ІТС. Мета не досягнута.

На думку колективу авторів, доцільно розглядати і військові злочини у кіберпросторі, оскільки, кіберпростір визнано сферою ведення бойових дій [1, 2].

Висновки. Виходячи з викладеного, можливо зробити наступні висновки:

1. Сучасна НПБ України сфери КБ та КО перебуває в стадії формування та становлення. При цьому вона має низку протиріч, які умовно можна об'єднати в три групи, а саме:

1.1. Дефініційно-термінологічні розбіжності НПБ України сфери КБ та КО.

1.2. Нормативно-правові розбіжності НПБ України сфери КБ та КО.

1.3. Законодавчі, нормативно-правові, дефініційно-термінологічні розбіжності між НПБ сфери КБ та КО України та міжнародного співтовариства.

В умовах глобалізації світу окрема держава практично не може протистояти можливим кіберзагрозам сучасності без інформаційного обміну з іншими. НПБ України [2, 5, 15, 17] значна увага приділяється співпраці з ЄС, НАТО іншими міжнародними суб'єктами щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, в т.ч. у військовій та оборонній сферах. Дуже важливим індикатором готовності систем кібербезпеки та кібероборони держав-партнерів є досягнення визначеного рівня їх інтероперабельності. Але, в ході проведення чисельних консультації, практичних навчань, науково-практичних

конференцій, семінарів та тренінгів, що займають значне місце серед різноманітних заходів програм взаємодії між Україною і НАТО та США у сфері кібербезпеки, були виявлені протиріччя базового термінологічного апарату, що як мінімум знижує ефективність заходів та не дозволить в майбутньому ефективно виконувати завдання передбачені [2, 5, 46] та рядом інших домовленостей. Аналіз існуючих законів України та інших нормативно-правових актів України [2, 5, 46], ЄС, НАТО, провідних країн світу, зокрема США, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області декількох десятків понять, що складають базовий термінологічний набір терміносистеми сфери КБ та КО, зокрема таких як: "кібербезпека", "кіберзахист", "кіберзброя", "кібероборона", "кібертероризм", "кіберпростір", тощо [45]. Так, США, ITU, ENISA розглядають кіберпростір як сферу діяльності складних технічних систем, а в Україні – складних соціотехнічних систем [30, 42, 47, 53].

2. З метою вирішення вищезазначених протиріч Законодавча та НПБ України потребує суттєвих змін, зокрема таких як:

2.1. Розроблення та ухвалення нових ЗУ:

"Про кібербезпеку" з метою вдосконалення системи державного управління, чіткого розмежування функцій та завдань КБ та КО між органами влади, самоврядування, ОВУ, іншими суб'єктами КБ та КО, а також усунення ряду протиріч дефініційно-термінологічного походження;

"Про критичну інфраструктуру України" з метою визнання ОКІ України суб'єктами кібербезпеки (кіберзахисту), визначення їм завдань, обов'язків та прав;

"Про ДССЗЗІУ" з метою впорядкування та розмежування регуляторних, наглядових, адміністративних, управлінських і правоохоронних функцій.

2.2. Внесення на підставі цього змін до ЗУ [13, 15, 16, 17, 43, 51, 52], з урахуванням вимог розроблених та ухвалених інших ЗУ, зокрема "Про СБУ", "Про безпеку класифікованої інформації".

2.3. Приведення НПБ України сфери КБ та КО, в т.ч. МО України та ЗС України, у відповідність до вимог нових Законів.

2.4. Врахування у законотворчій діяльності сфери КБ та КО необхідності реальної імплементації міжнародних стандартів ISO/IEC 27k, NIS Directive, NIST CS Framework, зокрема щодо запровадження базового рівня відповідності вимогам з кібербезпеки, оцінювання ризиків, реагування на кіберінциденти і врегулювання інцидентів, відновлення сталого функціонування ІТС, розвитку мережі CERT/CSIRT.

ЛІТЕРАТУРА:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 – Press Release (2016) 100 Issue don 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 [Електронний ресурс] – Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

2. Стратегія кібербезпеки України, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021, – Режим доступу https://www.president.gov.ua/documents/4472021-40013.

3. Живило Є.О., Черноног О.О. Стратегія кібероборони України // Збірник наукових праць ВІТІ № 4 – 2017 [Електронний ресурс] – Режим доступу: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Закон України "Про національну безпеку України" від 21.06.2018 р. № 2469-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Закон України “Про розвідку” від17.09.2020 № 912-IX [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/912-20#Text.

8. Закон України “Про електронні довірчі послуги” від 5 жовтня 2017 № 2155-VIII [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

9. Закон України “Про Національну програму інформатизації” від 04.02.1998 р. № 74/98-ВР // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

10. Закон України “Про ратифікацію Конвенції про кіберзлочинність” від 10.03.2006 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

11. Про Державну службу спеціального зв’язку та захисту інформації : Закон України від 23.02.2006 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

12. Закон України “Про державну таємницю”від 21 січня 1994 № 3855-XII(зі змінами) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

13. Закон України “Про доступ до публічної інформації” від 13 січня 2011 р. № 2939-VI. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

14. Закон України “Про захист персональних даних” від 01.06.2010 р. № 2297-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

15. Закон України “Про оборону України” від 06.12.1991 р. № 1932-XII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

16. Закон України України “Про інформацію” № 2938-VI. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

17. Закон України “Про Збройні Сили України” від 6 грудня 1991 року № 1934-XII (зі змінами) // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1934-12#Text.

18. Стратегія національної безпеки України, введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020 Про рішення Ради національної безпеки і оборони України], від 14 вересня 2020 року Про Стратегію національної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/3922020-35037.

19. Стратегія воєнної безпеки України, введена в дію Указом Президента України від 25 березня 2021 року № 121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року Про Стратегію воєнної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/1212021-37661.

20. Указ Президента України №473/2021 від 17 вересня 2021 року №473/2021 Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України” [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/4732021-40121.

21. Указ Президента України №27/2020 28 січня 2020 року Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/27/2020#Text.

22. Стратегія інформаційної безпеки України, введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року Про Стратегію інформаційної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/6852021-41069.

23. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Офіційний вісник України, 2006 р., № 13, ст. 878) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

24. Постанова Кабінет міністрів України від 19 червня 2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

25. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace. Annex. 32 sessio General Assebly UNESCO, 2003. [Електронний ресурс] – Режим доступу: https://unesdoc.unesco.org/ark:/48223/pf0000133171.

26. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT). Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Набув чинності відповідно до наказу Державного підприємства “Український науково-дослідний і навчальний центр

проблем стандартизації, сертифікації та якості" від 16.10.2019 № 312 Про прийняття та скасування національних стандартів, прийняття поправок до національних стандартів [Електронний ресурс] – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=85639.

27. Рекомендация МСЭ¬Т X.1205. Обзор кибербезопасности. – Женева:МСЕ, 2010. – С. 55. [Електронний ресурс] – Режим доступу: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru.\.

28. Рекомендації міжнародного союзу електрозв'язку. Мережі передачі даних, взаємозв'язок відкритих мереж та безпека. Безпека кіберпростору – кібербезпека. МСЕ-Х.1208 2014 р. ISO/IEC 27000.

29. ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperation in Cybersecurity. [Електронний ресурс] – Режим доступу: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf

30. Вдовенко С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення / С. Вдовенко, Ю. Даник, С. Фараон // Електронний журнал політики відкритого доступу "Комп'ютерні науки та кібербезпека" Харківського національного університету імені В.Н. Каразіна. – SSN2519-2310 (Online) № 1 (12) 2019 [Електронний ресурс] – Режим доступу: https://periodicals.karazin.ua/cscs/article/view/13080.

31. С.Соболев, А.Китов, О.Ляпунов. Основные черты кибернетики – М.: Вопросы философии - 1955, №4. [Електронний ресурс] – Режим доступу: https://www.computer-museum.ru/books/cybernetics.htm.

32. Енциклопедія кібернетики: [у 2 т.] / редкол.: В. М. Глушков (відп. ред) [та ін.]; АН Української РСР. – К. Голов. ред. Укр, рад. енцикл. 1973.

33. Закон України "Про основи національної безпеки України" N 964-IV від 19.06.2003 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/964-15#Text.

34. Стратегія національної безпеки України (в редакції від 12 лютого 2007 року № 105/2007) // Офіційний вісник України від 23.02.2007 — 2007 р., № 11, стор. 7, стаття 389, код акту 38751/2007 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/105/2007#Text.

35. Стратегія національної безпеки (в редакції Указу Президента № 389/2012 від 08.06.2012) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/389/2012#Text.

36. Законопроект № 2483 від 07.03.2013 "Про внесення змін до Закону України Про основи національної безпеки України щодо кібернетичної безпеки України", [Електронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=2483&skl=8.

37. Стратегія національної безпеки України, затвердженою Указом Президента України від 26.05.2015 № 287/2015 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

38. Концепція розвитку сектору безпеки і оборони України, введеною в дію Указом Президента України від 14.03.2016 №92/2016 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/92/2016#Text.

39. Стратегія кібербезпеки України Указ Президента України15.03.2016 № 96/2016 Про рішення Ради національної безпеки і оборони України від 27.01.2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/962016-19836.

40. Стратегія національної безпеки України, затвердженої Указом Президента України від 26.05.2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 06.05.2015 року "Про Стратегію національної безпеки України" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

41. Указ Президента України від 13.02. 2017 №32/2017 про затвердження Рішення Ради національної безпеки і оборони України від 29.12. 2016 "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/322017-21282.

42. Звіт про науково-дослідну роботу удосконалення понятійно-категорійного апарату у сфері кібероборони шифр "Дефініція" (заключний) № держреєстрації 0120U103696 8.06.5.035, К.2020, 203 с.

43. Закон України "Про контррозвідувальну діяльність" від 26.12.2002 р. № 374-IV// Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/374-15#Text.

44. Проект Закону України від 27.05.2019 N 10328 "Про критичну інфраструктуру та її захист" [Електронний ресурс] – Режим доступу:http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html.

45. Концепція боротьби з тероризмом в Україні, затверджена Указом Президента України від 5 березня 2019 року № 53/2019. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/53/2019#Text.

46. Указ Президента України № 473/2021 від 17 вересня 2021 року Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/4732021-40121.

47. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.

48. European Program for Critical Infrastructure Protection (EPCIP). [Електронний ресурс] – Режим доступу: https://ec.europa.eu/home-affairs/e-library/glossary/critical-infrastructure_en.

49. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve the protection [Електронний ресурс] – Режим доступу: http://eurlex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32008L0114.

50. European Critical Infrastructure Warning Information Network, CIWIN COM(2008) 676 [Електронний ресурс] – Режим доступу: – https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/viampa6xdqyw.

51. Кримінальний кодекс України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

52. Кодекс України про адміністративні правопорушення [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10#Text.

53. Трофименко О.Г. Аналіз дефініцій різновидів інформаційних війн: [Електронний ресурс] – Режим доступу: http://conf.inf.od.ua/doklady-konferentsii/150-trofimenko.

REFERENCES:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 – Press Release (2016) 100 Issue don 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 [Elektronny`j resurs] – Rezhy`m dostupu https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

2. Strategiya kiberbezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 26 serpnya 2021 roku # 447/2021, – Rezhy`m dostupu https://www.president.gov.ua/documents/4472021-40013.

3. Zhy`vy`lo Ye.O., Chernonog O.O. Strategiya kiberoborony` Ukrayiny` // Zbirny`k naukovy`x pracz` VITI # 4 – 2017 [Elektronny`j resurs] – Rezhy`m dostupu: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Zakon Ukrayiny` "Pro nacional`nu bezpeku Ukrayiny`" vid 21.06.2018 r. # 2469-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Zakon Ukrayiny` "Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`" vid 05.10.2017 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Zakon Ukrayiny` "Pro zaxy`st informaciyi v informacijno-telekomunikacijny`x sy`stemax" [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Zakon Ukrayiny` "Pro rozvidku" vid17.09.2020 # 912-IX [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/912-20#Text.

8. Zakon Ukrayiny` "Pro elektronni dovirchi poslugy`" vid 5 zhovtnya 2017 # 2155-VIII [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

9. Zakon Ukrayiny` "Pro Nacional`nu programu informaty`zaciyi" vid 04.02.1998 r. # 74/98-VR // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

10. Zakon Ukrayiny` "Pro raty`fikaciyu Konvenciyi pro kiberzlochy`nnist`" vid 10.03.2006 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

11. Pro Derzhavnu sluzhbu special`nogo zv'yazku ta zaxy`stu informaciyi : Zakon Ukrayiny` vid 23.02.2006 r. [Elektronny`j resurs]. – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

12. Zakon Ukrayiny` "Pro derzhavnu tayemny`cyu"vid 21 sichnya 1994 # 3855-XII (zi zminamy`) [Elektronny`j resurs]. – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

13. Zakon Ukrayiny` “Pro dostup do publichnoyi informaciyi” vid 13 sichnya 2011 r. # 2939-VI. [Elektronny`j resurs] – Rezhy`m dostupu : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

14. Zakon Ukrayiny` “Pro zaxy`st personal`ny`x dany`x” vid 01.06.2010 r. # 2297-VI [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

15. Zakon Ukrayiny` “Pro oboronu Ukrayiny`” vid 06.12.1991 r. # 1932-XII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

16. Zakon Ukrayiny` Ukrayiny` “Pro informaciyu” # 2938-VI. [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

17. Zakon Ukrayiny` “Pro Zbrojni Sy`ly` Ukrayiny`” vid 6 grudnya 1991 roku # 1934-XII (zi zminamy`) // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/1934-12#Text.

18. Strategiya nacional`noyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 14 veresnya 2020 roku # 392/2020 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny`], vid 14 veresnya 2020 roku Pro Strategiyu nacional`noyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/3922020-35037.

19. Strategiya voyennoyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 25 bereznya 2021 roku # 121/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 25 bereznya 2021 roku Pro Strategiyu voyennoyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/1212021-37661.

20. Ukaz Prezy`denta Ukrayiny` #473/2021 vid 17 veresnya 2021 roku #473/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 20 serpnya 2021 roku “Pro Strategichny`j oboronny`j byuleten` Ukrayiny`” [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/4732021-40121.

21. Ukaz Prezy`denta Ukrayiny` #27/2020 28 sichnya 2020 roku Pro vnesennya zmin do Ukaziv Prezy`denta Ukrayiny` vid 27 sichnya 2015 roku # 37 ta vid 7 chervnya 2016 roku # 242 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/27/2020#Text.

22. Strategiya informacijnoyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 28 grudnya 2021 roku # 685/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 15 zhovtnya 2021 roku Pro Strategiyu informacijnoyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/6852021-41069.

23. Postanova Kabinetu Ministriv Ukrayiny` vid 29 bereznya 2006 r. # 373 Pro zatverdzhennya Pravy`l zabezpechennya zaxy`stu informaciyi v informacijny`x, telekomunikacijny`x ta informacijno-telekomunikacijny`x sy`stemax (Oficijny`j visny`k Ukrayiny`, 2006 p., # 13, st. 878) [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

24. Postanova Kabinet ministriv Ukrayiny` vid 19 chervnya 2019 r. # 518 Pro zatverdzhennya Zagal`ny`x vy`mog do kiberzaxy`stu ob'yektiv kry`ty`chnoyi infrastruktury` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

25. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace. Annex. 32 sessio General Assebly UNESCO, 2003. [Elektronny`j resurs] – Rezhy`m dostupu: https://unesdoc.unesco.org/ark:/48223/pf0000133171.

26. DSTU ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT). Informacijni texnologiyi. Metody` zaxy`stu. Sy`stemy` keruvannya informacijnoyu bezpekoyu. Oglyad i slovny`k terminiv. Nabuv chy`nnosti vidpovidno do nakazu Derzhavnogo pidpry`yemstva "Ukrayins`ky`j naukovo-doslidny`j i navchal`ny`j centr problem standarty`zaciyi, serty`fikaciyi ta yakosti" vid 16.10.2019 # 312 Pro pry`jnyattya ta skasuvannya nacional`ny`x standartiv, pry`jnyattya popravok do nacional`ny`x standartiv [Elektronny`j resurs] – Rezhy`m dostupu: http://online.budstandart.com/ua/catalog/doc-page?id_doc=85639.

27. Rekomendacy`ya MSЭ¬T X.1205. Obzor ky`berbezopasnosty`. – Zheneva:MSE, 2010. – S. 55. [Elektronny`j resurs] – Rezhy`m dostupu: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru.\.

28. Rekomendaciyi mizhnarodnogo soyuzu elektrozv'yazku. Merezhi peredachi dany`x, vzayemozv'yazok vidkry`ty`x merezh ta bezpeka. Bezpeka kiberprostoru – kiberbezpeka. MSE-X.1208 2014 r. ISO/IEC 27000.

29. ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperation in Cybersecurity. [Elektronny`j resurs] – Rezhy`m dostupu: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf.

30. Vdovenko S. Definicijni problemy` terminologiyi u sferi kiberbezpeky` i kiberoborony` ta shlyaxy` yix vy`rishennya / S. Vdovenko, Yu. Dany`k, S. Faraon // Elektronny`j zhurnal polity`ky` vidkry`togo dostupu

“Komp'yuterni nauky` ta kiberbezpeka” Xarkivs`kogo nacional`nogo universy`tetu imeni V.N. Karazina. – SSN2519-2310 (Online) # 1 (12) 2019 [Elektronny`j resurs] – Rezhy`m dostupu: https://periodicals.karazin.ua/cscs/article/view/13080.

31. S.Sobolev, A.Ky`tov, O.Lyapunov. Osnovnыe chertы ky`bernety`ky` – M.: Voprosы fy`losofy`y` - 1955, #4. [Elektronny`j resurs] – Rezhy`m dostupu: https://www.computer-museum.ru/books/cybernetics.htm.

32. Ency`klopediya kibernety`ky`: [u 2 t.] / redkol.: V. M. Glushkov (vidp. red) [ta in.]; AN Ukrayins`koyi RSR. – K. Golov. red. Ukr, rad. ency`kl. —1973.

33. Zakon Ukrayiny` “Pro osnovy` nacional`noyi bezpeky` Ukrayiny`” N 964-IV vid 19.06.2003 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/964-15#Text.

34. Strategiya nacional`noyi bezpeky` Ukrayiny` (v redakciyi vid 12 lyutogo 2007 roku # 105/2007) // Oficijny`j visny`k Ukrayiny` vid 23.02.2007 — 2007 r., # 11, stor. 7, stattya 389, kod aktu 38751/2007 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/105/2007#Text.

35. Strategiya nacional`noyi bezpeky` (v redakciyi Ukazu Prezy`denta # 389/2012 vid 08.06.2012) [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/389/2012#Text.

36. Zakonoproekt # 2483 vid 07.03.2013 Pro vnesennya zmin do Zakonu Ukrayiny` Pro osnovy` nacional`noyi bezpeky` Ukrayiny` shhodo kibernety`chnoyi bezpeky` Ukrayiny`, [Elektronny`j resurs] – Rezhy`m dostupu: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=2483&skl=8.

37. Strategiya nacional`noyi bezpeky` Ukrayiny`, zatverdzhenoyu Ukazom Prezy`denta Ukrayiny` vid 26.05.2015 # 287/2015 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

38. Koncepciya rozvy`tku sektoru bezpeky` i oborony` Ukrayiny`, vvedenoyu v diyu Ukazom Prezy`denta Ukrayiny` vid 14.03.2016 #92/2016 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/92/2016#Text.

39. Strategiya kiberbezpeky` Ukrayiny` Ukaz Prezy`denta Ukrayiny`15.03.2016 # 96/2016 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 27.01.2016 roku "Pro Strategiyu kiberbezpeky` Ukrayiny`" [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/962016-19836.

40. Strategiya nacional`noyi bezpeky` Ukrayiny`, zatverdzhenoyi Ukazom Prezy`denta Ukrayiny` vid 26.05.2015 roku # 287 "Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 06.05.2015 roku "Pro Strategiyu nacional`noyi bezpeky` Ukrayiny`" [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/287/2015#Text.

41. Ukaz Prezy`denta Ukrayiny` vid 13.02. 2017 #32/2017 pro zatverdzhennya Rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 29.12. 2016 Pro zagrozy` kiberbezpeci derzhavy` ta nevidkladni zaxody` z yix nejtralizaciyi [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/322017-21282.

42. Zvit pro naukovo-doslidnu robotu udoskonalennya ponyatijno-kategorijnogo aparatu u sferi kiberoborony` shy`fr “Definiciya” (zaklyuchny`j) # derzhreyestraciyi 0120U103696 8.06.5.035, K.-2020, s. 203.

43. Zakon Ukrayiny` “Pro kontrrozviduval`nu diyal`nist`” vid 26.12.2002 r. # 374-IV// Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/374-15#Text.

44. Proekt Zakonu Ukrayiny` vid 27.05.2019 N 10328 Pro kry`ty`chnu infrastrukturu ta yiyi zaxy`st [Elektronny`j resurs]. – Rezhy`m dostupu:http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html.

45. Koncepciya borot`by` z terory`zmom v Ukrayini, zatverdzhena Ukazom Prezy`denta Ukrayiny` vid 5 bereznya 2019 roku # 53/2019. [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/53/2019#Text.

46. Ukaz Prezy`denta Ukrayiny` # 473/2021 vid 17 veresnya 2021 roku Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 20 serpnya 2021 roku “Pro Strategichny`j oboronny`j byuleten` Ukrayiny`” [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/4732021-40121.

47. Informacijna ta kiberbezpeka: sociotexnichny`j aspekt: pidruchny`k / V.L. Buryachok, V.B. Tolubko, V.O. Xoroshko, S.V. Tolyupa; za zag. red. V.B. Tolubka. – K.: DUT, 2015. – 288 s.

48. European Program for Critical Infrastructure Protection (EPCIP). [Elektronny`j resurs] – Rezhy`m dostupu:https://ec.europa.eu/home-affairs/e-library/glossary/critical-infrastructure_en.

49. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve the protection [Elektronny`j resurs] – Rezhy`m dostupu: http://eurlex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32008L0114.

50. European Critical Infrastructure Warning Information Network, CIWIN COM(2008) 676 [Elektronny`j resurs] – Rezhy`m dostupu: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/viampa6xdqyw.

51. Kry`minal`ny`j kodeks Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

52. Kodeks Ukrayiny` pro administraty`vni pravoporushennya [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/80731-10#Text.

53. Trofy`menko O.G. Analiz definicij riznovy`div informacijny`x vijn: [Elektronny`j resurs] – Rezhy`m dostupu: http://conf.inf.od.ua/doklady-konferentsii/150-trofimenko.

Vdovenko S.G., Ph.D. Zhivilo E.A., Chernonog A.A., Dokil V.N.

ANALYSIS OF THE REGULATORY AND LEGAL FRAMEWORK OF THE FUNCTIONING OF THE CYBER DEFENSE SYSTEM AND THE CYBER DEFENSE SYSTEM IN THE INFORMATION AND TELECOMMUNICATION SYSTEMS OF MILITARY PURPOSE

The urgency of this work is due to one of the priorities of the national security system of Ukraine to perform the functions and tasks of the defense forces of Ukraine in conditions of destructive activity on the cybersecurity environment of the state.

Modern development of information and cyber technologies and global informatization in the world have led to the fact that the information and cybersphere have become the object of various destructive influences on all spheres of society through cyberspace, which complemented existing ones, namely land, sea, air, space and became a sphere conflicts and possible hostilities.

States, depending on the degree of their development, build different systems (models) of protection of their information, telecommunications infrastructures, determine the use of technological processes circulating in these systems and protect critical infrastructure from cyber threats, determine the functions, directions and ways of action in cyberspace. Today, more than 60 countries in the world are openly and / or covertly working to improve the functionality of national cybersecurity and cyber defense systems. National and coalition cyber forces are being created, their functions and tasks are being determined, the content and procedure of activity, composition, algorithms for training units, military and civilian specialists are being formed, strategies are being developed, regulatory framework, hardware and software complexes, and special cyber defense software are being improved. and tactics of their application.

In general, the development and widespread implementation of communication systems and systems using innovative information and telecommunications technologies in military systems is in accordance with international rules for cyberwarfare, such as the Geneva Convention. At the same time, the main principles of formation of cybersecurity and cyber defense systems of the leading countries of the world are scientifically substantiated legislative, normative-legal, definition-terminological support. Under these conditions, the transformation of the regulatory framework takes into account the constant militarization of national segments of cyberspace, taking into account the criteria (indicators) of threats in cybersecurity and cyber defense of leading countries, the level of system readiness and acquisition of capabilities, etc.

To address the issues of regulation and implementation of norms and rules of international organizations in the field of cybersecurity and cyber defense, it is proposed to analyze the current provisions (axiomatics) of the existing legislative, state and departmental regulatory framework, as well as the regulatory framework of international organizations. ITU) on cybersecurity.

Keywords: cyberspace, cybersecurity, cyber defense, law of Ukraine, normative - legal base, normative legal act, object of critical information infrastructure.

УДК 004.891

к.т.н., доц., **Джулій В.М.** (ХмНУ)
к.т.н., с.н.с. **Мірошніченко О.В.** (ВІКНУ)
Солодєєва Л.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-07

МЕТОД КЛАСИФІКАЦІЇ ДОДАТКІВ ТРАФІКА КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ МАШИННОГО НАВЧАННЯ В УМОВАХ НЕВИЗНАЧЕНОСТІ

У роботі запропоновано метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності. Сучасні методи класифікація додатків трафіка комп'ютерних мереж (таких, як класифікація протоколів транспортного рівня за номерами портів) мають суттєві недоліки, що призводить і є причиною до зростання проведення досліджень в напрямку класифікація додатків трафіка комп'ютерних мереж. Стрімке зростання, за останні роки, типів та кількості мережевих протоколів транспортного рівня підвищують актуальність дослідження в даному напрямку, розробки відповідних алгоритмів та методів класифікації додатків трафіка комп'ютерних мереж, які забезпечують при цьому зниження обчислювальної складності. На сучасному етапі, задача, яка потребує термінового вирішення - класифікації додатків трафіка комп'ютерних мереж з використанням відповідних протоколів та алгоритмів шифрування.

Перспективним напрямком класифікації додатків трафіка комп'ютерних мереж є статистичні методи, які опираються на аналізі та виявленні статистичних характеристик IP-трафіка. Найбільш перспективними є інтелектуальний аналіз потоку даних, а також технології машинного навчання, які на сучасному етапі широко використовуються в суміжних областях науки. Вирішується задача дослідження та навчання по прецедентах - класифікація додатків трафіка комп'ютерних мереж на основі зазделегідь відомої сукупності атрибутів їх ознак, з метою вдосконалення технічної бази комп'ютерних мереж, а також теоретичної бази, при цьому забезпечення високих експлуатаційних та якісних показників мереж, на прикладі використання протоколів транспортного рівня (стека TCP/IP). Результат вирішення поставленої задачі полягає у віднесенні додатка, відповідно до правил навчальної вибірки, до одного з непересічних класів, які заздалегідь визначенні, який містить відповідні, але при цьому вже класифіковані додатки.

Статистичний аналіз та дослідження атрибутів інтернет додатків показав, що найважливіші атрибути, пов'язані зі зміною об'єму інтернет трафіка потоку даних, мають експоненційний вигляд. Для виявлення аномальних змін об'єму інтернет трафіка додатків для розрахунку середніх значень може бути використаний критерій Фішера. Для класифікації інтернет додатків у потоковому режимі даних, при безперервному надходженні потоку даних запропоновано алгоритм виявлення зміщення концепту (дрейфа) трафіка потоку даних. Детектор дрейфа Фішера базується на статистичних характеристиках атрибутів інтернет додатків, аналізуються з використанням ковзаючих вікон, які контролюють зміну трафіка поточних статистичних характеристик атрибутів додатків.

Ключові слова: моделі, класифікація додатків, комп'ютерні мережі, дрейф, трафік, ковзаюче вікно, машинне навчання.

Вступ. Класифікація додатків IP-трафіка комп'ютерних мереж є важливим завданням керуванням потоком даних, покращення експлуатаційних характеристик, техніко-економічних, а також захисту трафіка комп'ютерних мереж. Класифікація IP-трафіка комп'ютерних мереж дозволяє визначити структуру, тип додатка, також джерело програми. Системи класифікації додатків IP-трафіка комп'ютерних мереж використовуються в достатньо широкому спектрі функцій: забезпечення на достатньому рівні якості зв'язку, виконання та забезпечення політик інформаційної безпеки, а також при розробці відповідних алгоритмів, програмних продуктів, що забезпечують достатній рівень стан комп'ютерних мереж, діагностику, контроль, а також надають засоби набору статистичних даних, виявлення проблем комп'ютерних мереж.

Сучасні методи класифікація додатків трафіка комп'ютерних мереж (таких, як класифікація протоколів транспортного рівня за номерами портів) мають суттєві недоліки, що призводить і є причиною до зростання проведення досліджень в напрямку класифікація додатків трафіка комп'ютерних мереж. Стрімке зростання, за останні роки, типів та кількості мережевих протоколів транспортного рівня підвищують актуальність дослідження в даному напрямку, розробки відповідних алгоритмів та методів класифікації додатків трафіка комп'ютерних мереж, які забезпечують при цьому зниження обчислювальної складності. На сучасному етапі, задача, яка потребує термінового вирішення - класифікації додатків трафіка комп'ютерних мереж з використанням відповідних протоколів та алгоритмів шифрування.

Перспективним напрямком класифікації додатків трафіка комп'ютерних мереж є статистичні методи, які опираються на аналізі та виявленні статистичних характеристик IP-трафіка. Найбільш перспективними є інтелектуальний аналіз потоку даних, а також технології машинного навчання, які на сучасному етапі широко використовуються в суміжних областях науки.

Аналіз останніх досліджень та постановка задачі. Методи класифікація об'єктів, широко використовуються переважно в економічних дослідженнях, які можна вбудувати в область комп'ютерних мереж та телекомунікаційних досліджень [1-12]. Однак в даних роботах не отримали на достатньому рівні відображення як теоретичні так і практичні питання класифікації додатків трафіка комп'ютерних мереж, які використовують протоколи транспортного рівня (стек TCP/IP) в умовах невизначеності, при наявності «фонового» трафіка, а також проведення оцінки ефективності алгоритмів, які в основі реалізують методи машинного навчання при наявності режиму потокового надходження даних. Більшість використовуваних алгоритмів машинного навчання з учителем призначені для навчання мультикласових або бінарних класифікаторів. На основі навчального набору даних трафіка, що складається з екземплярів двох класів, біномні (бінарні) класифікатори вибирають між класами об'єктів. Мультикласові (мультиноміальні) класифікатори розподіляють екземпляри на множину класів згідно з тренувальним набором даних, що складається з екземплярів усіх класів. Дані типи класифікаторів засновані на припущеннях: всі класи відомі наперед; для кожного класу існує ефективний і показовий набір потоку даних.

Таким чином, класифікатори з учителем нездатні визначити екземпляри класу, які не представлені у навчальній вибірці простору ознак. Ідентифікація невідомого об’єкта типу трафіка є найважливішою вимогою на сьогоднішньому етапі ідентифікації мережного трафіку, оскільки у зв'язку з розвитком Інтернету з'являються нові інтернет протоколи та додатки, які на даний час невідомі, або представлені не в повній мірі на момент навчання. Також, навіть для існуючих протоколів та мережних додатків дорого і важко отримати повноцінний позначений набір потоку даних, які характеризують відповідні класи. Для того, щоб розробити практичний класифікатор мережевого трафіка з використанням методів машинного навчання з учителем, необхідно бути скурпульозним з визначенням відповідного класу та побудовою даних тренувального набору.

Розглянемо вплив фонового невідомого трафіку на якість класифікації з використанням методів машинного навчання. Будемо розглядати як «корисні» мережні протоколи та додатки DNS, HTTP, BitTorrent, Steam, Skype.

Крім перевірки роботи алгоритму на тестовій вибірці, яка має класовий склад, як і навчальна, оцінка якості класифікації здійснювалася за умов присутності домішок фонового трафіка, в тестовій вибірці присутні екземпляри класів, відсутніх у навчальній вибірці простору ознак. Така ситуація, коли в тестовій вибірці, яка ідентифікується, присутній мережевий фоновий трафік, більш наближена до реальності, в силу множини протоколів, що використовуються в Інтернет мережі. Такий набір даних дозволяє оцінити роботу якості класифікації алгоритму в реальній ситуації.

В умовах відсутності фонового трафіка потоку даних алгоритми C4.5 і Random Forest мають найкращі показники оцінки якості класифікації мережевих додатків. Однак за наявності в наборі даних фонового трафіка оцінка якості класифікації мережевих додатків суттєво

знижується, для алгоритму Random Forest зниження оцінка становить 15%, а для C4.5 оцінка зниження досягає 20%.

Класифікація мережевих додатків в наявності в наборі даних фонового трафіка показала, алгоритми машинного начання з учителем, не здатні визначити фоновий трафік, що призведе до неминучих та критичних помилок класифікації мережевого трафіка.

Розвитком у даному напрямку є застосування інших методів кластеризації (алгоритмів навчання), для визначення та розмежування мережевих невідомих типів трафіка потоку даних, які вже потім класифікуються та аналізуються відповідними системами.

При використанні змішаних даних набору трафіка, що складаються з великої кількості «корисних» екземплярів потоків даних і невеликої кількості фонових екземплярів, в даному випадку можливе застосування технік кластеризації для розподілу трафіка потоків даних в декілька груп відповідно до подібності статистичних показників трафіка.

Технології кластеризації важлива задача класифікації трафіка, на практиці отримання повного «корисного» трафіка набору даних для навчання є трудомістким та складним процесом. Одним з напрямків вирішення задачі – розробка нових шаблонів, які представлятимуть невідомі додатки або зміни в існуючих класах класифікації. Отриманий трафік у формі мережевих інтернет пакетів збирається в мережеві потоки даних, на основі вищезазначених п'яти параметрах для класифікації. Для проведення кластеризації кожен із потоків описується значеннями заздалегідь визначеним набором властивостей, тобто. точкою $x = (x_1, ..., x_d)$ в d – вимірному просторі ознак трафіка, d – кількість ознак в просторі ознак. На даній стадії може проводитись попередня обробка атрибутів, трансформації та їх відбору.

Фонові вектори властивостей можуть бути наперед оброблені алгоритмами кластеризації, які розподіляють трафік на по відстані. Задачею даного етапу створення чистих кластерів.

Основна частина. Для класифікації трафіка потоку даних в режимі on-line кластери трафіка необхідно пов'язати з конкретними класами інтернет додатків, і на їх основі побудувати класифікатори. Простим рішенням задачі є ручна ідентифікація потоків у кожному кластері даних з наступним розподіленням цих кластерів відповідно до потоків даних. Інший підхід полягає в подачі на вхід алгоритму змішаних даних, які складаються з «корисних» екземплярів та невеликої кількості фонових екземплярів потоку. Промарковані потоки даних, які містяться в кластерах, будуть використані для найменування кластерів. Розглянемо отримання максимально чистих кластерів трафіка потоку даних. У методі кластеризації, заснованому на «відстані», кластери представлені центральними точками (центроїдами), а екземпляри, відносяться до найближчої точки відповідно до метрики відстані (Евклідова відстань). Метод K-Means відносить екземпляри трафіка до кластерів з найближчим середнім значенням, а потім перетворює на локальний мінімум суми квадратів відстаней між кожним екземпляром трафіка потоку даних і центром кластера. Метод кластеризації, заснований на ймовірності, екземпляри з певною ймовірністю можуть бути віднесені найбільш можливого кластера. Традиційні методи кластеризації ґрунтуються на шаблонах в Евклідовому просторі ознак інтернет трафіка та припущенні, що всі ознаки, при цьому мають однакову вагу в кластеризації.

Методи неконтрольованого навчання (навчання без вчителя) значно поступаються алгоритмам Random Forest навчання з вчителем. Таким чином метод DBSCAN не придатний в режимі online, може бути критичним для ідентифікації додатків, що генерують мережеві інтернет потоки, у системах забезпечення інформаційної безпеки. У подібних системах мережний трафік потоку даних неоднорідний і може в процесі змінюватися, що призведе за собою постійного перенавчання алгоритму. Якість оцінки роботи алгоритмів DBSCAN і *k*-Means, в значній мірі залежить від мережевого типу трафіка, який класифікується. Для мережевих протоколів DNS і BitTorrent більш придатним - алгоритм DBSCAN, для мережевого трафіка Steam і SSL – *k*-Means, результати для класів додатків Skype та HTTP у розглянутих алгоритмів близькі.

Проведений аналіз характеристик алгоритмів класифікації з використанням фонового трафіка показав зниження якості оцінки класифікації додатків. Застосування різних методів кластеризації також показали низькі оцінки якості кластеризації.

Розглянемо кластеризацію мережного трафіка потоку даних, що базується на методі Random Forest. Даний підхід застосовується в біометричних дослідженнях для пошуку кластерів даних геномної послідовності. Random Forest один із контрольованих алгоритмів навчання, показав найкращі результати у задачах класифікації мережевого трафіка потоку даних. Random Forest забезпечує високу точність, дає незміщену оцінку помилки під час навчання, а також оцінку близькості між парами трафіка вхідних точок потоку даних, що надає можливість використовувати його для кластеризації трафіка вхідного потоку даних. Для побудови «лісу» необхідно визначити два базових параметри: кількість змінних, для розподілу вузлів (m) та кількість дерев (n). Для побудови дерева рішень метод генерує кореневий вузол шляхом випадкового відбору N точок даних трафіка з навчальної вибірки, де N - розмір тренувального набору ознак. Потім ітеративно розділяє вузли на основі m змінних, за критерієм індекса Джіні. Дерева рішень будують настільки великими, наскільки це можливо, без відсікання гілок. На початковому процесу відбору навчання близько третини всіх точок потоку даних залишаються поза набором, Ці дані, в подальшому, можна використовувати для оцінки помилки класифікації. Коли дерева рішень побудовані, дані можуть бути пропущені через отриманий «ліс» і також обчислені міри близькості кожної пари даних точок. Якщо дві точки даних потрапляють в листовий вузол, їхня близькість збільшується на одиницю, близькості нормалізуються шляхом поділу на число дерев. Таким чином створюється симетрична матриця близькості P, кожен елемент матриці має значення в інтервалі [0, 1]. За наявності фонових даних безпосередньо збудувати дерево неможливо. Для виділення показника близькості необхідна штучна класифікації, коли випадковий «ліс» будується шляхом розподілення штучних даних від вхідних. Результуючий ліс і значення близькості точок великою мірою залежить, в даному випадку від складу штучних об'єктів.

Метрики оцінки якості кластеризації простору ознак. Для оцінки ефективності кластеризації простору ознак алгоритмів використовувалися наступні метрики:

1. Однорідність - величина, що приймає максимальне значення - 1, якщо в кластер входять екземпляри одного класу. Близькість результатів кластеризації до визначається шляхом оцінки ентропії класів з урахуванням запропонованих кластерів:

$$H(C \mid K) = -\sum_{k=1}^{|K|}\sum_{c=1}^{|C|}\frac{n_{c,k}}{n}\cdot\log\left(\frac{n_{c,k}}{n}\right) = 0. \quad (1)$$

Отримане значення нормується за допомогою максимальної ентропії, яку може забезпечити, в даному випадку кластеризація - ентропії класу. Таким чином, однорідність кластера визначиться як $h = 1 - \frac{H(C \mid K)}{H(C)}$, де $H(C \mid K)$ – ентропія класу при умові кластера, а $H(C)$ – ентропія класу.

2. Повнота (completeness) – величина, симетрична однорідності кластера $c = 1 - \frac{H(K \mid C)}{H(K)}$,

де $$H(K \mid C) = -\sum_{c=1}^{|C|}\sum_{k=1}^{|K|}\frac{n_{c,k}}{n}\cdot\log\left(\frac{n_{c,k}}{n}\right). \quad (2)$$

3. V-міра - визначається обчисленням середнього гармонійного повноти та однорідності: $V = \frac{2\cdot c\cdot h}{c+h}$. Дана метрика не залежить від абсолютних значень міток кластера чи класу: перестановка значень не змінить значення оцінки класифікації.

4. Коефіцієнт силуету обчислюється для кожного екземпляра окремо:

$$s = \frac{b-a}{\max(a,b)},$$

де a - середня відстань від даного екземпляра до інших екземплярів кластера,

b - середня відстань від даного екземпляра всіх екземплярів найближчого кластера.

Коефіцієнт силуету для набору екземплярів визначається як середнє значення коефіцієнта силуету для кожного визначеного зразка. Коефіцієнт силуету приймає значення від -1 до 1. Від'ємне значення - неправильна кластеризаці, екземпляр поміщений не в той кластер. Значення близько нуля кластери перекриваються. Значення коефіцієнта силуету чим ближче до 1, тим щільніше розділені кластери.

5. Незміщений індекс Ранда - обчислює міру подібності між реальними значеннями міток і результатом кластеризації, при цьому розглядаються всі пари екземплярів, підраховуються пари, які призначені при класифікації в одні або різні кластери і класи, розраховується наступним чином:

$$RI = \frac{a+b}{C_2^n},$$

де a – кількість пар екземплярів у вибірці простору ознак, які потрапили в один кластер та клас;

b - кількість пар екземплярів у вибірці, що потрапили в кластер, що не відповідає даному класу, n - кількість елементів у вибірці простору ознак. Індекс Ранда дорівнює 1 при співпаданні результатів кластеризації додатків з істинними значеннями «корисних» об'єктів.

При застосуванні метрики Індекс Ранда навіть випадковий розкид екземплярів за класами (кластерами) матиме додатню оцінку. Для правильної оцінки випадкової кластеризації необхідно нормувати даний індекс:

$$ARI = \frac{RI - E[RI]}{\max(RI) - E[RI]},$$

де $E[RI]$- очікуваний зміщений індекс Ранда. Індекс Ранда може приймати значення від -1 до 1. Випадкове присвоєння міток об'єктам буде мати показник, близький до 0, для будь-яких кількостей класів і кластерів, Від'ємні значення позначають погану кластеризацію, правильна кластеризація має додатні значення Індекса Ранда. При ідеальному співпадані кластерів та класів Індекс Ранда дорівнює 1.

Класифікація додатків комп'ютерних мереж є процесом передбачення невідомого атрибута відповідного класу елемента, використовуючи модель, навченої на тренувальному набору потоку даних. На відміну від традиційних підходів класифікації, потокові методи класифікації не можуть оперувати з об'ємом потоку даних, який поділяється на тестовий та тренувальний набори, таким чином, тестування та побудова моделі необхідно здійснювати на льоту.

Вузьким місцем класифікації мережних потокових даних є необхідність аналізу за один перегляд. Однопрохідний перегляд та аналіз потоку даних не запам'ятовує зміни, що відбулися в моделі з початку обробки потокових даних.

Таким чином, процес класифікації потокових даних може вимагати побудови моделі та її тестування в змінному середовищі трафіка. Процес тестування моделі відбувається у постійній конкуренції з процесом тренування. Обчислювальні методи потокового аналізу даних повинні використовувати статистику та теорію обчислень. Швидкість мережевих потокових даних та великий об'єм, висувають додаткові вимоги до ресурсів у системі кластеризації. На сьогодні розроблено ряд підходів до обробки мережевих потокових даних. Дані методи дозволяють застосовувати алгоритми машинного навчання мережевих потокових

даних. Особливістю мережевого потокового режиму є дрейф (зміщення) концепту, в результаті поточних змін в атрибутах мережевого аналізованого трафіка потоку даних. Зміни виникають при появі зміни інтенсивності атрибутів, нових пристроїв в мережі. Таким чином, зміни відображаються в мережних об'єктах і знижують точність оцінки класифікаторів, побудованих на навчальних об'єктах отриманих раніше.

Зміщення концепту (дрейф) – виникає, коли розподіл вхідних потокових значень x і отриманих результатів y змінюється у часі. У навчанні з учителем дрейф впливає на умовну ймовірність вхідного значення $P(x|y)$, на оцінку ймовірності $P(y|x)$, на результуючий розподіл $P(y)$, на сам розподіл вхідних значення $P(x)$. Зміщення концепту (дрейф) - поняття між моментом часу t_0 і моментом часу t_1 визначається як $\exists X : p_{t_o}(X,y) \neq p_{t_1}(X,y)$, де p_{t_o} спільний розподіл потокових даних у момент t_0 між потоковим набором вхідних змінних X і цільової функцією y. Таким чином можуть змінитися умовні ймовірності класу $p(x|y)$, ймовірності класів $p(y)$, (y); в результаті змінюються ймовірності класів $p(y|x)$, впливаючи на результати кластеризації прогнозування.

Більшість методів зміни концепту використовують, для вирішення задачі, часове вікно, обробляють атрибути в часовому вікні, і «забувають» інформацію про «минуле» даних атрибутів. Методи використовують часові вікна, при цьому припускають, що важлива інформація лише останніх атрибутів. Таким чином, адаптивне навчання проводить оновлення прогнозуючих моделей трафіка у режимі онлайн, щоб адекватно реагувати на дрейф концепту.

Адаптивний алгоритм ADWIN для виявлення змін, використовує часове вікно. Нехай задана послідовність дійсних чисел - $x_1, x_2, x_3, ..., x_t$. На вхід алгоритму ADWIN необхідна вхідна послідовність на інтервалі [0,1], необхідне масштабування вхідних даних. Визначимо μ_t математичне очікування x_t, що підпорядковується D_t. Алгоритм ADWIN не передбачає конкретного розподілу даних і використовує фіксованого розміру W ковзне вікно з новими значеннями x_t. Позначимо $\tilde{\mu}_W$ середнє значення спостережень в W, μ_W - невідоме середнє значення μ_t для $t \in W$. Як тільки дві частини W демонструють середні значення, що відрізняються, алгоритм ADWIN вирішує, що математичні очікування цих частин відрізняються і стара частина вікна відкидається.

Основним обмеженням використовуваних методів виявлення дрейфа, які в основі використовують моніторинг двох розподілів, у порівнянні з детекторами послідовної обробки потоку даних, є вимоги до пам'яті. Основною перевагою методів виявлення дрейфа є точніша локалізація моменту дрейфу (із затримкою не менше W вибірок). Недоліком методу - він не враховує реального розподілу потоку даних, і вимагає, щоб дані знаходилися в інтервалі [0,1].

Алгоритм виявлення дрейфа (зміни концепту) за критерієм Фішера. Нехай заданий спостережуваний потік даних $Y = \{y_0, y_1, y_2, ..., y_{N-1}\}$, де y_t - значення елементів потоку даних (атрибутів і додатків), виміряне в $t \in T = \{0,1,2,...,N-1\}$, N - розмір множини Y. Виявлення зміни концепту (дрейфу) додатків здійснюється з використанням ковзних вікон W_1 і W_2, які контролюють зміну поточних статистичних характеристик додатків і атрибутів, як показано на рис. 1.

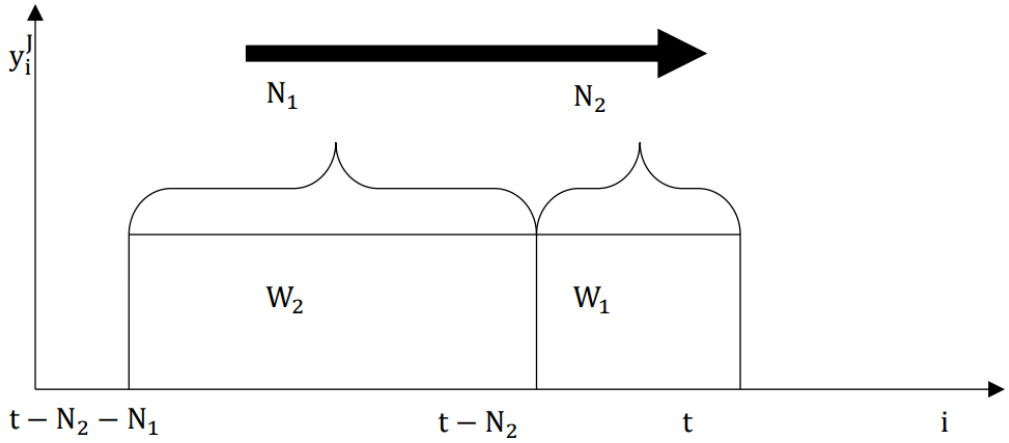

Рисунок 1 – Динаміка аналізу додатків за допомогою вікон W_1 і W_2

Вікно W_1 характеризує статистику атрибутів мережевого додатка в «минулому»:

$$Y_1^J = \left\{ y_{ij}^J ; j = \overline{1,K}; i = \overline{1;N_1} \right\}. \quad (3)$$

Вікно W_2 характеризує статистику атрибутів мережевого додатка на «поточний час»

$$Y_2^J = \left\{ y_{ij}^J ; j = \overline{1,K}; i = \overline{1;N_2} \right\}, \quad (4)$$

де, y_{ij}^J *j*-й атрибут додатка *J*, для *i*-го інтервалу спостереження; *K* - кількість атрибутів додатка *J*; N_1 - об'єм вікна пам'яті; N_2 - об'єм вікна аналізу $0 < N_2 < N_1$..

Використання алгоритму «ковзаючих вікон» дозволяє визначити незначні аномалії в реальному часі для виявлення зміни концепту (дрейфу) *i*-го мережевого додатка пропонується використовувати статистику, на основі статистичних даних приймається рішення про зміни концепту (дрейфу). Пропонується використовувати статистику відповідно до критерію Фішера для середніх значень вікон:

$$R_t^J = \frac{M_{W_2}^J(t)}{M_{W_1}^J(t)} > \lambda, \quad (5)$$

де, $M_{W_1}^J(t) = \frac{1}{N_2 K} \sum_{i=t}^{t-N_2} \sum_{j=1}^{K} y_{ij}^J$, $M_{W_2}^J(t) = \frac{1}{N_1 K} \sum_{i=t-N_2}^{t} \sum_{j=1}^{K} y_{ij}^J$,.

Перевищення порогового рівня вирішальної статистики $R(t) > \lambda$ свідчить про зміну характеристик мережевих додатків, і вказує на необхідність перенавчання поточного класифікатора. Збільшення порогу λ призводить до зменшення помилкових спрацьовувань класифікації трафіка, це можна призвести до пропуску зміни концепту (дрейфу), чи до затримок у виявленні дрейфу.

Для проведення практичної перевірки роботи запропонованого методу виявлення зміни концепту (дрейфу) в якості вхідних даних взято трафік мобільного інтернет додатка «Instagram». Для зміни тренда проведено множення значень отриманих ознак, що характеризують корисне навантаження трафіка на мережному та транспортному рівнях. В результаті запропонованого перетворення отриманий потік, який описується мережевим графіком, наведеним на рис. 2. Кожна точка наведеного графіка описується співвідношенням $D(t) = \sum_{j=1}^{K} y_{tj}$, де y_{tj} - значення *j*-го атрибута аналізованого інтернет додатка на інтервалі

часу - t. В правій частині графіка (рис. 2а) наведено результат множення ознак. Графіки (рис. 2б, рис. 2в) відображають значення, що спостерігаються відповідно у вікнах W_1 і W_2 у процесі проведення аналізу трафіка потоку даних. На рис. 2, через різке наростання тренда після $2{,}5\times10^5$, у вікні W_2 відбувається різке збільшення отриманого середнього значення. Збільшення середнього значення призводить до різкого наростання (стрибка) значення $R(t)$, що наведено на рис. 2г.

Таким чином для визначення різкого збільшення обєму корисного навантаження, може бути використаний запропонований метод.

Для виявлення дрейфу концепції розробленим методом необхідно обчислення для кожного значення t середніх значень $M_{W_1}(t)$ і $M_{W_2}(t)$. При великих розмірах вікон продуктивність методу може різко впасти. Для усунення даного недоліка можна розглядати значення $M_{W_1}(t)$ і $M_{W_2}(t)$ не для всіх значень t, а лише для кратних значень інтервалу S_t. Введення інтервалу впливає тільки на значення $M_{W_1}(t)$, $M_{W_2}(t)$ і $R(t)$, але не на трафік вхідного потоку елементів Y.

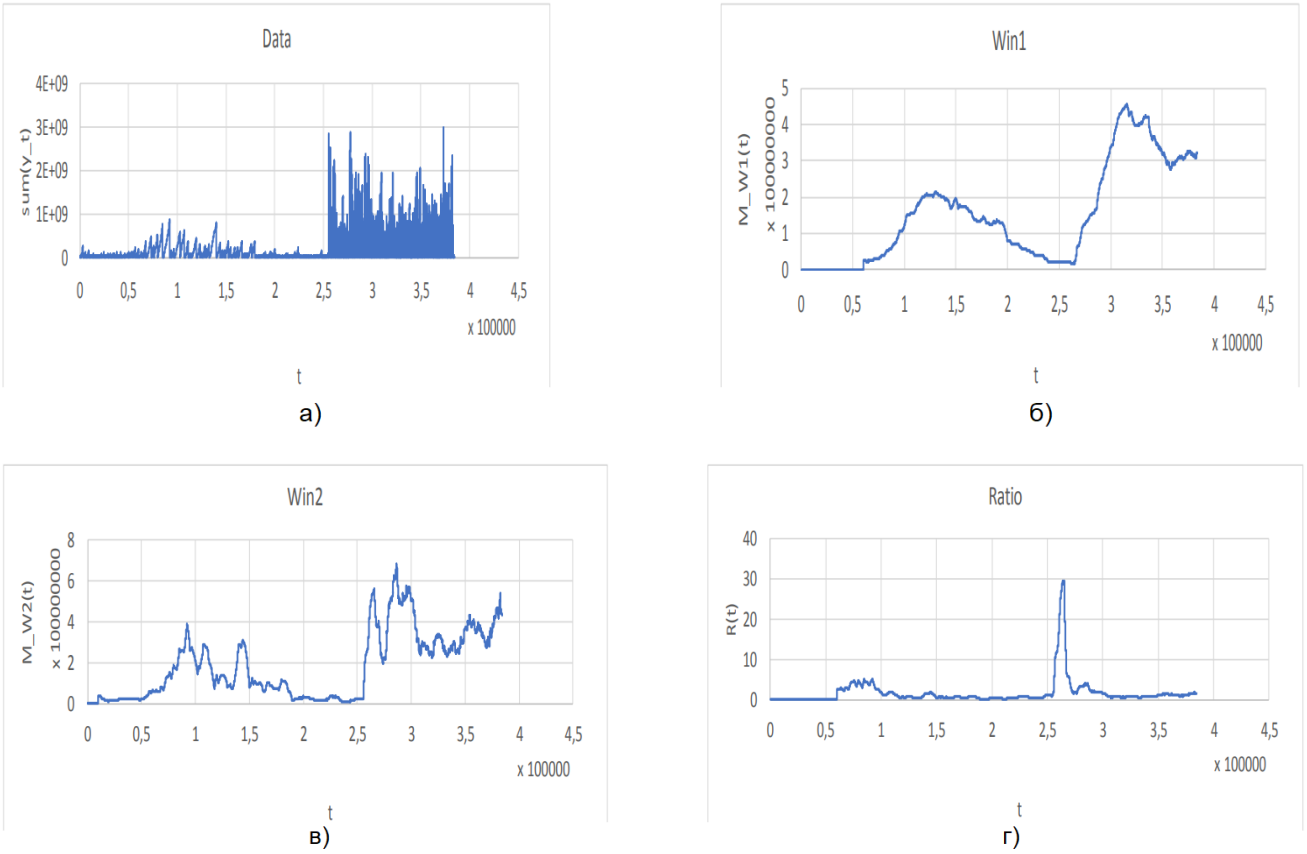

Рисунок 2 - Експериментальні дані
а) додатка «Instagram», б) залежності M_{W_1}, в) залежності, г) Залежності $R(t)$

Висновки. Наявність фонового трафіка значно погіршує оцінку якості і точності класифікації. Для інтернет додатка Skype зниження оцінки точності класифікації для алгоритму Random Forest - 13,2 %, для C4.5 до 35%. Для інтернет додатка BitTorrent зниження оцінки точності класифікації: для Random Forest -5,7%, для C4.5-37%, обумовлено помилковою класифікацією фонових інтернет додатків.

Алгоритми неконтрольованого навчання DBSCAN та *k*-Means значно поступаються алгоритмам які використовують навчання з вчителем (Random Forest). Алгоритм *k*-Means вирішує задачу кластеризацією мережного трафіка, лише за умови, що кількість кластерів

наперед відома, інакше якість класифікації погіршується і для інтернет додатків DNS, HTTP, Skype, Steam досягає 30%. Алгоритм DBSCAN видає значні помилки у змісті та кількості кластерів аналізованих інтернет додатків розкидані по багатьох кластерах.

Алгоритми оцінки якості і точності класифікації C4.5 та Random Forest показують близькі результати. Середня величина оцінки для інтернет додатків становить для алгоритму Random Forest - 0,984, для алгоритму C4.5 - 0,985. За часом тестування та навчання суттєво різняться. Час тестування Random Forest в середньому в 4 рази менше, алгоритму C4.5.

Статистичний аналіз та дослідження атрибутів інтернет додатків показав, що найважливіші атрибути, пов'язані зі зміною об'єму інтернет трафіка потоку даних, мають експоненційний вигляд. Для виявлення аномальних змін об'єму інтернет трафіка додатків для розрахунку середніх значень може бути використаний критерій Фішера.

Для класифікації інтернет додатків у потоковому режимі даних, при безперервному надходженні потоку даних запропоновано алгоритм виявлення зміщення концепту (дрейфа) трафіка потоку даних. Детектор дрейфа Фішера базується на статистичних характеристиках атрибутів інтернет додатків, аналізуються з використанням ковзаючих вікон, які контролюють зміну трафіка поточних статистичних характеристик атрибутів додатків.

ЛІТЕРАТУРА:

1. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, , В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

2. Джулій, В.М. Модель нелегітимного абонента забезпечення безпеки IP-телефонії / О.С. Андрощук, В.М. Джулій, Ю.П. Кльоц, І.В. Муляр // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький, 2020. – №2. – С. 38–45.

3. Джулій В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

4. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование/ О.И. Шелухин - М.: Горячая линия -Телеком, 2019. - 448 с.

5. Шелухин О.И. Классификация IP-трафика методами машинного обучения / О.И. Шелухин, С.Д. Ерохин - М.: Горячая линия -Телеком, 2018. - 284 с.

6. Батурин, Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М.: Юридическая литература, 2006. – 160 с.

7. Нестеров, С.А. Основы информационной безопасности: учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.

8. Олифер, В.Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия-Телеком, 2017. - 644 с.

9. Бабаш, А.В. Криптографические методы защиты информации: учебник для студетнов вузов / А. В. Бабаш, Є. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

10. Борисов, М.А. Основы для программно-аппаратной защиты информации : учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 4-е изд., переработаное и доп. - М. : ЛЕНАНД, 2016. - 416 с.

11. Васильева, И. И. Криптографические методы защиты информации : практикум и учебник для академ. бакалавриата / И. И. Васильева. - Санкт-Петерб. гос. эконом. университет . - М. : Юрайт, 2017. - 349 с.

12. Нестеров, С.А. Основы информационной безопасности : учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.

REFERENCES:

1. Lenkov, S.V. Model bezpeky poshyrennia zaboronenoi 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, 2020. – №68. – Pp. 53-64.

2. Dzhulii, V.M. Model nelehitymnoho abonenta zabezpechennia bezpeky IP-telefonii / O.S. Androshchuk, V.M. Dzhulii, Yu.P. Klots, I.V. Muliar // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – Khmelnytskyi, 2020. – №2. – Pp. 38–45.

3. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi, 2021. – №5. – Pp. 22–26.

4. Shelukhyn O.Y. Setevыe anomalyy. Obnaruzhenye, lokalyzatsyia, prohnozyrovanye/ O.Y. Shelukhyn - M.: Horiachaia lynyia -Telekom, 2019. - 448 s.

5. Shelukhyn O.Y. Klassyfykatsyia IP-trafyka metodamy mashynnoho obuchenyia / O.Y. Shelukhyn, S.D. Erokhyn - M.: Horiachaia lynyia -Telekom, 2018. - 284 s.

6. Baturyn, Yu.M. Kompiuternaia prestupnost y kompiuternaia bezopasnost / Yu.M. Baturyn, A.M. Zhodzynskyi. – M.: Yurydycheskaia lyteratura, 2006. – 160 s.

7. Nesterov, S.A. Osnovы ynformatsyonnoi bezopasnosty : uchebnyk / S. A. Nesterov. - SPb. : Lan, 2017. – 423 s.

8. Olyfer, V.H. Bezopasnost kompiuternыkh setei / V. H. Olyfer, N. A. Olyfer. - M. : Horiachaia lynyia-Telekom, 2017. - 644 s.

9. Babash, A.V. and Baranova, Ye. K. (2016), “Kryptohrafycheskye metodы zashchytы ynformatsyy : uchebnyk dlia studetnov vuzov” / M. : KNORUS, 190 p.

10. Borysov, M.A., Zavodtsev, Y.V. and Chyzhov Y.V.(2016), “Osnovы dlia prohrammno-apparatnoi zashchytы ynformatsyy : ucheb. posobye dlia vuzov” / M. : LENAND, 416 p.

11. Vasyleva, Y.Y. (2017),_”Kryptohrafycheskye metodы zashchytы ynformatsyy : praktykum y uchebnyk dlia akadem. Bakalavryata” / M. : Yurait, 349 p.

12. Nesterov, S.A. (2017), “Osnovы ynformatsyonnoi bezopasnosty : uchebnyk” / SPb. : Lan, 423 p.

PhD Dzhuliy V.M., PhD Miroshnichenko O.V., Solodeeva L.V.

METHOD OF CLASSIFICATION OF APPLICATIONS TRAFFIC OF COMPUTER NETWORKS ON THE BASIS OF MACHINE LEARNING UNDER UNCERTAINTY

The paper proposes a method for classifying applications of computer network traffic based on machine learning in conditions of uncertainty. Modern methods of classification of computer network traffic applications (such as the classification of transport layer protocols by port numbers) have significant shortcomings, which leads to and is the reason for the growth of research in the direction of classification of computer network traffic applications. The rapid growth in recent years of the types and number of transport layer network protocols increases the relevance of research in this area, the development of appropriate algorithms and methods for classifying applications of computer network traffic, which reduce computational complexity. At the present stage, the problem that needs to be urgently addressed is the classification of computer network traffic applications using appropriate protocols and encryption algorithms.

A promising area of classification of computer network traffic applications is statistical methods, which are based on the analysis and identification of statistical characteristics of IP traffic. The most promising are the intellectual analysis of data flow, as well as machine learning technologies, which are currently widely used in related fields of science. The problem of research and training according to precedents is solved - classification of computer network traffic applications on the basis of pre-known set of attributes of their features, in order to improve the technical base of computer networks and theoretical base, while ensuring high performance and quality networks. example of using transport layer protocols (TCP / IP stack). The result of solving this problem is to assign the application, in accordance with the rules of the educational sample, to one of the outstanding classes, which are predetermined, which contains the relevant, but already classified applications. Statistical analysis and research of the attributes of Internet applications showed that the most important attributes associated with changes in the volume of Internet traffic flow are exponential. Fisher's criterion can be used to calculate anomalous changes in the amount of Internet traffic of applications to calculate averages.

To classify Internet applications in data streaming mode, an algorithm for detecting the offset of the concept (drift) of data flow traffic is proposed for continuous data flow. Fisher's drift detector is based on the statistical characteristics of the attributes of Internet applications, analyzed using sliding windows that monitor changes in traffic current statistical characteristics of the attributes of applications.

Key words: models, application classification, computer networks, drift, traffic, sliding window, machine learning.

УДК 355+004.65

к.т.н., с.н.с. **Литвиненко Н.І.** (ВІКНУ)
к.геогр.н. **Коренець О.В.** (ВІКНУ)
к.військ.н., с.н.с. **Федченко О.П.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-08

ПРИНЦИПИ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ ЄДИНОГО ГЕОІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ЗБРОЙНИХ СИЛ УКРАЇНИ

У ході проведення досліджень з метою забезпечення наведених у даній статті загальних вимог до геоінформаційного забезпечення Єдиної автоматизованої системи управління Збройними Силами України (ЄАСУ ЗСУ) були обґрунтовані технічні рішення з питань створення та функціонування єдиної технології підготовки і використання просторових даних. Фундаментом єдиного геоінформаційного середовища ЗСУ повинна бути сервісно-орієнтована архітектура (СОА) розподілених баз геоданих. Метою розгортання сервісно-орієнтовані архітектури є забезпечення єдиної форми управління інформаційними ресурсами ЗСУ. Розгортання сервісно-орієнтованої архітектури дозволяє створити єдиний інтерфейс для внутрішніх користувачів, що використовують як внутрішні дані, які зберігаються у внутрішній (локальній) базі даних, так і зовнішні дані, надані іншими постачальниками. Дана модель організації даних з точки зору її архітектурної побудови може бути представлена у вигляді взаємозв'язаної сукупності моделей чотирьох рівнів (рівень метаописів сервісів і авторизації користувачів різних категорій; рівень функціональних веб-сервісів і порталів доступу; рівень інтеграції з успадкованими додатками, базами даних і сервісами; рівень технологій реінжинірингу і розвитку інформаційної системи).

Єдиний геоінформаційний простір ЄАСУ ЗСУ має утворюватися як середовище (мережа) взаємопов'язаних геопорталів, призначення яких полягає в консолідації інформації щодо наявних у ЄАСУ ЗСУ просторових даних, які оформлюються і надаються для використання у вигляді геосервісів, а також створенні єдиної точки входу користувачів у дане середовище. Визначено, що у якості програмної складової оптимально застосовувати серверне програмне багатокористувацьке забезпечення ArcGIS компанії ESRI з рівнем продуктивності Enterprise та класом функціональності Advanced.

Ключові слова: геоінформаційне забезпечення, сервісно-орієнтована архітектура (СОА), геопросторові дані, геопортал.

Вступ та постановка проблеми. На сьогоднішній день у Збройних Силах України впроваджено ряд інформаційно-аналітичних систем, що вирішують задачі автоматизації процесів мобілізаційного розгортання, оборонного планування, логістичного, кадрового, фінансового забезпечення, і всі вони мають бути інтегровані в Єдину автоматизовану систему управління (ЄАСУ). Інформація в таких інформаційно-аналітичних системах обробляється на всіх рівнях управління згідно правил і алгоритмів, розроблених в цих системах. У вирішенні даної задачі одну з ключових ролей може виконати геоінформаційне забезпечення як інструмент аналізу оперативної обстановки та засіб автоматизації процесу прийняття управлінських рішень посадовими особами органів військового управління. Таким чином, геоінформаційна складова ЄАСУ ЗСУ має забезпечувати інтероперабельність з існуючими в ЗСУ інформаційно-аналітичними системами та тими, що плануються з використанням інших технічних та програмних засобів.

Аналіз останніх досліджень та публікацій. Висвітленню методики створення та функціонування сервісно-орієнтованої архітектури організації даних та можливостям її використання для створення ГІС-додатків присвячені роботи [1-3]. В роботі [4] були визначені особливості концептуальної архітектури ГІС-платформи військового призначення на основі аналізу провідних підходів до проектування. Огляд різних напрямів та прикладів використання геоінформаційних технологій у військовій справі [5-7], а також актуальність розроблення автоматизованих геоінформаційних підсиситем управління військами [8,9] зумовлюють необхідність наукового обгрунтування технічних рішень з питань створення та

функціонування єдиної технології підготовки і використання просторових даних для геоінформаційних підсистем ЄАСУ ЗСУ.

Метою даної статті є визначення принципів створення та функціонування єдиного геоінформаційного середовища Збройних Сил України, що передбачає виконання наступних завдань:

– визначення основних вимог до геоінформаційного забезпечення як складової єдиної автоматизованої системи управління ЗСУ;

– характеристика оптимальної моделі організації просторових даних ЄАСУ ЗСУ;

– обґрунтування необхідності впровадження геоінформаційного порталу Збройних Сил України та визначення його структури та особливостей функціонування.

Виклад основного матеріалу дослідження. Геоінформаційне забезпечення як одна зі складових загального інформаційного забезпечення процесу управління підготовкою та застосуванням Збройних Сил України повинне забезпечувати наступне:

– формування єдиного інформаційного простору в межах театру воєнних дій військ (сил);

– відображення оперативної обстановки на картографічному фоні з використанням умовних знаків у відповідності із затвердженим Класифікатором, прийнятим у Збройних Силах України;

– генералізацію (масштабування) картографічної інформації в залежності від завдань, що вирішуються;

– постачання картографічних даних для забезпечення постановки завдань щодо реалізації рішень командирів всіх рівнів ієрархії підпорядкованості;

– обробку координатної та растрової (космічні знімки, аеро-,фото-) інформації від всіх видів розвідки;

– поєднання просторово-розподіленої інформації з інформацією з тематичних баз даних, довідковою та іншою інформацією;

– надання технологій для автоматизованого аналізу оперативної обстановки з метою отримання вихідних даних для виявлення загроз та прогнозування їх розвитку, проведення моделювання і надання рекомендацій командирам відповідних рівнів;

– геоінформаційну підтримку автоматизованого вирішення завдань щодо видів оперативного забезпечення Збройних Сил України (комплекси розрахункових задач);

– забезпечення автоматизованого видання бойових графічних документів;

– забезпечення сумісності автоматизованих систем та засобів автоматизації ЄАСУ ЗСУ в частині просторово розподіленої інформації з іншими подібними системами за умов виконання завдань у складі коаліції військ (сил).

Виходячи з основних завдань, геоінформаційне забезпечення являє собою сучасну просторово-розподілену підсистему загальносистемного інформаційного забезпечення ЄАСУ ЗСУ, яка здатна обробляти просторові дані сумісно з іншою інформацією, що циркулює в ЄАСУ ЗСУ. Крім того, побудова геоінформаційного забезпечення повинна відповідати сучасним вимогам щодо апаратної та програмної уніфікації, надання професійного зручного і зрозумілого інтерфейсу користувача, відповідати вимогам щодо роботи окремих елементів в режимі реального часу, ґрунтуватися на архітектурі та технологіях, що дозволяють досягнути інтероперабельності по відношенню до інших підсистем ЄАСУ ЗСУ.

Фундаментом єдиного геоінформаційного середовища ЗСУ повинна бути сервісно-орієнтована архітектура (СОА) розподілених баз геоданих. Мета розгортання сервісно-орієнтованої архітектури – забезпечення єдиної форми управління інформаційними ресурсами ЗСУ. Вона дозволяє організувати ці ресурси так, щоб постійно задовольняти потреби здійснення геоінформаціного забезпечення ЗСУ, що постійно розвиваються. Керівна роль СОА в тому, що вона надає загальну для всіх суб'єктів і користувачів платформу для доступу до ресурсів ЄАСУ ЗСУ. У випадку застосування гнучких методів проектування перехід на СОА має здійснюватися шляхом одного або декількох пілотних проектів. Розгортання сервісно-орієнтованої архітектури (СОА) дозволяє створити єдиний інтерфейс для внутрішніх

користувачів, що використовують як внутрішні дані, які зберігаються у внутрішній (локальній) базі даних, так і зовнішні дані, надані іншими постачальниками. Сервісно-орієнтована архітектура і методи проектування баз геоданих створюють фундамент для взаємосумісності даних та систем.

Дана модель організації просторових даних виходить за рамки редагування однієї бази геоданих шляхом створення децентралізованої бази геоданих. Багато суб'єктів (користувачів) можуть публікувати свої дані і реєструвати їх для пошуку та використання будь-якою кількістю віддалених користувачів. Ті, у свою чергу, можуть або завантажувати до себе набір даних цілком, або використовувати картографічні WEB-служби (WMS) для динамічної вибірки і загрузки невеликої частини даних, що є необхідними у їх поточному екстенті карти. Процес асинхронного редагування і публікації може бути розширеним для підтримки процесу розповсюдження даних відповідно до підписки, коли кожний користувач може звертатися до оновлених даних тільки тоді, коли вони йому потрібні [3].

До складу базових засобів ГІС ЄАСУ ЗСУ мають входити серверні компоненти, які спеціально призначені для підтримки СОА (як інструментальні, так і засоби підтримки функціонування СОА). ГІС-сервіси дають можливість використовувати ресурси ГІС ЄАСУ ЗСУ через різні додатки клієнтів: настільні програмні комплекси, картографічні WEB-додатки і мобільні пристрої. В залежності від типу ресурсу, що публікується, конфігуруються відповідні базові сервіси. Після публікації сервіси реєструються на ГІС- сервері, а їх метадані заносяться у каталоги.

Референтна модель ГІС ЄАСУ ЗСУ, яка підтримує об'єднання інформації з різних джерел, що мають різне походження, різну структуру і, можливо, різне місцезнаходження, з точки зору, її архітектурної побудови може бути представлена у вигляді взаємозв'язаної сукупності моделей наступних рівнів:

– рівень метаописів сервісів і авторизації користувачів різних категорій;

– рівень функціональних веб-сервісів і порталів доступу;

– рівень інтеграції з успадкованими додатками, базами даних і сервісами;

– рівень технологій реінжинірингу і розвитку інформаційної системи.

Організація прикладних систем з сервіс-орієнтованою архітектурою на базі Web-служб припускає створення і використання Web-сервісів, що визначають функціональність послуг, що надаються додатками. При цьому Web-сервіс виступає як об'єкт, що реалізує один або декілька методів, до яких можна звертатися засобами Web з будь-якого додатку.

Технологія Web-служб ГІС ЄАСУ ЗСУ має базуватися на трьох основних специфікаціях, що мають статус Web-стандартів:

– SOAP (Simple Object Access Protocol) – протокол, що визначає правила взаємодії з віддаленими об'єктами за Internet-протоколами, зокрема, за протоколом http;

– WSDL (Web Services Description Language) – мова опису програмних інтерфейсів для Web-служб;

– UDDI (Universal Description, Discovery and Integration) – служба довідника для реєстрації Web-послуг (сервісів).

Для створення єдиного геоінформаційного середовища для ЄАСУ ЗСУ найбільш оптимальним шляхом є впровадження геоінформаційного порталу Збройних Сил України (далі – геопортал), у якості програмної, інформаційно-комунікаційної платформи, призначеної для створення єдиного геоінформаційного та інформаційно-аналітичного середовища органів військового управління, військових частин та підрозділів Збройних Сил України з розмежуванням прав доступу користувачів до цих ресурсів. На рис. 1 представлена інфраструктура геопросторових даних ГІС ЄАСУ ЗСУ у вигляді мережі геопорталів.

Геопортал як комплекс програмно-технічних засобів, мережевих сервісів та сервісів геопросторових даних, що забезпечують відображення в мережі геопросторових даних, повинен виконувати наступні основні завдання:

–оброблення та видача інформації на автоматизовані робочі місця (далі АРМ) посадових осіб органів військового управління (військових частин);

–надання доступу до єдиного геоінформаційного простору посадовим особам органів військового управління (військових частин, підрозділів);

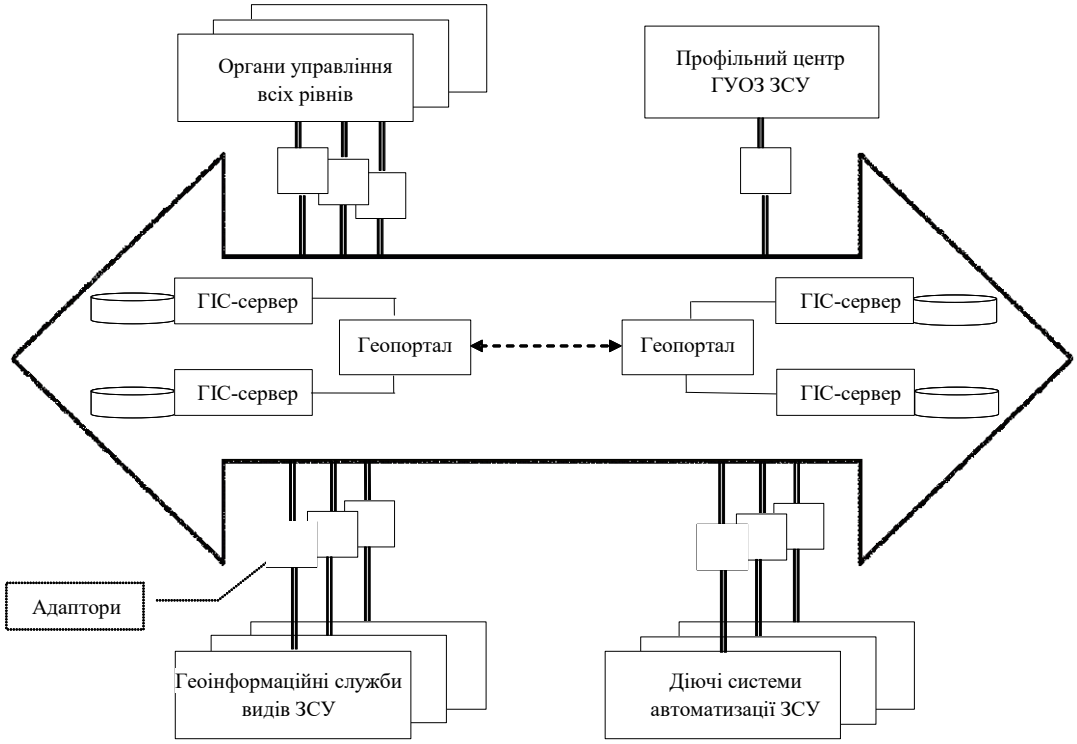

Рисунок 1 - Інфраструктура геопросторових даних ГІС ЄАСУ ЗСУ (мережа геопорталів)

–забезпечення взаємодії з іншими військовими формуваннями та правоохоронними органами України в рамках єдиного геоінформаційного простору;

–забезпечення пошуку/доступу до необхідної інформації.

Геопортал повинен мати наступний базовий набір картографічних сервісів:

1) картографічний сервіс електронних (цифрових) карт - мультимасштабний картографічний сервіс, який містить векторну інформацію всього масштабного ряду топографічних та оглядово-географічних карт;

2) картографічний сервіс електронних (цифрових) карт у тривимірному відображенні - копія картографічного сервісу електронних (цифрових) карт з можливістю візуалізації геоінформаційної інформації у тривимірному відображенні;

3) картографічний сервіс матеріалів дистанційного зондування Землі (ДЗЗ) – сервіс, який містить матеріали ДЗЗ (аерофотознімання, космічне знімання та знімання з БПЛА) та дозволяє оперативно створювати фотодокументи про місцевість;

4) картографічний сервіс дистанційного зондування Землі у тривимірному відображенні;

5) картографічний сервіс для завантаження растрових карт - картографічний сервіс дозволяє завантажити на АРМ топографічні карти всього масштабного ряду в растрових форматах з можливістю їх подальшого друку (розмноження).

У якості програмної складової оптимально застосовувати серверне програмне багатокористувацьке забезпечення ArcGIS компанії ESRI з рівнем продуктивності Enterprise та класом функціональності Advanced. Для забезпечення безперервної роботи програмно-технічних засобів та сервісів геопорталу, недопущення втрати даних необхідне розгортання відмовостійкої конфігурації за архітектурою «active-passive», де основний «active» ГІС-сервер

(сайт) розміщується в картографічному центрі Командування сил підтримки ЗСУ, а резервний «passive» ГІС-сервер (сайт) розміщується в Головному інформаційно-комунікаційному вузлі ГШ ЗСУ. Кожен з них має власні локальні сховища конфігурацій і серверні директорії та здійснює їх резервне копіювання. В разі програмних чи технічних збоїв на основному ГІС-сервері резервний «passive» ГІС-сервер автоматично приймає функції «active» до відновлення працездатності основного. Завдяки зазначеному принципу забезпечується триступеневий рівень збереження сервісів і даних.

Користувачі геопросторових даних Збройних Сил (штаби органів управління, геоінформаційні підсистеми АСУ тощо) здійснюють запит, отримують доступ до ресурсів і сервісів геопортала через Головний інформаційно-комунікаційний вузол ГШ ЗСУ. Збір, обробка та публікація геопросторових даних, отриманих від підрозділів топографічної служби, а також із зовнішніх джерел (Держгеокадастр, Державне космічне агентство тощо) здійснюється в картографічному центрі. Загальну схему організації відмовостійкого геопорталу ЗСУ показано на рис. 2.

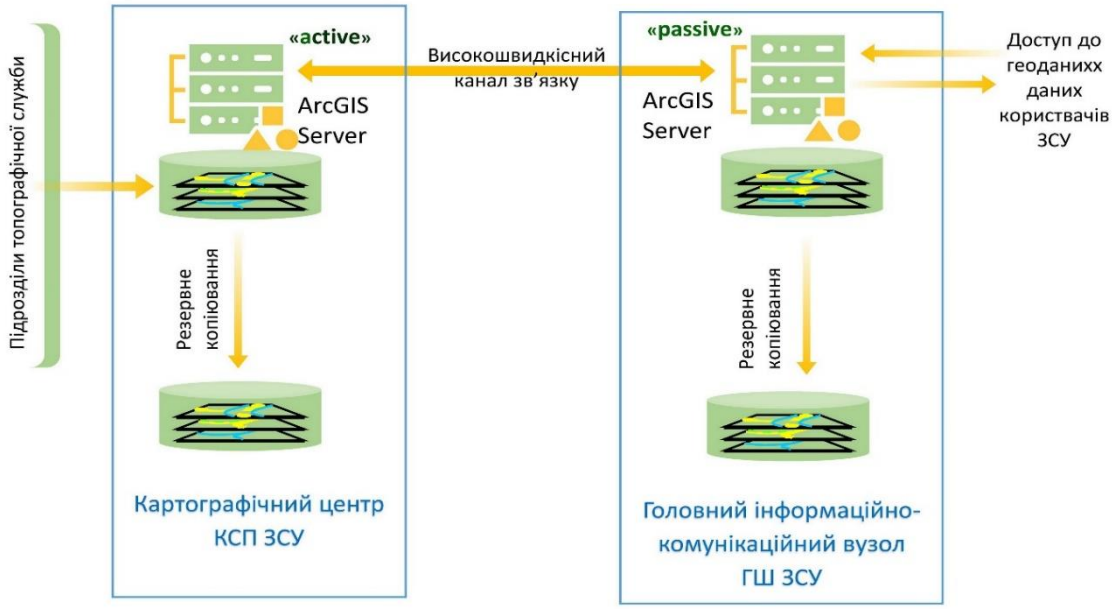

Рисунок 2 - Загальна схема організації відмовостійкого геопорталу ЗСУ

Висновки. Висвітлені в статті принципи створення єдиного геоінформаційного середовища для ЄАСУ ЗСУ, що ґрунтуються на основних завданнях геоінформаційного забезпечення ЗСУ та технологічних моделях організації просторової інформації, є важливим компонентом інтеграції всіх інших технології, які використовуються або плануються до впровадження в складі ЄАСУ ЗСУ для вирішення різноманітних задач з питань управління військами.

Подальші дослідження мають стосуватися аспектів практичної реалізації визначених принципів шляхом створення геоінформаційного порталу Збройних Сил України як основної платформи створення, зберігання і поширення просторових даних.

ЛІТЕРАТУРА:

1. Уэстерман Дж. Сервис-ориентированная архитектура сегодня: введение в SOA (SOA Today: Introduction to Service-Oriented Architecture).[Електронний ресурс]. Режим доступу: https://2dice.ru/hematoma/soa-arhitekturnye-osobennosti-i-prakticheskie-aspekty-servis-orientirovannaya-arhitektura.html.

2. Финкельштейн К. Корпорация: сервис-ориентированная архитектура (The Enterprise: Service-Oriented Architecture (SOA)). [Електронний ресурс]. Режим доступу: http://iso.ru/ru/press-center/journal/2046.phtml

3. Geospatial Service-Oriented Architecture (SOA). Esri. [Electronicresource]. Modeofaccess: https://proceedings.esri.com/library/userconf/devsummit06/papers/soa_solutions.pdf.

4. Федорієнко В.А., Головченко О.В., Васюхно С.І. Особливості сучасної концептуальної архітектури ГІС платформи військового призначення. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2017. № 2(60). С. 86-92.

5. Федченко О.П., Литвиненко Н.І., Литвиненко О.І., Прищепа С.В. Аналіз використання геоінформаційних технологій в управлінні Збройними Силами України. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ, 2021. № 72. С. 73-80.

6. Лукіянчук А., Халіманенко С. Геоінформаційні системи військового призначення. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. Київ, 2021. Вип. 4 (48). С. 70-73.

7. Беленков В.В., Корж М.М. Основные направления применения геоинформационных технологий в военном деле.Международный научно-технический журнал "Информационные технологии и компьютерная инженерия". Москва, 2006. №3(7). [Електронний ресурс]. Режим доступу: http://gisinfo.ru/item/41.htm.

8. Литвиненко Н.В., Коренець О.В. Актуальність розроблення та впровадження автоматизованих геоінформаційних підсистем управління військами. Збірник тез доповідей Міжнародної науково-технічної конференції "Перспективи розвитку озброєння та військової техніки Сухопутних військ" (м. Львів, 14 травня 2021 р.). Львів, 2021. С. 230.

9. Мясіщев О., Литвиненко Н., Федченко О. Доцільність використання геоінформаційних підсистем у складі Автоматизованої системи управління Збройних Сил України. DIGITAL REALITY: матеріали міжнародного наук.-практ. форуму (м. Одеса, 13-19 вересня 2021 р.). Одеса, 2021. С. 265-271.

REFERENCES:

1. Westerman, J. (2014), "Servis-orientirovannaya arhitektura segodnya: vvedenie v SOA" [SOA Today: Introduction to Service-Oriented Architecture], https://2dice.ru/hematoma/soa-arhitekturnye-osobennosti-i-prakticheskie-aspekty-servis-orientirovannaya-arhitektura.html.

2. Finkelstein, C. (2005), " Korporaciya: servis-orientirovannaya arhitektura " [The Enterprise: Service-Oriented Architecture (SOA)], http://iso.ru/ru/press-center/journal/2046.phtml.

3. Geospatial Service-Oriented Architecture (SOA). (2018), Esri, https://proceedings.esri.com/ library/userconf/devsummit06/papers/soa_solutions.pdf.

4. Fedoriienko, V.A., Holovchenko, O.V., Vasiukhno, S.I. (2017), "Osoblyvosti suchasnoi kontseptualnoi arkhitektury GIS platformy viiskovoho pryznachennia"[Features of modern conceptual architecture of GIS military platform], Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho, № 2(60), pp. 86-92.

5. Fedchenko, O.P., Lytvynenko, N.I., Lytvynenko, O.I., Pryshchepa, S.V. (2021), "Analiz vykorystannia heoinformatsiinykh tekhnolohii v upravlinni Zbroinymy Sylamy Ukrainy" [Analysis of the use of geographic information technologies in the management of the Armed Forces of Ukraine], Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, № 72, pp. 73-80.

6. Lukiianchuk, A., Khalimanenko, S. (2021) "Heoinformatsiini systemy viiskovoho pryznachennia" [Geographic information systems for military purposes], Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky, №4 (48), pp. 70-73.

7. Belenkov, V.V., Korzh, M.M. (2006), "Osnovnye napravleniya primeneniya geoinformacionnyh tekhnologij v voennom dele" [The main directions of application of geoinformation technologies in military affairs], Mezhdunarodnyj nauchno-tekhnicheskij zhurnal "Informacionnye tekhnologii i komp'yuternaya inzheneriya", №3(7), http://gisinfo.ru/item/41.htm.

8. Lytvynenko, N.I., Korenets, O.V. (2021), "Aktualnist rozroblennia ta vprovadzhennia avtomatyzovanykh heoinformatsiinykh pidsystem upravlinnia viiskamy" [Relevance of development and implementation of automated geographic information subsystems of military management], Zbirnyk tez dopovidei Mizhnarodnoi naukovo-tekhnichnoi konferentsii "Perspektyvy rozvytku ozbroiennia ta viiskovoi tekhniky Sukhoputnykh viisk" (m. Lviv, 14 travnia 2021 r.), p. 230.

9. Miasishchev, O., Lytvynenko, N., Fedchenko, O. (2021), "Dotsilnist vykorystannia heoinformatsiinykh pidsystem u skladi Avtomatyzovanoi systemy upravlinnia Zbroinykh Syl Ukrainy"

[Expediency of using geoinformation subsystems as a part of the Automated control system of the Armed Forces of Ukraine], DIGITAL REALITY: materialy mizhnarodnoho nauk.-prakt. forumu (m. Odesa, 13-19 veresnia 2021 r.), pp. 265-271.

PhD Lytvynenko, N.I., PhD Korenets O.V., PhD Fedchenko O.P.

PRINCIPLES OF CREATION AND FUNCTIONING OF THE UNIFIED GEOINFORMATION ENVIRONMENT OF THE ARMED FORCES OF UKRAINE

In the course of research to ensure the general requirements for geographic information support of the Unified automated control system of the Armed Forces of Ukraine (UACS of the Armed Forces of Ukraine), technical decisions on the establishment and operation of a technology for preparation and use of spatial data were substantiated. The foundation of the unified geoinformation environment of the Armed Forces should be service-oriented architecture (SOA) of distributed geodatabases. The purpose of deploying service-oriented architectures is to provide a single form of information resources management of the Armed Forces. Deploying a service-oriented architecture allows to create a single interface for internal users, who use both internal data stored in the internal (local) database and external data provided by other vendors. This model of data organization in terms of its architectural construction can be represented as an interconnected set of four levels models (the level of meta descriptions of services and authorizations of different categories users; the level of functional web services and access portals;the level of integration with legacy applications, databases and services, the level of technology reengineering and information system development).

The geoinformation space of the UACS of the Armed Forces of Ukraine should be formed as an environment (network) of interconnected geoportals, the purpose of that is to consolidate information on available spatial data in the UACS of the Armed Forces of Ukraine environment. It's determined that it's optimal to use ESRI's ArcGIS server multi-user software with Enterprise performance level and Advanced functionality class as a software component.

Keywords: geoinformation support, service-oriented architecture (SOA), geospatial data, geoportal.

УДК 004.92

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Грищак О.М.** (НУОУ)
к.т.н., с.н.с. **Жиров Г.Б.** (КНУ)
к.т.н., доц. **Пампуха І.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-09

ОЦІНКА "ПРАКТИЧНОСТІ" ТА "КОРЕКТНОСТІ" СПЕЦІАЛЬНОГО ПРОГРМАНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ВОЄННОГО ПРИЗНАЧЕННЯ

В статті проведено оцінка "практичності" та "коректності" спеціального програмного забезпечення автоматизованих інформаційних систем воєнного призначення. Показано, що інформаційний ресурс високоточної зброї повинний мати повний набір програмних засобів як активного і пасивного захисту від атак на його інформаційні системи, так і його активних і пасивних впливів стосовно всіх існуючих і перспективних систем озброєння противника. Серед проблем, що пов'язані із створенням спеціального програмного забезпечення (СПЗ) автоматизованих інформаційних систем воєнного призначення, можливо виділити дві основні: проблема створення якісного спеціального програмного забезпечення; проблема раціоналізації ефективності праці учасників життєвого циклу СПЗ. Одним з перспективних напрямків їх вирішення є реалізація регламентованого технологічного процесу. Системний полягає в скороченні помилок у програмному забезпеченні шляхом їх своєчасного виявлення та локалізації, зменшення трудомісткості їх виявлення та виправлення за рахунок чітких і упорядкованих структури та зв'язків.

Характеристикою практичності СПЗ є вивчаємість, що характеризується (зусиллями, необхідними для освоєння користувачами умов, процедур і правил застосування ПЗ). Вони описуються наступними показниками: середній час освоєння програмного виробу обслуговуючим персоналом, коефіцієнт повноти демонстраційної версії, коефіцієнт повноти та гнучкості довідкової системи.

Характеристика зручність експлуатації та коректність СПЗ характеризується легкістю підготовки вхідних даних і запуску в роботу СПЗ. Кількісна оцінка характеризується такими показниками: коефіцієнт ступеню автоматизації контролю вводу даних, коефіцієнт використання ефективних засобів введення даних. Оцінювання необхідних інтелектуальних зусиль для створення програми характеризується кількістю необхідних елементарних рішень при створення програмного коду, однак він не враховує дії по відлагодженню програми, тому автори пропонують ввести коефіцієнт реальної складності, що полягає в оцінці витрат на сприйняття готової програми. Наведені метрики дозволяють отримати їх чисельні значення, на основі яких можливо порівнювати програми за цими характеристиками якості.

Ключові слова: спеціальне програмне забезпечення, автоматизовані інформаційні системи, оцінка практичності та коректності, адекватність та достовірність рівня якості програмування.

Вступ та постановка задачі. Сьогодні спостерігається значний зріст науково-технічних досліджень в напрямку інформатизації і автоматизації управління військами і зброєю. На прикладі розвитку Збройних сил провідних країн світу треба очікувати автоматизації всіх рівнів їх організаційних структур. Нажаль в Україні у перехідний період інформаційно-аналітичне забезпечення поки що зберігається як один з видів забезпечення всіх інших видів боротьби. Вже після завершення перехідного періоду, інформаційно-аналітичне забезпечення поступове вийде за межі виду, що забезпечує, і стане бойовим, тобто придбає самостійний характер серед багатьох інших форм і способів забезпечення військ (сил) головним чином буде досягатися через перевагу в одержанні достовірної інформації, мобільності, швидкості реакції, у точному вогневому й інформаційному впливі в реальному масштабі часу по численних об'єктах його економіки, військових об'єктах стратегічних та тактичних діях і при мінімально можливому ризику для своїх сил і засобів.

При цьому буде потрібна максимальна інтеграція механізмів обробки і аналізу інформації багатофункціональних ударних і оборонних систем на основі автоматичних пристроїв управління та за рахунок значного зниження кількості рівнів управління військами, силами, засобами. Також буде потрібна надійна захищеність як окремих ударних і оборонних елементів високоточних систем, так і стратегічної системи в цілому від впливу всіх видів сучасного інформаційного впливу.

Інформаційний ресурс високоточної зброї повинний мати повний набір програмних засобів як активного і пасивного захисту від атак на його інформаційні системи, так і його активних і пасивних впливів стосовно всіх існуючих і перспективних систем озброєння противника.

Серед проблем, що пов‘язані із створенням спеціального програмного забезпечення (СПЗ) автоматизованих інформаційних систем воєнного призначення, можливо виділити дві основні:

- проблема створення якісного спеціального програмного забезпечення;
- проблема раціоналізації ефективності праці учасників життєвого циклу СПЗ;

Одним з перспективних напрямків їх вирішення є реалізація детально регламентованого технологічного процесу. При цьому необхідний рівень регламентації може бути досягнутий в результаті системного підходу до забезпечення заданих характеристик якості СПЗ на різних стадіях життєвого циклу програмного забезпечення. Суть системного підходу відповідно до забезпечення цільової якості СПЗ полягає в скороченні помилок у програмному забезпеченні шляхом їх своєчасного виявлення та локалізації, зменшення трудомісткості їх виявлення та виправлення за рахунок чітких і упорядкованих структури та зв‘язків.

Значної частини труднощів, що виникають при розробці та впровадженні СПЗ воєнного призначення, можливо уникнути, якщо з самого початку створити систему спеціального програмного забезпечення у відповідності з певною методологією. Ця методологія повинна враховувати безперервність процесів розробки та впровадження, статичність цілей розробника, динамічність вимог замовника, необхідність забезпечення високої надійності та точності функціонування, зручності експлуатації та гнучкості системи при зміні нормативних даних та інформаційних масивів.

Крім критичності СПЗ ВП в плані правильного, надійного та стійкого функціонування, витрати на доробку вже діючих програм та усунення помилок, що виявляються в процесі використання, досягають іноді 75% загальної суми експлуатаційних витрат, [1,2]. За іншими даними [1, 3] на це витрачається від 30 до 50% загального бюджету розробки, а помилки, що не виявлені на початку життєвого циклу, коштують від 70 до 85% вартості переробки.

Як показано на рис. 1, набагато дорожче виправити помилки, які знайдено пізніше в проекті [3].

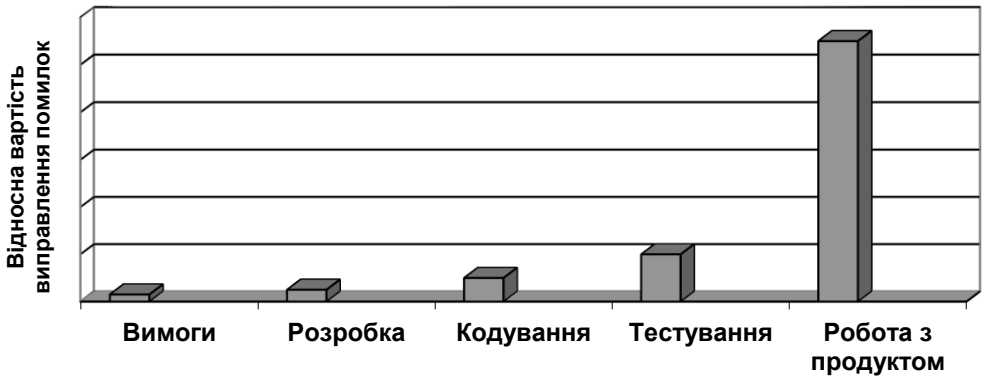

Рисунок 1 – Відносна вартість виправлення помилок в залежності від етапу, на якому вони виявлені

У 1994 році Консалтингова група фірми IBM провела дослідження стану справ у 24 провідних компаніях США, що розробляють великі програмні системи. В її звіті [4] як і у статті [5] зазначалося, що:

- у 55% проектів перевищено заплановану вартість розробки;
- у 68% проектів порушено договірні строки розробки;
- 88% проектів довелось суттєво переробляти.

Аналогічні дослідження були проведені Standish Group у 1994 році по 8380 програмним проектам, що розроблялись у державному та приватному секторах США. Ці дослідження [6], а також аналіз вітчизняних досліджень [7] показують, що:

- 31% всіх програмних проектів закриваються до їх повного закінчення;
- 53% успішно закінчених проектів в середньому на 18% перевищують заплановану вартість;
- з цих 53% проектів тільки 42% забезпечують в програмних продуктах всі властивості та функції, що планувалися;
- тільки 9% проектів закінчується у встановлений термін і не перевищують заплановані для проекту кошти.

В своїх дослідженнях Standish Group виділяє наступні критерії успішності виконання проектів у розглянутій області:

Таблиця 1

№	**Критерій успіху**	**Ступінь важливості**
1.	Участь користувачів у проекті	19%
2.	Належне управління на виконавчому рівні	16%
3.	Ясні вимоги до розроблювального продукту	15%
4.	Кваліфіковане планування	11%
5.	Реалістичні очікування результатів	10%
6.	Більш частий контроль виконання етапів плану	9%
7.	Компетентність персоналу	8%
8.	Чіткий розподіл обов'язків і прав у команді виконавців	6%
9.	Чітка постановка цілей і їхня відповідність стратегічним задачам організації	3%
10.	Мотивація персоналу на напружену роботу	3%

Можна зробити висновок, що більшість перерахованих критеріїв відноситься до області управління проектами [8].

Тому в циклі робіт авторами вирішується важлива для теорії і практики діяльності Збройних Сил та держави в цілому наукова проблема розробки науково-методичних основ гарантування та оцінки цільової якості спеціального програмного забезпечення автоматизованих інформаційних систем воєнного призначення.

Складовими цієї проблеми є:

1. Створення системи гарантування цільової якості СПЗ.
2. Формалізація процесу оцінки якості СПЗ.
3. Розробка пропозицій щодо організаційно-штатної структури та алгоритму роботи підрозділу, який займається розробкою спеціального програмного забезпечення.

Мета даної статті. Оцінка "практичності" та "коректності" спеціального програмного забезпечення автоматизованих інформаційних систем воєнного призначення.

Основні результати дослідження. Зупинимось на основних поняттях кваліметрії та інженерії програмного забезпечення, якими будемо оперувати у подальшому. *Якість СПЗ* – це сукупність властивостей (атрибутів), що визначають його корисність для користувачів у відповідності з функціональним призначенням та висунутими вимогами. *Характеристика якості* – поняття, що відображає окремі чинники, які впливають на якість програм та є такими,

що можуть бути виміряні. *Критерій якості* – чисельний показник, що характеризує ступінь, в якій програмі властиві атрибути якості, що оцінюються. Критерій якості повинен відповідати таким вимогам: чисельно характеризувати основну цільову функцію програми; забезпечувати можливість визначення витрат, необхідних для досягнення потрібного рівня якості, а також ступеню впливу на показник якості різноманітних зовнішніх чинників; бути по можливості простим, добре вимірюватись та мати малу дисперсію. Для вимірювання характеристик і критеріїв якості СПЗ використовуються метрики. *Метрика якості* – це система оцінок якості СПЗ. Ці оцінки можуть здійснюватись на рівні критеріїв якості СПЗ, або на рівні окремих характеристик. При першому підході система оцінок дозволяє порівнювати програмне забезпечення за якістю безпосередньо. При цьому оцінки не можуть бути проведені без суб‘єктивних вимірів властивостей СПЗ. При другому підході оцінку характеристик СПЗ можливо здійснити об‘єктивно і достовірно, але оцінювання якості СПЗ в цілому буде пов‘язана із суб‘єктивною інтерпретацією отриманих оцінок.

Стандартами, які прийняті в області якості програмного забезпечення в Україні, характеристика якості програмного забезпечення *usability* перекладається як зручність чи простота використання. В той же час однією з її підхарактеристик є *зручність експлуатації та обслуговування, щ*о не є коректним з точки зору семантики поняття цієї характеристики. Пропонується використовувати поняття "практичність" як інтегральну характеристику більш високого рівня ієрархії ніж "зручність". Під практичністю СПЗ будемо розуміти його здатність бути зрозумілим, вивчаємим, зручним в експлуатації та обслуговуванні при використанні в заданих умовах. Однією з підхарактеристик практичності є *зрозумілість* СПЗ – його здатність надавати можливість користувачу зрозуміти, чи підходить йому даний програмний продукт, і як його застосовувати для конкретних завдань і умов використання.

Як найбільш просту метрику зрозумілості СПЗ пропонується використовувати оцінку рівня коментованості програми, L_{com}:

$$L_{com} = \frac{N_{com}}{N_{line}}, \tag{1}$$

де – N_{com} - кількість коментарів в програмі;

N_{line} - загальна кількість рядків або операторів вихідного тексту програми.

Отже, метрика L_{com} відображає насиченість програми коментарями. Виходячи з практичного досвіду будемо вважати, що $L_{com} >= 0.1$, тобто на кожні десять рядків або операторів програми має бути мінімум один коментар. Але, як свідчить аналіз, дуже часто коментарі розподіляються у тексті програми нерівномірно: на початку програми спостерігається їх надлишок, а в середині чи в кінці – їх бракує. Це пояснюється, очевидно, тим, що на початку програми, як правило, розміщені оператори опису ідентифікаторів, які потребують більш ретельного коментування. Крім того, на початку програми також розташовані блоки з інформацією про виконавця, функціональне призначення програми та ін. Така насиченість компенсує брак коментарів у тілі програми і тому формула (1) недостатньо адекватно відображає коментованість функціональної частини тексту програми. Пропонується варіант, коли вся програма поділяється на n рівних сегментів і для кожного з них окремо визначається $L_{com}^{(i)}$:

$$L_{com}^{(i)} = sign(\frac{N_{com}^{(i)}}{N_{line}^{(i)}} - 0.09). \tag{2}$$

При цьому рівень коментованості всієї програми, L_{com} буде визначатись, як:

$$L_{com} = \sum_{i=1}^{n} L_{com}^{(i)}. \tag{3}$$

Виходячи з мінімально достатньої кількості коментарів відносно кількості рядків або операторів програми ($L_{com} >= 0.1$) мінімально достатній рівень коментованості програми будемо вважати досягнутим, якщо виконується умова $L_{com} = n$. В іншому випадку *i*-й фрагмент програми, для якого $L_{com}^{(i)} <0$, доповнюється коментарями до номінального рівня.

Наступною підхарактеристикою практичності СПЗ є вивчаємість. Стандартом [9] ця підхарактеристика практичності СПЗ характеризується "зусиллями, необхідними для освоєння користувачами умов, процедур і правил застосування ПЗ". Для її кількісної оцінки пропонуються наступні показники:

1. *Середній час освоєння програмного виробу* обслуговуючим персоналом, $\overline{T_{fam}}$ (статистичний показник). Мінімальне та максимальне значення цього показника повинно визначатись на етапі формулювання специфікацій на програмний продукт в процесі спілкування представників замовника та виконавця (можливо в формі тестування):

$$\overline{T_{fam}} = \frac{\sum_{i=1}^{n} T_i}{n}, \tag{4}$$

де – T_i - час освоєння програмного засобу *i*-м користувачем;

n - кількість користувачів, які вивчали правила користування програмним засобом.

2. *Коефіцієнт повноти демонстраційної версії* K_{DV}, який відображає повноту та детальність ілюстрації функцій СПЗ та об‘єктів, над якими вони виконується:

$$K_{DV} = \frac{\sum_{i=1}^{n} N_i^{(func)}}{n}, \tag{5}$$

де – $N_i^{(func)}$ - кількість функцій СПЗ, демонстрація виконання яких доступно і повно представлена у демоверсії;

n - загальна кількість функціональних блоків в СПЗ.

3. *Коефіцієнт повноти та гнучкості довідкової системи* K_{help}, одиничними показниками ступеню реалізації якого є такі:

наявність загальних відомостей про систему (0, 1);

можливість організації тематичного пошуку в загальній довідковій системі (0, 1);

можливість доступу при будь-якому режимі роботи до повної довідки за допомогою командної кнопки чи комбінації керуючих клавіш (0, 1);

використання контекстної довідки (0, 1);

варіанти роботи з даними довідки (друкування чи занесення в файл), (0, 1);

$$K_{help} = \frac{\sum_{i=1}^{5} N_i^{(index)}}{5}, \tag{6}$$

де – $N_i^{(index)}$ - одиничні показники ступеню реалізації повноти та гнучкості довідкової системи.

Підхарактеристика зручність експлуатації та обслуговування характеризується "легкістю підготовки вхідних даних і запуску в роботу ПЗ, а також необхідними умовами інтерфейсу користувача в процесі функціонування ПЗ" [9]. Для її кількісної оцінки пропонуються наступні показники:

1. Коефіцієнт ступеню автоматизації контролю вводу даних, K_{avtinp}:

$$K_{avtinp} = \frac{V_{avt}}{V}, \tag{7}$$

де – V_{avt} - обсяг початкових даних, під час введення яких здійснюється контроль їх правильності реалізованими у програмному виробі засобами;

V - загальний обсяг вхідних даних, які необхідно перевіряти.

2. Коефіцієнт використання ефективних засобів введення даних, K_{effinp}:

$$K_{effinp} = \frac{V_{eff}}{V_{inp}}, \tag{8}$$

де – V_{eff} - обсяг початкових даних, для вводу яких застосовуються автоматизовані засоби;

V_{inp} - загальний обсяг початкових даних, що вводиться.

Коректність СПЗ міжнародним стандартом ISO 9126-1 [10] трактується як спроможність програмного засобу забезпечувати правильні та прийнятні для користувача результати та зовнішні ефекти.

Наступні п‘ять характеристик базуються на метриці М.Холстеда V^*, за допомогою якої описується потенційний об‘єм коду, який відповідає максимально компактному тексту програми, що реалізує даний алгоритм [11]:

$$V^* = n^* \log_2(n^*). \tag{9}$$

Для оцінки теоретичної довжини програми, L_t М.Холстед вводить апроксимуючу формулу:

$$L_t = n_1 \log_2(n_1) + n_2 \log_2(n_2), \tag{10}$$

де n_1 – кількість унікальних операторів програми (словник операторів);

n_2 – кількість унікальних операндів програми (словник операндів).

Фізичний зміст цієї оцінки базується на основних концепціях теорії інформації, за аналогією з якими частота використання операторів та операндів в програмі пропорційна двійковому логарифму кількості їх типів. Вираз (10) являє собою ідеалізовану апроксимацію виразу (9), тобто справедливий для потенційно коректних програм, які не мають надмірності та недосконалостей (стилістичних помилок). М.Холстед [11] стверджує, що для стилістично коректних програм відхилення в оцінці теоретичної довжини L_t від реальної L не перевищує 10%. Пропонується застосовувати L_t як еталонне значення довжини програми із словником n. Вимірюючи n_1 (кількість унікальних операторів програми), n_2 (кількість унікальних операндів програми), N_1 (загальну кількість операторів у програмі) та N_2 (загальну кількість операндів у програмі) та порівнюючи L_t з L для певної програми, при більш, ніж 10%-вому відхиленні можливо зробити висновок про наявність в програмі стилістичних помилок, тобто недосконалостей.

В якості наступної оцінки, яка належить до метрик коректності СПЗ, згідно М.Холстеду, пропонується застосовувати коефіцієнт рівня якості програмування, K_{LQ} [12]:

$$K_{LQ} = \frac{V^*}{V}, \tag{11}$$

де – V^* - розраховується за формулою (9);

V - фактичний обсяг програми $V = N \log_2(n_1 + n_2)$ (біт).

Під бітом розуміється логічна одиниця інформації – символ, оператор, операнд.

Вихідною посилкою для введення цієї оцінки є припущення про те, що при зниженні стилістичної якості програмування зменшується змістовне навантаження на кожний компонент програми і, як наслідок, збільшується фактичний обсяг реалізації вихідного алгоритма. Враховуючи це, можливо оцінити якість програмування на основі ступеня

збільшення фактичного обсягу програми відносно потенційного V^*. Очевидно, що для ідеальної програми $K_{LQ} = 1$, а для реальної – завжди $K_{LQ} < 1$.

Для підвищення адекватності та достовірності коефіцієнту рівня якості програмування М.Холстед пропонує апроксимувати цю оцінку виразом, що включає тільки фактичні параметри, тобто параметри реальної програми: $\hat{K}_{LQ} = \frac{2n_2}{n_1 N_2}$. Доцільність цього пояснюється тим, що список параметрів програми може бути штучно розширений (оскільки залежить від рівня реалізації вихідного алгоритму), що, в свою чергу, веде до збільшення метрики рівня якості програмування. На основі $\hat{K}_{LQ}$ М.Холстед вводить характеристику I, яку трактує як інтелектуальний зміст конкретного алгоритма, інваріантний відносно мови реалізації:

$$I = \hat{K}_{LQ} V . \tag{12}$$

Перетворюючи (12) з урахуванням (11), отримаємо: $I = \hat{K}_{LQ} V = K_{LQ} V = \frac{V^* V}{V} = V^*$.

Еквівалентність I та V^* очевидно свідчить про те, що ми маємо справу з характеристикою інформативності програми. Введення характеристики I дозволяє оцінити розумові витрати на створення програми. Процес створення програми умовно можливо розділити на два етапи: осмислення алгоритму; перетворення алгоритму в терміни мови програмування, тобто пошук в словнику мови відповідної конструкції, її змістовне наповнення і запис. Використовуючи цю формалізацію в методиці М.Холстеда, можливо стверджувати, що написання програми у відповідності з відомим алгоритмом є L_t-кратна вибірка операторів і операндів із словника програми n, причому кількість порівнянь складе $\log_2(n)$. Якщо врахувати, що кожна вибірка-порівняння містить, в свою чергу, певну кількість розумових елементарних рішень, то можливо поставити у відповідність змістовному навантаженню кожної конструкції програми кількість та складність цих елементарних розумових рішень. Кількісно це можливо характеризувати за допомогою K_{LQ}, оскільки $1/K_{LQ}$ можливо використовувати як середній коефіцієнт складності, що впливає на швидкість вибірки для даної програми. За таких умов оцінювання необхідних інтелектуальних зусиль щодо створення програми, K_{int} може бути визначена наступним чином:

$$K_{\text{int}} = L_t \log_2\left(\frac{n}{K_{LQ}}\right). \tag{13}$$

Таким чином, K_{int} характеризує кількість необхідних елементарних рішень при створенні програмного коду. Але K_{int} адекватно характеризує тільки початкові зусилля по створенню програми, оскільки цей коефіцієнт не враховує дії щодо відлагодження програми, які потребують інтелектуальних зусиль іншого характеру. Тому пропонується ввести коефіцієнт реальної складності, K_{int}^{real}, фізичний зміст якого полягає в оцінці не інтелектуальних витрат на розробку програми, а витрат на сприйняття готової програми. При цьому замість теоретичної довжини програми L_t використовується її реальна довжина L:

$$K_{\text{int}}^{real} = L \log_2\left(\frac{n}{K_{LQ}}\right). \tag{14}$$

Перетворюючи формулу (13) з урахуванням виразів для V^* та V, отримаємо $K_{\text{int}} = \frac{V^2}{V^*}$.

Таке подання K_{int} наглядно ілюструє доцільність розбиття програми на окремі модулі,

оскільки інтелектуальні витрати виявляються пропорційними квадрату обсягу програми, який завжди більше суми квадратів обсягів окремих модулів.

Висновки. Таким чином, наведені метрики, які пропонується застосовувати для оцінки практичності та коректності СПЗ АІС ВП, дозволяють отримати їх чисельні значення, на основі яких можливо порівнювати програми за цими характеристиками якості. Крім того, розглянуті метрики базуються на аналізі вихідних текстів програм, що забезпечує єдиний підхід до автоматизації їх обчислення.

ЛІТЕРАТУРА

1. Boehm B.W., Philip N. Papaccio. Understanding and Controling Software Costs. IEEE Transactions on Software Engineering, №14(10), 1988, P. 1462-1476.

2. Черников Б.В., Поклонов Б.Е. Управление качеством программного обеспечения. Практикум. М.: НД «Форум», 2012, 240 с.

3. Grady R.B. An economic release decision model: insights into software project management // In proceedings of the applications of software measurement conference, Orange Park, Fl: Software Quality Engineering, 1999. - P. 227-239.

4. Barlas S. Anatomy of a Runaway: What Grounded the AAS // IEEE Software, January 1996. - P. 104-106.

5. Наумов А.И., Взоров В.Н. Концепция управления знаниями и практика компании. Вестник Московского университета. Серия 24. Менеджмент. – 2012. - №2 – С. 33 – 78.

6. Gibbs W. Software's Chronic Crisis // Scientific America, September 1994. - P. 86-95.

7. Основы инженерии качества программных систем / Ф.И. Андон, Г.И. Коваль, Г.М. Коротун, В.Ю. Суслов: НАН Украины, Институт программных систем. - К.: Академпериодика, 2002. - 503с.

8. Липаев В.В. Выбор и оценивание характеристик качества программых средств. Методы и стандарты. М.: СИНТЕГ, 2001, 228 с.

9. ДСТУ 2850-94 Програмні засоби ЕОМ. Показники і методи оцінювання якості

10. ISO/IEC 9126-1. 2001. Software engineering – Software product quality – Part 1: Quality model. Geneva, Switzerland: International Organization for Standardization;

11. Молодцова О.П. Управління якістю програмної продукції: Навч. посібник // Київський національний економічний університет. – К.: КНЕУ, 2001. – 248с.

12. Холстед М.Х. Начало науки о программах. – М.: Финансы и статистика, 1981. – 128с.

REFERENCES:

1. Boehm B.W., Philip N. Papaccio. Understanding and Controling Software Costs. IEEE Transactions on Software Engineering, №14(10), 1988, pp. 1462-1476.

2. Chernikov B.V., Poklonov B.E. (2012), Upravlenie kachestvom programmnogo obespechenija. Praktikum. Moskva.: ND «Forum», 240 p.

3. Grady R.B. An economic release decision model: insights into software project management // In proceedings of the applications of software measurement conference, Orange Park, Fl: Software Quality Engineering, 1999. P. 227-239.

4. Barlas S. Anatomy of a Runaway: What Grounded the AAS // IEEE Software, January 1996. - P. 104-106.

5. Naumov A.I., Vzorov V.N. (2012), Koncepcija upravlenija znanijami i praktika kompanii. Vestnik Moskovskogo universiteta. Serija 24. Menedzhment. №2, S. 33 – 78.

6. Gibbs W. Software's Chronic Crisis // Scientific America, September 1994. - P. 86-95;

7. F.I. Andon, G.I. Koval', G.M. Korotun, V.Ju. Suslov (2002), Osnovy inzhenerii kachestva programmnyh sistem / NAN Ukrainy, Institut programmnyh sistem. K.: Akademperiodika, 503s.

8. Lipaev V.V. (2001), Vybor i ocenivanie harakteristik kachestva programmyh sredstv. Metody i standarty. M.: SINTEG, 228 s.

9. DSTU 2850-94 Programni zasoby EOM. Pokaznyky i metody ocinjuvannja jakosti;

10. ISO/IEC 9126-1. 2001. Software engineering – Software product quality – Part 1: Quality model. Geneva, Switzerland: International Organization for Standardization;

11. Molodcova O.P. (2001), Upravlinnja jakistju programnoi' produkcii': Navch. posibnyk // Kyi'vs'kyj nacional'nyj ekonomichnyj universytet. – K.: KNEU, 248s.

12. Holsted M.H.(1981), Nachalo nauki o programmah. M.: Finansy i statistika, 128s.

D.Sci. Tech. Lienkov S.V., PhD Gryschak O., PhD Zhyrov G., Phd Pampukha I.

ASSESSMENT OF "PRACTICALITY" AND "CORRECTNESS" OF SPECIAL SOFTWARE OF AUTOMATED MILITARY INFORMATION SYSTEMS

The assessment of the "practicality" and "correctness" of special software of the automated military information systems is consider in the article. It's shown that the information resource of the high-precision weapons must have a full set of software as active and passive protection against attacks on its information systems, and its active and passive influences on all existing and promising weapons systems. Among the problems associated with the creation of special software (SS) of the automated information military systems, there are two main ones: the problem of creating high-quality special software; the problem of rationalizing the efficiency of the participants of the SS life cycle. One of the promising areas of their solution is the implementation of the regulated technological process. The systematic approach is to reduce software errors by detecting and locating them in the timely manner, reducing the complexity of detecting and correcting them through clear and orderly structures and connections.

A characteristic of the SS's practicality is the studied, that is characterized by efforts required for users to master the conditions, procedures and rules of application of the software. They are described by the following indicators: the average time of development of the software product by service personnel, the completeness coefficient of the demo version, the completeness and flexibility coefficient of the help system.

The characteristics of ease operation and correctness of SS is characterized by ease of preparation of input data and start-up of SS. The quantitative assessment is characterized by the following indicators: the coefficient of the degree of automation of data entry control, the coefficient of use of effective means of data entry. The estimating of the necessary intellectual effort to create a program is characterized by the number of necessary basic solutions when creating program code, but it doesn't take into account debugging actions, so the authors propose to introduce a factor of real complexity, that is to estimate the cost of program perception. The given metrics allow to receive their numerical values on the basis of that it's possible to compare programs on these quality characteristics.

Keywords: special software, automated information systems, assessment of practicality and correctness, adequacy and reliability of the programming quality level.

УДК 355/359.07

к.т.н. **Максименко Ю.А.** (ВА м. Одеса)
д.т.н., проф. **Скачков В.В.** (ВА м. Одеса)
д.н. з держ. упр., проф. **Попов С.А.** (ВА м. Одеса)
к.т.н., доц. **Маміч В.В.** (ВА м. Одеса)

DOI: https://doi.org/10.17721/2519-481X/2022/74-10

АНАЛІЗ ФАКТОРІВ, ЯКІ ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ РОБІТ ПОСАДОВИХ ОСІБ ОРГАНІВ УПРАВЛІННЯ РОЗВІДКОЮ ЩОДО ОРГАНІЗАЦІЇ ТА ВЕДЕННЯ РОЗВІДУВАЛЬНО-ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Керівниками розвідувальних органів, інформаційно-аналітичними (інформаційними) підрозділами, органами розвідки та офіцерами розвідки усіх рівнів організовується і проводиться розвідувально-інформаційна діяльність. Процес інформаційної діяльності це – послідовна сукупність операцій (збирання, реєстрація, систематизація, аналіз, передавання, накопичення, зберігання, видача інформації), яка дає змогу швидко знайти у повному обсязі розвідувальні дані, необхідні командиру та штабу.

Для пошуку більш ефективних підходів щодо покращення якості і оперативності робіт органів управління розвідкою в статті проведений аналіз факторів, які впливають на ефективність організації та ведення розвідувально-інформаційної діяльності.

В результаті аналізу сукупності факторів, що впливають на ефективність робіт посадових осіб органів управління розвідкою, зроблені висновки, які дозволять визначити заходи, що впливають на більш суттєвий ефект підвищення ефективності щодо організації та ведення розвідувально-інформаційної діяльності за усіма напрямками.

Це дасть можливість не тільки скоротити часові показники проходження інформації на всіх етапах роботи, що дозволить забезпечити її безперервність та повноту, а також підвищити рівень семантичної обробки розвідувальної інформації за той час самий час, що забезпечить більш вищий ступень її достовірності, надасть можливість приймати на її основі більш адекватні та ефективні рішення.

Ключові слова: органи управління розвідкою; розвідувально-інформаційна діяльність; вплив факторів; інформаційне забезпечення.

Вступ та постановка проблеми. Посадові особи органів управління розвідкою (ОУР) займаються комплексом заходів з організації та ведення розвідувально-інформаційної діяльності. Розвідувально-інформаційна діяльність (РІД) – безперервний процес, який здійснюють органи військового управління та їхні органи управління розвідкою, керівники органів військового управління та органи розвідки оперативного та стратегічного рівнів, підпорядковані їм інформаційні (інформаційно-аналітичні) підрозділи та органи розвідки і включає комплекс заходів з організації та ведення розвідувально-інформаційної роботи в загальній системі воєнної розвідки для задоволення інформаційних потреб керівництва держави, командувачів (командирів), органів військового управління та інших, визначених нормативними документами, споживачів розвідувальної інформації [1].

Тому розгляд питань удосконалення роботи посадових осіб під час розвідувально-інформаційної діяльності в інтересах забезпечення командирів в сучасних умовах є актуальним.

Аналіз останніх досліджень і публікацій. За останні роки з’явилось достатньо матеріалів в наукових працях з питань що впливають на ефективність робіт посадових осіб органів управління розвідкою. Однак найбільш наближеними до теми статті є [2,3]. У них проведений аналіз порядку роботи посадових осіб органів управління розвідки (ОУР) у антитерористичній операції та операції об’єднаних сил [2], а також аналіз чинників, що впливають на ефективність функціонування пункту управління артилерійською розвідкою [3], що стало підставою для дослідження факторів, які впливають на ефективність робіт посадових осіб органів управління розвідкою щодо організації та ведення розвідувально-інформаційної діяльності.

Мета статті полягає в проведенні аналізу сукупності факторів, що впливають на ефективність робіт посадових осіб органів управління розвідкою, які дозволять визначити заходи, що впливають на більш суттєвий ефект підвищення ефективності щодо організації та ведення розвідувально-інформаційної діяльності.

Виклад основного матеріалу

Процес інформаційної діяльності – послідовна сукупність операцій (збирання, реєстрація, систематизація, аналіз, передавання, накопичення, зберігання, видача інформації), яка дає змогу швидко знайти у повному обсязі розвідувальні дані, необхідні командиру та штабу [4].

Засоби інформаційної роботи – сукупність документальних, технічних та інших пристроїв, призначених для накопичення, оброблення, систематизації, зберігання та видачі інформації [4] – табл. 1.

Таблиця 1

<table>
<tr><th colspan="6">Розвідувально-інформаційна діяльність</th></tr>
<tr><td colspan="6">Організовується і проводиться керівниками розвідувальних органів, інформаційно-аналітичними (інформаційними) підрозділами, органами розвідки та офіцерами розвідки усіх рівнів</td></tr>
<tr><td rowspan="2">Збір розвідувальних відомостей</td><td colspan="4">Обробка та облік розвідувальної інформації (матеріалів, відомостей, даних)</td><td rowspan="2">Розробка інформаційних документів</td></tr>
<tr><td>Первинна (попередня) обробка:</td><td>Аналіз</td><td>Оцінка</td><td>Узагальнення</td></tr>
<tr><td>Організація збору, ознайомлення</td><td>Систематизація та облік</td><td>Розподіл за категоріями:
перша;
друга;
третя</td><td>Особливої важливості;
цінна;
становить інтерес;
не становить інтересу;
оцінці не підлягає;
вірогідні;
сумнівні;
брехливі</td><td>Формування обґрунтованих висновків прийняття інформаційного рішення</td><td>Термінові;
нетермінові інформ.
звітні;
довідкові;
для доповіді вищому керівництву;
для інформування підлеглих та взаємодіючих штабів (відомств)</td></tr>
</table>

Сукупність факторів, що впливають на ефективність робіт посадових осіб органів управління розвідкою щодо організації та ведення розвідувально-інфораційної діяльності пропонується розмежувати на внутрішні та зовнішні. Внутрішніми факторами є: укомплектованість розвідувальних органів особовим складом та рівнем професійної підготовки, завчасної підготовки інформаційного забезпечення військ, збільшення інтенсивності процесів збору та обробки інформації органами управління розвідкою, оснащення засобами інформатизації та телекомунікації. Зовнішніми чинниками є: збільшення просторового розмаху бойового простору, зростання обсягу інформації, фактор часу при управлінні військами [3, 5].

Проаналізуємо більш детально фактори, які впливають на ефективність робіт посадових осіб органів управління розвідкою щодо організації та ведення РІД.

Вплив внутрішніх факторів:

Укомплектованість розвідувальних органів особовим складом та рівнем професійної підготовки. Ефективність функціонування ОУР чимало залежить від наявності особового складу для виконання робіт за призначенням. Тому визначення раціонального складу є важливим і актуальним завданням, яке має як практичне, так і теоретичне значення. Звичайно для порядку обґрунтування порядку виконання робіт в ОУР використовуються часові оцінки (нормативи) тривалості і виконання робіт особовим складом. Однак мало уваги приділяється визначенню потрібного складу для виконання робіт за призначенням, зокрема не у повній мірі ураховується рівень кваліфікації особового складу, необхідність одночасного (паралелізм) виконання декількох робіт. Тому необхідно удосконалення методичних положень обґрунтування потрібного складу ОУР для виконання робіт за призначенням, рівнем професійної підготовки та практичних навичок відповідних посадових осіб щодо використання засобів автоматизації.

Завчасна підготовка інформаційного забезпечення військ. В зв'язку з прийняттям в Україні оборонної доктрини та сучасною обстановкою на кордонах України, можливий противник заздалегідь буде володіти ініціативою. Це підвищує ймовірність раптового початку агресії, що призводить до значного підвищення ролі оборонної операції. Звідси виникла потреба завчасної підготовки інформаційного забезпечення військ, особливо в достовірній розвідувальній інформації. Це завдання вирішується в мирний час шляхом накопичення баз даних, які містять інформацію про противника, свої війська та опис оперативного напрямку бойових дій, які плануються. Інформаційна база повинна постійно корегуватися згідно з змінами обстановки. Це дозволяє скоротити час на підготовку вихідної інформації, на видання довідкових даних, забезпечити їх ідентичність для всієї сукупності розрахунків, що проводять посадові особи ОУР.

Збільшення інтенсивності процесів збору та обробки інформації органами управління розвідкою. Внаслідок попередніх факторів виникає збільшення інтенсивності процесів збору та обробки інформації органами управління розвідкою.

Обсяг та складність роботи офіцерів штабів підвищились настільки, що трудовитрати на збір, обробку інформації, проведення розрахунків, оформлення документів складають 80..85% загальних трудовитрат і, як наслідок, на творчу, логіко-аналітичну діяльність офіцерів залишається лише 15-20% всього часу, що витрачається.

Сучасні технології передачі та обробки інформації, впровадження автоматизованих систем управління (АСУ) може дозволити змінити це співвідношення в бік скорочення у 2..3 рази, що складатиме 16..20% загального ресурсу часу. В таких умовах на творчу і організаторську діяльність командир і штаб може витрачати до 80% часу [6].

Оснащення засобами інформатизації та телекомунікації. Рівень автоматизації полягає у насиченості органів і пунктів управління, системи зв'язку, джерел інформації та спеціальних систем її збирання й оброблення засобами автоматизації. Розглядаючи рівень автоматизації, доцільно мати не кількість засобів автоматизації, а кількість автоматизованих функцій. За загально прийнятою практикою, розрізняють три рівні автоматизації: 50% – 65% – задовільний; 65 % – 75 % – добрий; 75% та більше – відмінний [7].

Низький рівень автоматизації роботи приводить до того, що оперативність організації ОУР в 2-2,5 рази, а збору і обробки розвідувальних відомостей (даних) у 8-10 разів відстає від армій провідних у військовому відношенні країн світу. Використання АСУ для управління ОУР значно підвищує оперативність управління за рахунок зменшення часу на збирання, оброблення, розподіл розвідувальної інформації, прийняття рішення та планування і доведення рішень. У середньому тривалість циклу управління на оперативному рівні скорочується в 3-4 рази [7].

Вплив зовнішніх факторів:

Збільшення просторового розмаху бойового простору. На сучасному етапі розвитку воєнного мистецтва, коли поряд з класичними оборонними та наступальними операціями для Збройних Сил України все більш набирають актуальності операції щодо нейтралізації

незаконно створених збройних формувань, попередження та локалізації прикордонного збройного конфлікту відмічається певне збільшення просторового розмаху операції.

Для забезпечення ефективного застосування військ (сил) розвідка повинна викривати від 60% до 80% усіх важливих об'єктів які можуть бути в смузі його відповідальності, у тому числі 100% високоточної зброї [2,3].

Зростання обсягу інформації. Сучасні операції (бойові дії) носять загальновійськовий характер, що вимагає чіткої взаємодії органів управління видів і родів військ, взаємного обміну інформацією між ними.

На сучасному етапі відмічається зростання обсягу інформації, що впливає на командирів і штабів, а також, що циркулює між органами управління. Високу інтенсивність обміну інформацією має взаємодія всередині самого штабу, відділами, посадовими особами. Обсяг разової інформації, що поступає до ОУР в найбільш напружені періоди операції просто вражає, може надходити одночасно з декількох джерел інформації, її необхідно систематизувати, проаналізувати, обробити і т.д.

Фактор часу при управлінні військами. Збільшення можливостей сучасної зброї щодо ураження та скорочення термінів приведення зброї у готовність до застосування призвели до того, що принципово змінилася роль фактору часу при управлінні військами. Вплив цього фактору визначає таку вимогу до управління військами як оперативність. Вона полягає в здатності командування та штабу вирішувати задачі управління в режимі часу, який забезпечує упередження противника в діях, швидко реагувати на зміни обстановки та своєчасно впливати на хід бойових дій.

Вирішальне значення для забезпечення оперативності управління військами має розвідка. Фактор часу завжди має велике значення для розвідки, а термін "своєчасність" характеризує оцінку якості отриманої розвідувальної інформації. Швидкоплинність сучасних бойових дій потребує значного скорочення витрат часу на добування, обробку і передачу розвідувальної інформації. Відомо, що найбільш повні та достовірні дані втрачають свою цінність, якщо вони доставлені з запізненням. Але розглянуте вище переконливо показує, що цінність розвідувальних даних може губитися саме під час передачі їх від органів розвідки, від нижчестоящих штабів до вищестоящих за рахунок втрати їх своєчасності подання. Таким чином, процеси передачі інформації як в розвідувальних органах так і між штабами повинен бути автоматизованим і базуватися на сучасних цифрових каналах зв'язку.

В результаті аналізу сукупності факторів, що впливають на ефективність робіт посадових осіб органів управління розвідкою щодо організації та ведення розвідувально-інформаційної діяльності можливо зробити висновки що дозволяють заключити, що на сьогоднішній день основним доступним шляхом для отримання значного приросту ефективності РІД є впровадження в практику роботи розвідувальних органів усіх ланок сучасних інформаційних систем і технологій обробки інформації.

Досвід локальних війн, збройних конфліктів, проведення АТО та ООС, результати проведених навчань, особистий практичний досвід свідчать про те, що автоматизація процесів збору і обробки розвідувальних відомостей, як основи розвідувально-інформаційної та інформаційно-аналітичної роботи органів управління розвідкою Збройних Сил, а також впровадження в їх діяльність сучасних інформаційних технологій є дуже важливим завданням на сьогоднішній день [9,10].

Ця робота виконується в загальній системі інформатизації Збройних Сил України. На сьогодні в Збройних Силах існує Концепція інформатизації Збройних Сил України, а також розроблення програми створення Єдиної автоматизованої системи управління Збройних Сил України.

Для виконання поставленого завдання пропонується впровадження конкретних сучасних інформаційних технологій (ІТ) основні з яких відповідно до етапів РІД наведені в таблиці 2 [8,9].

Таблиця 2

№ з/п	Етапи	Технології
1	Добування, збір, доставка, накопичення	Технологія визначення точних координат на місцевості (GPS - приймачі); цифрова відео, фото, космічна зйомка; мобільний цифровий зв'язок; дистанційне встановлення та керування різноманітними сенсорними датчиками; технологія геоінформаційної системи (ГІС) на мобільних автоматизованих робочих місцях; технології перетворення в електронний вигляд та вводу інформації з паперових носіїв; технології накопичення та збереження великих обсягів інформації; технології криптографічного захисту інформації при передачі відкритими каналами зв'язку; технології ідентифікації особи за відбитками пальців, сітчаткою ока, голосом, або біополем для запобігання несанкціонованого доступу до інформаційної системи.
2	Пошук, обробка, оцінка, прогноз	WEB – технологія; технологія ГІС в локальній мережі; технології визначення та накопичення знань та створення банків знань; нейролінгвістичні технології обробки текстової інформації; технології автоматизованої підготовки інформаційних документів.
3	Надання розвідувальної інформації споживачу	Технологія відображення відео та комп'ютерних даних на великих екранах; технології автоматизованої підготовки звітних документів; технологія електронного підпису; технології захищеного дистанційного доступу до інформаційних ресурсів.

Крім впровадження інформаційних технологій велику роль грає укомплектованість розвідувальних органів особовим складом за рівнем професійної підготовки та практичних навичок щодо використання засобів автоматизації.

Висновки. Все це викликає потребу по-перше, в завчасній підготовці інформаційного забезпечення дій військ, по-друге, пред’являє підвищення вимоги щодо оперативності здійснення процесів розвідувально-інформаційної діяльності.

На показники ефективності РІД значно рівень застосування інформаційних систем, а саме оснащеність і якість засобів інформатизації, спеціального математичного і програмного забезпечення, наявність інформаційної бази і спеціально підготовленого особового складу. Наявний рівень оснащення штабів та органів управління розвідкою засобами інформатизації та телекомунікації залишає бажати кращого, що обумовлює низький рівень інформаційного забезпечення органів управління розвідкою та вимагає здійснювати пошук більш ефективних підходів щодо, впровадження в практику сучасних технологій передачі та обробки інформації,

створення оптимальної інформаційної інфраструктури, впровадження сучасних інформаційних систем.

Результати дослідження можуть бути використані в практиці бойової та оперативної підготовки військ, у застосуванні під час формування показників ефективності функціонування РІД та у подальших наукових дослідженнях за даним напрямом.

ЛІТЕРАТУРА:

1. ВСТ 01.101.004-2019. Військовий стандарт. Воєнна розвідка. Інформаційно-аналітична діяльність. Терміни та визначення. [Чинний від 2020-01-01] Вид. Київ: Міністерство оборони України, 2019. 24 с.

2. Савельєв А.С. Удосконалення порядку роботи посадових осіб органів управління розвідки під час планування розвідки. Збірник наукових праць Національного університету оборони України імені Івана Черняховського. Київ. 2019. Вип. 2 (35). С. 165-170.

3. Таранець О., Дорофєєв М. Аналіз чинників, що впливають на ефективність функціонування пункту управління артилерійською розвідкою. *Журнал наукових статей «Соціальний розвиток та безпека»*, Київ. 2020. Вип. 10 (3). С. 135-144.

4. Розвідувально-інформаційна та інформаційно-аналітична діяльність у системі воєнної розвідки: навч. посіб. / О. Ф. Анікєєнко та ін. Київ: НУОУ, 2016. – 48 с.

5. Мозговий Р. Аналіз чинників, які впливають на ефективність функціонування системи управління військами у ході ведення стабілізаційної операції. Збірник наукових праць національної академії Державної прикордонної служби України. Хмельницький: 2016. Вип. 4(70). С. 133-142.

6. Антіпов Ю., Базь Ю., Мішков О. Теоретичні основи розвідувально-інформаційної діяльності: навч. посіб. Київ: ВДА, 2014. – 172 с.

7. Інформаційні технології інформаційно-аналітичного забезпечення органів управління військами (силами): навч. посіб. С. Микусь та ін. Київ: НУОУ, 2019. – 352 с.

8. Лаврут О.О., Климович О.К., Лаврут Т.В. Перспективи розвитку автоматизованих систем управління тактичної ланки управління Сухопутних військ Збройних Сил України. Системи обробки інформації. Харків. 2014. Вип. 5 (121). С. 116-120.

9. Вернер І., Козаков Ю., Рябцев В. Застосування сучасних інформаційних технологій в роботі органів управління: навч. посіб. Київ: НУОУ, 2006. – 368 с.

10. Максименко Ю., Маміч В., Шаріпова І., Скачков В. Комп'ютерне моделювання в органах управління розвідки для аналізу та обробки даних. Збірник наукових праць центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ 2020. Вип. 3 (70). С. 113-116.

11. Стандарт НАТО. Союзницька об'єднана настанова AJP-2.1 (Видання B. варіант 1) Процеси розвідувальної діяльності. 2016, 80 с.

12. Стандарт НАТО. Концептуальні засади об'єднаної розвідки (на основі об'єднаної спільної доктрини з питань розвідки AJP 2.0). 2016, 44 с.

REFERENCES:

1. 01.101.004-2019. Military standard. Military intelligence. Information and analytical activities. Terms and definitions. [Effective from 2020-01-01] Ed. Kyiv: Ministry of Defense of Ukraine, 2019. 24 p.

2. Savelyev A. Improving the order of work of officials of intelligence agencies during intelligence planning. Collection of scientific works of the National University of Defense of Ukraine named after Ivan Chernyakhovsky. Kyiv. 2019. №. 2(35), pp.165-170.

3. Taranets O., Dorofeev M. Analysis of the factors influencing the efficiency of the artillery reconnaissance control point. Journal of Scientific Articles "Social Development and Security", Kyiv. 2020. № 10 (3), pp. 135-144.

4. Intelligence-information and information-analytical activity in the system of military intelligence: textbook. way / O. Anikeenko and others. Kyiv: NUOU, 2016. – 48 p.

5. Mozgovyi R. Analysis of factors that affect the effectiveness of the management system of troops during the stabilization operation. Collection of scientific works of the National Academy of the State Border Guard Service of Ukraine. Khmelnytsky: 2016. №.4(70), pp. 133-142.

6. Antipov Yu., Baz Yu., Mishkov O. Theoretical foundations of intelligence and information activities: textbook. way. Kyiv: VDA, 2014. – 172 p.

7. Information technologies of information and analytical support of troops (forces): textbook. way. S. Mykus and others. Kyiv: NUOU, 2019. – 352 p.

8. Lavrut O., Klimovich O., Lavrut T. Prospects for the development of automated control systems of the tactical unit of the Land Forces of the Armed Forces of Ukraine. Information processing systems. Kharkiv. 2014. № 5 (121). pp.116-120.

9. Werner I., Kozakov Yu., Ryabtsev V. Application of modern information technologies in the work of government: textbook. way. Kyiv: NUOU, 2006. – 368 p.

10. Maksymenko Yu., Mamich V., Sharipova I., Skachkov V. Computer modeling in intelligence management bodies for data analysis and processing. Collection of scientific works of the Center for Military Strategic Studies of the Ivan Chernyakhovsky National University of Defense of Ukraine. Kyiv. 2020. № 3 (70). pp.113-116.

11. NATO standard. Allied Joint Guidance AJP-2.1 (Edition B. Option 1) Intelligence Processes.2016, 80 p.

12. NATO Standard. Conceptual Framework for Joint Intelligence (Based on the AJP 2.0 Joint Common Doctrine of Intelligence). 2016, 44 p.

PhD Maksymenko Yu.A., D.Sci. Tech. Skachkov V.V.,
d.n. from the state manager Popov S.A., PhD Mamich V.V.

ANALYSIS OF FACTORS AFFECTING THE EFFICIENCY OF WORK OF OFFICIALS OF INTELLIGENCE MANAGEMENT BODIES ON ORGANIZATION AND MANAGEMENT OF INTELLIGENCE ACTIVITIES

Heads of intelligence agencies, information-analytical (information) units, intelligence agencies and intelligence officers of all levels organize and conduct intelligence activities. The process of information activities is a consistent set of operations (collection, registration, systematization, analysis, transmission, accumulation, storage, issuance of information), which allows you to quickly find the full intelligence required by the commander and staff.

To find more effective approaches to improving the quality and efficiency of intelligence agencies, the article analyzes the factors that affect the effectiveness of the organization and conduct of intelligence activities.

As a result of the analysis of the set of factors influencing the efficiency of intelligence officials, conclusions were made that will identify measures that affect the more significant effect of improving the organization and conduct of intelligence activities in all areas.

This will not only reduce the time of information at all stages of work, which will ensure its continuity and completeness, as well as increase the level of semantic processing of intelligence information at the same time, which will ensure a higher degree of reliability. based on more adequate and effective solutions.

Key words: intelligence management bodies; intelligence and information activities; influence of factors; information support.

УДК 351.86

к.т.н. **Саєнко О.Г**(ВІТІ ім. Героїв Крут)
к.т.н., доц. **Шаціло П.В.** (ВІТІ ім. Героїв Крут)

DOI: https://doi.org/10.17721/2519-481X/2022/74-11

ІНСТИТУЦІОНАЛЬНЕ УПРАВЛІННЯ ОРГАНІЗАЦІЙНОЮ КОМПОНЕНТОЮ ОБ'ЄКТА ВІЙСЬКОВОЇ СФЕРИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Досягнення науково-технічного прогресу, особливо в галузі інформаційних технологій, суттєво впливають на розвиток економічної, соціальної, військової, культурної та інших сфер суспільства. Разом із тим інформаційні технології виступають як джерела розвитку, так і джерела загроз такому розвитку та діяльності суспільства взагалі.

Національна безпека являє собою складну багаторівневу функціональну систему, в якій безперервно відбуваються процеси взаємодії та протиборства інтересів держави, суспільства та особистості із загрозами цим інтересам – як внутрішніми, так і зовнішніми. Як цільова функція цієї системи виступає ступінь захищеності цих інтересів від загроз. Для організації захисту інформаційного простору держави необхідно розробляти шляхи протидії інформаційним агресіям з боку тих чи тих суб'єктів: зовнішнього агресора, іноземних спецслужб, транснаціональних компаній, кримінальних кланів тощо.

У статті розглянуто актуальну проблему управління організаційними компонентами об'єктів військової сфери в умовах інформаційної боротьби та реалізації механізмів інституціонального управління цими компонентами. Досягнення теорії організаційного управління і структурного системного аналізу дають змогу з площини декларацій про наміри інформаційної безпеки воєнних і оборонних об'єктів перейти в практичну площину розробки механізмів функціонування організаційними компонентами органів військового управління і механізмів управління ними та їх впровадження в процес функціонування системи управління інформаційною безпекою.

Ключові слова: інформаційне протиборство, інформаційна безпека, інформаційна війна, організаційна компонента, інституціональне управління.

Вступ та аналіз останніх досліджень. Сьогодні досягнення науково-технічного прогресу, особливо в галузі інформаційних технологій, суттєво впливають на розвиток економічної, соціальної, військової, культурної та інших сфер суспільства. Але разом із тим інформаційні технології виступають як джерела розвитку, так і джерела загроз такому розвитку та діяльності суспільства взагалі.

Як показує досвід останніх років, жодна держава не в змозі захистити себе, використовуючи лише військово-технічні засоби. Безпека дедалі більше стає комплексним завданням, яке включає політичні, економічні, інформаційні та інші заходи. Успішно виконувати це завдання можливо лише завдяки оптимальному застосуванню усіх форм та засобів протиборства, включаючи й інформаційне. В багатьох державах відбувається об'єднання в одне ціле сил та засобів інформаційно-психологічного впливу, призначених для досягнення воєнних, ідеологічних і політичних цілей; розвивається велика кількість концепцій формування політики національної безпеки.

Україна, як молода європейська держава, яка намагається стати рівноправним членом світової спільноти, також мусить дбати про захищеність свого інформаційного простору. Для цього необхідно на державному рівні розробляти шляхи протидії інформаційним агресіям із боку тих чи тих суб'єктів: зовнішнього агресора, іноземних спецслужб, транснаціональних компаній, кримінальних кланів тощо.

Цілком очевидно, що національна безпека являє собою складну багаторівневу функціональну систему, в якій безперервно відбуваються процеси взаємодії та протиборства інтересів держави, суспільства та особистості із загрозами цим інтересам – як внутрішніми,

так і зовнішніми. Як цільова функція цієї системи виступає міра захищеності цих інтересів від загроз.

Питання протидії інформаційним загрозам розглядались у роботах торського колективу Національного інституту стратегічних досліджень за редакцією В. Горбуліна [1], В. Кротюка [2], В. Алещенко [3], В. Антипенка [4], В. Богуша, О. Юдіна [5] та інших.

Інформаційна безпека (ІБ) як одна із складових національної безпеки держави являє собою стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через [6]:

– неповноту, невчасність та недостовірність інформації;

– негативний інформаційний вплив;

– негативні наслідки застосування інформаційних технологій;

– несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Складовими ІБ, які водночас є характеристиками основних властивостей інформації, як об’єкта захисту є:

– конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем;

– цілісність – означає неможливість модифікації неавторизованим користувачем;

– доступність – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Елементами системи забезпечення ІБ (у вузькому розумінні) є (рис. 1):

– нормативно-правові акти (НПА), які регламентують суспільні відносини в інформаційній сфері та встановлюють юридичні взаємовідносини;

– державні та недержавні організації, які забезпечують продукцією ринок інформаційних послуг;

– сукупність спеціально уповноважених органів держави, які контролюють дотримання інформаційного законодавства;

Практична діяльність зазначених суб’єктів, спрямована на розвиток вітчизняного інформаційного простору.

У цьому контексті ІБ потребує свого забезпечення на державному рівні.

У широкому розумінні до системи забезпечення ІБ необхідно віднести: Верховну Раду України; Президента України; регуляторні та контролюючі державні органи; споживачів інформації та інших суб’єктів.

Правове регулювання у сфері інформаційної безпеки буде тією чи іншою мірою стосуватися закріплених у Конституції прав особи на інформацію, положень про демократичний устрій, плюралізм думок тощо, законодавства про інформацію, про забезпечення національної (державної) безпеки, охорону державної та комерційної таємниці, діяльність засобів масової інформації, інтернету, а також питань захисту інформації з обмеженим доступом [7].

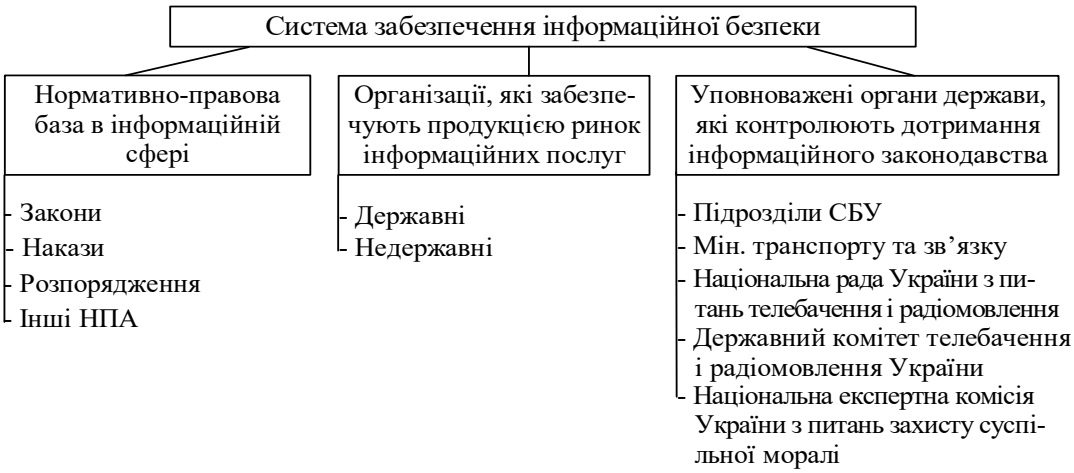

Рисунок 1 – Елементи системи забезпечення інформаційної безпеки

Слід зазначити, що на сьогодні у науковій літературі поки бракує єдиного погляду на зміст поняття «інформаційна безпека», а також не вироблено єдиного методологічного погляду до оцінки такого явища, як «інформаційна безпека суспільства». Так, існує твердження, що інформаційна безпека – це сукупність суспільних відносин, які забезпечують безпечні умови життя кожного члена суспільства, громадський порядок, безпеку державних, громадських чи особистісних інтересів [8].

Однак, не зважаючи на відсутність єдиного визначення поняття ІБ, значимість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення ІБ як одне з глобальних і пріоритетних завдань політики національної безпеки сучасної держави. У цілому ця політика повинна бути спрямована на мінімізацію або уникнення чинних чи потенційних внутрішніх або зовнішніх загроз ІБ держави у відповідності з цілями її розвитку [9].

В Указі Президента України «Про Доктрину інформаційної безпеки України» зазначається, що забезпечення інформаційної безпеки України має здійснюватися за такими принципами:

– свобода збирання, зберігання, використання та поширення інформації;
– достовірність, повнота та неупередженість інформації;
– обмеження доступу до інформації виключно на підставі закону;
– гармонізація особистих, суспільних і державних інтересів;
– запобігання правопорушенням в інформаційній сфері;
– економічна доцільність;
– гармонізація українського законодавства в інформаційній сфері з міжнародним;
– пріоритетність національної інформаційної продукції.

Прийняття Доктрини інформаційної безпеки закріпило офіційну систему поглядів на зміст стратегічних національних інтересів України в інформаційній сфері, погроз цим інтересам, методи протидії погрозам і систему забезпечення ІБ в довгостроковій перспективі [9]. Доктрина створила політичну основу узгодження діяльності органів державної влади з реалізації національних інтересів в інформаційній сфері й захисті їх від зовнішніх і внутрішніх погроз. Але оскільки навіть на принциповому рівні Доктрину ІБ не можна вважати цілком реалізованою, то це веде до досить критичних оцінок інформаційної політики і, водночас, діяльності держави як суб'єкта розвитку інформаційних відносин і забезпечення ІБ.

У свою чергу загрози національній безпеці України в інформаційній сфері представляють собою сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість та поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру.

На сьогодні існує цілий комплекс інформаційних загроз, починаючи від відсутності яскравої ідентифікації України у глобальному інформаційному просторі та чіткої стратегії входження в світове інформаційне суспільство і закінчуючи ІБ окремо взятого громадянина [9].

Так, згідно з Законом України „Про основи національної безпеки України" [10] основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Однак, деякі автори [11, 12] доповнюють цей перелік загроз, відносячи до нього наступні загрози національній безпеці України в інформаційній сфері:

– розповсюдження ідей, що провокують конфлікти на національному, релігійному і соціальному ґрунті та масові заворушення, а також розпалення серед українського населення ідей сепаратизму;

– заклики щодо посягання з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал нашої держави;

– проведення на шкоду інтересам України спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії;

– комп'ютерна злочинність;

– інформаційний тероризм;

– розвідувально-підривна діяльність іноземних спеціальних служб;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– дискредитація політики держави та авторитету окремих державних діячів;

– прояви обмеження свободи слова і доступу громадян до інформації та інших їхніх прав і свобод;

– поширення ЗМІ культу насильства, жорстокості та інших проявів аморальності;

– намагання маніпулювати громадською думкою, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;

– значний обсяг іноземної присутності в інформаційному просторі України;

– небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки, пов'язаних з інформаційною сферою;

– науково-технологічне відставання України від розвинутих країн;

– низька конкурентоспроможність продукції з обслуговування інформаційної сфери;

– нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії;

– зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності;

– відтік учених, фахівців, кваліфікованої робочої сили за межі України;

– інспірування інших деструктивних процесів в інформаційній сфері нашої держави.

Діяльність держави та її органів у сфері забезпечення ІБ є багатогранною: це захист державних секретів, дотримання та охорона конституційних прав громадян в інформаційній

сфері тощо. Через те організація діяльності держави щодо гарантування ІБ – це послідовний безперервний процес, спрямований на розробку і здійснення правових, організаційних, технічних та інших заходів у цій сфері. Крім цього, ІБ повинна забезпечуватися шляхом проведення цілісної державної програми відповідно до Конституції, чинного законодавства України та норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України [13].

На законодавчому рівні основні напрями державної політики з питань національної безпеки в інформаційній сфері визначені у Законі України «Про основи національної безпеки України»:

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Враховуючи практичну складову сьогодення слід зазначити, що, ІБ, як поняття в ході проведення відкритого протистояння або актів зовнішньої інформаційної агресії, набуває нових форм та методів поширення та застосування. Так аналіз бойових дій на сході України, вказує на використання інформаційних операцій для порушення ІБ держави. В ході воєнних дій інформаційна операція відбувається шляхом залучення множини інформаційних атак різного виду та напрямків. Метою таких атак може бути: порушення захищеності інформаційних, програмних та апаратних компонентів інформаційного простору, а також свідомість і психіка особового складу, який бере участь у воєнних діях.

У свою чергу спеціальні інформаційні операції та акти зовнішньої інформаційної агресії поділяються на такі види:

– направлені проти суб’єктів, що беруть участь у підготовці і прийнятті рішень;

– направлені на компрометацію та розповсюдження деструктивних дій щодо опонентів;

– направлені на політичну, економічну та іншу дестабілізацію.

З метою здійснення та реалізації деструктивних дій під час інформаційної агресії можуть застосовуватись методи дезінформації, пропаганди, диверсифікації суспільної думки, психологічного тиску, поширення слухів та міфів.

Загалом у військовій сфері виділяють два види інформаційної боротьби: інформаційно-технічний та інформаційно-психологічний.

У свою чергу у військовій та оборонній сфері об’єктами інформаційної зброї є: інформаційні ресурси стратегічного управління, науково-дослідні підрозділи військової галузі, системи зв’язку та управління військами, інформаційне забезпечення, інформаційні інфраструктури, морально-психологічний стан військ [14]. Перший вид інформаційної боротьби направлений на інформаційно-технічну інфраструктуру (інформаційні, інформаційно-телекомунікаційні системи, автоматизовані системи класу 1,2,3, радіоелектронні засоби) та інформаційний ресурс цих об’єктів, а другий вид інформаційної боротьби спрямовується на їх організаційні компоненти (як об’єднання оперативного складу, що бере участь у підготовці прийняття рішень).

Інформаційна боротьба під час протистояння ведеться на стратегічному, оперативному та тактичному рівнях. На стратегічному рівні інформаційне протистояння планують та координують вищі органи державної влади. На оперативному та тактичному рівнях ця діяльність здійснюється силами та засобами збройних сил, спеціальних служб, а також суспільно-політичними інститутами держави. Таким чином, інформаційна боротьба, об'єктами якої є військові формування та підрозділи (військові об'єкти), ведеться на оперативно-тактичному рівні.

Найбільш вагомим інструментом сучасної інформаційної боротьби з противником є інформаційна зброя. У сучасному світі за допомогою інформаційної зброї супротивники здатні вирішувати стратегічні завдання: здійснювати вплив на державні інтереси; дискредитувати органи влади; провокувати ворожість на суспільному ґрунті та інше.

Множина проблем в управлінні ІБ об'єктів військової сфери виникає через те, що за декларацією цілей ІБ йде низка дій і заходів, які мають віддалене відношення до цих цілей. У масштабах держави це проявляється, наприклад, у тому, що закони, які приймаються, не працюють, в масштабах, наприклад, об'єкта інформаційної боротьби в тому, що розпорядження керівництва призводять до результатів, які прямо протилежні запланованим. Причина полягає у тому, що мало прийняти закон чи розпорядження – необхідно розробити і запровадити механізми їх реалізації.

Стосовно організаційного компонента (ОК) органу управління військовим об'єктом такими механізмами є:

– механізми управління ОК (як сукупність процедур підготовки і прийняття рішень);

– механізми функціонування ОК (як сукупність правил і процедур, які регламентують взаємодію оперативного складу);

– моделі об'єкта, яким управляють.

Ці механізми використовує система управління інформаційною безпекою (СУІБ) військового об'єкта в процесі виконання покладених на неї завдань.

Методи і алгоритми рішення задачі синтезу оптимального механізму функціонування ОК характеризуються високою структурною і обчислювальною складністю [15]. Тому пропонується для побудови механізмів функціонування ОК застосувати наступні складові методології структурного аналізу і моделювання IDEF (IntegratedDefinition-цілісна точність) [10], яка базується на принципах системного аналізу:

– IDEF0 (FunctionModeling) методологія функціонального моделювання;

– IDEF1 (InformationModeling) методологія моделювання інформаційних потоків в середині системи;

– IDEF3 (ProcessDescriptionCapture) методологія документування технологічних процесів, які мають місце в системі. Має безпосередній зв'язок з методологією IDEF0;

– IDEF5 (OntologyDescriptionCapture) методологія онтологічного дослідження складних систем. За допомогою IDEF5 онтологія системи може бути описана термінами і правилами, на базі яких формуються достовірні твердження про стан системи в деякий момент часу та висновки про подальший її розвиток;

– DFD (DataFlowsDiagrams) методологія структурного аналізу систем, яка дозволяє описати зовнішні по відношенню до системи джерела і адреси, логічні функції, потоки і сховища даних, до яких система здійснює доступ.

Оскільки в процесі інформаційної боротьби ОК органу управління військового об'єкта знаходиться під інформаційним впливом 2-го виду, то управління інформаційною безпекою доцільно представити як управління наступних типів [16,17]:

– управління складом ОК;

– управління структурою ОК;

– інституціональне управління ОК;

– мотиваційне управління ОК;

– інформаційне управління ОК.

Інституціональне управління ОК можна визначити як управління обмеженнями і нормами діяльності осіб оперативного складу (агентів), які беруть участь у підготовці прийняття рішень. Сутність його полягає в тому, що СУІБ обмежує множину можливих дій і результатів діяльності членів ОК. Таке обмеження може здійснюватися правовими актами, директивами, наказами, розпорядженнями, нормами (у тому числі морально-етичними нормами), посадовими інструкціями та інше. Прийнято явні норми діяльності (наприклад, закони, накази, директиви, посадові інструкції) називати обмеженнями діяльності, а неявні норми (морально-етичні норми, службова етика) – спонукальними нормами діяльності.

У теорії управління соціальними системами моделі управління спонукальними нормами діяльності агентів практично не розглядались. Окремі моделі управління обмеженнями діяльності агентів розглянуті в роботі Новикова Д.А., Смирнова И.А., Шохиної Т.Е. «Механизмы управления динамическими активными системами», в якій множина допустимих дій агента залежить від параметра, який вибирає центр (у нашому випадку – СУІБ).

Задача обмеження діяльності осіб оперативного складу ОК органу управління об'єкта військового призначення, що діє в умовах інформаційної боротьби, може бути сформульована таким чином.

Задано:

– універсальна множина X дій агента;

– агент вибирає таку дію із множини A своїх допустимих дій, яка максимізує його цільову функцію $f(y)$, тобто $C(f, A) = Arg\max f(y);\ y \in A$.

Необхідно:

СУІБ вибрати обмеження $B \le X$ множини допустимих дій агента при умові, що агент вибере дію (діяльність) із множини: $C(f, B) = Arg\max f(y);\ y \in B$.

Нехай переваги СУІБ в такий момент інформаційної боротьби задані функціоналом $\Phi(y, A)$, який дає змогу порівнювати пари «дії агента-множина допустимих дій агента». Якщо вважати, що функціонал $\Phi(y, B)$ не залежить від множини B допустимих дій агента (тобто – введення тих чи тих обмежень дій агента не потребує від СУІБ відповідних затрат), то задача інституціонального управління ОК вироджується: СУІБ достатньо вибрати $B = \{x\}$,

де $x = Arg\max \Phi(y);\ y \in X$.

Висновки. Таким чином досягнення теорії організаційного управління і структурного системного аналізу дають змогу з площини декларацій про наміри інформаційної безпеки воєнних і оборонних об'єктів перейти в практичну площину розробки механізмів функціонування організаційними компонентами органів військового управління і механізмів управління ними та їх впровадження в процес функціонування СУІБ.

Враховуючи вказане, актуальним питанням залишається проведення оцінки ефективності використання методів, засобів, способів, підходів та механізмів забезпечення рівня ІБ, що повинне ґрунтуватися на аналізі вразливостей системи безпеки, загроз системі безпеки, ризиків здійснення порушень та інше.

Саме тому сучасний стан забезпечення національної та ІБ України в цілому, та об'єктів військової сфери, зокрема, потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для гарантування безпеки в усіх її сферах.

Отже, в умовах стрімкого розвитку інформаційних технологій, досягнень теорії організаційного управління та структурного системного аналізу, ефективний розвиток підходів у забезпеченні ІБ вимагає розробки не тільки різних методів протидії інформаційним агресіям з боку тих чи тих суб'єктів, а і розробки механізмів функціонування та управління

організаційними компонентами, які беруть участь у підготовці прийняття рішень і самі знаходяться під постійним впливом інформаційного тиску.

Можливими шляхами удосконалення державного управління забезпеченням ІБ можуть бути такі: удосконалення нормативно-правової бази; створення умов для ефективної участі України в міжнародному інформаційному обміні в межах єдиного інформаційного простору світу; унеможливлення поширення спеціальних технічних засобів прихованого отримання інформації; наукове обґрунтування шляхів та механізмів забезпечення ІБ України, оцінка сучасних методів ведення конфліктів та інше.

ЛІТЕРАТУРА:

1. Світова гібридна війна: український фронт / За заг. ред. В.П. Горбуліна. Національний інститут стратегічних досліджень. – К.: НІСД, 2017. – 496 с.

2. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М. Ю., 2021. 558 с.

3. Алещенко В. Інформаційно-психологічний вплив у ході збройної боротьби. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2018. Вип. 1. С. 6-10.

4. Антипенко І.В. Гібридна війна в Україні як ризикоутворюючий чинник глобалізації. Ефективність державного управління. 2020. Вип. 4 (1). С. 13-26.

5. Богуш В., Юдін О. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.

6. Закон України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”, від 09.01.2007 № 537-V [Електронний ресурс] / Верховна Рада України: Законодавство України. – Назва з титул. екрану. – Режим доступу до інформації: http://zakon.rada.gov.ua.

7. Конституція України від 28.06.1996 [Електронний ресурс] / Верховна Рада України: Законодавство України. – Режим доступу до інформації: http://zakon.rada.gov.ua.

8. Ліпкан В.А. Національна безпека України: [навч. посіб.] / В.А. Ліпкан. – [2-е вид.]. – К.: КНТ, 2009. – 576 с.

9. Указ Президента України „Про Доктрину інформаційної безпеки України” від 08.07.2009 № 514/2009 [Електронний ресурс] / Верховна Рада України: Законодавство України. – Назва з титул. екрану. – Режим доступу до інформації: http://zakon4.rada.gov.ua/laws/show/514/2009.

10. Закон України „Про основи національної безпеки України”, від 19.06.2003 № 964-IV [Електронний ресурс] / Верховна Рада України: Законодавство України. – Назва з титул. екрану. – Режим доступу до інформації: http://zakon.rada.gov.ua/go/964-15.

11. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / Петрик Валентин // Юридичний журнал. – 2009. – № 5. – Назва з титул. екрану. – Режим доступу до журналу: http://justinian.com.ua/article.php? id=3222.

12. Галамба М. Інформаційна безпека України: поняття, сутність та загрози [Електронний ресурс] / Галамба Микола // Юридичний журнал. – 2006. – № 11. – Назва з титул. екрану. – Режим доступу до журналу: http://justinian.com.ua/article.php?id=2463.

13. Соціально-правові основи інформаційної безпеки: Навч. посіб. / [Петрик В.М., Кузьменко А.М., Остроухов В.В. та ін.]; за ред. В.В. Остроухова. – К.: Росава, 2007. – 496 с.

14. Информационно-психологическаябезопасность в епоху глобализации: Учебноепособие / [Петрик В.М., Остроухов В.В., А.А. Штоквиш та ін.]; под ред. В.В. Остроухова. – К., 2008. – 544 с.

15. Методологія аналізу, моделювання та проектування систем і процесів IDEF: Навч.посібникґ/ П.В.Шаціло, В.В.Цуркан.: Вид-во ІСЗЗІ НТУУ „КПІ” 2011-146 с.

16. Новиков Д.А. Теорияуправленияорганизационными системами. М.: МПСИ. – 2005.– 584 с.

17. Психологическиепроблемыдеятельности в особыхусловиях / Под ред. Б.Ф. Ломова, Ю.Н. Забродина – М.: Наука, 1985. – 232 с.

REFERENCES:

1. V.P. Gorbulin, Svitovagibrydnaviina: Ukrainskii front. [World Hybrid War: the Ukrainian front] /ed. By V.P Gorbulin. National Institute for Strategic Studies. - K .:NISD, 2017. - 496 p.

2. V.A. Krotuk, Viinyinformatsiinoiepokhy: mizhdystsyplinarnyidyskurs: monographiia. [Wars of the information age: interdisciplinary discourse: a monograph] / ed. by V.A. Krotuk. Kharkiv: FedorkoM .FOP., 2021. 558 p.

3. V. Aleshchenko. Information and psychological influence during the armed struggle. Bulletin of the Taras Shevchenko National University of Kyiv. Military special sciences. 2018. Ed. 1. pp. 6-10.

4. I.V. Antipenko, Ukrainian hybrid war as a risk factor for globalization. Efficiency of public administration. 2020. Vip. 4 (1). pp. 13-26.

5. V. Bogush, O. Yudin, Information security of the state. Kyiv: MK-Press, 2005. 432 p

6. Law of Ukraine "Basic Principles of Information Society Development in Ukraine for 2007-2015", ed. 09.01.2007 № 537-V [Electronic resource] / The VerkhovnaRada of Ukraine: Legislation of Ukraine. Link: http://zakon.rada.gov.ua

7. Constitution of Ukraine of 28.06.1996 [Electronic resource] / VerkhovnaRada of Ukraine: Legislation of Ukraine. - Link: http://zakon.rada.gov.ua.

8. Lipkan V.A. NatsionalnabezpekaUkrainy [National Security of Ukraine]: [textbook. aid.] / V.A. Lipkan. - [2nd ed.]. - K .: KNT, 2009. - 576 p.

9. Decree of the President of Ukraine "Doctrine of Information Security of Ukraine" of 08.07.2009 № 514/2009 [Electronic resource] / The VerkhovnaRada of Ukraine: Legislation of Ukraine. - Link: http://zakon4.rada.gov.ua/laws/show/514/2009.

10. Law of Ukraine "Fundamentals of National Security of Ukraine", dated 19.06.2003 № 964-IV [Electronic resource] / The VerkhovnaRada of Ukraine: Legislation of Ukraine. - Title with title. screen. - Mode of access to information: http://zakon.rada.gov.ua/go/964-15.

11. Petryk V. The essence of information security of the state, society and person [Electronic resource] / PetrykValentyn // Legal magazine. - 2009. - № 5. - Link: http://justinian.com.ua/article.php? id = 3222.

12. Galamba M. Information security of Ukraine: concept, essence and threats [Electronic resource] / GalambaMykola // Legal magazine. - 2006. - № 11. – Link: http://justinian.com.ua/article.php?id=2463.

13. Sotsialno-pravovi osnovy informatsiinoi bezpeky [Socialand legal foundations of information security]: Trainingmanual. / [PetrikV.M, KuzmenkoA.M, OstroukhovV.Vetc.]; fored. V.V. Ostroukhova. – K. Rosava, 2007. - 496 p.

14. Informatsionno-psikhologicheskaia bezopasnost v epokhy globalizatsii [Informational and psychological security intheera of globalization]: Trainingmanual / [PetrikV.M., OstroukhovV.V., A.A. Stockvishandin.]; ed. V.V. Ostroukhova. - K., 2008, 544 p.

15. Metodologiia analizu, modeliuvannia system Iprotsesiv IDEF[Methodology of analysis, modeling and designof IDEFsystem sandprocesses]: Trainingmanual / PVShatsilo, VVTsurkan .: Publishing house ISZZINTUU "KPI"2011-146 p.

16. Novikov DA Teoriia upravleniia organizatsionnymi sistemami [Theory of organizational systems management]. M .: MPSI. - 2005.– 584 p.

17. Psikhologicheskii problemy deiatelnosti v osobykh usloviiakh [Psychological problems of activity in special conditions] / Ed. B.F. Lomova, Yu.N. Zabrodina - M .: Nauka, 1985. - 232 p.

PhD Saienko O.G., PhD Shatsilo P.V.

INSTITUTIONAL MANAGEMENT ORGANIZATIONAL COMPONENT OF OBJECT MILITARY SPHERE IN CONDITIONS INFORMATION WARFARE

Achievements of scientific and technological progress, especially in the information technology field, significantly affect the development of economic, social, military, cultural and other spheres of society. But at the same time, information technology acts as a source of development and a source of threats to this development and society in general. National security is a complex multilevel functional system with continuous processes of interaction and confrontation of state, society and the individual interests with threats to them - both internal and external. The purpose of this system is to protect these interests from threats. In order to organize the protection of the state information space, it is necessary to develop ways to counter information aggression by certain entities: external aggressors, foreign intelligence services, multinational companies, criminal clans, etc.

The article considers the topical problem of management of organizational components of military facilities in the conditions of information struggle and implementation of mechanisms of institutional management of these components. Advances in the theory of organizational management and structural systems analysis allow us to move from the plane of declarations of intent of information security of military and defense facilities to the practical plane of developing mechanisms for functioning of organizational components of military management and management mechanisms and their implementation in the information security management system.

Keywords: information confrontation, information security, information warfare, organizational component, institutional management.

Taras Shevchenko National University of Kyiv Military Institute Collection of scientific works

ISSN-252400056
(74)2022

http://miljournals.knu.ua/

DOI: https://doi.org/10.17721/2519-481X/2022/74-12

ТЕХНІЧНІ НАУКИ
(оформлені за вимогою Web of Science та Scopus)

CONSTRUCTION OF THE ROTOR AND AIRCRAFT UAVS FOR FLIGHT ALONG A GIVEN TRAJECTORY USING TELEMETRY. COMPARISON OF THE TECHNOLOGIES, BENEFITS AND PROSPECTS FOR USING

Serhii Lienkov
Doctor of Technical Sciences, Professor, Head of Research Center

Research Center

E-mail: lenkov_s@ukr.net

Alexander Myasischev
Doctor of Technical Sciences, professor

Professor, Department of Telecommunications and Radio Engineering,

Khmelnitsky National University

E-mail: alex56ma@gmail.com

Yurii Husak

Doctor of Military Sciences

Senior Researcher, Research Center, Institute of the Armed Forces

E-mail: husak1512@gmail.com

Nataliia Lytvynenko

Research Center, Military Institute of Taras Shevchenko National University of Kyiv

E-mail: n123n@ukr.net

Evgeny Lenkov

Scientific Central Research Center of the Armed Forces of Ukrain

E-mail: torwer007@gmail.com

Abstract

In this research, the budgetary (no more than $ 120) UAVs of aircraft and rotary types have been designed, that are able to maintain altitude and position, automatically return to the takeoff point on command from the control panel or in case of loss of communication with it, perform automatic flight along a given trajectory and fly with taking into account telemetry data. It has been shown experimentally, that for flight on the mission on airplane to ensure a straight-line flight, it's advisable to use only a GPS receiver for navigation. The compass setting distorts the plane's straight flight. It was found that in navigation mode, the UAV flight along waypoints, the INAV firmware works more correctly, when the compass is installed in the direction corresponding to the direction of the gyroscopic sensor of the flight controller. Based on the results of flight tests, it was found, that a quadcopter flies waypoints much more accurately, than aircraft. It's shown, that it's possible, using the Blackbox INAV 2.5.0 toolkit and the Google Earth Pro service, to form

a real flight path of the aircraft and quadrocopter, to determine the speed parameters, and the flight altitude according to the readings of the GPS receiver. The possibility of using 3DR modules for telemetry flight has been established. It's noted in the work, that for ground stations implemented by INAV Configurator ver.2.5, the Mission Planner for INAV (Android) only MSP protocol works. No automatic switching to LTM protocol detected, that limits telemetry range compared to Ardupilot firmware. The constructed aircraft and quadrocopter can be used to perform photo and video surveys of the terrain in automatic mode with a route length of 6-8 km, using a lithium polymer battery with a capacity of 1500-2200 mAh.

Keywords: OMNIBUSF4V3, INAV 2.5, GPS receiver, STM32F405, UAV, OSD, ESC controller, Google Earth Pro, MPU6000, Firefly q6, FlySky FS-i6, Failsafe, 3DR, telemetry.

Анотація

У роботі спроектовані бюджетні (не більше 120$) БПЛА літакового та роторного типів, які в змозі утримувати висоту та позицію, автоматично повертатися в точку зльоту по команді з пульта управління або при втраті зв'язку з ним, виконувати автоматичний політ по заданій траєкторії та політ з обліком даних телеметрії. Експериментально показано, що для польоту місією на літаку для забезпечення прямолінійного польоту доцільно для навігації використання лише GPS приймача. Установка компаса перекриває прямолінійний політ літака. Встановлено, що в режимі навігації, польоті БПЛА по маршрутних точках прошивка INAV коректніше працює при установці компаса в напрямку, що відповідає напрямку установки гіроскопічного датчика польотного контролера. За результатами польотних випробувань встановлено, що квадрокоптер значно точніше пролітає маршрутні точки, ніж літак. Показано можливість за допомогою інструментарію Blackbox INAV 2.5.0 та сервісу Google Earth Pro формування реальної траєкторії польоту літака та квадрокоптера, визначення швидкісних параметрів, висоти польоту за показаннями GPS приймача. Встановлено можливість використання модулів 3DR для польоту телеметрією. У роботі зазначено, що наземних станцій, реалізованих програмами INAV конфігуратор ver.2.5, Mission Planner для INAV (Android) працює лише протокол MSP. Автоматичного перемикання на протокол LTM не виявлено, що обмежує дальність телеметрії в порівнянні з прошивками Ardupilot. Побудовані літак та квадрокоптер можуть застосовуватися для виконання фото та відео зйомок місцевості в автоматичному режимі з протяжністю маршруту 6-8 км при використанні літій полімерної батареї, ємністю 1500-2200 мАг.

Ключові слова: OMNIBUSF4V3, INAV 2.5, GPS приймач, STM32F405, БПЛА, OSD, ESC регулятор, Google Earth Pro, MPU6000, Firefly Q6, FlySky FS-i6, Failsafe, 3DR, телеметрія.

Introduction

For the study of the terrain, for carrying out rescue operations, in the work of fire services for monitoring crops, reconnaissance, including military, other special operations, it's currently of interest to build vehicles that fly along the given trajectory both in fully automatic mode and in manual mode, using the technology of the flight by FPV and telemetry [1-5]. For these purposes, the most common vehicles are both fixed-wing (the flying wing, airplane) [2] and the rotary type [1] (the quadrocopters, hexacopters). It's of interest to consider the flight of such device using telemetry data, that are constantly displayed during the flight at the ground station [6]. As such a station, the computer with software is usually used, that allows to visually form the UAV flight on the monitor screen, overlaying it on the map and displaying such parameters as flight speed, direction, altitude, current consumption, battery voltage, etc. To ensure such flight, in addition to software, the radio stations installed both on the aircraft and on the ground station are used. The telemetry for some protocols

makes it possible to change the coordinates of predetermined points on the trajectory in real time, that allows to quickly change the flight trajectory in the On-line mode. Since telemetry equipment operates at lower frequencies than control consoles and video transmission systems for flying in the FPV mode, this makes it possible to control an object and track its flight over long distances with the same transmitter power. The paper considers aircraft assembled from fairly common budget components that use free software products that are open to correction and support the following flight modes [7]:

1. The horizon holding. A gyroscope and an accelerometer are used.

2. The given height maintaining. It requires the GPS receiver and barometric sensor.

3. The maintaining the position both in the horizontal plane and in the height. The GPS receiver and the barometric sensor are used.

4. The mode of returning to the starting point on command from the control panel and in case of communication's loss with the control equipment. Additionally, the magnetometer is used.

5. The flight mode along the trajectory specified on the map. Used the GPS receiver, barometer, magnetometer.

6. The semi-automatic flight mode using the telemetry data and ground station.

Materials and methods

To build the UAVs mentioned above, that are able to perform the presented flight modes, the authors propose to use a 32-bit STM32F405 microcontroller with sensors connected to it, forming the flight controller (FC). The processing of the received data from the gyroscope, accelerometer, barometer, magnetometer, GPS receiver, control receiver is performed by the microcontroller using the free software INAV ver.2.5.2 [8], the release of that appeared in August 2020. The result of data processing is the formation of control signals on motors and servos for the UAV flight control. The choice of this software from the cleanflight / betaflight firmware family is due to the fact that INAV provides automatic point-to-point flight, return to take-off point, and is capable of holding the altitude and position of the UAV. The study of the capabilities of the freely distributed Ardupilot firmware, that has similar capabilities, isn't considered in this reseach. The computer with the installed INAV ver.2.5 configurator is used [8] to install the firmware into the microcontroller, configure its parameters to ensure the performance of the specified UAV functions. It will also act as a ground telemetry flight control station [6].

The firmware is software for the microcontroller that uses mathematical models such as PID regulators [9-11], Kalman filter, complementary filter, LPF and Notch lowpass filters, dynamic Matrix Filter [10], etc.

To ensure a stable UAV flight, to fulfill the specified flight modes, the firmware is adjusted by selecting parameters that depend on the UAV geometry, the installed propulsion system, sensors, speed parameters, and flight trajectory [9,10]. In some cases, the program code is also partially corrected. The aim of the reseach is to create a budget (no more than $ 120) UAV (the aircraft and quadrocopter), the experimental study of them on the implementation of the above flight modes based on the STM32F405 microcontroller and the latest version of the INAV firmware [12,13]. The method for solving the problem is the design and improvement of flight controllers for aircraft and rotary UAVs that provide automatic flight along the given trajectory and flight by telemetry, as well as setting up freely distributed firmware for performing the above flight modes as a result of numerous flight test tests. When designing modern UAVs, the authors used their own developments of

technologies and tools to improve quality and reliability, as well as to extend the technical resource of the developed equipment [14-17].

The solution to this problem is to design the flight controller for airplane and quadrocopter, adjust the firmware parameters together with the performance of test flight tests to adjust these parameters and, based on the data obtained from the blackbox [12], check the compliance of the actual flight path specified by the program.

The simple standard layout of aircraft with the rectangular wing, a span of 1250 mm and the fuselage length of 800 mm was chosen as the carrier for the fixed-wing UAV (Fig. 1). The optimization of geometric parameters in order to obtain the high aerodynamic parameters of the aircraft wasn't considered in the work.

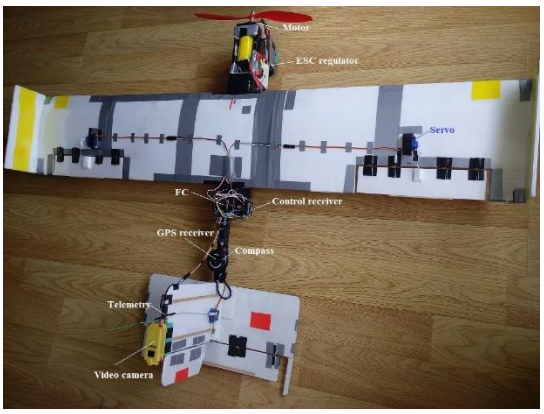

Figure 1 The photo of the tested aircraft.

The equipment is installed on the aircraft [18]:
– the A2212 / 1000KV motor with 30A ESC regulator;
– the propeller 12x4.5 inches;
– the GPS receiver - module GY-NEO6MV2 - GPS receiver u-blox NEO-6M;
– the budget control equipment - FlySky FS-i6 flashed from 6 to 10 channels with the communication range of up to 1.5 km [17];
– the flight controller - OMNIBUSF4V3 [19] based on STM32F405 LQFP64 microcontroller (168 Mhz, 1M Flash, 192 kB SRAM) with built-in gyroscope, MPU6000 accelerometer and BMP280 barometer;
– the battery 1800 mAh, 11.1 V;
– the recording video camera - Firefly q6;
– the telemetry 3 DR [6].
The flight weight of the aircraft was about 900 g.
The quadrocopter with the frame of 250 mm was chosen as the carrier for the rotor-type UAV (Fig. 2). The equipment is installed on the quadcopter:
the 2204 / 2300KV motor with 30 A ESC controller;

the propeller 5x3 inches;

the GPS receiver - u-blox NEO-6M;

the low-cost control equipment - FlySky FS-i6 flashed from 6 to 10 channels with a communication range of up to 1.5 km;

the flight controller - OMNIBUSF4V3 based on STM32F405 LQFP64 microcontroller (168 Mhz, 1M Flash, 192 kB SRAM) with built-in gyroscope, MPU6000 accelerometer and BMP 280 barometer;

the battery 1500 mAh, 11.1 V;

the video camera and video transmitter.

The flight weight of the quadcopter was about 500 g.

The connection diagram of electronic components for the aircraft is shown in Fig. 3. The servos of the wing ailerons, elevators and rudders are connected to the separate 5 V power supply. The flight controller, control receiver, GPS receiver are connected to another 5 V power supply, that is installed on the flight controller. The telemetry is connected to a 5V source, that is integrated with the ESC motor controller.

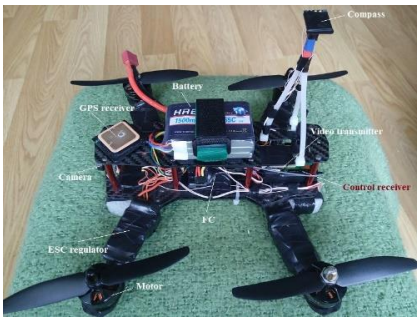

Figure 2 The photo of the tested copter.

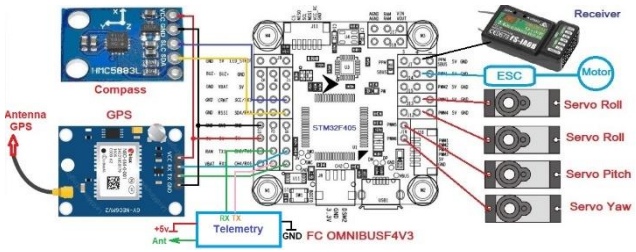

Figure 3 The connection diagram of the main electronic components for the aircraft.

The wiring diagram of electronic components for the copter is shown in Fig. 4. The video camera and video transmitter are connected to the separate power source. The copter sends telemetry data through the video transmitter, that are superimposed on the terrain image obtained from the video camera.

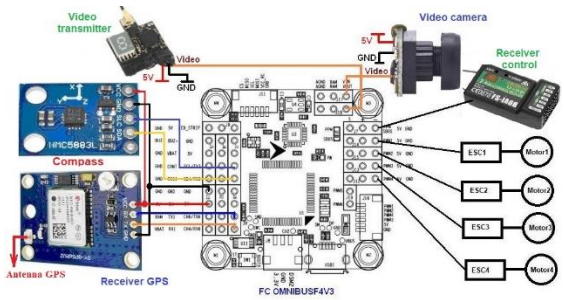

Figure 4 The wiring diagram of the main electronic components for the copter.

The firmware for the flight controller of the aircraft and the quadcopter is downloaded from the site: https://github.com/iNavFlight/inav/releases/tag/2.5.2, using the INAV 2.5.0 configurator, that is installed on the computer from the site: "https://github.com /iNavFlight/inav-configurator/releases/tag/2.5.0". The firmware can also be loaded into the controller, as presented in [19], if there are difficulties in loading through the configurator.

After starting the INAV 2.5.0 configurator, the computer is connected to the flight controller and the firmware parameters are set depending on the configuration of the aircraft and copter, used equipment, flight parameters, flight modes. For this, a sequential entry into the tabs of the configurator is performed with the setting of the necessary parameters [10,19]. The most necessary settings are discussed below.

The Mixer tab (on the Fig. 5a is shown for airplane and on the Fig. 5b is shown for quadcopter separately). The type of aircraft, the connection diagram of motors and servos to the flight controller are established. Sets the servo functions, such as which actuators control the elevators (Pitch), directions (Yaw), aileron (Roll).

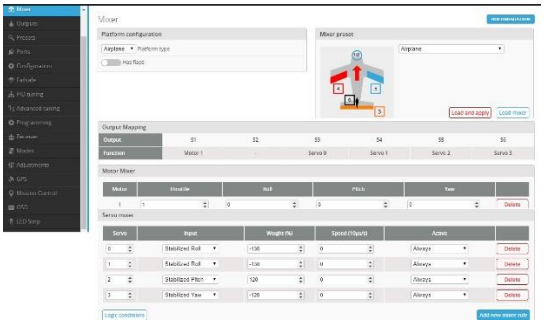

Figure 5 The Mixer Tab.

In the Calibration tab, the accelerometer is calibrated according to the scheme presented in this tab. In the Outputs tab, the protocols for the ESC operation of the motor controller, servo drives are set. The motor and servos are turned on - the Enable motor and servo output parameter and the motor is turned off, when the throttle is low - the Stop motors on low throttle parameter. In the Ports tab, the GPS receiver with speed of 38400 Bit / s is installed on the 6th port in accordance with the diagram of its connection to the flight controller in Figs. 3 and 4. For the aircraft, telemetry is connected to the flight controller on the UART1 port. The Fig. 6 shows the port setup in the Ports tab.

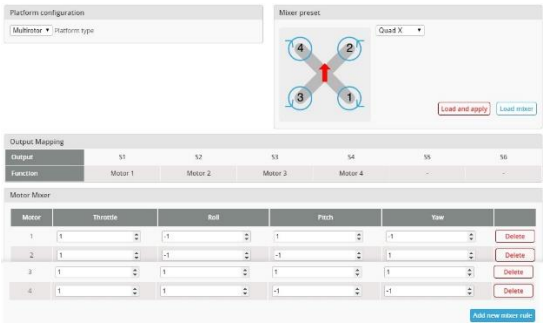

Figure 5b The Mixer Tab.

Figure 6 The installing ports for an airplane with telemetry.

In the Configuration tab, the parameters are set that determine the accelerometer, barometer, magnetometer, GPS receiver operation protocol, and the takeoff assistant mode is also enabled – "Permanently enable Launch Mode for Fixed Wing" (for an aircraft).

The Failsafe mode is being configured. To do this, use the Failsafe tab and the corresponding commands for this mode, that are entered in the CLI tab. The work uses the following case of failsafe activation.

Any channel is out of range, that can be determined using the commands in the cli tab: "get rx_min_usec"; "get rx_max_usec". In the reseach, in the CLI tab the command "set rx_min_usec = 940 was executed" is completed. When the control equipment is on, the minimum gas corresponds to the value greater than 1000. When it's off - 900 (it's how the receiver is configured). The value 900 is less than the minimum value of 940. It will trigger the Failsafe.

Before setting up Failsafe, the Flysky FS-iA6 receiver is preconfigured so that, when the remote control is turned off, it sends 900 μs pulse to the flight controller via the throttle channel (the 3rd channel - throttle), as presented in the source [20]. It means that failsafe will be triggered on this condition.

There are 4 commands available in Failsafe that are executed, when the failsafe occurs. The work uses the RTH command - return to the starting point. The INAV firmware automatically moves the UAV back to its original position and performs the landing of the quadcopter or circling the aircraft within a radius of 50 m above the landing site. The GPS receiver is used for this.

In the PID tuning tab, the parameters of the PID regulator of the aircraft and the quadcopter are set [9,18,21] (Fig. 7). Their determination was carried out by sequential selection during test flights in order to ensure maximum flight stability. The INAV firmware allows automatic tuning according to the special algorithm during manual flight. However, it doesn't always provide the best PID tuning.

Figure 7 The parameters of the PID controller.

The flight parameters are set in the Advanced tuning tab. The airplane is set to Cruise, and the copter is set to Attitude. In this case, the flight controller of the aircraft constantly reads the coordinates from the GPS receiver. For an airplane, the flight speed by points is set to 10 m / s – the parameter is “max CRUISE speed = 1000”. For the copter – 8 m / s. When approaching the launch point, the aircraft will circle circles with a radius of 50 m without landing – the parameter is “Loiter radius = 5000”. The aircraft will land. The experimental setting of the throttle valve (throttle) values are important parameters for the automatic flight of the aircraft. For example, the value of the parameters “Cruise throttle” and “Max. throttle”. If they are too small, then the altitude hold mode will not be possible. With an insufficiently powerful motor, their values are chosen large. For the aircraft being tested, “Cruise throttle = 1700” (it is the throttle value for maintaining straight flight while maintaining altitude) and “Max. throttle = 1950” - corresponds to the maximum engine speed for taking the aircraft to the set altitude. In this tab, the roll, lift and dive angles are set for automatic flight. They are chosen depending on the power of the engine and the strength of the aircraft. For the considered aircraft, they have values: 20, 20 and 15 degrees, respectively. The “At least mode” is selected as the mode for returning to the starting point [21]. It returns the aircraft, quadcopter to the starting point at an altitude not less, than that specified in the RTH altitude parameter (set to 30 m). If the aircraft's altitude was less, than the RTH altitude, when the RTH was triggered, then it rises to the return altitude. If more, then it returns at the same height. In this tab, you can set the number of satellites to which the GPS receiver must be connected in order to be able to confidently fly along the trajectory and perform the Arming procedure. Six satellites have been installed in the research. During testing, the installed GPS receiver in the open area is connected to 9-11 satellites. Similar settings were chosen for the aircraft, except that “the Fixed Wing Navigation Settings” item wasn’t considered for the aircraft. It was experimentally found that the altitude determined by the GPS receiver within 15 min fluctuated in the range of no more than 1 m (at the launch site 323-324 m). Therefore, when the flight controller OMNIBUSF4V3 was configured, the barometer, installed in it, was sometimes turned off during experiments. As experience with quadrocopters has shown, at speeds of about 30 km / h, the effect of "blowing" the barometer occurs, that leads to incorrect altitude determination. Therefore, the barometer was pasted over with foam rubber.

In the Receiver tab, the protocol with the receiver works - PPM, is set and the correct operation of the control equipment channels and the throttle channel triggering, when the equipment power is turned off is checked to enter the Failsafe mode.

The airplane and quadcopter flight modes are set on the control panel switches in the Modes tab (Fig. 8), the description of the modes set for the UAV:

ANGLE - provides automatic holding of the UAV in the horizontal plane using the accelerometer;

NAV ALTHOLD - when the switch associated with the 6th channel is turned on, the flight is performed at a constant altitude determined by the GPS receiver and the barometer (if enabled) at the time of switching;

NAV POSHOLD – the automatic horizontal position holding.

If the NAV ALTHOLD mode is on, the position will also be held in altitude. Therefore, the modes NAV ALTHOLD, NAV POSHOLD are linked to the three-position switch. The aircraft maintains a position by flying in the circle with radius of 50 m at a constant altitude. In this case, the quadcopter

hovers in the given 3D position. The gyroscope, accelerometer, GPS receiver, barometer are used.

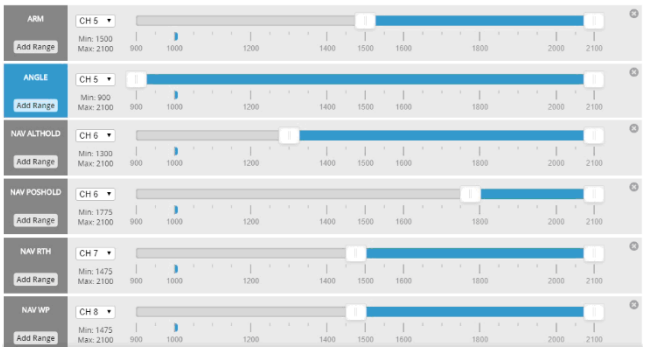

Figure 8 The setting flight modes on the control panel switches.

NAV RTH – the turning on of the 7th channel switch causes the UAV to return to the starting point. When approaching the launch point, the aircraft describes the circle with the radius of 50 m at the altitude specified by “the At least” and “RTH altitude” parameters of “the Advanced tuning tab”. The landing is performed in manual mode (ANGLE). The quadrocopter, when approaching the launch point, makes an automatic landing.

NAV WP - performs automatic flight to specified points on the geographic map. The launch is performed in manual mode, then this switch is turned on to follow the route. When approaching the launch point, the aircraft, as in the NAV RTH mode, flies in the circle with the radius of 50 m. The landing is carried out in manual mode after turning off the 8th channel switch. The quadcopter, when approaching the launch point, performs the smooth landing in automatic mode.

In the Mission Control tab (Fig. 9), the UAV flight is configured along the given trajectory. The computer with the INAV configurator must be connected to the Internet. The section of the map, where the flight is planned, is selected. The waypoints are set by clicking the mouse button. Each waypoint after the second click on it with the mouse displays its coordinates with the parameters of the flight height above it and the speed. These values can be edited. If you need to return to the starting point, check the box on the RTH at the end of the mission parameter. Above it, the plane will circle with radius of 50 m, that is specified in the Loiter radius parameter in the Advanced tuning tab. The quadcopter will hover over the start point at the RTH altitude parameter. If set to “Landing”, the aircraft will automatically land. The generated route is recorded by “the Save mission to FC” and “Save Eeprom mission” commands. The waypoint flight can be performed, if the radio control switch is set to NAV WP flight mode in the Modes tab.

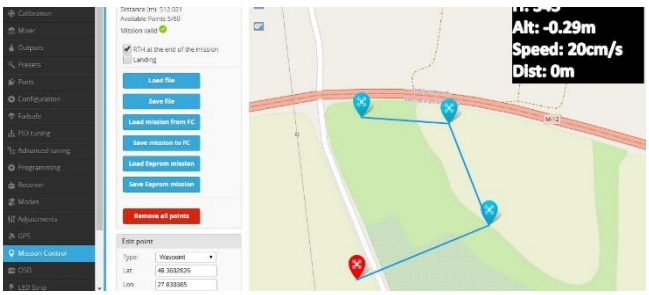

Figure 9 The formation of the aircraft flight path.

The point, to that the UAV returns after completing the mission, isn't displayed on the map. This point corresponds to the launch point, that can be anywhere. The sequence of points flown corresponds to the sequence of forming points on the map.

After loading the mission, "Arming" will be executed only, if the distance from the launch point of the aircraft, quadcopter to the first waypoint is less, than specified in "the nav_wp_safe_distance = 10000" parameter (100 m by default), the value of that can be increased to 650 m.

The parameter "nav_wp_radius = 100" in cm by default determines the distance of the UAV to the given waypoint in order to accept it as reached. For a quadrocopter, this value is set at 200 cm in operation. For an airplane, this parameter is set at 1000-3000 cm. It is due to the slowness of the GPS receiver (takes coordinates 5 times per second), the high speed of the airplane and the probable deviation from the trajectory, for example, due to wind. In operation, in the CLI tab, the command set "nav_wp_radius = 1500" (15 m) was executed. If the plane, for example, due to the wind deviates from the route and doesn't hit the point with diameter of 30 m, then it will describe the arc and return to re-pass the point until it hits it (Fig. 10).

To record the UAV flight parameters on the MicroSD card, in particular, the trajectory, speed, flight altitude, etc., the Blackbox tab is used. This tab enables recording of flight parameters to MicroSD [18].

In [18] it's shown, that for the aircraft-type UAV, it isn't necessary to use the compass and barometer for automatic flight along the given trajectory and return to the starting point. In this research, we experimentally studied the behavior of the aircraft, when flying by points with compass, barometer and GPS receiver and only with GPS receiver. To do this, using the INAV configurator, the flight mission was set as in Fig. 9, and the real flight route of the aircraft was drawn, using the generated LOG files on the MicroSD and the method for decrypting LOG files, that is indicated in [18], using the Google Earth Pro program [22]. The barometer and magnetometer were turned on and off in the Configuration tab. In fig. 10, from left to right, the aircraft flight paths are shown in the cases (the GPS receiver is turned on in all cases):

1) the flight trajectory without barometer and compass;

2) the flight trajectory with barometer and compass. The direction of installation of the compass and the flight controller is the same;

3) the flight trajectory with barometer and compass. The direction of the compass is rotated 270 degrees relative to the direction of the flight controller. This rotation is typical for GPS receivers with the integrated compass, for example, the Beitian BN-880 model, that is allowed by the INAV software. The rotation of the compass relative to the flight controller is set in the Configuration tab.

Figure 10 The flight trajectories of the aircraft with and without compass.

In Fig. 10 the yellow buttons show the points, that are set in the INAV navigator, when setting flight mission (Fig. 9). The analysis showed, that the INAV firmware works more correctly, when the compass is installed in the direction of the flight controller. The best results for the aircraft-type UAV are obtained, when using only the GPS receiver while flying along the trajectory in automatic mode.

The quadcopter initially requires the installation of GPS receiver, compass and barometer for flying to points. Based on the experience with aircraft-type UAV, the compass on the quadcopter is installed as in Fig. 11. In Fig. 12 shows the formation of the route, using the INAV configurator and the real flight route of the quadcopter according to the data from the Blackbox.

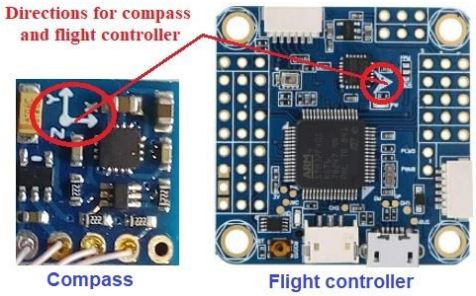

Figure 11 The selecting of the correct compass and flight controller direction.

The experimental studies have shown, that the quadcopter flies points much more accurately, than airplane. Despite the significant speed (about 30 km / h), the quadcopter manages to slow down, when approaching the point, turn around in the area of this point (the radius of 2 m is indicated), calculate the new direction and fly to the next point at given speed while maintaining the straight-line route. The plane overshoots the point at speed of 36 km / h at distance of 15-30 m. At high speeds, this distance increases.

Let's consider the use of telemetry, when flying the UAV, using the INAV firmware. Currently, it's of interest to track UAV flight on the map in real time displayed on the computer screen, using the INAV software. With stable operation of equipment and software, it's also possible to consider the possibility of controlling the aircraft based on the display of its flight on the computer screen according to telemetry data. To use this feature, you must use and configure some supporting technologies, including [6]:

- the GCS (the ground control station). GCS typically provides functions for creating the waypoint (WP) missions, loading WP missions to the flight controller (PC), checking a mission, completing a mission and registering a mission;

- the telemetry equipment. In order to transfer the mission to the PC and monitor it in real time during the mission, it's necessary to install and configure the telemetry system between the GCS and the aircraft.

In order to transfer missions from the GCS to the flight controller and track / log flight data, a data link must be established between the GCS and the aircraft. For this purpose, the following most popular technologies are used [6]: Bluetooth; 3DR (433 MHz / 915 MHz); Wi-Fi (ESP8266); HC-12 (433 MHz, analog 3DR); Openlrs / Openlrsng devices (e.g. orangerx 433 tx / rx combo); LoRA (868/433 MHz options).

The work uses radio stations 3DR. They operate in the 433 MHz and 900 MHz bands. The 3DR standard firmware is designed for the MAVLink protocol. The current INAV recommendation is to use standard firmware with MAVLink options disabled. 3DR - medium range technology, at least 1 km.

Figure 12 The comparison of the quadcopter planned and real flight by points.

The data is transferred between the GCS and the flight controller using a "telemetry protocol". The INAV currently offers two protocols: MSP and LTM [6], MSP - Serial MultiWii is the “native” messaging protocol for INAV. It’s well supported by the INAV configurator and many OSDs that overlay telemetry parameters on the flight terrain display screen. The protocol has everything for loading missions and tracking flights. The disadvantage is that it’s the polling protocol and to monitor a mission, the GCS must request data, and the flight controller must respond to requests. This limits performance, when monitoring the mission.

LTM is a "push" telemetry protocol. Here, the flight controller is sending unsolicited data to the GCS. This avoids the "half duplex" MSP time delay on 3DR radios. Unlike MSP, LTM only provides flight data. To improve performance and increase range, MSP is used before Arming, LTM for Arming.

For INAV, the following rules apply [6]:

- if the UART detects both MSP and Telemetry Protocol (LTM), then MSP is active, when there is no Arming, and push-telemetry protocol is sent from FC, when it’s in Arming – e;

- if only MSP is enabled for USART, it’s always available (with Arming and without Arming).

Figure 13 The Example of Configuring Telemetry Ports.

In the example, shown in Fig. 13, MSP is available on USART1, when there is no Arming and LTM, when Arming (in this case, the 3DR telemetry radio and an mwp ground station are used). The baud rate is set the same for MSP and LTM. In operation, the port settings for telemetry are shown in Fig. 6, i.e. only MSP is enabled, as it has been experimentally determined, that the INAV configurator doesn’t support LTM during flight.

In operation, the 3DR radio station was selected as the equipment for telemetry. Its main characteristics: the weight <4 grams without antenna; the working frequency 433-434.79 MHz; the range is determined by the antenna, for a half-wave dipole at least 1 km; the receiver sensitivity - 121 dBm; the transmitter power 20 dBm (100 mW); the data rate up to 250 kbps (default 56700 bps).

A photograph of the 3DR radio modules with the supplied antenna is shown in Fig. 14. The experiment showed, that the range of the modules with such an antenna doesn't exceed 100-150 m for viewing the flight using the INAV ver.2.5 configurator as a ground station. The Mission Planner for INAV (Android) showed similar results. The module on the plane was connected to the UART1 port as in Fig. 3. To increase the operating range, instead of installing the supplied antenna, two pieces of wire from the "twisted pair" network cable 165 mm long were soldered to the antenna output. Thus, the "classical half-wave dipole" antenna was installed. During testing such an antenna made it possible to establish a stable radio communication at the distance of up to 1 km. No further testing was performed.

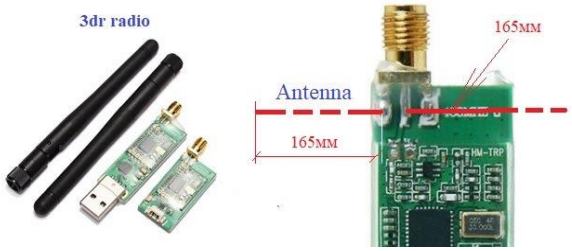

Figure 14 The modified antenna-dipole 3DR modules with the frequency of 433 MHz.

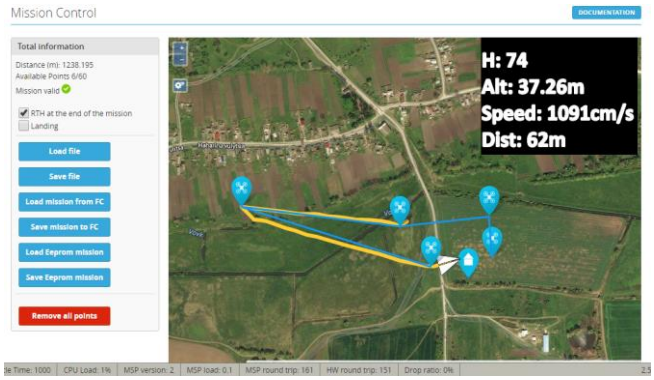

Figure 15 Airplane flight trajectory in on-line mode according to telemetry data.

During testing, the 3DR ground module with USB port was connected to the laptop via the USB extension cable. The 3DR module was attached to the wooden pole and the dipole antenna was positioned vertically. On the plane, the module was attached to the keel of the plane, so that the antenna - dipole was also vertical. Figure 15 shows a screenshot of computer screen during an aircraft's flight along the given trajectory in the Mission Control tab of the INAV configurator.

In the reseach, using Blackbox, the LOG files of flight parameters were obtained using only the GPS receiver. The data from these files were converted into the flight path and displayed, using the Google Earth Pro service, as presented in [18]. The maximum distance from the starting point was chosen at the distance of about 1 km so, that the communication is guaranteed to receive telemetry data.

In Fig. 16 shows the flight paths of the aircraft along the flight points set in the INAV configurator. The flight trajectory of the aircraft was tracked in on-line mode, using telemetry data, as in Fig. 15. The function of the ground station was performed by the INAV configurator in the Mission Control tab. No signal loss was observed, when the 3DR modules were operating at this distance and flight altitude of 50 m. The red buttons in Fig. 16 indicate the points on the map set by the configurator, when forming the route and recording it into the microcontroller's memory. The use of only the GPS receiver for navigation without the compass showed an accurate passage through the flight points and a straight line flight from point to point, that wasn't observed with the additional use of the compass (Fig. 9).

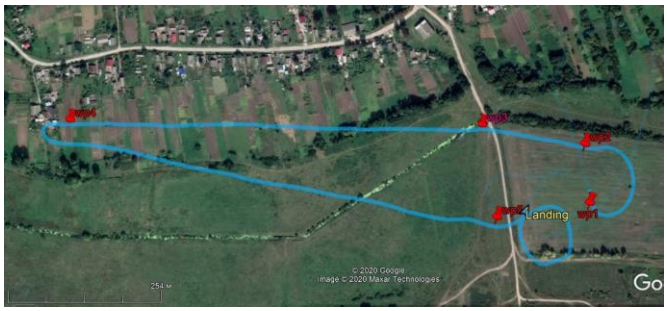

Figure 16 Flying using only GPS receiver at the distance of up to 1 km from the starting point.

For quadcopter flight using telemetry, the OSD setup was performed for INAV firmware. The OSD (On Screen Display) is a software chip (AT7456) in the flight controller, that overlays flight data (the telemetry: flight altitude, speed, distance from take-off point, direction to take-off point, etc.) to the video transmitted from the quadcopter. In Fig. 17 shows the OSD setting [9]. As a result, the video image of the terrain will be superimposed on the flight speed, distance to the take-off point, flight altitude, flight time, number of received satellites, battery voltage, flight mode, horizon level.

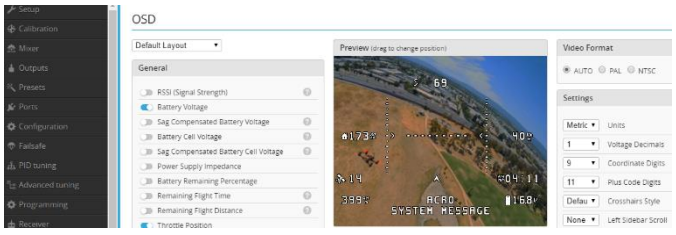

Figure 17 The OSD setup.

With so using of telemetry, the set telemetry parameters are located in the convenient form on the monitor screen of the video receiver, while simultaneously viewing the flight terrain. However, the range of the video transmitter is shorter, than, when using the telemetry presented above for an aircraft at the same transmit power. Also, the ground station better allows you to track the route on the map. Experience has shown that the best control option, tracking UAV flight, is the simultaneous use of these two technologies.

Results and discussion

As a result of the research:

1. The low-cost (no more than $ 120) UAVs of aircraft and rotary types have been created, that are able to maintain altitude and position, automatically return to the take-off point on command from the control panel or if communication with it is lost, perform automatic flight along the given trajectory and fly from taking into account telemetry data.

2. It has been experimentally shown, that for flight on the mission on airplane to ensure the straight-line flight, it's advisable to use only the GPS receiver for navigation. The compass setting distorts the plane's straight flight. It's shown as for INAV firmware ver.2.5 on the example of airplane and it was noted, when testing the quadrocopter on the INAV firmware with an earlier version (ver.2.2.1).

3. It's shown, that in the navigation mode, the flying along waypoints, the INAV firmware works more correctly, when the compass is set in the direction corresponding to the direction of the gyro sensor of the flight controller.

4. Based on the results of flight tests, it was found, that the quadcopter flies waypoints much more accurately, than an aircraft. Despite the significant speed (30 km/h), the quadcopter manages to slow down, when approaching a point, turn around in the area of this point, calculate a new direction and fly to the next point, maintaining the straight-line route. The aircraft overshoots the waypoint at speed of 36 km / h at the distance of 15-30 m.

5. It's shown, that it's possible, using the Blackbox INAV 2.5.0 toolkit and the Google Earth Pro service, to form a real flight path of an aircraft and the quadrocopter, to determine the speed parameters, and the flight altitude according to the readings of the GPS receiver.

6. It has been established, that for ground stations implemented by INAV Configurator ver.2.5, the Mission Planner for INAV (Android), only the MSP protocol works. No automatic switching to LTM protocol detected, that limits telemetry range compared to the Ardupilot firmware.

7. It has been established, that for the significant increase in the telemetry range on 3DR modules, it's necessary to replace the supplied antennas with the simpler and lighter antenna "half-wave dipole". Its disadvantage is its increased size (the length of the dipole is 330 mm).

aircraft flight controller prior to launch, using the configurator.

Conclusions

1. The paper presents the results of designing budget UAVs of aircraft and rotor types with a cost of no more than $ 120, that are able to maintain altitude and position, automatically return to the take-off point on command from the control panel or in case of communication's loss with it, perform automatic flight according to the given trajectory and flight taking into account telemetry data. It's shown that for flight on a mission on an airplane to ensure a straight-line flight, it's advisable to use only the GPS receiver for navigation.

2. It was found, that in the navigation mode, the UAV flight along waypoints, the INAV firmware works more correctly, when the compass is set in the direction corresponding to the gyroscopic sensor's direction of the flight controller. Based on the results of flight tests, it was found, that the quadcopter flies waypoints much more accurately than an aircraft.

3. The possibility is shown, that with the help of the Blackbox INAV 2.5.0 toolkit and the Google Earth Pro service, the formation of a real flight path of aircraft and the quadcopter, determination of

speed parameters, flight altitude according to the readings of thr GPS receiver. The possibility of using 3DR modules for telemetry flight has been established.

4. There is no automatic switching to LTM protocol detected, that limits telemetry range compared to Ardupilot firmware. The constructed aircraft and quadrocopter can be used to perform photo and video surveys of the terrain in automatic mode with the route length of 6-8 km, using the lithium polymer battery with capacity of 1500-2200 mAh.

References

[1] A. Boyko. Fields of application of drones, Available at: http://robotrends.ru/robopedia/oblasti-primeneniya-bespilotnikov, accessed December 2020.

[2] Modernized Spectator Drone from OJS S.P. Korolyova “Meridian Company”, Available at: https://www.youtube.com/watch?time_continue=6&v=HvLErmgBRX4&feature=emb_logo, accessed December 2020.

[3] S. A. Shvorov, N. A. Pasichnyk, S. D. Kuznichenko, I. V. Tolok., S. V. Lienkov, L. A. Komarova. Using UAV during Planned Harvesting by Unmanned Combines, *IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments*, ISBN: 978-172812592-3, 2019, p. 252-257.

[4] V. Lysenko, Y. Gunchenko, S. Shvorov, S. Lenkov, S. Kuznichenko, E. Lenkov. Methodological Bases of Construction of Intensive Training Flight Simulators of Aircrews. *Proceedings 5th International Conference “Methods and Systems of Navigation and Motion Control”,* ISBN: 978-153865870-3, p. 198 – 203.

[5] First Person View (FPV), Available at: https://ru.wikipedia.org/wiki/First_Person_View_(FPV), accessed December 2020

[6] INAV Flight Missions, Available at: https://github.com/iNavFlight/inav/wiki/iNavFlight-Missions, accessed November 2020.

[7] Modes, Available at: https://github.com/iNavFlight/inav/wiki/Modes, accessed November 2020.

[8] INAV Configurator 2.5.0, Available at: https://github.com/iNavFlight/inav-configurator/releases/tag/2.5.0, accessed October 2020.

[9] S. Lienkov, A. Myasischev, O. Banzak, Y. Husak, I. Starynski. Use of rescue mode for UAV on the basis of STM32 microcontrollers. *International Journal of Advanced Trends in Computer Science and Engineering.* Vol. 9, No.3, ISSN 2278-3091, p. 3506-3513, DOI: 10.30534/ijatcse/2020/156932020.

[10] A. A. Myasishchev. Features of Implement of INAV Firmware On Omnibusf4v3 Flight Controller for Rotor Type UAV, Khmelnytskyi: ХНУ, № 2, 2020, p. 126-134.

[11] N. Pasichnyk, S. Lienkov, S. Shvorov, L. Komarova, D. Komarchuke, O. Opryshko. The use of UAVs with the "Slantrange" sensor system to estimation crop safety base on technological stress and intoxication of plants. *Information Security*. №45, ISSN: 0861-5160, p. 21-33, 2020, DOI: 10.11610/isij4502.

[12] The Basics of Getting iNav Working on an Airplane, Available at: https://github.com/iNavFlight/inav/wiki/Fixed-wing-guide, accessed December 2020 .

[13] Serhii Lienkov, Oksana Banzak, Yuriy Husak, Ihor Muliar, Viktor Cheshun, Evgeny Lenkov. The Development of an Intelligent Complex of Radiation-Technological Control of a Safety Barrier. *International Journal of Emerging Trends in Engineering Research.* Vol. 8., No. 7, ISSN 2347 – 3983, p. 3483-3486, 2020, DOI: 10.30534/ijeter/2020/97872020.

[14] S. Lienkov, G. Zhyrov, O. Sieliukov, I. Tolok, A.-S. M. Talib, I. Pampukha. Calculation of Reliability Indicators of Unmanned Aerial Vehicle Class 'μ' taking into account Operating Conditions at the Design Stagempukha, *IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments*, ISBN: 978-172812592-3, p. 52-56, 2019.

[15] S. Lenkov, G. Zhyrov, D. Zaytsev, I. Tolok, E. Lenkov, T. Bondarenko, Y. Gunchenko, V. Zagrebnyuk, O. Antonenko. Features of modeling failures of recoverable complex technical objects with a hierarchical constructive structure. *Eastern European Journal of Advanced Technology.* №4/4(88), p. 34 – 42, DOI:10.15587/1729-4061.2017.108395.

[16] G. Zhyrov, S. Lienkov, Yu. Husak, H. Banzak, I. Tolok. Analysis of problem optimization of parameters maintenance process according to state with constant periodicity of control. *International Journal of Emerging Trends in Engineering Research*. Vol. 8, No. 6, ISSN 2347–3983, DOI: 10.30534/ijeter/2020/63862020.

[17] S. Lienkov, O. Sieliukov, E. Lienkov, I. Tolok, V. Loza. Evolution of Radars Resolution Capability Using Simulation Mathematical Model. *Proceedings 5th International Conference "Methods and Systems of Navigation and Motion Control",* ISBN: 978-153865870-3, 2018, p. 195 – 197.

[18] S. Lienkov, A. Myasischev, O. Banzak, L. Komarova, N. Lytvynenko, O. Miroshnichenko. Construction of an Aircraft-Type UAV for Flight Along a Given Trajectory in the Automatic Mode. *International Journal of Emerging Trends in Engineering Research*. Vol. 8, No. 9, ISSN 2347 - 3983, DOI: 10.30534/ijeter/2020/200892020.

[19] A. Myasishchev. Possibilities of the CC3D Flight Controller with INAV Firmware, *Visnik KhN, Technical sciences*, №1, 2019, p. 129-136.

[20] Failsafe quick setup for APM with Flysky-i6 Setup arducopter failsafe, available at: https://www.youtube.com/watch?v=aZ1A5rAK0uo&t=127s.

[21] S. Lienkov, A. Myasischev, L. Komarova, N. Lytvynenko, V. Shvab, O. Lytvynenko. Creation of a Rotor-Type UAV with Flight Controllers, Based On a ATmega2560 and STM32f405

Microprocessors. *International Journal of Emerging Trends in Engineering Research*. Vol. 8, No. 8, ISSN 2347 – 3983, DOI: 10.30534/ijeter/2020/104882020.

[22] Google Earth, Available at: https://en.wikipedia.org/wiki/Google_Earth, accessed December 2020.

ЗАГАЛЬНІ ПИТАННЯ

УДК 004

д.т.н., проф. **Боровик О.В.** (АДПСУ)
д.пед.н., проф. **Боровик Л.В.** (НАДПСУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-13

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ПЕРСПЕКТИВНИХ МОДЕЛЕЙ ОСВІТНЬОЇ ПІДГОТОВКИ ПЕРСОНАЛУ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ: РЕЗУЛЬТАТИВНИЙ АСПЕКТ

На даний час перед військовою освітою визначено низку важливих завдань, зокрема: розвиток воєнної науки та підготовка особового складу на основі принципів і стандартів НАТО; підготовка офіцерського, сержантського та старшинського складу за євроатлантичними стандартами; трансформація військової освіти, в основу якої покладається набуття нових освітніх і професійних компетентностей військовослужбовцями; перехід на програми, які сумісні з програмами закладів освіти держав – членів НАТО та держав – партнерів НАТО. Виконання визначених завдань має бути забезпечене суб'єктами сектору безпеки і оборони України, до числа яких відноситься і Державна прикордонна служба України (ДПСУ).

В останній період науковцями та керівництвом ДПСУ була приділена значна увага питанням удосконалення системи відомчої освіти. Результатом дослідження її стану, шляхів і механізмів удосконалення стала Концепція трансформації освітньої підготовки персоналу ДПСУ, у рамках якої опрацьовано перспективні моделі освітньої підготовки здобувачів освіти, які навчаються за різними рівнями вищої освіти та спеціальностями.

Однак прийняття рішення щодо доцільності реалізації запропонованих перспективних моделей передбачає оцінку їх ефективності з різних позицій, зокрема, правової, кадрової, фінансової тощо. Особливої ваги при цьому набуває оцінка за результативним аспектом. Слід проте зазначити, що така оцінка на даний час відсутня і, що найбільш проблемно, відсутнє саме розуміння того, як її можна здійснити.

У статті опрацьовано методичний підхід до оцінки ефективності реалізації перспективних моделей освітньої підготовки персоналу ДПСУ з позиції результативного аспекту. При його обгрунтуванні запропоновані технології формування удосконалених програм прикордонної і військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ, формування переліку (комплексу) задач, які спроможні вирішувати підрозділи охорони державного кордону (ПОДК) за результатами реалізації удосконалених програм підготовки, здійснення порівняльної оцінки задач, які спроможні вирішувати ПОДК. Крім цього, здійснено попередню оцінку результатів реалізації програм підготовки перспективних моделей.

Ключові слова: освітня підготовка персоналу; трансформація військової освіти; концепція; перспективна модель; оцінка ефективності; Державна прикордонна служба України; результативний аспект.

Вступ. На сьогодні проблеми національної безпеки загострилися не лише для України, а й для інших країн Європи та світу. Це пов'язано із змінами глобального безпекового середовища, яке містить у собі велику кількість загроз і викликів різного характеру. Зважаючи на це, питання забезпечення належного рівня національної безпеки є одним із найбільш пріоритетних для України. Для його вирішення держава та суспільство, з урахуванням геополітичного становища країни, зробили свій вибір і поступально здійснюють рух у напрямку інтеграції в Організацію Північноатлантичного договору (НАТО).

Постановка проблеми у загальному вигляді. При цьому пріоритети воєнної політики держави зорієнтувались на здійснення заходів оборонної реформи, спрямованої на посилення спроможностей сил оборони, підвищення їх готовності до виконання завдань за призначенням та участі у проведенні спільних із підрозділами НАТО бойових дій (операцій) [1]. Одним із

актуальних завдань, вирішення яких сприятиме заходам оборонної реформи, є забезпечення ефективної підготовки військових фахівців.

Стратегічний оборонний бюлетень України [1] визначає низку важливих завдань перед військовою освітою. До числа таких, зокрема, відносяться:

розвиток воєнної науки та підготовка особового складу на основі принципів і стандартів НАТО;

підготовка офіцерського, сержантського та старшинського складу за євроатлантичними стандартами;

трансформація військової освіти, в основу якої покладається набуття нових освітніх і професійних компетентностей військовослужбовцями;

перехід на програми, які сумісні з програмами закладів освіти держав – членів НАТО та держав – партнерів НАТО, зокрема щодо оволодіння іноземною мовою на рівні не нижче СМР-2.

Виконання визначених завдань має бути забезпечене суб'єктами сектору безпеки і оборони України, до числа яких відноситься і Державна прикордонна служба України (ДПСУ).

Аналіз останніх досліджень і публікацій. Саме тому науковцями та керівництвом ДПСУ питанням пошуку шляхів удосконалення відомчої системи освіти приділяється значна увага. Підтвердженням цього є аналіз ряду актуальних питань, що наведений у працях [3-5].

Так, у роботі [3] представлено результати аналізу системи освітньої підготовки персоналу в ДПСУ, діючого варіанту реалізації освітньої підготовки у відомчому вищому військовому навчальному закладі (ВВНЗ), діючих моделей підготовки здобувачів освіти в навчальних закладах ДПСУ, а також проблем, що потребують розв'язання в кожному з них.

Праця [4] присвячена обгрунтуванню необхідності удосконалення освітньої підготовки персоналу складових сектору безпеки і оборони України, загалом, і ДПСУ, зокрема. У ній наведено результати аналізу актуальних на даний час для освіти та військової освіти положень, що мають бути враховані, як початкові умови при формуванні шляхів і способів розв'язання актуальних проблем освітньої підготовки персоналу ДПСУ в контексті трансформації військової освіти, теоретично можливих шляхів вирішення актуальних проблем, перспективних моделей освітньої підготовки в навчальних закладах ДПСУ, способів вирішення актуальних проблем.

У статті [5] визначено перелік нормативно-правових документів, що повинні бути враховані при оцінці механізмів реалізації шляхів і способів удосконалення освітньої підготовки персоналу ДПСУ в умовах трансформації військової освіти, здійснено оцінку базових положень, що повинні бути прийняті до уваги при цьому, чітко визначено мету і строки реалізації досліджуваного завдання, а також здійснено прогноз очікуваних результатів.

Дослідницька робота, що проведена колективом науковців і керівництва ДПСУ, дозволила сформувати проєкт Концепції трансформації освітньої підготовки персоналу ДПСУ, в якій знайшли відображення бачення щодо адаптації системи відомчої освіти до викликів, що стосуються розбалансування системи національної безпеки. В основі Концепції знаходяться перспективні моделі освітньої підготовки персоналу ДПСУ.

Однак їх реалізація потребує попередньої оцінки ефективності окреслених у Концепції підходів. Така оцінка передбачає аналіз за різними аспектами – зокрема, правовим, кадровим, фінансовим. Проте, найбільш важливим є аспект результативності Концепції. Саме він має бути покладений в основу прийняття позитивного рішення щодо реалізації Концепції.

Слід відмітити, що така оцінка на даний час відсутня і, що найбільш проблемно, відсутнє саме розуміння того, як можна оцінити результативний аспект Концепції.

Саме тому **метою даної статті** є опрацювання методичного підходу до оцінки ефективності реалізації перспективних моделей освітньої підготовки персоналу ДПСУ з позиції результативного аспекту.

Виклад основного матеріалу дослідження. Для досягнення визначеної мети вбачається за доцільне: запропонувати технології формування удосконалених програм прикордонної і

військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ, формування переліку (комплексу) задач, які спроможні вирішувати підрозділи охорони державного кордону (ПОДК) за результатами реалізації удосконалених програм підготовки, здійснення порівняльної оцінки задач, які спроможні вирішувати ПОДК за результатами реалізації відповідних програм підготовки; здійснити попередню оцінку результатів реалізації програм підготовки перспективних моделей.

Технологія формування удосконалених програм прикордонної і військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ.

Для формування удосконалених програм прикордонної і військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ необхідно врахувати той факт, що удосконалені програми мають бути сформовані на основі діючих програм підготовки, в яких знайшов відображення не лише сучасний стан розвитку відомчої освіти і науки, а й досвід виконання завдань ПОДК в АТО та ООС. Крім цього, у програмі прикордонної підготовки мають бути враховані положення Уніфікованої програми підготовки прикордонників країн ЄС (ССС), а в програмі військової підготовки мають бути враховані положення програм лідерських курсів (L-курсів), що сформовані за стандартами НАТО.

Технологічну схему формування удосконалених програм прикордонної і військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ можна оцінити з табл. 1.

Таблиця 1

Технологічна схема формування удосконалених програм прикордонної і військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ

Вид програм, що є джерелом удосконалення системи освітньої підготовки персоналу ДПСУ в умовах трансформації військової освіти	Уніфікована програма підготовки прикордонників країн ЄС - ССС	Програми L-курсів
Операційна дія	Порівняння	Порівняння
Вид програм підготовки в рамках реалізації діючих моделей освітньої підготовки персоналу ДПСУ (див. робочі програми навчальних дисциплін, що визначають вид прикордонної або військової підготовки)	$Пр_{пп}^{Д}$ - програма прикордонної підготовки персоналу згідно діючої моделі	$В_{пп}^{Д}$ - програма військової підготовки персоналу згідно діючої моделі
Операційна дія	Удосконалення програм підготовки персоналу згідно діючої моделі за результатами їх порівняння з відповідними програмами джерел удосконалення	
Вид удосконалених програм підготовки в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ	$Пр_{пп}^{П}$ - програма прикордонної підготовки персоналу згідно перспективної моделі	$В_{пп}^{П}$ - програма військової підготовки персоналу згідно перспективної моделі

Технологія формування переліку (комплексу) задач, які спроможні вирішувати ПОДК за результатами реалізації удосконалених програм підготовки.

Для визначення переліку (комплексу) задач, які спроможні вирішувати ПОДК за результатами реалізації удосконалених програм підготовки, необхідно врахувати той факт, що задачі визначаються наступними складовими: функціями ДПСУ, що відображені в Законі

України «Про Державну прикордонну службу України»; переліком компетентностей випускника відомчого ВВНЗ, які відображені в Стандарті вищої освіти зі спеціальності, за якою здійснюється підготовка в відомчому ВВНЗ; переліком компетентностей і програмних результатів навчання, які відображені в освітньо-професійній програмі (ОПП) зі спеціальності, за якою здійснюється підготовка в відомчому ВВНЗ; вміннями за результатами вивчення дисциплін, що наведені в робочих програмах навчальних дисциплін, які входять до переліку освітніх компонент ОПП і визначають відповідну програму підготовки в рамках реалізації діючої або перспективної моделей освітньої підготовки персоналу ДПСУ.

Технологічну схему формування переліку (комплексу) задач, які спроможні вирішувати ПОДК за результатами реалізації удосконалених програм підготовки, можна оцінити з табл. 2.

Таблиця 2

Технологічна схема формування переліку (комплексу) задач, які спроможні вирішувати ПОДК за результатами реалізації удосконалених програм підготовки

<table>
<tr><th>Перелік документів, що визначають зміст задач, які спроможні вирішувати ПОДК за результатами реалізації програм підготовки, Перелік 1</th><th>Операційна дія</th><th>Вид програм підготовки в рамках реалізації моделей освітньої підготовки персоналу ДПСУ</th><th>Операційна дія</th><th colspan="2">Перелік (комплекс) задач, які спроможні вирішувати ПОДК за результатами реалізації програм підготовки, Перелік 2</th></tr>
<tr><td>Про Державну прикордонну службу України: Закон України від 3 квіт. 2003 р. № 661-IV. Відомості Верховної Ради України. 2003. № 27. Ст. 208. Зі змінами ; ост. ред. 13 січ. 2011 р.</td><td rowspan="3">Аналіз документів з Переліку 1 і програм підготовки, порівняння складових з Переліку 1 із програмами підготовки</td><td>$Пр_{пп}^{Д}$</td><td rowspan="3">Формування (синтез) переліку (комплексу) задач, які спроможні вирішувати ПОДК за результатами реалізації програм підготовки, на основі аналізу вмінь, що формуються під час вивчення відповідних дисциплін, або реалізації ОПП</td><td>$Пз_{Пр_{пп}^{Д}}$</td><td rowspan="3">$Пз_{Пр_{пп}^{Д}+В_{пп}^{Д}}$</td></tr>
<tr><td>Стандарт вищої освіти зі спеціальності, за якою здійснюється підготовка в НАДПСУ</td><td>$В_{пп}^{Д}$</td><td>$Пз_{В_{пп}^{Д}}$</td></tr>
<tr><td>Освітньо-професійна програма зі спеціальності, за якою</td><td>$Пр_{пп}^{П}$</td><td>$Пз_{Пр_{пп}^{П}}$</td><td>$Пз_{Пр_{пп}^{П}+В_{пп}^{П}}$</td></tr>
</table>

здійснюється підготовка в НАДПСУ					
Робочі програми навчальних дисциплін, що входять до переліку освітніх компонент ОПП і визначають відповідну програму підготовки в рамках реалізації діючої або перспективної моделей освітньої підготовки персоналу ДПСУ		$В_{пп}^{П}$		$ПЗ_{В_{пп}^{П}}$	

У табл. 2 використані наступні умовні позначення:

$ПЗ_{Пр_{пп}^{Д}}$ - перелік задач, які спроможні вирішувати ПОДК за результатами реалізації програми прикордонної підготовки персоналу згідно діючої моделі;

$ПЗ_{В_{пп}^{Д}}$ - перелік задач, які спроможні вирішувати ПОДК за результатами реалізації програми військової підготовки персоналу згідно діючої моделі;

$ПЗ_{Пр_{пп}^{Д}+В_{пп}^{Д}}$ - перелік задач, які спроможні вирішувати ПОДК за результатами реалізації програм військово-прикордонної підготовки персоналу згідно діючої моделі;

$ПЗ_{Пр_{пп}^{П}}$ - перелік задач, які спроможні вирішувати ПОДК за результатами реалізації програми прикордонної підготовки персоналу згідно перспективної моделі;

$ПЗ_{В_{пп}^{П}}$ - перелік задач, які спроможні вирішувати ПОДК за результатами реалізації програми військової підготовки персоналу згідно перспективної моделі;

$ПЗ_{Пр_{пп}^{П}+В_{пп}^{П}}$ - перелік задач, які спроможні вирішувати ПОДК за результатами реалізації програм військово-прикордонної підготовки персоналу згідно перспективної моделі.

Технологія здійснення порівняльної оцінки задач, які спроможні вирішувати ПОДК за результатами реалізації відповідних програм підготовки.

Для здійснення порівняльної оцінки задач, які спроможні вирішувати ПОДК за результатами реалізації відповідних програм підготовки, необхідним є порівняння відповідних пар $ПЗ_{Пр_{пп}^{Д}}$ і $ПЗ_{Пр_{пп}^{П}}$, $ПЗ_{В_{пп}^{Д}}$ і $ПЗ_{В_{пп}^{П}}$, $ПЗ_{Пр_{пп}^{Д}+В_{пп}^{Д}}$ і $ПЗ_{Пр_{пп}^{Д}+В_{пп}^{Д}}$, та виокремлення за результатами порівняння переліку додаткових задач, які будуть спроможними виконувати ПОДК за результатами реалізації перспективних моделей, а також додаткових компетентностей, якими оволодіє випускник відомчого ВВНЗ.

Технологічну схему здійснення порівняльної оцінки задач, які спроможні вирішувати ПОДК за результатами реалізації відповідних програм підготовки, можна оцінити з табл. 3.

Таблиця 3

Технологічна схема здійснення порівняльної оцінки задач, які спроможні вирішувати ПОДК за результатами реалізації відповідних програм підготовки

Перелік (комплекс) задач, які спроможні вирішувати ПОДК за результатами реалізації програм підготовки діючої моделі	**Операційна дія**	**Перелік (комплекс) задач, які спроможні вирішувати ПОДК за результатами реалізації програм підготовки перспективної моделі**	**Операційна дія**	**Висновки з порівняння (результат виявлення відмінностей)**	
				Перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації перспективної моделі	**Перелік додаткових компетентностей персоналу ПОДК за результатами реалізації перспективної моделі**
$Пз_{Пр_{пп}^{Д}}$	Порівняння	$Пз_{Пр_{пп}^{П}}$	Виявлення відмінностей	$\Delta Пз_{Пр}$	$\Delta К_{Пр}$
$Пз_{В_{пп}^{Д}}$		$Пз_{В_{пп}^{П}}$		$\Delta Пз_{В}$	$\Delta К_{В}$
$Пз_{Пр_{пп}^{Д}+В_{пп}^{Д}}$		$Пз_{Пр_{пп}^{П}+В_{пп}^{П}}$		$\Delta Пз_{Пр+В}$	$\Delta К_{Пр+В}$

У табл. 3 використані наступні умовні позначення:

$\Delta Пз_{Пр}$ - перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації програми прикордонної підготовки перспективної моделі;

$\Delta Пз_{В}$ - перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації програми військової підготовки перспективної моделі;

$\Delta Пз_{Пр+В}$ - перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації програми військово-прикордонної підготовки перспективної моделі;

$\Delta К_{Пр}$ - перелік додаткових компетентностей персоналу ПОДК за результатами реалізації програми прикордонної підготовки перспективної моделі;

$\Delta К_{В}$ - перелік додаткових компетентностей персоналу ПОДК за результатами реалізації програми військової підготовки перспективної моделі;

$\Delta К_{Пр+В}$ - перелік додаткових компетентностей персоналу ПОДК за результатами реалізації програми військово-прикордонної підготовки перспективної моделі.

Наведені в табл. 1-3 технологічні схеми формування програм, переліку (комплексу) задач і здійснення їх порівняльної оцінки, дозволяють запропонувати механізм змістовного наповнення перспективних моделей освітньої підготовки персоналу ДПСУ, який можна оцінити з табл. 4.

Таблиця 4

Механізм змістовного наповнення перспективних моделей освітньої підготовки персоналу ДПСУ

Вид моделі освітньої підготовки персоналу ДПСУ	**Вид програм підготовки в рамках реалізації моделей освітньої підготовки персоналу ДПСУ**	**Перелік (комплекс) задач, які спроможні вирішувати ПОДК за результатами реалізації програм підготовки**	
Діюча	$Пр_{пп}^{Д}$	$Пз_{Пр_{пп}^{Д}}$	$Пз_{Пр_{пп}^{Д}+В_{пп}^{Д}}$
	$В_{пп}^{Д}$	$Пз_{В_{пп}^{Д}}$	
Перспективна	$Пр_{пп}^{П}$	$Пз_{Пр_{пп}^{П}}$	$Пз_{Пр_{пп}^{П}+В_{пп}^{П}}$
	$В_{пп}^{П}$	$Пз_{В_{пп}^{П}}$	

Результати (висновки з) порівняльної оцінки задач, які спроможні вирішувати ПОДК за результатами реалізації відповідних програм підготовки					
$Пз_{Пр_{пп}^{Д}} <> Пз_{Пр_{пп}^{П}}$		$Пз_{В_{пп}^{Д}} <> Пз_{В_{пп}^{П}}$		$Пз_{Пр_{пп}^{Д}+В_{пп}^{Д}} <> Пз_{Пр_{пп}^{П}+В_{пп}^{П}}$	
Перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації перспективної моделі (висновки з порівняння)	**Перелік додаткових компетентностей персоналу ПОДК за результатами реалізації перспективної моделі (висновки з порівняння)**	**Перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації перспективної моделі (висновки з порівняння)**	**Перелік додаткових компетентностей персоналу ПОДК за результатами реалізації перспективної моделі (висновки з порівняння)**	**Перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації перспективної моделі (висновки з порівняння)**	**Перелік додаткових компетентностей персоналу ПОДК за результатами реалізації перспективної моделі (висновки з порівняння)**
$\Delta Пз_{Пр}$	$\Delta К_{Пр}$	$\Delta Пз_{В}$	$\Delta К_{В}$	$\Delta Пз_{Пр+В}$	$\Delta К_{Пр+В}$

Попередня оцінка результатів реалізації програм підготовки перспективних моделей.

Проведений аналіз і запропоновані технології формування удосконалених програм прикордонної і військової підготовки персоналу в рамках реалізації перспективних моделей освітньої підготовки персоналу ДПСУ, формування переліку (комплексу) задач, які спроможні вирішувати ПОДК за результатами реалізації удосконалених програм підготовки, технології здійснення порівняльної оцінки вказаних задач, дозволяють здійснити попередню оцінку результатів реалізації удосконалених програм підготовки перспективних моделей.

Для цього слід лише врахувати перелік очікуваних результатів реалізації Концепції трансформації освітньої підготовки персоналу ДПСУ та оцінити можливість їх досягнення за рахунок появи наступного переліку додаткових задач і компетентностей: $\Delta Пз_{Пр}$, $\Delta К_{Пр}$, $\Delta Пз_{В}$, $\Delta К_{В}$, $\Delta Пз_{Пр+В}$, $\Delta К_{Пр+В}$.

Прогнозований результат такої оцінки можна оцінити з табл. 5.

Таблиця 5

Попередня оцінка результатів реалізації програм підготовки перспективних моделей

Додаткові можливості ПОДК за результатами реалізації перспективної моделі		**Очікувані результати реалізації Концепції трансформації освітньої підгтовки персоналу ДПСУ**		
		Результат 1 - професіоналізація персоналу для ефективного виконання функцій ДПСУ	**Результат 2 - досягнення максимальної взаємосумісності складових сектору безпеки і оборони з відповідними органами держав – членів НАТО**	**Результат 3 - посилення спроможості ДПСУ щодо забезпечення недоторканності державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні**
Перелік додаткових задач, які будуть спроможні виконувати ПОДК за результатами реалізації перспективної моделі	$\Delta ПЗ_{Пр}$			Посилення
	$\Delta ПЗ_{В}$		Покращення	
	$\Delta ПЗ_{Пр+В}$		Покращення	Посилення
Перелік додаткових компетентностей персоналу ПОДК за результатами реалізації перспективної моделі	$\Delta К_{Пр}$	Покращення		
	$\Delta К_{В}$	Покращення		
	$\Delta К_{Пр+В}$	Покращення		

Висновки й перспективи подальших досліджень. Таким чином, за результатами проведеного дослідження можна зробити висновок про те, що запропонований підхід є методичним інструментарієм оцінки ефективності реалізації перспективних моделей освітньої підготовки персоналу ДПСУ з позиції результативного аспекту, які опрацьовані в рамках реалізації Концепції.

Перспективами подальших досліджень авторам вбачається безпосередньо застосування запропонованого методичного підходу для проведення оцінки ефективності Концепції трансформації освітньої підготовки персоналу ДПСУ за результативним аспектом.

ЛІТЕРАТУРА:

1. Указ президента України №473/2021 Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України».

2. Про національну безпеку України. Закон України 21 червня 2018 року № 2469-VIII Відомості Верховної Ради України, 2018, № 31, ст.241.

3. Левадний І. А., Фігура О. В., Боровик О. В. Стан та актуальні проблеми освітньої підготовки персоналу Державної прикордонної служби України в контексті трансформації військової освіти. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: педагогічні науки*, 28 (1), частина 1. Ст. 105-127. URL https://periodica.nadpsu.edu.ua/index.php/pedzbirnyk. (дата звернення: 16.02.2022)

4. Сердюк С. І., Луцький О. Л., Боровик О. В. Шляхи та способи розв'язання актуальних проблем освітньої підготовки персоналу Державної прикордонної служби України в контексті трансформації військової освіти. *Збірник наукових праць Національної академії Державної прикордонної служби*

України. Серія: педагогічні науки, 28 (1), частина 1. Ст. 194-221. URL https://periodica.nadpsu.edu.ua/index.php/pedzbirnyk. (дата звернення: 16.02.2022)

5. Васильчук І. І., Коваль Б. М., Боровик О. В. Нормативно-правові і технологічні засади вдосконалення освітньої підготовки персоналу Державної прикордонної служби України в контексті трансформації військової освіти. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: педагогічні науки*, 28 (1), частина 1. Ст. 5-19. URL https://periodica.nadpsu.edu.ua/index.php/pedzbirnyk. (дата звернення: 16.02.2022)

REFERENCES:

1. Ukaz prezydenta Ukrai'ny №473/2021 Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 20 serpnja 2021 roku «Pro Strategichnyj oboronnyj bjuleten' Ukrai'ny».

2. Pro nacional'nu bezpeku Ukrai'ny. Zakon Ukrai'ny 21 chervnja 2018 roku № 2469-VIII Vidomosti Verhovnoi' Rady Ukrai'ny, 2018, № 31, st.241.

3. Levadnyj I. A., Figura O. V. and Borovyk O. V. (2022), "Stan ta aktual'ni problemy osvitn'oi' pidgotovky personalu Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny v konteksti transformacii' vijs'kovoi' osvity". *Zbirnyk naukovyh prac' Nacional'noi' akademii' Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny. Serija: pedagogichni nauky*, 28 (1), chastyna 1. Pp. 105-127. URL https://periodica.nadpsu.edu.ua/index.php/pedzbirnyk. (data zvernennja: 16.02.2022)

4. Serdjuk S. I., Luc'kyj O. L. and Borovyk O. V. (2022), "Shljahy ta sposoby rozv'jazannja aktual'nyh problem osvitn'oi' pidgotovky personalu Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny v konteksti transformacii' vijs'kovoi' osvity". *Zbirnyk naukovyh prac' Nacional'noi' akademii' Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny. Serija: pedagogichni nauky*, 28 (1), chastyna 1. Pp. 194-221. URL https://periodica.nadpsu.edu.ua/index.php/pedzbirnyk. (data zvernennja: 16.02.2022)

5. Vasyl'chuk I.I., Koval' B.M. and Borovyk O.V. (2022), "Normatyvno-pravovi i tehnologichni zasady vdoskonalennja osvitn'oi' pidgotovky personalu Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny v konteksti transformacii' vijs'kovoi' osvity". *Zbirnyk naukovyh prac' Nacional'noi' akademii' Derzhavnoi' prykordonnoi' sluzhby Ukrai'ny. Serija: pedagogichni nauky*, 28 (1), chastyna 1. Pp. 5-19. URL https://periodica.nadpsu.edu.ua/index.php/pedzbirnyk. (data zvernennja: 16.02.2022)

Prof. Borovyk O.V., prof. Borovyk L.V.

METHODICAL APPROACH TO ASSESSING THE EFFECTIVNESS OF THE PROMISING MODELS IMPLEMENTATION OF PERSONNEL TRAINING OF STATE BORDER GUARD SERVICE OF UKRAINE: THE EFFECTIVE ASPECT

At present, military education has a number of important tasks, including: the development of military science and the training of personnel based on NATO principles and standards; training of officers, sergeants and non-commissioned officers according to Euro-Atlantic standards; transformation of military education, which is based on the acquisition of new educational and professional competencies by servicemen; transition to programs that are compatible with the programs of educational institutions of NATO member states and NATO partner countries. The fulfillment of certain tasks should be ensured by the subjects of the security and defense sector of Ukraine, including the State Border Guard Service of Ukraine (SBGS). Recently, scientists and the leadership of the SBGS have paid considerable attention to improving the departmental education system. The result of the study of its condition, ways and mechanisms of improvement was the Concept of transformation of educational training of SBGS staff, which developed promising models of educational training of students studying at different levels of higher education and specialties. However, the decision on the feasibility of implementing the proposed promising models involves assessing their effectiveness from different positions, in particular, legal, personnel, financial and so on. Of particular importance is the evaluation of the performance aspect. It should be noted, however, that such an assessment is currently lacking and, most problematically, there is no understanding of how it can be carried out. The article develops a methodical approach to assessing the effectiveness of the implementation of promising models of educational training of SBGS staff from the standpoint of performance. At its substantiation technologies of formation of the improved programs of frontier and military preparation of the personnel within the limits of realization of perspective models of educational preparation of the personnel of SBGS, formation of the list (complex) of tasks which are capable to solve divisions of protection of the state border (PODK). tasks that can be solved by PODK. In addition, a preliminary assessment of the results of the implementation of programs for the preparation of promising models.

Key words: educational training of personnel; transformation of military education; concept; perspective model; evaluation of efficiency; State Border Guard Service of Ukraine; performance aspect.

УДК 35.082.38

к.т.н. **Гришин С.П.** (НМЦ КП МОУ)
к.псих.н **Зубовський Д.С.** (НМЦ КП МОУ)
Ряба Л.О. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/74-14

РОЛЬ ТА МІСЦЕ КАДРОВОЇ БЕЗПЕКИ В СИСТЕМІ ВІЙСЬКОВОЇ КАДРОВОЇ ПОЛІТИКИ

Проблема кадрової безпеки є особливо актуальною для Міністерства оборони та Збройних Сил України. Сучасна суспільно-політична обстановка, що склалася у нашій країні, як ніколи вимагає як створення надійної системи кадрової безпеки так і пошуку та впровадження принципово нових форм та методів її забезпечення.

Формування військової кадрової політики України відбувається в період нових форм військових конфліктів, «гібридних війн», трансформації способів ведення бойових дій, інформаційних війн, політичними ускладненнями євроінтеграційного процесу України тощо. Кадрову безпеку в системі військової кадрової політики розглянуто з позицій цільового, процесного, структурного і функціонального підходів у контексті забезпечення економічної безпеки. Разом з тим, кадрова безпека у сфері оборони держави, в першу чергу, покликана вирішувати завдання національної безпеки, що накладає свої специфічні вимоги до її вивчення. Окреслено основні загрози з боку персоналу МО та ЗС України. Також проаналізовано та визначено потенційні сфери зловживань і ймовірні корупційні ризики у різних сферах військової діяльності як у мирний так і у воєнний час, а також окреслено основні чинники, що сприяють появі цих ризиків у оборонній сфері.

Визначено, що кадрова безпека охоплює усі напрями розвитку військової кадрової політики Міністерства оборони, а саме: рекрутинг; управління персоналом; освіту та підготовку кадрів; соціальне та гуманітарне забезпечення персоналу, а забезпечення кадрової безпеки та зниження ризиків зі сторони персоналу залишається пріоритетним і домінуючим напрямком забезпечення комплексної безпеки у сфері оборони та одним з першочергових завдань, яке необхідно вирішувати. Питання кадрової безпеки повинні вирішуватися на кожному етапі управління персоналом (пошук, відбір, прийом, адаптація, розвиток, оцінка і т.д.). Будь-яка дія працівника служби персоналу на будь-якому етапі – це або посилення, або ослаблення безпеки військової організації по головній її складовій – по персоналу.

Ключові слова: кадрова безпека, військова кадрова політика, персонал.

Вступ та постановка проблеми (задачі). Реалії сучасного стану діяльності організації свідчать про те, що одним із найважливіших аспектів ефективної діяльності будь-якої організації виступає персонал. Практика підтверджує, що саме персонал організації є найбільшим джерелом ризиків для неї самої, адже має стосунок до усіх сфер та аспектів організаційного процесу. За даними досліджень більше трьох четвертих злочинів в організації здійснюється співробітниками, при цьому більша частина злочинів виявляється випадково. З огляду на це, першочерговим завданням, яке необхідно вирішувати будь-якій організації для її нормального функціонування, є забезпечення надійності діяльності персоналу, виявлення, зниження ризиків та загроз пов’язаних з персоналом.

Тобто, зараз перед світовою спільнотою та Україною, зокрема, постала проблема, справжні масштаби якої поки ще недостатньо усвідомлюються, і вона недостатньо досліджується. Йдеться про створення інноваційної теорії і практики державного управління, а отже, про формування управлінських кадрів, державних службовців нової генерації, здатних мислити і діяти в умовах кризового стану суспільства, коли глобалізований світ стає не тільки більш відкритим, прозорим і толерантним, але і конфліктним , небезпечним і вразливим, не тільки схожим, але і різноманітним, не тільки технологічно і інформаційно могутнім, але і бездуховним, несправедливим.

Аналіз останніх досліджень та публікацій. Кадрова безпека держави є досить новим, а тому малодослідженим напрямком забезпечення національної безпеки. Останнім часом виявляється посилення взаємозалежності кадрової політики і політики зміцнення національної безпеки України. Значний внесок у дослідження проблем кадрової безпеки на підприємствах чи суб'єктах господарювання внесли такі закордонні та вітчизняні вчені, як Панченко В.А., Шевченко М.М., Астахова Л.В., Бурда І.Я., Єгорова Л.С., Жидецька Х.В., Мішин О.Ю., Мішина С.В., Момот Т.В., Назарова Г.В., Палига Є.М., Цветкова І.І. та багато інших.

Аналіз наукових праць свідчить про те, що переважна більшість дослідників розглядає поняття кадрової безпеки в контексті забезпечення економічної безпеки організації, підприємства чи компанії. Водночас, слід зазначити, що останнім часом вітчизняне та зарубіжне наукове співтовариство все частіше стало говорити про проблему кадрової безпеки в органах державної влади та в секторі державного управління загалом, як про важливу, а можливо й найважливішу складову національної безпеки.

Так, наприклад, такі українські дослідники, як Г.П. Ситник, В.І. Абрамов, М.М. Шевченко висвітлюють проблеми кадрової безпеки в контексті удосконалення системи державного управління забезпеченням національної безпеки України. Питання сутності та змісту кадрової безпеки, її характерних рис в системі державного управління України розглядаються у працях О. Пархоменко-Куцевіл, В. Ананьїна, В. Горлинського, О.О. Пучкова. Питання кадрової безпеки в органах державної влади є предметом вивчення таких авторів, як: З.М. Бурик, С. Дембіцька, М. Кизим, В. Карковська, Н. Плахотнюк та інших вітчизняних науковців.

Питання кадрової безпеки у вітчизняних силових відомствах, зокрема у Міністерстві оборони та Збройних Силах України піднімались і у наукових працях та дослідженнях фахівців НМЦ КП МО України С.П. Гришина, Ю.С. Дмитренка, Д.С.Зубовського, М.Д. Кузьменка, В.М. Малюги та інших. Ці праці не можна вважати фундаментальними у зазначеній сфері, оскільки питання кадрової безпеки у них розглядались в контексті застосування психофізіологічних досліджень з використанням поліграфа в інтересах забезпечення кадрової безпеки у МО та ЗС України, проте вони мають свою цінність для аналізу. Автори цих праць чи не вперше в Україні піднімають проблему кадрової безпеки у силових відомствах України і наголошують на необхідності досить серозного підходу до її забезпечення.

Значний інтерес для вивчення проблеми кадрової безпеки, в контексті усвідомлення зарубіжних підходів до розуміння поняття кадрової безпеки та питань щодо її забезпечення у силових структурах, є аналіз офіційних документів, що визначають політику кадрової безпеки і процедури їх функціонування у МО і збройних силах США, проведений у наукових працях фахівців НМЦ КП МОУ [1-5] та в установчих документах.

Так, як свідчить аналіз, у Меморандумі помічника заступника міністра оборони США від 13 червня 2013 року поняття кадрова безпека визначено як галузь знань з безпеки, яка оцінює лояльність, благонадійність та надійність людей щодо первинної та триваючої оцінки придатності (відповідності) до надання доступу до закритої інформації або призначення на певні посади. З огляду на це визначення, можна стверджувати, що питання кадрової безпеки у МО та збройних силах США розглядаються переважно в контексті призначення осіб на посади, пов'язані з національною безпекою або надання їм допуску до роботи з таємною інформації. Основу забезпечення кадрової безпеки, на думку американських фахівців складають такі категорії як лояльність, благонадійність та надійність персоналу.

Політика та процедури функціонування кадрової безпеки силових структур США, як стверджують М. Кузьменко та О. Алєксєєв, вибудована як ефективний комплекс нормативно забезпечених заходів для вирішення завдань національної безпеки [3]. Ключові аспекти, особливості та процедури забезпечення кадрової безпеки у МО та збройних силах США визначені низкою окремих нормативно-правових документів, серед яких Програма кадрової безпеки МО США, впроваджена Інструкцією № 5200.02 [14] та Настанова 5200.02 "Процедури для Програми кадрової безпеки МО США" [15].

Зміст цих документів свідчить, що метою Програми кадрової безпеки є забезпечення стану, коли особи, призначені на посади національної безпеки залишаються надійними і такими, яким можна довіряти. В межах цієї програми важливим є акцент на тому, що визначення права обіймати посади у сфері національної безпеки повинне чітко відповідати інтересам національної безпеки США. Будь-які сумніви мають тлумачитися на користь національної безпеки. Жодна людина не може бути затвердженою або призначеною на посади національної безпеки, коли встановлено існування несприятливої інформації в контексті забезпечення кадрової безпеки [14].

Серед методів та засобів забезпечення кадрової безпеки у МО США значна увага приділяється використанню психофізіологічних досліджень із застосуванням поліграфа, які проводяться як на етапі відбору персоналу так і в процесі контролю за його діяльністю. Такі дослідження застосовуються в межах програми Оцінки Достовірності з метою забезпечення призначень на посади осіб, що визнані надійними й такими, яким можна довіряти, а їхнє проведення чітко регламентується низкою документів, серед яких Директива МО № 5210.48 [16], Інструкція № 5210.91 [17], Армійська настанова 195-6 [18] Армійська настанова 380–67 [19] та інші.

Аналіз наукових праць дає підстави стверджувати про досить складний і неоднозначний стан дослідженості проблем кадрової безпеки. Не зважаючи на те, що теоретичні аспекти зазначеної проблематики розглянуті багатьма вченими, єдиної точки зору, що всебічно розкриває поняття кадрової безпеки, її місця в системі комплексної безпеки і схеми процесу управління нею, до теперішнього часу немає, що підкреслює необхідність подальших наукових досліджень.

Актуальність і необхідність наукових розробок з питань кадрової безпеки підкреслюється досить високим рівнем імовірності заподіяння шкоди майновим і немайновим інтересам, масштабними втратами в разі реалізації загроз, причини яких так чи інакше пов’язані з співробітниками організації, а також відсутністю уніфікованих заходів профілактики, що дозволяють максимально наблизитися до стану абсолютної безпеки і захищеності.

Особливо актуальною проблема кадрової безпеки є і для МО та ЗС України. Сучасна суспільно-політична обстановка, що склалася у нашій країні, як ніколи вимагає як створення надійної системи кадрової безпеки так і пошуку та впровадження принципово нових форм та методів її забезпечення.

В межах цього процесу, керівництво оборонного відомства України вже здійснює низку ефективних заходів для забезпечення високого рівня кадрової безпеки та демонструє рішучість і наполегливість у здійсненні якісного відбору висококваліфікованого, доброчесного, не пов’язаного з корупційними діями у минулому, добропорядного персоналу для МО України та ЗС України. Особливо прискіплива увага приділяється відбору кандидатів для призначення на посади керівників структурних підрозділів МО України, ГШ ЗС України), органів військового управління ЗС України, що беруть участь в ООС та кандидатів на посади, які мають доступ до фінансових, матеріальних ресурсів, державної таємниці тощо. Однак, формування системи кадрової безпеки у МО та ЗС України ще не завершене. Цей процес потребує вирішення ще цілої низки питань, що стосуються інституціонального статусу кадрової безпеки, його нормативно-правового забезпечення з урахуванням вимог європейських стандартів тощо.

Виклад основного матеріалу. На протязі останніх років українськими вченими здійснено низку наукових розробок щодо проблем кадрової безпеки організації та доброчесності персоналу. Проте, ґрунтовні дослідження цих питань стосовно МО України і ЗС України знаходиться на стадії свого становлення. А питання теоретико-психологічних положень доброчесності та кадрової безпеки у МО та ЗС України у вітчизняному науковому середовищі досі залишаються недостатньо дослідженими та висвітленими, що значно актуалізує тему даної науково-дослідної роботи.

На думку науковців НМЦ КП МО України, головною метою кадрової безпеки МО України та ЗС України є забезпечення ефективності діяльності МО та ЗС України та виконання покладених на них завдань. Виходячи з цього, поняття "Кадрова безпека Міністерства оборони та Збройних Сил України" доцільно розглядати як стан, при якому мінімізовані ризики та загрози, пов'язані з персоналом, які можуть негативно вплинути на ефективність діяльності МО і ЗС України та виконання покладених на них завдань. А під поняттям "Забезпечення кадрової безпеки Міністерства оборони та Збройних Сил України" слід розуміти процес запобігання негативним впливам на діяльність МО і ЗС України та виконання ними покладених завдань за рахунок здійснення комплексу заходів, спрямованих на попередження та мінімізацію ризиків і загроз, пов'язаних з персоналом [4, 5].

Дослідники вважають, що фактично забезпечення кадрової безпеки – це процес попередження та мінімізації ризиків і загроз з боку свого персоналу, який включає в себе: підбір досвідчених і благонадійних співробітників; контроль благонадійності та лояльності персоналу в динаміці; своєчасне виявлення і локалізація причин і обставин загроз; відсіювання тих, хто створює певні загрози діяльності.

Передумовами виникнення загроз кадрової безпеки можуть стати, наприклад, значний спад в економічній сфері, який відбувся за перші роки незалежності держави, а також зниження ефективності багатьох галузей народного господарства, погіршення геополітичного становища України, важка демографічна криза, руйнування національно-патріотичної складової в духовному житті, особливо у молодого покоління.

Переважна більшість дослідників розглядає кадрову безпеку з позицій цільового, процесного, структурного і функціонального підходів у контексті забезпечення економічної безпеки. Разом з тим, кадрова безпека у сфері оборони держави, в першу чергу, покликана вирішувати завдання національної безпеки, що накладає свої специфічні вимоги до її вивчення.

У цьому контексті, кадрову безпеку у сфері оборони слід розглядати у вузькому та широкому змістах. У вузькому змісті – це захист персоналу органів влади та силових структур держави, забезпечення його розвитку, самореалізації, самовдосконалення. У широкому змісті – це сукупність методів, механізмів, прийомів, які забезпечують захищеність силових структур і самої держави в цілому від загроз непрофесіоналізму, деструктивного професіоналізму, корупційних проявів, зловживання службовим становищем, осіб, які мають приховані негативні мотиви вступу на військову чи державну службу, незаконні (несанкціоновані) зв'язки з установами ворожих держав, представниками терористичних організацій та кримінального середовища, наркотичну чи алкогольну залежність, схильні до розголошення відомостей, що становлять державну таємницю, службову або конфіденційну інформацію та інше.

Фактично, забезпечення кадрової безпеки – це процес попередження та мінімізації ризиків і загроз з боку свого персоналу, який включає в себе: підбір досвідчених і благонадійних співробітників; контроль благонадійності та лояльності персоналу в динаміці; своєчасне виявлення і локалізація причин і обставин загроз; відсіювання тих, хто створює певні загрози діяльності [4].

До основних загроз з боку персоналу МО та ЗС України, на думку науковців НМЦ КП МО України, можна віднести такі: зв'язок з установами ворожих держав, представниками терористичних організацій та кримінального середовища; зловживання службовим становищем; здійснення корупційних діянь; наркотичну чи алкогольну залежність; розголошення відомостей, що становлять державну таємницю, службову або конфіденційну інформацію; непрофесіоналізм; приховані негативні мотиви вступу на військову чи державну службу; крадіжки, зумисне псування або знищення майна; наявність боргів або фінансових зобов'язань; причетність до діянь, що передбачають юридичну відповідальність та інше [1]. Перше, що мінімізує всі ці загрози, – правильна і ефективна оцінка благонадійності кандидата. Для забезпечення цього необхідно систему відбору кандидатів на посади в підрозділи МО та ЗС України організувати з точки зору оцінки тенденції ризиків щодо деструктивної поведінки

на службі (роботі). У кадровій роботі, наголошують науковці, необхідно проводити серйозний і всебічний відбір співробітників, при якому не допускається прийом на роботу людей, які можуть нанести шкоду інтересам МО України, ЗС України та забезпеченню обороноздатності держави в цілому [5].

Цінність досліджень НМЦ КП МО України в контексті проблеми забезпечення кадрової безпеки у МО України та ЗС України полягає ще й у тому, що у них досить ґрунтовно проаналізовано та чіткого визначено потенційні сфери зловживань і ймовірні корупційні ризики у різних сферах військової діяльності як у мирний так і у воєнний час, а також окреслено основні чинники, що сприяють появі цих ризиків у оборонній сфері [4].

Оцінка ризиків у діяльності органів влади

З 2016 року в Україні запроваджена оцінка ризиків у діяльності органів влади, яка здійснюється на підставі Методології оцінювання корупційних ризиків у діяльності органів влади, затвердженої рішенням Національного агентства з питань запобігання корупції від 02.12.2016 р. № 126, зареєстрованим у Міністерстві юстиції України 28 грудня 2016 року за №1718/29848, згідно яко ї[6-13]:

- За ймовірністю виникнення ризики оцінюються за критеріями:

низької ймовірності виникнення (ризики, виникнення яких може відбутися у виняткових випадках);

середньої ймовірності виникнення (ризики, за якими існує незначна ймовірність їх виникнення);

високої ймовірності виникнення (ризики, за якими існує велика ймовірність їх виникнення).

- За впливом на спроможність суб'єктів внутрішнього контролю досягати визначені стратегічні цілі ризики оцінюються за критеріями:

низького рівня впливу. Це ризики, вплив яких є мінімальним та/або невеликої тяжкості на досягнення суб'єктами внутрішнього контролю визначених цілей.

До таких ризиків можуть бути віднесені окремі прорахунки у діяльності виконавців, несвоєчасне опрацювання окремих документів, недостатній рівень професійних знань окремих посадових осіб та інші;

середнього рівня впливу. Це ризики, вплив яких є середньої тяжкості на досягнення суб'єктами внутрішнього контролю визначених цілей. До цієї категорії ризиків може бути віднесено, зокрема, відсутність документації, неналежна якість проведення оформлення результатів інвентаризації, використання майна та ресурсів не за цільовим призначенням та інші;

високого рівня впливу. Це ризики, вплив яких є тяжким та/або особливо тяжким на досягнення суб'єктами внутрішнього контролю визначених цілей. До них, зокрема, належать нормативна неврегульованість (зарегульованість) окремих управлінських процесів, висока ймовірність корупції та шахрайства, неефективність та втрата контролю за управлінськими процесами, відсутність бухгалтерського обліку, висока плинність кадрів, невизначеність відповідальності за виконання окремих функції та інші [6].

У Міністерстві оборони України наказом Міністерства оборони України від 02.04.2019 № 145 «Про затвердження Порядку організації в системі Міністерства оборони України внутрішнього контролю та управління ризиками» усі ризики класифікуються за категоріями та за видами.

Так, за категоріями ризики поділяються на:

зовнішні - ризики, імовірність виникнення яких не пов'язана з виконанням організацією функцій і завдань;

внутрішні - ризики, імовірність виникнення яких безпосередньо пов'язана з виконанням структурними підрозділами та особовим складом покладених на неї функцій та завдань.

За видами ризики поділяються на:

кадрові - ризики, пов’язані з професійною підготовкою особового складу, якістю виконання ним функціональних обов’язків (посадових інструкцій), у тому числі ризики, пов’язані зі зниженням вмотивованості, станом їхнього здоров’я;

корупційні - це сукупність правових, організаційних та інших факторів і причин, які заохочують (стимулюють) осіб до скоєння корупційних правопорушень під час виконання ними функцій держави;

нормативно-правові - це ризики, що виникають у зв’язку з відсутністю, суперечністю або нечіткою регламентацією в законодавстві виконання функцій та завдань;

операційно-технологічні - ризики, пов’язані з порушенням визначеного порядку виконання функцій та завдань;

програмно-технічні - ризики, імовірність виникнення яких пов’язана із неналежною роботою технічних засобів та прикладного програмного забезпечення, внесенням до них змін, відповідно до законодавства або їх відсутністю;

ризики інформаційної безпеки - ризики, пов’язані із впливом на інформаційні системи, які використовуються установою, наслідком яких є порушення конфіденційності, цілісності, автентичності або доступності інформаційних ресурсів;

репутаційні - дії або події, які можуть негативно вплинути на репутацію установи чи її керівника;

фінансові - ризики, пов’язані з імовірністю втрат фінансових ресурсів (грошових коштів);

фінансово-господарські - ризики, пов’язані з неналежним ресурсним, матеріальним забезпеченням тощо;

інші ризики.

Також, у даному нормативно-правовому акті зазначається, що процес управління ризиками здійснюється з урахуванням розподілу ризиків на ***зовнішні та внутрішні***, а також з урахуванням спроможності установи реагувати на відповідні ризики, у межах наданих повноважень та компетенції:

внутрішні ризики, які оцінено в числових значеннях від 1 до 7, потребують прийняття рішень та/або вжиття заходів контролю безпосередньо в установі, в якій ідентифіковано ризики;

внутрішні ризики, які оцінено в числових значеннях від 8 до 14, потребують прийняття рішень та/або вжиття заходів контролю на рівні органів військового управління, у разі неможливості їх вирішення - на рівні керівництва установи, в якій ідентифіковано ризик;

внутрішні ризики, які оцінено в числових значеннях від 15 до 25, потребують розгляду та оцінки їх на рівні органу військового управління на предмет можливого їх систематичного характеру та вироблення способів реагування на такі ризики, а за неможливості реагування - ініціювання питання розроблення відповідальними за діяльність регламентів, або вироблення інших способів реагування;

зовнішні ризики, які оцінено в числових значеннях від 1 до 16, потребують прийняття рішень та вжиття заходів контролю на рівні відповідних органів військового управління до виду Збройних Сил включно та відповідальних за діяльність;

зовнішні ризики, які оцінено в числових значеннях від 20 до 25, потребують прийняття рішень та/або вжиття заходів контролю на рівні керівництва Генерального штабу та Міноборони [7].

З метою реалізації пріоритетних напрямків діяльності Міністерства оборони України та основних завдань, визначених на 2021-2022 роки, в частині оновлення процесів внутрішнього контролю та управління ризиками, Головною інспекцією спільно зі структурними підрозділами Міністерства оборони України та органами військового управління опрацьовано проект Плану управління ризиками Міністерства оборони України на 2021 рік [8].

У документі перелічено 28 основних напрямків діяльності Міністерства оборони України з відповідними процесами. Кожен процес відповідного напрямку передбачає певні ризики, які відображені у зазначеному Плані.

У наказі Міністерства оборони України від 14 квітня 2015 року №164 (Із змінами, внесеними згідно з Наказом Міністерства оборони № 394 від 22.07.2019) «Про затвердження Інструкції з організації та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України та Збройних Силах України» [9], у межах виконання завдання забезпечення кадрової безпеки при підготовці та прийнятті кадрових рішень щодо прийняття (поновлення) на військову службу за контрактом, призначення (переміщення) осіб офіцерського складу на посади номенклатури призначення Міністра оборони України, при вступі громадян України на державну службу на посади у структурні підрозділи МО України та ГШ ЗС України, а також для підвищення ефективності проведення службових розслідувань в МО України та ЗС України проводиться процедура психофізіологічного дослідження персоналу із застосуванням поліграфа.

Під час її проведення при підготовці та прийнятті кадрових рішень оцінюються наступні ризики:

виявлення ознак приховування чи викривлення анкетних даних, окремих фактів біографії;

ознаки алкогольної залежності, вживання наркотичних та (або) психотропних речовин без призначення лікаря;

приховані мотиви прийняття (вступу) на військову (державну) службу, призначення (переміщення) на посади номенклатури призначення Міністра оборони України;

наявність боргів або фінансових зобов'язань, причетність до діянь, що передбачають юридичну відповідальність;

вчинення об'єктом опитування протиправних дій, порушення стосовно нього кримінального провадження;

виявлення контактів з членами злочинних організацій;

виявлення участі у діяльності заборонених громадських об'єднань, членства в політичних партіях, наявності виду на проживання (іншого документа), що підтверджує право на тривале проживання на території іншої держави;

розголошення об'єктом опитування відомостей, що становлять державну таємницю, службову або конфіденційну інформацію.

А при проведенні службових розслідувань в МО України та ЗС України, для підвищення їх ефективності, у рамках процедури ПФДВП, відповідно до цього ж наказу оцінюються наступні ризики:

звужування кола ймовірно причетних осіб до події, що перевіряється;

виявлення можливості причетності об'єкта опитування до підготовки або вчинення правопорушення;

правдивість інформації, наданої об'єктом опитування;

напрями здобуття доказів про підготовку або вчинення правопорушень;

механізм і спосіб здійснення правопорушення;

підготовку до вчинення корупційних та інших протиправних дій з боку посадових осіб;

наявність боргів або фінансових зобов'язань, причетності до діянь, що передбачають юридичну відповідальність;

ознаки небезпеки, незаконних посягань, пов'язаних з виконанням об'єктом опитування посадових обов'язків;

розголошення об'єктом опитування відомостей, що становлять державну таємницю, службову або конфіденційну інформацію.

Виходячи з наведеного бачимо, що за допомогою процедури ПФДВП можна охопити дуже широкий спектр існуючих ризиків і загроз кадровій безпеці.

Необхідно відзначити, що існує ще один блок ризиків і загроз - знищення наукових і технологічних шкіл, старіння дослідних і викладацьких кадрів, ліквідація цілих напрямків професійної підготовки або помилкове прогнозування майбутніх кадрових потреб.

Як показує практика, серед чинників, що сприяють появі наведених ризиків у оборонній сфері, зокрема, можна зазначити наступні:

- недостатній контроль за службовою діяльністю підлеглих;

- безмежна довіра до військовослужбовців, які проходять службу в ЗС України тривалий час;

- негативний приклад прийняття подарунків керівництвом;

- безкарність осіб, які були викриті при скоєні корупційних дій, що призводить до формування почуття вседозволеності у інших співробітників [10].

Формування військової кадрової політики України

Формування військової кадрової політики України відбувається в період нових форм військових конфліктів, «гібридних війн», трансформації способів ведення бойових дій, інформаційних війн, політичними ускладненнями євроінтеграційного процесу України тощо.

Одним із ключових напрямів оборонної реформи є кадровий менеджмент щодо особового складу ЗСУ. Наприклад, у 2014 році керівний склад ЗСУ зіткнувся з вагомою всеосяжною проблемою відсутності військово-навчених людських ресурсів військовозобов'язаних для комплектування посад, передбачених штатами воєнного часу, і, навіть, збільшення їх чисельності до 250 т. осіб значно не покращило ситуацію. Основними причинами зменшення кількості підготовленого мобілізаційний ресурсу країни стало скорочення чисельності ЗС України та перехід на контрактний принцип комплектування.

Отже, чисельність військовослужбовців строкової служби постійно зменшувалась, і все менше громадян України здобували військово-облікову спеціальність під час проходження строкової військової служби та набували практичних навичок і умінь, необхідних для збройного захисту держави. І це лише один з аспектів, що потребує реформування.

Проблема ефективного кадрового менеджменту в Збройних Силах України є дуже актуальною. Управління кадровими процесами здійснюється не завжди послідовно через брак відповідного науково-методичного та аналітичного забезпечення. Потребує удосконалення нормативно-правове забезпечення в галузі військової кадрової політики, оскільки цей напрям визначає ефективність механізмів реалізації оборонних реформ в Україні загалом. Виникає необхідність розробки дієвих механізмів реалізації кадрової політики на державному рівні та, зокрема, в системі Збройних Сил України.

Нові умови трансформації військової сфери, прийняті останнім часом нормативно-правові документи щодо підвищення обороноздатності країни зумовлюють вироблення нових підходів до системи кадрового забезпечення та менеджменту в ЗСУ.

Основним систематизованим документом, в якому стисло викладено стратегічне бачення розвитку військової кадрової політики Міністерства оборони є Концепція військової кадрової політики Міністерства оборони України [11].

Відповідно до цього документа **ключовою проблемою військової кадрової політики, що негативно впливає на укомплектованість** Збройних Сил належно підготовленим та вмотивованим персоналом, є наявність тенденції щодо скорочення кількості громадян з належними особистими морально-діловими та професійними якостями, які бажають проходити військову службу за контрактом у Збройних Силах, та збереження динаміки плинності кадрів, а саме: відтік певної кількості кваліфікованих та досвідчених військовослужбовців, відсутність у них бажання тривалого проходження військової служби за контрактом.

Незважаючи на упровадження протягом останніх років комплексу мотиваційних чинників (збільшене грошове забезпечення військовослужбовців, упровадження компенсації за піднайом житла для рядового та сержантського складу, підвищення додаткових виплат за виконання завдань в операції об'єднаних сил на лінії розмежування, за особливості проходження військової служби тощо), відтік військовослужбовців продовжується.

З початку 2017 року до Збройних Сил прийнято на військову службу за контрактом на посади рядового, сержантського та старшинського складу близько 150 тис. осіб, на посади офіцерського складу - близько 12 тис. осіб. Водночас звільнено з військової служби близько 110 тис. військовослужбовців рядового, сержантського та старшинського складу та близько 17 тис. офіцерів. З числа звільнених осіб рядового, сержантського та старшинського складу

переважна більшість, біля 77 тис. осіб (72 %), не виявили бажання укладати наступний контракт та звільнились після закінчення контракту. З числа офіцерського складу з цієї ж причини звільнилося близько 10 тис. осіб (58 %).

Основні причини проблеми:

низький рівень реалізації заходів щодо патріотичного виховання та військово-професійної орієнтації громадян, відсутність потужної рекламної кампанії на рівні держави щодо підвищення популярності військової служби та її позитивного сприйняття суспільством, а також заходів стосовно підвищення її престижу у Збройних Силах;

існуюча система управління кар'єрою військовослужбовців не достатньою мірою зорієнтована на чіткому баченні кожним військовослужбовцем свого кар'єрного зростання та перспективи проходження військової служби;

система підготовки кадрів та військової освіти не повного мірою сприяє можливості самовдосконалення та саморозвитку військовослужбовців;

рівень грошового забезпечення військовослужбовців не є конкурентоспроможним на ринку праці України та не відповідає вимогам сьогодення;

рівень забезпеченості житлом та соціально-побутовими об'єктами інфраструктури військових містечок залишається низьким, грошова компенсація військовослужбовцям за піднайом житла не покриває реальної вартості піднайому, а забезпечення новими гуртожитками потребує тривалого часу;

відсутні результативні зміни у соціальних відносинах "командир - підлеглий", зокрема недотримання розпорядку дня та залучення військовослужбовців до виконання непритаманних завдань (господарських робіт);

значна частина пільг, соціальних і правових гарантій військовослужбовців мають декларативний характер, система охорони здоров'я військовослужбовців та осіб, звільнених з військової служби, потребує удосконалення відповідно до стандартів (протоколів) НАТО.

Таким чином, відсутність дієвих механізмів утримання на військовій службі, чіткого бачення кожним військовослужбовцем перспектив свого кар'єрного зростання та професійного розвитку, недостатній рівень соціального та правового захисту військовослужбовців та членів їх сімей не сприяють досягненню високої мотивації у громадян щодо вступу на військову службу за контрактом та тривалого її проходження у Збройних Силах, негативно впливають на їх спроможність виконувати завдання за призначенням в умовах воєнно-політичної, оперативно-стратегічної та економічної ситуації, яка склалася в Україні.

Зважаючи на вищенаведене, очікуваними результатами оновленої військової кадрової політики мають бути досягнення високого рівня мотивації персоналу Збройних Сил до проходження військової служби, створення умов для професійного та кар'єрного зростання військовослужбовців, забезпечення конкурентоспроможності професії військовослужбовця Збройних Сил на ринку праці України.

В Концепції визначено 8 основних цілей військової кадрової політики Міністерства оборони з відповідними їх завданнями:

Ціль 1. Впровадження у військовій кадровій політиці принципів та підходів, прийнятих у збройних силах держав - членів НАТО.

Ціль 2. Переведення Збройних Сил на комплектування військовослужбовцями військової служби за контрактом, поступове зменшення обсягів призову громадян України на строкову військову службу, створення необхідного військового резерву.

Ціль 3. Створення ефективної, побудованої за принципами НАТО системи управління кар'єрою військовослужбовців за військовим званням. Запровадження військового лідерства. Забезпечення прозорого і доброчесного підбору, розстановки, присвоєння чергових військових звань та призначення на посади військовослужбовців.

Ціль 4. Уточнення повноважень командирів (начальників) щодо прийняття кадрових рішень та основних завдань і функцій служб персоналу Міністерства оборони та Збройних Сил.

Ціль 5. Розвиток людського капіталу Збройних Сил, зокрема через модернізацію систем охорони здоров'я, соціального та правового захисту, забезпечення тендерної рівності.

Ціль 6. Розвиток професійного сержантського (старшинського) складу.

Ціль 7. Створення ефективної та прозорої системи грошового забезпечення військовослужбовців, побудованої на основі ієрархії військових звань.

Ціль 8. Розвиток системи військової освіти та підготовки персоналу на основі принципів і стандартів НАТО, підготовка за євроатлантичними стандартами офіцерського, сержантського та старшинського складу.

З метою забезпечення кадрової безпеки, при формуванні завдань цілі військової кадрової політики Міністерства оборони №3 «Створення ефективної, побудованої за принципами НАТО системи управління кар'єрою військовослужбовців за військовим званням. Запровадження військового лідерства. Забезпечення прозорого і доброчесного підбору, розстановки, присвоєння чергових військових звань та призначення на посади військовослужбовців», з метою удосконалення порядку проходження військової служби, одним із завдань цієї цілі визначено:

підвищити рівень доброчесності, сформувати нетерпимість до корупції та забезпечити невідворотність відповідальності за корупційні дії, організувати та проводити на добровільних засадах перевірки доброчесності персоналу - кандидатів на посади керівного складу у Міністерстві оборони та Збройних Силах шляхом проведення психофізіологічного дослідження із застосуванням поліграфа та процедури психологічного вивчення.

Тобто, забезпечення кадрової безпеки у МОУ та ЗСУ в рамках виконання цієї цілі здійснюється двома її інструментами: проведенням ПФДВП та процедури психологічного вивчення.

Відповідно до Концепції результатами виконання цього завдання стануть:

впровадження у військову кадрову політику принципів та підходів, прийнятих в державах – членах НАТО та адаптація їх до основних положень Конституції України, вимог законів України та інших нормативно-правових актів з питань національної безпеки і оборони;

створення умов для комплектування Збройних Сил мотивованим та професійним особовим складом;

забезпечення комплектування Збройних Сил мотивованим та професійним персоналом, з урахуванням перспективної структури Збройних Сил, можливих джерел надходження особового складу, визначених до нього вимог, рівня його підготовки, ротації (переміщення) та звільнення;

реформування системи управління людськими ресурсами Збройних Сил у відповідності до оновлених процесів прийняття управлінських (кадрових) рішень, з урахуванням уточнених повноважень Президента України, Міністра оборони України, Головнокомандувача ЗС України, інших керівників органів військового управління і служб персоналу Міністерства оборони та Збройних Сил;

створення ефективної системи управління кар'єрою військовослужбовців за військовим званням, прозорої та доброчесної системи присвоєння військових звань, підбору, розстановки та призначення особового складу.

Показником результативності виконання вказаного вище завдання стане забезпечення управління кар'єрою військовослужбовців у відповідності до стандартів збройних сил держав – членів НАТО.

16 червня 2021 року Північноатлантична рада оприлюднила новий пакет Цілей партнерства України з НАТО, який містить 46 Цілей. Вони були одностайно ухвалені всіма 30 державами-членами Альянсу. Україна стала першою державою-партнером НАТО, яка отримала такий оновлений пакет Цілей партнерства, який розрахований на період до 2025 року. У ньому наведено сили і засоби, які Україна готує для участі в програмі «Партнерство заради миру», операціях та місіях Альянсу. Цілі партнерства підтримують інші завдання з реформування сектору безпеки та оборони, а заходи оборонної реформи є важливим інструментом вимірювання прогресу України на обраному шляху [12].

Імплементацію 27 із 46 Цілей партнерства покладено на Міністерство оборони України і Збройні Сили України (МОУ і ГШ ЗС України - 18, ЗС України - 9).

Цілі партнерства є одним із найбільш дієвих інструментів впровадження в Україні стандартів НАТО, посилення інституційних спроможностей оборонного відомства, розвитку спроможностей Збройних Сил України та набуття взаємосумісності оборонних і безпекових структур України з відповідними структурами держав-членів НАТО. Цілі партнерства передбачають побудову системи дієвого демократичного цивільного контролю та подальшу трансформацію системи управління Збройних Сил України.

Пакетом Цілей партнерства для України у 2021 році передбачається реалізація широкого спектру завдань на короткострокову перспективу, основними з яких є:

посилення обороноздатності та нарощування оперативних спроможностей Збройних Сил України;

досягнення Збройними Силами України критеріїв, необхідних для членства в НАТО, включно з підвищенням їх взаємосумісності зі збройними силами держав Альянсу;

сприяння реформуванню та професіоналізації Збройних Сил України, впровадження у їхню діяльність найкращих європейських та євроатлантичних стандартів, практик і процедур;

забезпечення участі Збройних Сил України в операціях з підтримання миру та безпеки під проводом Альянсу, залучення визначених військових формувань до Сил реагування НАТО.

Реалізація Цілей партнерства є необхідною передумовою для приєднання до Плану дій щодо членства в НАТО. Так, у червні цього року на Саміті НАТО в Брюсселі було зазначено, що наша держава стане членом Альянсу, а План дій щодо членства є невід'ємною частиною цього процесу.

Кадрові питання розглядаються тільки у двох цілях, це цілі **G0201** та **G0204**.

Ціль G0201 має назву «Управління персоналом (кадровий менеджмент)».

За результатами виконання даної цілі система оборонного управління персоналом повинна відповідати потребам МОУ та ЗСУ у робочій силі та сприяти реалізації військовим персоналом його повної реалізації.

В G0201 зазначається, що оборонний сектор України потребує підготовленого, кваліфікованого та мотивованого військового персоналу. Для цього потрібна дієва система управління персоналом, яка є прозорою, заснованою на заслугах (мерикатичною), справедливою та здатною задовольнити потреби МОУ та ЗСУ у робочій силі. Система управління персоналом повинна гарантувати, що військовий персонал забезпечений належною оплатою праці, кар'єрними можливостями, підготовкою та освітою, щоб були спроможними виконувати свої обов'язки ефективно та успішно.

Також, система управління персоналом повинна відповідати чинним урядовим нормам та законодавству, враховуючи специфічні умови оборонної системи. Вона повинна належним чином використовувати сучасні технологій та системи автоматизації і функціонувати у тісному взаємозв'язку з процесами планування сил.

Досягнення цієї цілі забезпечується поступовим виконанням 5 етапів, першим з яких визначено, що до кінця 2023 року політики, програми та процеси планування для прогнозування вимог управління людськими ресурсами ЗСУ здійснюють ефективно та успішно наступні функції:

a. Надають якісні та кількісні індикатори робочої сили;
b. Визначають можливі джерела для рекрутингу;
c. Прогнозують вимоги до рекрутингу;
d. Рекрутингують персонал необхідної якості та кількості у визначені строки;
e. Забезпечують освіту та підготовку;
f. Керують (управляють) поданнями та призначеннями;
g. Забезпечують дисциплінарні процедури та порядок звільнення (розірвання контракту);
h. Забезпечують належні соціальні гарантії для військового персоналу та членів їх сімей;

i. Забезпечують підтримку завершення служби військовим персоналом після закінчення строку служби, виходу на пенсію, переселення та соціальні виплати, за необхідності.

В рамках виконання цієї цілі забезпечення кадрової безпеки шляхом проведення процедури психофізіологічного дослідження персоналу із використанням поліграфа можливо при виконанні функції f. управління поданнями та призначеннями.

А при виконанні функції d. рекрутингу персоналу ЗСУ необхідної якості та кількості у визначені строки, можливо проведення процедури психологічного вивчення особового складу.

Ціль G0204 «Розбудова доброчесності».

Результатом виконання **G0204** має стати скорочення корупції у МОУ та ЗСУ, впровадження актуальної політики і процедур для упередження неправомірного використання ресурсів у всіх інституційних функціональних сферах, а також просування принципів доброчесності, прозорості та підзвітності в секторі оборони.

Належне управління ресурсами є необхідною умовою миру та стабільності. Як визнали глави держав і урядів НАТО, корупція є ризиком для безпеки, який руйнує довіру громадськості: мир і стабільність можуть бути ослаблені поганою практикою управління ресурсами, будь то людські, фінансові чи матеріальні ресурси. Отже, розбудова доброчесності в оборонних та безпекових установах, сприяння прозорості та підвищення підзвітності є важливими аспектами побудови ефективних інститутів оборони та безпеки, які перебувають під демократичним цивільним контролем і діяльність яких відповідає міжнародним стандартам.

НАТО “Розбудова доброчесності” (БІ) надає країнам практичні інструменти на стратегічному, оперативному та тактичному рівнях, що сприяють зміцненню доброчесності, прозорості та підзвітності та зменшенню ризику корупції у секторі безпеки. Це сприяє передовій практиці, процесам та методологіям та надає країнам спеціальну підтримку для підвищення ефективності, дієвості, прозорості та підзвітності установ оборони та безпеки, щоб уникнути наслідків поганого управління людьми, фінансами та матеріалами для ефективності оборони та оборонних інститутів.

Оборонні структури “Розбудова доброчесності” (БІ) повинні функціонувати під безпосереднім керівництвом Міністра Оборони. Вони повинні забезпечувати вичерпні вказівки щодо політики БІ, директиви, координацію та моніторинг. Це включає всеосяжний «План Доброчесності» та механізм координації та моніторингу для його реалізації.

Досягнення цієї цілі забезпечується поступовим виконанням 4 етапів.

В рамках виконання цієї цілі забезпечення кадрової безпеки можливо при виконанні функцій третього етапу:

3. До кінця 2024 року: План доброчесності та його реалізація забезпечили реалізацію політики управління людськими ресурсами, яка забезпечує неупереджений, прозорий процес відбору на всіх етапах кар’єри. Цей процес відбирає персонал з відповідною кваліфікацією та навичками за допомогою відповідної комбінації найму, навчання, підготовки, та призначення, а також пропонує людям складні та цікаві перспективи кар’єрного росту.

Для забезпечення виконання цього етапу ЗСУ здійснюють ефективно та успішно наступні функції:

a. Система оцінки персоналу, яка забезпечує ефективний інструмент для розвитку персоналу та сприяє прозорості та справедливості при призначенні та підвищенні персоналу (підвищення на основі заслуг).

b. Контроль за призначенням і звільненням вищого керівництва МОУ та ЗСУ з метою мінімізації можливості зловживання політичними повноваженнями.

c. Розподіл персоналу на ключові посади з урахуванням вимог до посад та особистої кваліфікації.

d. Перевірка осіб, обраних на посади, які є чутливими або мають ризик корупції, та регулярна ротація цього персоналу.

При цьому забезпечення кадрової безпеки шляхом проведення процедури психофізіологічного дослідження персоналу із використанням поліграфа можливо при виконанні функцій «a», «b», «d» цього етапу, а виконання функції «c» можливо за рахунок проведення процедури психологічного вивчення особового складу.

Основний нормативно-правовий акт, що визначає принципи, напрями, умови, організацію та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України (далі - Міноборони) та Збройних Силах України це Наказ Міністерства оборони України від 14 квітня 2015 року №164 [9].

У загальних положеннях наказу першим з основних завдань дослідження визначено - забезпечення кадрової безпеки, прозорості, об'єктивності у разі підготовки та прийняття кадрових рішень.

У документі висвітлені основні принципи та напрями проведення дослідження, загальні умови проведення процедури, організація проведення ПФДВП, порядок оформлення результатів дослідження, їх зберігання та використання результатів, а також особливості виконання обов'язків спеціалістом поліграфа.

На виконання пункту 7 наказу Міністерства оборони України від 14.08.2020 №283 "Про організацію виконання окремих заходів оборонної реформи на середньострокову перспективу" у Департаменті соціального та гуманітарного забезпечення Міністерства оборони України за участі членів проектної групи розроблено Статут проекту "Управління людськими ресурсами" [13].

Стратегічною метою даного проекту є створення у середньостроковій перспективі умов для комплектування Збройних Сил України та інших складових сил оборони мотивованим та висококваліфікованим персоналом, який демонструє готовність проходити військову службу відповідно до євроатлантичних принципів та володіє здатністю виконувати покладені на них завдання.

Ціль №2 Проєкту - Створення ефективної системи управління військовою кар'єрою за військовими званнями; удосконалення порядку проходження військової служби, соціального та правового захисту військовослужбовців та членів їх сімей; забезпечення прозорого і доброчесного підбору, розстановки та призначення на посади персоналу, присвоєння йому чергових військових звань.

Одним з результатів виконання даної цілі повинні бути організовані та проводитися на добровільних засадах перевірки доброчесності персоналу – кандидатів на посади вищого керівного складу у Міністерстві оборони та Збройних Силах України шляхом проведення психофізіологічного дослідження із застосуванням поліграфа та процедури психологічного вивчення кандидатів.

У подальшому функціонування системи управління людськими ресурсами буде спрямовано на забезпечення прозорого і доброчесного підбору, розстановки та призначення на посади персоналу, присвоєння йому чергових військових звань, всебічне забезпечення персоналу з урахуванням змін у характері та веденні війн, координації та інтеграції з силами оборони держав - членів НАТО.

Висновки. Таким чином, кадрова безпека охоплює усі напрями розвитку військової кадрової політики Міністерства оборони, а саме: рекрутинг; управління персоналом; освіту та підготовку кадрів; соціальне та гуманітарне забезпечення персоналу, а персонал Міністерства оборони та Збройних Сил України, як людський ресурс не лише впливає і ліквідує ризики комплексної безпеки, але і в деяких випадках є основною загрозою, як військової так й будь-якої іншої організації. З огляду на це, забезпечення кадрової безпеки та зниження ризиків зі сторони персоналу залишається пріоритетним і домінуючим напрямком забезпечення комплексної безпеки у сфері оборони та одним з першочергових завдань, яке необхідно вирішувати будь-якій організації для її нормального функціонування, особливо в сучасних умовах несприятливої і нестабільної ситуації в нашій країні.

Аналіз наукових праць та керівних документів дозволяє стверджувати, що питання кадрової безпеки повинні вирішуватися на кожному етапі управління персоналом (пошук,

відбір, прийом, адаптація, розвиток, оцінка і т.д.). Будь-яка дія працівника служби персоналу на будь-якому етапі – це або посилення, або ослаблення безпеки військової організації по головній її складовій – по персоналу. Для забезпечення належного рівня кадрової безпеки та, як наслідок, мінімізації можливих збитків військової організації, службам управління персоналом, як суб'єкту кадрової безпеки, необхідно постійно розробляти і впроваджувати профілактичні заходи, а також заходи швидкого реагування.

ЛІТЕРАТУРА:

1. Удосконалення методики проведення опитування персоналу з використанням поліграфа у Міністерстві оборони України та Збройних Силах України. Звіт про науково-дослідну роботу у 2-х частинах. НМЦ КП МО України. Держ. реєстр. номер 0116U000633. Київ, 2016. 460 с.
2. Кузьменко М. Д. Концептуальні аспекти застосування поліграфа в системі кадрової безпеки силових структур США. Оцінка достовірності: наукові дослідження та практика: журнал ГО “Колегія поліграфологів Украни”. Київ. 2018. Вип. 1. С. 73-82.
3. Кузьменко М. Д. Алєксєєв О. О. Напрямки застосування поліграфа в силових структурах США: психолого-прикладні та нормативно-правові аспекти кадрової безпеки. Вісник ОНУ ім. І.І. Мечникова. Психологія. 2017. Том 22. Випуск 3 (45). С. 51-60.
4. Обґрунтування шляхів застосування психофізіологічних досліджень з використанням поліграфа з метою кадрової безпеки для прийняття кадрових рішень. Звіт про науково-дослідну роботу у 2-х частинах / НМЦ КП МО України. – Держ. реєстр. номер 0117U002430. – К., 2017. – 416 с.
5. Застосування психофізіологічних досліджень персоналу з використанням поліграфа у Міністерстві оборони та Збройних Силах України: навч.-метод. посіб. / [В.М. Малюга, С.П. Гришин, М.Д. Кузьменко та ін.]; за заг. ред. В.М. Малюги. – К.: НМЦ КП МО України, 2018. – 294 с.
6. Рішення Національного агентства з питань запобігання корупції від 02.12.2016 р. № 126 “Про затвердження Методології оцінювання корупційних ризиків у діяльності органів влади”, зареєстровано у Міністерстві юстиції України 28 грудня 2016 року за № 1718/29848.
7. Наказ Міністерства оборони України від 02.04.2019 № 145 «Про затвердження Порядку організації в системі Міністерства оборони України внутрішнього контролю та управління ризиками».
8. План управління ризиками Міністерства оборони України на 2021 рік, затверджений ТВО Міністра оборони України 06.01.2021.
9. Наказ Міністерства оборони України від 14 квітня 2015 року №164 (Із змінами, внесеними згідно з Наказом Міністерства оборони № 394 від 22.07.2019) «Про затвердження Інструкції з організації та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України та Збройних Силах України».
10. Кузьменко М. Д Концептуальні аспекти системи кадрової безпеки високонадійної організації / Вісник Національного університету оборони України 1 (48) /2017 р., С. 121-125.
11. Концепція військової кадрової політики Міністерства оборони України на період до 2025 року, затверджена наказом Міністерства оборони України № 280 від 14.09.2021 р.
12. Цілі партнерства для України (Україна-НАТО) Електронній ресурс: https://armyinform.com.ua/2021/11/03/ukrayina-stala-pershoyu-derzhavoyu-partnerom-nato-yaka-otrymala-takyj-onovlenyj-paket-czilej-partnerstva-do-2025-roku/].
13. Статут проекту “Управління людськими ресурсами” Електронний ресурс: https://www.mil.gov.ua/content/tenders/proect_08062021.pdf.
14. DoD Instruction “DoD Personnel Security Program (PSP)” 5200.02 September 09, 2014 URL: www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf
15. Dod manual “Procedures for the dod personnel security program (PSP)” 5200.02 April 3, 2017 URL: http://www.dtic.mil/whs/directives/520002_dodm _2017.pdf
16. DoD Directive 5210.48 April 24, 2015 Credibility Assessment Program URL: www.dtic.mil/whs/directives/.../521048p.pdf
17. DoD Instruction 5210.91 August 12, 2010 URL: www.dtic.mil/whs/directives/.../521091p.pdf
18. Army Regulation 195–6 Department of the Army Polygraph Activities. Electronic resourse. https://fas.org/irp/doddir/army/ar195-6.pdf
19. 313 Army Regulation 380–67 Personnel Security Program 24 January 2014 URL: www.apd.army.mil/epubs/DR_pubs/DR_a/.../r380_67.pdf

REFERENCES:

1. “Udoskonalennia metodyky provedennia opytuvannia personal z vykorystanniam poligrafa u Ministerstvi oborony ta Zbroinykh Silakh Ukrainy” [Improving the method of conducting a survey of personnel using a polygraph in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine]. Report on research work in 2 parts. NMC KP MoD of Ukraine. State register. number 0116U000633. Kyiv, 2016. 460 p.

2. Kuzmenko M.D. “Conceptualni aspekty zastosouvannia poligrafa v systemi kadrovoy bezpeky sylovyh struktur USA”. [Conceptual aspects of the use of the polygraph in the personnel security system of US law enforcement agencies]. Reliability assessment: research and practice: the journal of the "Board of Polygraphists of Ukraine". Kyiv. 2018. Vip. 1. pp. 73-82.

3. Kuzmenko M.D., Alekseev O.O. “Naprijamky zastosuvannija poligrafa v sylovykh strukturakh USA: psyhologo-prykladni ta normatyvno-pravovi aspekty kadrovoi bezpeky”. [Directions of application of the polygraph in US law enforcement agencies: psychological and applied and regulatory aspects of personnel security]. Bulletin of ONU named after I.I. Мечникова. Psychology. 2017. Volume 22. Issue 3 (45). Pp. 51-60.

4. “Obgruntuvannia shliakhiv psihofiziologichnykh doslidjen z vykorystanniam poligrafa z metou kadrovoi bezpeky dlia pryiniattia kadrovykh rishen” [Substantiation of ways of application of psychophysiological researches with use of the polygraph for the purpose of personnel safety for acceptance of personnel decisions]. Report on research work in 2 parts / NMC KP MoD of Ukraine. - State. register. number 0117U002430. - K., 2017. - 416 p.

5. Maliuga V/M, Hryshyn S.P., Kuzmenko M.D. and others “Zastosuvannia psihofiziologichnykh doslidjen personalu z vykorystanniam poligrafa u Ministerstvi oborony ta Zbroynykh Sylakh Ukrainy” [Application of psychophysiological research of personnel using a polygraph in the Ministry of Defense and the Armed Forces of Ukraine]: teaching method. way, Kyiv: NMC KP MoD of Ukraine, 2018. - 294 p.

6. Decision of the National Agency for the Prevention of Corruption dated 02.12.2016 № 126 “Pro zatverdjennia Metodologii otcinuvannia korrupciynykh ryzykiv u dijialnosti organov vlady” [On approval of the Methodology for assessing corruption risks in the activities of public authorities], registered with the Ministry of Justice of Ukraine on December 28, 2016 under № 1718/29848.

7. Order of the Ministry of Defense of Ukraine dated 02.04.2019 № 145 “Pro zatverdjennia poriadku organizacii v systemi Ministerstvi oborony Ukrainy vnutrishniogo kontrolu ta upravlinnia ryzykami” [On approval of the Procedure for organization in the system of the Ministry of Defense of Ukraine of internal control and risk management].

8. Risk Management Plan of the Ministry of Defense of Ukraine for 2021, approved by the TEC of the Minister of Defense of Ukraine on January 6, 2021.

9. Order of the Ministry of Defense of Ukraine of April 14, 2015 №164 (As amended in accordance with the Order of the Ministry of Defense № 394 of 22.07.2019) “Pro zatvedjennia Instrukcii z orhanizacii ta provedennia psyhofiziolohichnoho doslidjennia iz zastosuvanniam poligrafa u Ministerstvi oborony ta Zbroinykh Sylakh Ukrainy” [On approval of the Instruction on the organization and conduct of psychophysiological examination of personnel using a polygraph Forces of Ukraine].

10. Kuzmenko M.D. “Konceptualni aspekty systemy kadrovoi bezpeky vysokonadiynoi organizacii”. [Conceptual aspects of the system of personnel security of a highly reliable organization] / Bulletin of the National University of Defense of Ukraine 1 (48) / 2017 p., P. 121-125.

11. The concept of military personnel policy of the Ministry of Defense of Ukraine for the period up to 2025, approved by the order of the Ministry of Defense of Ukraine № 280 of 14.09.2021.

12. Goals of the Partnership for Ukraine (Ukraine-NATO) Electronic resource: https://armyinform.com.ua/2021/11/03/ukrayina-stala-pershoyu-derzhavoyu-partnerom-nato-yaka-otrymala-takyj-onovlenyj- package-czilej-partnerstva-do-2025-roku /].

13. Charter of the project "Human Resources Management" Electronic resource: https://www.mil.gov.ua/content/tenders/proect_08062021.pdf.

14. DoD Instruction “DoD Personnel Security Program (PSP)” 5200.02 September 09, 2014 URL: www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf.

15. Dod manual “Procedures for the dod personnel security program (PSP)” 5200.02 April 3, 2017 URL: http://www.dtic.mil/whs/directives/520002_dodm _2017.pdf.

16. DoD Directive 5210.48 April 24, 2015 Credibility Assessment Program URL: www.dtic.mil/whs/directives/.../521048p.pdf.

17. DoD Instruction 5210.91 August 12, 2010 URL: www.dtic.mil/whs/directives/.../521091p.pdf.

18. Army Regulation 195–6 Department of the Army Polygraph Activities. Electronic resources. https://fas.org/irp/doddir/army/ar195-6.pdf.

19. 313 Army Regulation 380–67 Personnel Security Program 24 January 2014 URL: www.apd.army.mil/epubs/DR_pubs/DR_a/.../r380_67.pdf.

PhD Grishin S.P., PhD Zubovsky D.S., Ryaba L.O.

THE ROLE AND PLACE OF PERSONNEL SAFETY IN THE SYSTEM OF MILITARY HUMAN RESOURCES POLICY

The problem of personnel security is especially relevant for the Ministry of Defense and the Armed Forces of Ukraine. The current socio-political situation in our country requires, as never before, the creation of a reliable system of personnel security and the search for and implementation of fundamentally new forms and methods of its provision.

The formation of Ukraine's military personnel policy takes place in the period of new forms of military conflicts, "hybrid wars", transformation of methods of warfare, information wars, political complications of Ukraine's European integration process, etc. Personnel security in the system of military personnel policy is considered from the standpoint of targeted, process, structural and functional approaches in the context of economic security. At the same time, personnel security in the field of state defense is firstly aimed to solve the problem of national security, which imposes its own specific requirements for its study. The main threats from the personnel of the Ministry of Defense and the Armed Forces of Ukraine are outlined. Potential areas of abuse and possible corruption risks in various spheres of military activity, both in peacetime and in wartime, are also analyzed and identified, and the main factors contributing to the emergence of these risks in the defense sphere are outlined.

It is determined that personnel security covers all areas of development of military personnel policy of the Ministry of Defense, namely: recruitment; HR; education and training; social and humanitarian provision of personnel, and ensuring personnel security and reducing risks on the part of personnel remains a priority and dominant area of ensuring comprehensive security in the field of defense and one of the priority tasks to be solved. Personnel security issues should be solved at each stage of personnel management (search, selection, recruitment, adaptation, development, evaluation, etc.). Any action of a personnel officer at any stage is either strengthening or weakening the security of a military organization by its main component - personnel.

Key words: personnel security, military personnel policy, personnel.

УДК 338.47+336.1

к.е.н. **Слуцький Є.В.** (ВА, м.Одеса)
к.т.н. **Булгаков Р.В.** (ВА, м.Одеса)
д.е.н., проф. **Стоянова-Коваль С.С.** (ВА, м.Одеса)
к.е.н., доц. **Бурдейна Н.М.** (ВА, м.Одеса)
к.т.н. **Березенський Р.В.** (ВА, м.Одеса)

DOI: https://doi.org/10.17721/2519-481X/2022/74-15

ОБҐРУНТУВАННЯ ВИМОГ ДО ЗАСОБІВ ПРОГНОЗУВАННЯ ФІНАНСОВИХ ВИТРАТ НА ТРАНСПОРТНІ ЛОГІСТИЧНІ ОПЕРАЦІЇ

У статті визначено й проаналізовано характерні вимоги, що впливають на розрахунок вартості вантажного перевезення різними видами транспорту. Проаналізовано держаний бюджет України в частині транспортних витрат міністерства оборони України. З'ясовано завдання забезпечення військових перевезень. Звертається увага на особливості вантажних залізничних перевезень військових вантажів та особливості нарахування плати за них. Підкреслюється, що планування військових перевезень залежить від постачальника і отримувача вантажу. Сформовано пропозиції щодо сумісності програмного продукту НАТО LOGFAS з нормативною базою України в частині планування та здійснення наземних, повітряних та водних військових перевезень. Здійснено аналіз факторів, що враховуються при розрахунку вартості військових залізничних перевезень та врахування їх у програмному продукті LOGFAS. Визначено організаційні показники військових залізничних перевезень та проаналізовано врахування їх у програмному продукті LOGFAS. Уточнено особливості вантажно-розвантажувального комплексу морських та річкових портів визначених у програмному продукті LOGFAS та проведено ідентифікацію вимог у наявних керівних документах Збройних Сил України. Упорядковано додаткове обладнання аеропортів у програмному продукті LOGFAS врахування яких покращить інформаційний аспект майбутніх прогнозованих витрат. Виокремлено проблеми з якими можна зіткнутися під час планування транспортних витрат за допомогою програмного продукту LOGFAS. Визначено загальні вимоги до системи програмного продукту організації транспортних операцій, вимоги щодо кількісно-якісних показників елементів транспортно-логістичної системи та вимоги щодо системи в частині фінансово-економічних питань.

Ключові слова: транспортні операції, прогнозування транспортних витрат, програмний продукт НАТО LOGFAS, транспортна логістика, фінансовий облік, вантажні залізничні перевезення, забезпечення військових перевезень.

Вступ та постановка проблеми. На сучасному етапі для здійснення прогнозування будь-яких фінансово-господарських операцій необхідно накопичення масивів інформації, на підставі якої відбуваються поточні припущення щодо об'єкту прогнозування у майбутньому. Аналіз накопиченої інформації відбувається на підставі даних бухгалтерського, фінансового обліку та якісних характеристик об'єктів управління. Проте із початком військового конфлікту на сході нашої держави, керівництвом країни було прийнято рішення про припинення використання переважної більшості програмних бухгалтерських продуктів країни-агресора. Такі заходи пов'язані з небезпекою витоку накопиченої службової інформації оборонно-фінансового характеру. Однак наявні бази даних управлінського обліку не є взаємосумісними.

Додатково слід додати, що відсутність вітчизняних програмних продуктів спричиняє вакуум у сучасній системі бухгалтерського обліку державних підприємств, які є найбільш вразливими від зовнішньої загрози. Як наслідок, система стійкого підґрунтя для аналізу вже накопиченого досвіду не відповідає сучасним вимогам та ускладнює методику прогнозування видатків, що передує пошуку альтернативних варіантів програмного забезпечення.

Така сама ситуація спостерігається і у програмних продуктах системи логістики, зокрема транспортної. Адекватна оцінка витрат на транспортування покликана з одного боку необхідністю прийняття рішення про придбання конкретного об'єкту (матеріально-технічних

засобів, робіт, послуг) в конкретній організації, а з іншого боку ефективністю використання національного ресурсу.

Сучасний курс нашої країни на інтеграцію у Європейський Союз та НАТО висуває вимоги до певних трансформаційних процесів сучасної національної системи бухгалтерського обліку та системи логістики. З іншого боку, особливості прогнозування транспортних операцій та інші аспекти адаптації сучасної обліково-програмної системи України до вже сформованих стандартів партнерів потребує нової уніфікації програмних продуктів, що підтримують операції обліку. Такий широкий фронт роботи стає новим викликом в частині, що пов'язана із адаптацією сучасних українських реалій до вимог цих стандартів.

Аналіз останніх досліджень і публікацій. Питаннями покращення обліку та прогнозування транспортних витрат займались такі наукові діячи: Ареф'єва О.В. [1], Бабина О.Є. [2], Концева В.В. [3], Репіч Т.А. [4], Толпежнікова Т.Г. [5], Ярмоліцька О. В. [6] та інші.

Суттєві напрацювання, щодо програмного продукту LOGFAS на можливість його впровадження і використання займались такі вітчизняні і зарубіжні вчені: Степанюк М. Ю. [7], Сініцин І.П. [7], Котеля О. В. [7], Пецина М. [8], Дуфек Р. [8], Сзабадос Дж.Дж.[9], Ронгтін С. [10], Мінгдін Л. [10], Ли Дж. [10], Беляченко В.В. [11], Педан Ф. Ф. [11], Романченко О.А. [11], Слоан Є. [12], Розан Є. [12] та інші.

Метою статті є обґрунтування низки елементів національної системи фінансово-бухгалтерського забезпечення транспортно-логістичних процесів, що мають бути узгоджені та взаємосумісні з програмним забезпеченням країн-партнерів на підставі аналізу сучасних видатків Міністерства оборони України на транспортні послуги, а також аналізу заходів щодо впровадження нових зразків програмних продуктів для оборонного планування, порівняння можливостей цих програмних продуктів, узагальнення їх властивостей та ступеню адаптивності до сучасних реалій обліку в частині прогнозування майбутніх фінансових потоків на транспортні послуги.

Виклад основного матеріалу дослідження. Для досягнення поставленої мети було розглянуто Закон України «Про Державний Бюджет України на 2021 рік» [13], згідно із яким видатки Міністерства оборони України за загальним і спеціальним фондом склали – 117 626 443,4 тис. грн., що складає 9,6% від загальної частини видатків державного бюджету. Для реалізації поставлених завдань в Міністерстві оборони передбачено 6 програм: 5 з яких фінансують видатки апарату Міністерства оборони України і 1 за якою фінансується Адміністрація Державної спеціальної служби транспорту України. Кожна з цих програм має свої цілі та завдання для яких вони застосовуються.

В ході вивчення наказів Міністерства оборони України від 10.02.2021 № 38 «Про затвердження паспортів бюджетних програм на 2021 рік» [14] та 13.02.2021 № 42 «Про затвердження паспортів бюджетних програм на 2021 рік» [15] встановлено, що за кодом програмної класифікації видатків (КПКВ) 2101020, покладено на підрозділи Збройних Сил України завдання забезпечення військових перевезень, ремонт під'їзних колій, страхування повітряних суден та відповідальних за шкоду заподіяну третім особам, загальний обсяг видатків на зазначені заходи склали 741 698,8 тис. грн. або 1% від питомої ваги загальних витрат Міністерства оборони України.

Зазначений обсяг витрат на транспортні витрати є суттєвим для економіки держави, тому в розпорядженні Кабінету Міністрів України від 16 червня 2021 р. № 690-р «Про затвердження плану заходів з виконання Річної національної програми під егідою Комісії Україна – НАТО на 2021 рік та показників ефективності її виконання» [16] таким витратам приділена особлива увага. Річна національна програма Україна – НАТО є невід'ємною частиною цілі по організації комплементарної системи логістичного забезпечення Збройних Сил України, сумісної із стандартами НАТО, що забезпечує виконання завдань до існуючих наявних загроз. При детальному вивчені цього плану встановлено, що початковим етапом є підготовка в якості операторів сервісу LOGFAS особового складу Збройних Сил України, що здійснює планування логістичного забезпечення, наслідком чого має стати пришвидшення процесу

прогнозування транспортних процесів та оптимізацію витрат для Міністерства оборони України. Додатковим підтвердженням активних дій щодо тестування програмного забезпечення LOGFAS є підписання ліцензійної угоди терміном на 5 років з Агенцією НАТО, результатом якої є налагодження додаткового зв'язку та підтримка інформативного середовища.

Виникає логічне питання сумісності програмного продукту НАТО LOGFAS з нормативною базою України в частині планування та здійснення наземних, повітряних та водних військових перевезень [22], а також врахування факторів, що мають істотне значення при розрахунку вартості вантажного перевезення.

Особливістю вантажних залізничних перевезень військових вантажів є те, що до місця навантаження, як правило, прибуває порожній рейковий рухомий склад. Така ситуація викликана тим, що на відміну від цивільних вантажів, які навантажуються і формуються до контейнерного поїзду, військовий вантаж навантажується і формується у вантажний – поїзд. Контейнерний поїзд має, як правило, обмінний характер вантажу, а вантажний прямує до кінцевого місця призначення. Додаткова різниця викликана тим, що використовується різні типи вагонів, а саме: для перевезення військової техніки найчастіше використовуються платформи; для перевезення тарно-штучного вантажу використовують криті вагони; для перевезення світлих та темних нафто-продуктів використовують цистерни; для перевезення особового складу використовують людські, плацкартні та купейні вагони.

Згідно із наказом міністерства транспорту та зв'язку від 26.03.2009 №317 «Про затвердження Збірника тарифів на перевезення вантажів залізничним транспортом у межах України та пов'язані з ними послуги та Коефіцієнтів, що застосовуються до Збірника тарифів на перевезення вантажів залізничним транспортом у межах України та пов'язані з ними послуги» [17] вартість військових вантажів округлюється до цілих гривень та в залежності від особливостей військового вантажу можуть використовуватись до 9 різних тарифних схем. Така широка варіативність тарифних схем з одного боку дає можливість раціонального витрачання коштів, а з іншого потребує додаткової уваги і постійного контролю.

Слід наголосити, що ключовим для визначення вантажу, як військовий вантаж є те, що відправником і одержувачем є військові частини. Транспортні витрати пов'язані з вантажем який постачається з цивільного сектору економіки до військової частини оплачується як правило цивільним постачальником і враховується до вартості товару, що постачається.

Додатково слід додати, що наказом Міністерства оборони України від 01.12.2015 № 666/503 «Про затвердження Інструкції з планування військових залізничних перевезень» [18] одиницями військових залізничних перевезень є оперативні військові перевезення та постачальні військові перевезення. Такий поділ покликаний оптимізувати вартість перевезення, а також конкретизувати та визначити пріоритет всіх транспортних операцій відносно одна одної під час їх планування. З іншого боку такий поділ транспортних операцій дає можливість орієнтуватись не на кількість проведення операцій та середнє значення часу необхідного для проведення транспортної операції, а на пріоритетність транспортної операції в загальному списку перевезень Збройних Сил України.

Планування військових перевезень здійснюється в поточному місяці на наступний на підставі заявок із наступним складанням плану перевезень. Такий план підлягає зміні в залежності від зміни суспільно-політичної обстановки в державі. Під час складання плану перевезень враховують забезпеченість коштами на оплату перевезень але відсутність коштів на перевезення може бути замінена на кредиторську заборгованість.

Програмний комплекс НАТО LOGFAS дає можливість виокремити оперативні військові перевезення та постачальні військові перевезення. В зв'язку з цим, наступним кроком є дослідження особливостей формування вартості перевезення.

Не зважаючи на те, що раніше було визначено, що перевезення військових вантажів відбувається за КПКВ 2101020, у заявці на планування військових залізничних перевезень другим пунктом є повідомлення про наявність коштів на проведення заходу перевезення із вказання КПКВ, коду економічної класифікації видатків (КЕКВ) та кодом видатків за

кошторисом Міністерства оборони України. Додатково міститься деталізація на такі заходи як, кошти на навантаження, вивантаження, воєнізовану охорону та на кріплення. Це підтверджує те, що кожного року КПКВ може змінюватись і для його уточнення необхідно здійснювати вивчення паспортів бюджетних програм Міністерства оборони України.

У свою чергу, заявка на забезпечення навантаження військових ешелонів і військових транспортів на ім'я військового коменданта комендатури військових сполучень залізничної дільниці та станції та начальника станції говорить про те, що військова частина може мати кошти на розрахунковому рахунку або «коді Тех. ПД» відкритому у АТ «Українська залізниця», що залишились від минулих операцій. Це також підтверджує те, що КПКВ може відрізнятися у порівнянні із минулим роком. Додатково це говорить про те, що під час інтенсивних перевезень, кошти які витрачаються на військові перевезення можуть бути значно більше ніж ті які заплановані в Державному бюджеті на відповідний рік за рахунок раніше зекономлених коштів.

Наказом Міністерства оборони України від 05.09.2013 № 595 «Про затвердження Положення з військових перевезень залізничним, морським, річковим та повітряним транспортом» [19] визначено, що організація військових перевезень включає такий захід як здійснення взаєморозрахунків за надані послуги, тобто з одного боку таке визначення дає можливість використовувати раніше зекономлені кошти, а з іншого використовувати кошти поточного кошторису Міністерства оборони України.

Слід додати, що не включаються до вартості перевезення супутні витрати пов'язані із забезпеченням особового складу військового ешелону продуктами харчування на весь шлях прямування, пального для забезпечення розвантаження та руху, а також медичне забезпечення, фінансування яких здійснюється за рахунок інших статей Міністерства оборони України.

Згідно з вимогами п.7.1.2 Доктрини Об'єднана логістика (СП 4-00(30)03.01), для забезпечення логістичною інформацією під час проведення спільних операцій НАТО використовує програмне забезпечення LOGFAS.

Особливості національної організації військових залізничних перевезень потребують порівняння із програмним забезпечення LOGFAS для визначення ступеню інформативності у разі її подальшого використання в інтересах Збройних Силах України.

Під час складання розрахунку на перевезення військової частини враховується ціла низка факторів, що впливають на вартість перевезення. Аналіз факторів, що враховуються при розрахунку вартості військового перевезення та врахування їх у програмному продукті LOGFAS наведено у таблиці 1.

Таблиця 1

Аналіз факторів, що враховуються при розрахунку вартості військових залізничних перевезень та врахування їх у програмному продукті LOGFAS

(складено авторами згідно з даними [19; 20])

№ пп	Найменування факторів, що впливають на вартість військового перевезення	Враховано у LOGFAS
1.	Збереження організаційної цілісності військових частин та підрозділів, їх готовність до самостійного виконання бойового завдання	+
2.	Прихованість під час виконання вантажно-розвантажувальних робіт та на шляху прямування	-
3.	Перехід військової частини під час перевезення на комбіноване пересування, для чого підрозділи з важкою військовою технікою, що має малий запас ходу і малі маршові швидкості, навантажуються в окремі поїзди	-

№ пп	Найменування факторів, що впливають на вартість військового перевезення	Враховано у LOGFAS
4.	Розподіл засобів зв'язку та інших матеріально-технічних засобів по військових ешелонах	-
5.	Визначення черговості відправлення підрозділів та їх прибуття в пункти призначення з урахуванням характеру завдань, що будуть виконуватись після розвантаження	+
6.	Можливість ущільненого розміщення озброєння та військової техніки на транспортних засобах з урахуванням дотримання заходів безпеки і забезпечення швидкого навантаження (розвантаження, перевантаження) військового ешелону	-
7.	Максимально можливе розміщення запасів матеріально-технічних засобів, що перевозяться, у кузовах автомобілів	-

Як видно з табл. 2, переважна частина показників, що впливають на організацію військових залізничних перевезень врахована в програмному продукті LOGFAS.

Таблиця 2

Аналіз організаційних показників військових залізничних перевезень та врахування їх у програмному продукті LOGFAS
(складено авторами згідно з даними [19; 20])

№ пп	Найменування організаційних показників військових залізничних перевезень	Враховано у LOGFAS
1.	Військові частини (підрозділи), які підлягають перевезенню	+
2.	Порядок і черговість перевезення	+
3.	Вихідні райони перед навантаженням	+
4.	Основні та запасні райони навантаження (перевантаження, розвантаження)	+
5.	Райони зосередження військових частин після розвантаження та маршрути виходу з них	+
6.	Строки початку та закінчення перевезення	-
7.	Порядок забезпечення та управління під час виконання військових залізничних перевезень	-

Особлива увага приділена підготовці вантажно-розвантажувального комплексу, до складу якого входять такі можливості, як: встановлення збірно-розбірної металевої апарелі, наявність водних колонок, наявність стаціонарного освітлення із засобами світломаскування, вантажно-розвантажувальні пристрої та укриття для особового складу. Слід зазначити, що подібна деталізація у програмному комплексі LOGFAS в частині об'єктів залізничних станцій на карті не застосовується.

При організації військових перевезень морським та річковим транспортом враховуються наявність вантажопідйомних, вантажно-розвантажних і перевантажувальних засобів. Як і при підготовці вантажно-розвантажувального місця залізничної станції, так і при підготовці вантажно-розвантажувального місця морського та річкового портів враховуються наявність водних колонок, наявність стаціонарного освітлення із засобами світломаскування та місця для укриття особового складу, що приймає участь у вантажно-розвантажувальних роботах, а

також засоби систем пожежогасіння. Додатковим аспектом є наявність плавучого причалу та його готовність до використання. При навантаженні на рейді враховуються плавзасоби, матеріали та інструменти для забезпечення навантаження (розвантаження) військових ешелонів, що надаються підприємствами порту. Такі додаткові послуги мають оплатний і безоплатний характер, а також впливають на темп вантажно-розвантажувальних робіт.

Хотілося б наголосити, що вимоги на організацію військових перевезень повітряним транспортом не висуваються. В свою чергу у програмному комплексі LOGFAS наведені такі параметри, згідно рис. 1.

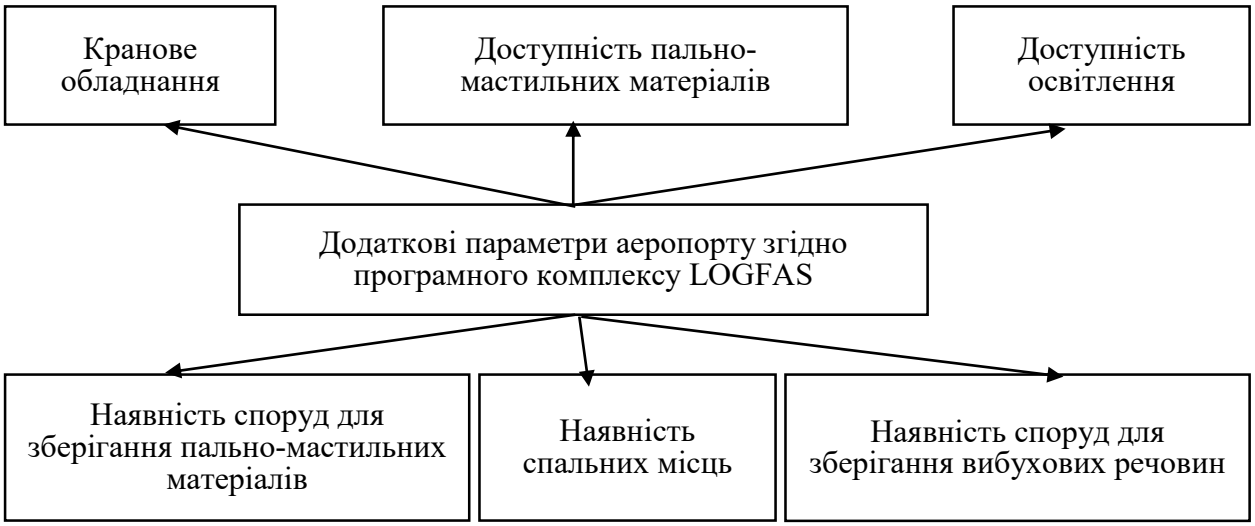

Рисунок 1 - Аналіз додаткового обладнання аеропортів, що враховується у програмному продукті LOGFAS
(Розробка авторів на підставі [19; 20])

Проведене дослідження дає змогу виокремити проблематику при впровадженні та переході планування транспортних операцій за допомогою програмного продукту НАТО LOGFAS.

Проблеми з якими можна зіткнутися під час планування транспортних витрат за допомогою програмного продукту LOGFAS:

висока вартість самого програмного продукту та технічних засобів з параметрами відповідної продуктивності;

необхідність розгалуженої мережі користувачів;

неповне врахування всього спектру факторів, які впливають на вартість транспортних витрат.

Позитивні наслідки застосування програмного продукту LOGFAS:

додаткова взаємосумісність ЗС України з країнами НАТО;

примусове прискорення процесів оновлення електронної обчислювальної техніки у військових частинах та установах ЗС України;

покращення рівня володіння англійською мовою серед особового складу, оскільки програма використовує виключно англійську мову;

Отже, кінцевою метою проведеного дослідження є вироблення вимог до програмного продукту, що відповідає за планування/прогнозування, економне, ефективне і цільове виконання транспортно-логістичних операцій з елементами обліку і звітності – тобто обґрунтування комплексу припущень (якісного та кількісного характеру) щодо майбутніх параметрів транспортно-логістичної системи з урахуванням витрат фінансового характеру, що буде реалізовуватись на певному театрі (бойових) дій.

Загальні вимоги до системи:

конфіденційність, захищеність від зовнішнього та внутрішнього втручання;

оперативність підготовки інформації, можливість внесення коректив;

узгодженість з програмним забезпеченням у частині фінансово-бухгалтерського забезпечення;

взаємосумісність з програмними продуктами країн-членів НАТО;

Вимоги щодо кількісно-якісних показників елементів транспортно-логістичної системи:

габаритно-вагові, швидкісні та погодні характеристики засобів транспортування (з розподілом за видами: наземні, водні, повітряні та трубопровідні) [21];

габаритно-вагові, швидкісні (режими руху, коридори, ешелони, пропускна здатність тощо) та погодні характеристики шляхів транспортування;

технічні характеристики місць розвантаження (перевантаження, завантаження), наявність технічних засобів механізації, відповідної інфраструктури (освітлення, апарелі, підйомники, кранове обладнання, складські приміщення, укриття, можливість обладнання пунктів розподілу вантажів, наявність дорожньої мережі тощо)

Вимоги щодо системи в частині фінансово-економічних питань:

спроможність застосовувати різні види класифікації видатків (програмну, функціональну, відомчу, економічну класифікацію видатків, а також класифікацію за кодами видатків Міністерства оборони України);

спроможність застосовувати маркери, що позначають вид фонду за яким здійснюються видатки бюджету (загальний, спеціальний);

можливість прогнозування транспортно-логістичних операцій за умов мирного та воєнного часу (особливого періоду);

можливість враховувати для різних видів транспорту тарифи на перевезення та на додаткові послуги, збори за роботи пов'язані з перевезенням вантажів;

здатність врахувати можливості послуг наявної інфраструктури з метою постачання матеріально-технічних засобів різних класів постачання.

Висновки. Програмний продукт LOGFAS задовольняє значну кількість потреб які впливають на планування транспортних перевезень різними видами транспорту. Проте для розрахунку вартості перевезень необхідна програмна адаптація до сучасних транспортних реалій Збройних Сил України, врахування бюджетних особливостей України в частині класифікації видатків, а також інтеграція умов перевезення з розрахунковими програмами. Також необхідна програмна адаптація до кількісно-якісних показників елементів української транспортно-логістичної системи та чинників, що на неї впливають.

Враховуючи визначені пріоритетні напрямки України щодо вступу до НАТО є гостра необхідність у створенні національної єдиної інформаційної системи логістичного забезпечення, сумісної з програмним забезпеченням, яке використовується в НАТО [20].

На думку авторів, перспективним у подальшому є дослідження особливостей транспортно-логістичних операцій щодо переміщення (перевезення) матеріально-технічних засобів різних класів постачання та персоналу.

ЛІТЕРАТУРА:

1. Ареф’єва О.В. Теоретичні основи управління конкурентоспроможністю авіатранспортного підприємства / О. В. Ареф’єва, Н. М. Кравчук, М. Я. Катан // Проблеми економіки. – 2018. – № 4. – С. 127–134.

2. Бабина О. Є. Антикризовий менеджмент на підприємствах водного транспорту / О. Є. Бабина, О. О. Карпенко, М. В. Ковбатюк, В. В. Шкляр. – К.: КВІЦ, 2015. – 240 с.

3. Концева В. В. Проблеми оновлення основних засобів дорожніх підприємств / В. В. Концева, А. І. Харченко // Економіка та управління на транспорті. – 2018. – Вип. 7. – С. 36–43.

4. Репіч Т.А. Оптимізація логістичної інфраструктури міжнародних вантажних перевезень [Електронний ресурс] / Т.А. Репіч, Д. Ю. Великий // Електронний журнал «Ефективна економіка». – 2017. – Режим доступу до ресурсу: http://www.economy.nayka.com.ua/?op=1&z=5377.

5. Толпежнікова Т.Г. Шляхи підвищення ефективності зовнішньоекономічної діяльності транспортного підприємства [Електронний ресурс] / Т.Г. Толпежнікова, К. А. Зеленський //

Електронний журнал «Ефективна економіка». – 2017. – Режим доступу до ресурсу: http://www.economy.nayka.com.ua/?op=1&z=5971.

6. Ярмоліцька О. В. Фактори впливу на інноваційно-інвестиційне відтворення основних засобів вітчизняних залізниць / О. В. Ярмоліцька // Проблеми і перспективи економіки та управління. – 2015. – № 2. – С. 140–149.

7. Степанюк М. Ю., Сініцин І. П., Котеля О. В. Проблема створення інформаційної системи логістики в Збройних Силах України, що відповідає стандартам НАТО // Проблеми програмування. – 2018. – № 4. – С. 101–110. https://doi.org/10.15407/pp2018.04.101 10.

8. Pecina Miroslav, Dufek Roman. Use of LOGFAS tools in logistics planning in NATO // Revista academiei forţelor terestre.–2016.– N 2 (82).–P. 120–126.

9. Szabados János József. A logisztikai információs rendszer szükségessége és fejlesztési lehetőségei a Magyar Honvédségben // HSz Logisztika.–2018. –N 4. –P. 89–102 [Електронний ресурс]. – Режим доступу: https://honvedelem.hu/files/files/111397/hsz_2018_4_beliv_089_102.pdf

10. Rongting Sun, Mingding Liu, Li Zhao. Research on logistics distribution path optimization based on PSO and IoT // International Journal of Wavelets, Multiresolution and Information Processing. – Available from: https://doi.org/10.1142/S0219691319500516

11. Беляченко В.В., Педан Ф.Ф., Романченко О.А. Підходи до створення, підтримки і вдосконалення АСУ логістичного забезпечення ЗС України з урахуванням досвіду країн-членів НАТО.–2018. [Електронний ресурс]. – Режим доступу: http://znp-cvsd.nuou.org.ua/article/view/177510/177369

12. Elliot B. Sloane, Eric Rosow, Joe Adam, Dave Shine. JEDI – An Executive Dashboard and Decision Support System for Lean Global Military Medical Resource and Logistics Management. International Conference of the IEEE Engineering in Medicine and Biology Society, 2006 [Електронний ресурс]. – Режим доступу:https://doi.org/10.1109/IEMBS.2006.259658

13. Закон України від 15.12.2020 № 1082-IX «Про Державний Бюджет України на 2021 рік». – Режим доступу: https://zakon.rada.gov.ua/laws/show/1082-20#Text

14. Наказ Міністерства оборони України від 10.02.2021 № 38 «Про затвердження паспортів бюджетних прогам на 2021 рік». – Режим доступу: https://www.mil.gov.ua/content/mou_orders/mou_2021/38_nm.pdf

15. Наказ Міністерства оборони України від 13.02.2021 № 42 «Про затвердження паспортів бюджетних прогам на 2021 рік». – Режим доступу: https://www.mil.gov.ua/content/mou_orders/mou_2021/42_nm.pdf

16.Розпорядженні Кабінету Міністрів України від 16 червня 2021 р. № 690-р «Про затвердження плану заходів з виконання Річної національної програми під егідою Комісії Україна - НАТО на 2021 рік та показників ефективності її виконання». – Режим доступу: https://zakon.rada.gov.ua/laws/show/690-2021-%D1%80#Text

17.Наказ Міністерства Транспорту та Зв’язку України від 26.03.2009 №317 «Про затвердження Збірника тарифів на перевезення вантажів залізничним транспортом у межах України та пов'язані з ними послуги та Коефіцієнтів, що застосовуються до Збірника тарифів на перевезення вантажів залізничним транспортом у межах України та пов'язані з ними послуги». – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0340-09#Text

18.Наказ Міністерства оборони України від 01.12.2015 № 666/503 «Про затвердження Інструкції з планування військових залізничних перевезень». – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1606-15#Text

19.Наказ Міністерства оборони України від 05.09.2013 № 595 «Про затвердження Положення з військових перевезень залізничним, морським, річковим та повітряним транспортом» . – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1662-13#Text

20.Allied deployment and movements system (ADAMS). Logistics Functional Area Services (LOGFAS) [Електронний ресурс] / Allied Deployment And Movements System (ADAMS) // version 6.1. – 2019. – Режим доступу до ресурсу: https://aktivity.unob.cz/logfas/SiteAssets/Stranky/Tutorial/ADAMS_61_1108.pdf.

21.Доктрина Об’єднана логістика (СП 4-00(30)03.01), затверджена ГК ЗСУ від 09.2020р.

22.Доктрина з організації переміщень та перевезень (транспортувань) у Збройних Силах України (ВКП 4-00(03).01), затверджена НГШ ЗСУ від 08.2020р.

REFERENCES:

1. Aref'jeva, O.V., Kravchuk N.M. and Katan, M. Ja.(2018), "Teoretychni osnovy upravlinnja konkurentospromozhnistju aviatransportnogho pidpryjemstva" [Theoretical bases of air transport enterprise competitiveness management], Problems of the economy, № 4, pp. 127–134

2. Babyna, O.Je., Karpenko, O.O., Kovbatjuk, M.V., and Shkljar, V.V.(2015), " Antykryzovyj menedzhment na pidpryjemstvakh vodnogho transportu " [Anti-crisis management at water transport enterprises], Kiev, KVIC, p. 240.

3. Konceva, V.V., and Kharchenko, A.I.(2018), " Problemy onovlennja osnovnykh zasobiv dorozhnikh pidpryjemstv" [Problems of renewal of fixed assets of road enterprises], Economics and management of transport, № 7., pp. 36–43.

4. Repich, T.A., and Velykyj, D.Ju., (2017), "Optymizacija loghistychnoji infrastruktury mizhnarodnykh vantazhnykh perevezenj " [Optimization of the logistics infrastructure of international freight transport], E-journal "Effective Economy", http://www.economy.nayka.com.ua/?op=1&z=5377.

5. Tolpezhnikova, T. Gh., and Zelensjkyj, K. A., (2017), " Shljakhy pidvyshhennja efektyvnosti zovnishnjoekonomichnoji dijaljnosti transportnogho pidpryjemstva " [Ways to increase the efficiency of foreign economic activity of the transport enterprise], E-journal "Effective Economy", http://www.economy.nayka.com.ua/?op=1&z=5971.

6. Jarmolicjka, O. V., (2017) " Faktory vplyvu na innovacijno-investycijne vidtvorennja osnovnykh zasobiv vitchyznjanykh zaliznycj" [Factors influencing the innovation and investment reproduction of fixed assets of domestic railways], Problems and prospects of economics and management, № 2., pp. 140–149.

7. Stepanjuk, M.Ju., Sinicyn, I.P., and Kotelja, O.V.(2018) " Problema stvorennja informacijnoji systemy loghistyky v Zbrojnykh Sylakh Ukrajiny, shho vidpovidaje standartam NATO " [The problem of creating a logistics information system in the Armed Forces of Ukraine that meets NATO standards], Programming problems, № 4, pp. 101–110. https://doi.org/10.15407/pp2018.04.101 10.

8. Pecina Miroslav, Dufek Roman.(2016) Use of LOGFAS tools in logistics planning in NATO. Revista academiei forţelor terestre, № 2 (82).–P. 120–126.

9. Szabados János József.(2018) A logisztikai információs rendszer szükségessége és fejlesztési lehetőségei a Magyar Honvédségben, HSz Logisztika, № 4. pp. 89–102, https://honvedelem.hu/files/files/111397/hsz_2018_4_beliv_089_102.pdf

10. Rongting Sun, Mingding Liu, Li Zhao. Research on logistics distribution path optimization based on PSO and IoT , International Journal of Wavelets, Multiresolution and Information Processing, https://doi.org/10.1142/S0219691319500516

11. Beljachenko, V.V., Pedan, F.F. and Romanchenko, O. A., (2018) " Pidkhody do stvorennja, pidtrymky i vdoskonalennja ASU loghistychnogho zabezpechennja ZS Ukrajiny z urakhuvannjam dosvidu krajin-chleniv NATO" [Approaches to the creation, support and improvement of AMS logistics of the Armed Forces of Ukraine, taking into account the experience of NATO member countries], http://znp-cvsd.nuou.org.ua/article/view/177510/177369

12. Elliot B. Sloane, Eric Rosow, Joe Adam and Dave Shine.(2006) JEDI – An Executive Dashboard and Decision Support System for Lean Global Military Medical Resource and Logistics Management. International Conference of the IEEE Engineering in Medicine and Biology Society, https://doi.org/10.1109/IEMBS.2006.259658

13. Pro Derzhavnyj Bjudzhet Ukrajiny na 2021 rik : Zakon Ukrajiny (2020), https://zakon.rada.gov.ua/laws/show/1082-20#Text (accessed 15 December 2021).

14. Pro zatverdzhennja pasportiv bjudzhetnykh progham na 2021 rik : Nakaz Ministerstva oborony Ukrajiny (2021), https://www.mil.gov.ua/content/mou_orders/mou_2021/38_nm.pdf (accessed 10 February 2021).

15. Pro zatverdzhennja pasportiv bjudzhetnykh progham na 2021 rik : Nakaz Ministerstva oborony Ukrajiny (2021), https://www.mil.gov.ua/content/mou_orders/mou_2021/42_nm.pdf (accessed 13 March 2021).

16. Pro zatverdzhennja planu zakhodiv z vykonannja Richnoji nacionaljnoji proghramy pid eghidoju Komisiji Ukrajina - NATO na 2021 rik ta pokaznykiv efektyvnosti jiji vykonannja : Rozporjadzhenni Kabinetu Ministriv Ukrajiny (2021), https://zakon.rada.gov.ua/laws/show/690-2021-%D1%80#Text, (accessed 16 June 2021).

17. Pro zatverdzhennja Zbirnyka taryfiv na perevezennja vantazhiv zaliznychnym transportom u mezhakh Ukrajiny ta pov'jazani z nymy poslughy ta Koeficijentiv, shho zastosovujutjsja do Zbirnyka taryfiv na perevezennja vantazhiv zaliznychnym transportom u mezhakh Ukrajiny ta pov'jazani z nymy poslughy :

Nakaz Ministerstva Transportu ta Zv'jazku Ukrajiny (2009), https://zakon.rada.gov.ua/laws/show/z0340-09#Text, (accessed 26 March 2021).

18. Pro zatverdzhennja Instrukciji z planuvannja vijsjkovykh zaliznychnykh perevezenj : Nakaz Ministerstva oborony Ukrajiny (2015), https://zakon.rada.gov.ua/laws/show/z1606-15#Text, (accessed 01 December 2015).

19. Pro zatverdzhennja Polozhennja z vijsjkovykh perevezenj zaliznychnym, morsjkym, richkovym ta povitrjanym transportom (2013), https://zakon.rada.gov.ua/laws/show/z1662-13#Text, (accessed September 2013).

20. Allied deployment and movements system (ADAMS). Logistics Functional Area Services (LOGFAS),(2019). Allied Deployment And Movements System (ADAMS). version 6.1., https://aktivity.unob.cz/logfas/SiteAssets/Stranky/Tutorial/ADAMS_61_1108.pdf.

21. Doktryna Ob'jednana loghistyka : Nakaz Gholovnokomanduvacha Zbrojnykh Syl Ukrajiny (accessed September 2020).

22. Doktryna z orghanizaciji peremishhenj ta perevezenj (transportuvanj) u Zbrojnykh Sylakh Ukrajin : Nakaz Gholovnokomanduvacha Zbrojnykh Syl Ukrajiny (accessed August 2020).

PhD Slutskyi Ev.V., PhD Bulhakov R.V., D. Sci. Econ., Prof. Stoyanova-Koval S.S., PhD Burdeina N.N., PhD Berezens′kyy R.V.

JUSTIFICATION OF REQUIREMENTS FOR FINANCIAL EXPENDITURE FOR FORECASTING FOR LOGISTICS TRANSPORT LOGISTICS OPERATIONS

The article identifies and analyzes the characteristic requirements that affect the calculation of the cost of freight transportation by different modes of transport. The state budget of Ukraine in terms of transport costs of the Ministry of Defense of Ukraine is analyzed. The task of providing military transportation has been clarified. Attention is paid to the peculiarities of rail freight transportation of military cargo and the peculiarities of charging for them. It is emphasized that the planning of military transportation depends on the supplier and consignee. Proposals have been made on the compatibility of the NATO software product LOGFAS with the regulatory framework of Ukraine in terms of planning and implementation of land, air and water military transport. An analysis of the factors taken into account when calculating the cost of military rail transport and taking them into account in the software product LOGFAS. The organizational indicators of military railway transportation are determined and their consideration in the LOGFAS software product is analyzed. The peculiarities of the loading and unloading complex of sea and river ports defined in the LOGFAS software product have been clarified and the requirements in the existing guiding documents of the Armed Forces of Ukraine have been identified. Additional airport equipment has been streamlined in the LOGFAS software product, which will improve the information aspect of future projected costs. The problems that can be encountered when planning transport costs with the help of the LOGFAS software product are highlighted. The general requirements to the system of the software product of the organization of transport operations, the requirements for the quantitative and qualitative indicators of the elements of the transport and logistics system and the requirements for the system in terms of financial and economic issues are determined.

Key words: transport operations, transport cost forecasting, NATO software product LOGFAS, transport logistics, financial accounting, rail freight, military transport.

ДАНІ ПРО АВТОРІВ

Банзак Геннадій В'ячеславович, кандидат технічних наук, доцент, доцент кафедри Метрології та інформаційно-вимірювальної техніки Державного університету інтелектуальних технологій і зв'язку, ORCID: 0000-0003-1684-3785.

Банзак Оксана Вікторовна, доктор технічних наук, професор, завідувач кафедри Електроніки та мікросистемної техніки Державного університету інтелектуальних технологій і зв'язку, ORCID: 0000-0002-6649-5013.

Березенський Руслан Володимирович, кандидат технічних наук, заступник начальника кафедри, Військова академія, м.Одеса, ORCID: 0000-0002-1778-816X.

Боровик Людмила Володимирівна, доктор педагогічних наук, професор, завідувач кафедри загальнонаукових та інженерних дисциплін Національної академії Державної прикордонної служби України імені Б. Хмельницького, ORCID: 0000-0003-2949-2187.

Боровик Олег Васильович, доктор технічних наук, професор, Заслужений працівник освіти України, заступник начальника відділу організації освітньої та наукової діяльності управління професійної підготовки Департаменту персоналу Адміністрації Державної прикордонної служби України, ORCID: 0000-0003-3691-662X.

Булгаков Руслан Валерійович, кандидат технічних наук, начальник кафедри, Військова академія, м.Одеса, ORCID: 0000-0002-8825-718X.

Бурдейна Надія Миколаївна, кандидат економічних наук, доцент, професор кафедри, Військова академія, м.Одеса, ORCID: 0000-0002-3070-1866.

Вдовенко Сергій Григорович, доцент кафедри зв'язку та автоматизованих систем управління інституту забезпечення військ (сил) та інформаційних технологій Національного Університету оборони України імені Івана Черняховського, ORCID: 0000-0001-8139-7975.

Возікова Людмила Михайлівна, старший викладач кафедри Стандартизації та оцінки відповідності Державного університету інтелектуальних технологій і зв'язку, ORCID: 0000-0002-9983-5731.

Габер Антоніна Анатоліївна, кандидат технічних наук, доцент, декан факультету Метрології, автоматизації та електроніки Державного університету інтелектуальних технологій і зв'язку, ORCID: 0000-0001-7670-9911.

Гришин Сергій Павлович, кандидат технічних наук, науковий співробітник Науково-методичного центру кадрової політики Міністерства оборони України, ORCID: 0000-0003-1936-9089.

Грищак Олег Миколайович, кандидат технічних наук, доцент, Національний університет оборони України імені Івана Черняховського.

Гусак Юрій Аркадійович, доктор військових наук, професор, головний науковий співробітник, Центральний науково-дослідний інститут Збройних Сил України, ORCID: 0000-0002-3423-2112.

Джулій Володимир Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, ORCID: 0000-0003-1878-4301.

Докіль Валентин Миколайович, слухач інституту державного військового управління Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0002-6321-0940.

Живило Євген Олександрович, кандидат наук з державного управління, начальник кафедри зв'язку та автоматизованих систем управління інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0003-4077-7853.

Жиров Генадій Борисович, кандидат технічних наук, старший науковий співробітник, доцент кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, http://orcid.org/0000-0001-7648-7992.

Зіатдінов Юрій Кашафович, доктор технічних наук, професор, Заслужений працівник освіти України, провідний науковий співробітник Державного науково-дослідного інституту авіації: ORCID: 0000-0003-2035-7376.

Зубовський Дмитро Сергійович, кандидат психологічних наук, старший науковий співробітник Науково-методичного центру кадрової політики Міністерства оборони України, ORCID: 0000-0003-1936-9089.

Ільченко Володимир Васильович, доктор фізико-математичних наук професор, директор Інституту високих технологій Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-5844-2248.

Коноваленко Олексій Іванович, в/ч А 3814, ORCID: 0000-0002-2179-5477.

Коренець Олександр Володимирович, кандидат географічних наук, молодший науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-6352-9591.

Кульський Олександр Леонідович, кандидат техничних наук старший науковий співробітник, старший науковий співробітник інституту високих технологій Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-8065-6338.

Лещенко Олег Іванович, кандидат технічних наук, доцент, завідувач кафедри Електроніки та мікросистемної техніки Державного університету інтелектуальних технологій і зв'язку, ORCID: 0000-0001-8589-8596

Лєнков Євген Сергійович, кандидат технічних наук, старший дослідник, старший науковий співробітник наукового центру Центрального науково-дослідного інституту Збройних Сил України, ORCID: 0000-0001-5819-2656.

Лєнков 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, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-7689-239X.

Литвиненко Наталія Ігорівна, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного відділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-2203-2746.

Лоза Віталій Миколайович, кандидат технічних наук, старший дослідник, начальник відділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-8050-3614.

Мавренков Олексій Єфремович, доктор технічних наук, старший науковий співробітник, начальник науково-дослідної лабораторії Державного науково-дослідного інституту авіації, ORCID: 0000-0002-6578-4833.

Максименко Юрій Анатолійович, кандидат технічних наук, начальник кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки Військової академії (м. Одеса), ORCID: 0000-0002-1227-2009.

Маміч Віктор Володимирович, кандидат технічних наук, доцент, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки Військової академії, ORCID: 0000-0001-5574-0901.

Мірошніченко Олег Вікторович, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного управління науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-3969-9758.

Мостовой Василь Сергійович, доктор фізико-математичних наук, старший науковий співробітник, старший науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-1759-1893.

Мясищев Олександр Анатолійович, доктор технічних наук, професор, профссор Хмельницького політехнічного фахового коледжу Національного університету "Львівська політехніка", ORCID: 0000-0003-1269-425X.

Нікіфоров Микола Миколайович, кандидат військових наук, старший дослідник, провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-2849-5688.

Пампуха Ігор Володимирович, кандидат технічних наук, доцент, Лауреат Державної премії України в галузі науки і техніки, начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-4807-3984.

Попков Борис Олексійович, кандидат військових наук, Лауреат Державної премії України в галузі науки і техніки, заступник начальника Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-9750-1220.

Попов Сергій Афанасійович, доктор наук з державного управління, професор, професор кафедри, організації розвідувально-інформаційної роботи та технічних засобів розвідки Військова академія, м.Одеса, ORCID: 0000-0002-0729-9581.

Ряба Людмила Олександрівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-7436-4443.

Саєнко Олександр Григорович, кандидат технічних наук, начальник кафедри Військово-гуманітарних дисциплін Військового інституту телекомунікацій та інформатизації імені Героїв Крут, ORCID: 0000-0001-7127-6686.

Сєлюков Олександр Васильович, доктор технічних наук, професор, старший науковий співробітник, Лауреат Державної премії України в галузі науки і техніки, професор кафедри Київський національний університет будівництва та архітектури, ORCID: 0000-0001-7979-3434.

Скачков Валерій Вікторович, доктор технічних наук, професор, головний науковий співробітник наукового центру, Військова академія, м.Одеса, ORCID: 0000-0003-2432-4176.

Слуцький Євген Володимирович, кандидат економічних наук, викладач, Військова академія, м.Одеса, ORCID: 0000-0003-2696-5831.

Солодєєва Людмила Василівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-7979-8443.

Стоянова-Коваль Світлана Савівна, доктор економічних наук, професор, професор кафедри, Військова академія, м.Одеса, ORCID:0000-0002-1945-0509.

Толок Ігор Вікторович, кандидат педагогічних наук, доцент, Заслужений працівник освіти України, Лауреат Державної премії України в галузі освіти, начальник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-6309-9608.

Федченко Олексій Петрович, кандидат військових наук, старший науковий співробітник, старший науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0003-1343-3828.

Харченко Олександр Володимирович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник Державного науково-дослідного інституту авіації, ORCID: 0000-0002-9972-5233.

Черноног Олександр Олександрович, державний експерт експертної групи кібербезпеки Директорату політики цифрової трансформації Директорату політики цифрової трансформації та інформаційної безпеки у сфері оборони Міністерства оборони України, ORCID: 0000-0002-3667-8994.

Шаціло Петро Васильович, кандидат технічних наук, доцент, доцент кафедри Військово-гуманітарних дисциплін Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Алфавітний покажчик

Увага!

Редакційна колегія починає підготовку до включення «Збірника наукових праць Військового інституту КНУ імені Тараса Шевченка» до наукометричних баз Web of Science та Scopus.

В дійсному випуску розміщується перша стаття з виконанням усіх вимог для цих баз даних (С.115 – 131). Звертаємось до авторів щодо пріоритетності цих вимог в опублікуванні в подальшому. Ці вимоги поки що не обов`язкові, однак у разі вдалості експерименту вони будуть змінені, а автори будуть мати певні пріоритети.

Просимо постійних авторів надавати зауваження та пропозиції щодо представлення та оформлення перспективних матеріалів до «Збірника наукових праць Військового інституту КНУ імені Тараса Шевченка»

Редакційна колегія, т. +38 (044) 521 – 33 – 82
Ел.адреса редактора: lenkov_s@ukr.net
моб.т. 067 976 15 39

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

№ 74

Усі матеріали надруковані в авторській редакції.

Підписано до друку 4.02.22 р.
Авт. друк. Арк. 11. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ломоносова 81

т. 521-32-89