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

№ 68

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 – 2020

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2020. № 68. 132с.

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.

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», в якому можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата технічних наук.

Затверджено на засіданні вченої ради ВІКНУ від 17.12.2020р., протокол № 6.

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

ЗАГАЛЬНІ ПИТАННЯ

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

INFORMATION TECHNOLOGIES

GENERAL QUESTIONS

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

UDC 621.039.564

D.Sc. **Banzak O.V.** (OSATRQ)
D.Sc. **Maslov O.V.** (ONPU)
D.Sc. **Mokritsky V.A.** (ONPU)
Ph.D. **Leschenko O.I.** (OSATRQ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-01

DETECTOR SIMULATION FOR RADIATION MONITORING SYSTEMS

In the work, a model of primary transducer - gamma radiation sensor has been created. It is based on the following properties of a semiconductor crystal: maximum quantum efficiency; maximum mobility of charge carriers; minimum density of structural defects; maximum values of resistivity and density. The combination of these properties provides significant sensor sensitivity with a minimum crystal size. The inconsistency of this combination must be eliminated both in the process of crystal fabrication (for example, a high-resistance crystal is obtained by the simultaneous use of purification, components, and compensating doping) and subsequent processing by the methods proposed in this work (thermal field method, ionization annealing).

To register small signals, it is necessary to have minimal loss currents at sufficiently high voltages applied to the sensor. This means that the semiconductor material must be highly resistive.

Among the known materials for gamma radiation sensors, single crystals of $Cd_xZn_{1-x}Te$ solid solutions have an optimal combination of the properties listed above and the possibilities of their production.

The creation of a model gamma-radiation detector as a single system of primary and secondary converters is considered. It contains physical analysis and analytical presentation of processes occurring in CdZnTe-sensor and electronic preamplifier. It is shown that the charge collection in the sensor differs in time, which leads to a spread of signal pulses in duration and amplitude. In this regard, the model shows need to use a charge-sensitive preamplifier.

Keywords: model of primary converter, gamma radiation sensor, detector, maximum quantum efficiency, single crystals of solid solutions

Introduction and problem statement. 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 more close to us in time works by Dmitriev A.B., Perelman S.N., Tchaikovsky V.G., as well as Baranov V.I., Golbek G.R., Nemirovsky B.V., Yakubovich A.L. and many others. The basis of the progress nuclear instrumentation was the simultaneous development of two directions - 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 the appearance of such a complex is provided in materials science by the works of V.S. Vavilov, P.I. Baransky, in applied nuclear physics research - M.V. Maksimov, O.V. Maslov 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, development of atomic energy, the spread of 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 NES protective barriers that meet the requirements of the existing automatic control of radiation safety (ACR).

Main part. The structural diagram of the detector consists of two main parts: a primary converter of ionizing radiation energy (IR) into an electrical signal - sensor; secondary converter of this electrical signal.

The characteristics of the detector are mainly determined by the physical properties of the semiconductor crystal as a sensitive element of the primary converter, as well as by the features of process recording an electrical signal.

Model of physical processes in the primary and secondary converters of detector.

The equivalent circuit of the semiconductor sensor contains, in addition to the diode *D* itself, depletion zone capacitance C_D, parasitic capacitance C_S, leakage resistance R_L and "trajectory" resistance R_S. The latter is a combination of resistances of output electrodes. The capacitance of a diode also depends on the voltage and quality of crystal. This dependence can be approximately represented in form [1, 2]:

$$C_{Д} = 21 \cdot 10^3 A \left(\rho U_b\right)^{-\frac{1}{2}}, \text{ pF}, \tag{1}$$

where A – is sensor area, sm^2; ρ – resistivity of semiconductor material; U_b – locking voltage.

The given dependence can be used for a comparative assessment of sensor activation modes.

One of important characteristics of the sensor is level of signal parasitic components – noise that are not associated with the physical processes of interaction between crystal and IR. The noise level determines the minimum threshold for recording IR energy.

The conversion of the energy lost by particle in sensor into an electrical signal of the corresponding amplitude occurs with an accuracy characterized by the resolution of system. The latter depends on many reasons, in particular, on properties of amplifier. Indeed, since the amplitude of signal generated by semiconductor sensor is small, distortion of amplitude spectrum is caused, first of all, by modulation by noise pulses arising in it and in the resistances. Adding chaotically to the useful signals, the noises "blur" original amplitude spectrum. Distribution of noise in amplitude – Gaussian:

$$p(U) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{-\frac{(U_i - \overline{U})^2}{2\sigma^2}}, \tag{2}$$

where σ^2 – is variance or mean square of deviation amplitude U_i from mean $\overline{U}$.

Let us assume that all other reasons that distort the spectrum of the signal amplitude, compared to influence of noise, are negligible and register monochromatic charged particles, leaving all the energy in the sensor. In this case, the measured spectrum of signal amplitudes (Fig. 1) is also determined by expression (2). However, now $\overline{U}$ – is average signal amplitude and σ is determined by the noise, with equal to the rms noise voltage $\sqrt{\overline{U_ш^2}} = U_ш$. The width of curve at half maximum is called resolution $\frac{1}{2}\Delta$. Substituting the value $\boldsymbol{p}(\boldsymbol{U}) = \frac{1}{2}\boldsymbol{p}(\overline{\boldsymbol{U}})$ in equation (2), it is easy to obtain

$\frac{1}{2}\Delta = 2.36\sigma$. By measuring the resolution in units of energy (in electron volts), it is possible to determine what part of energy corresponds to noise level, recalculated to the input of this amplifier [3, 4].

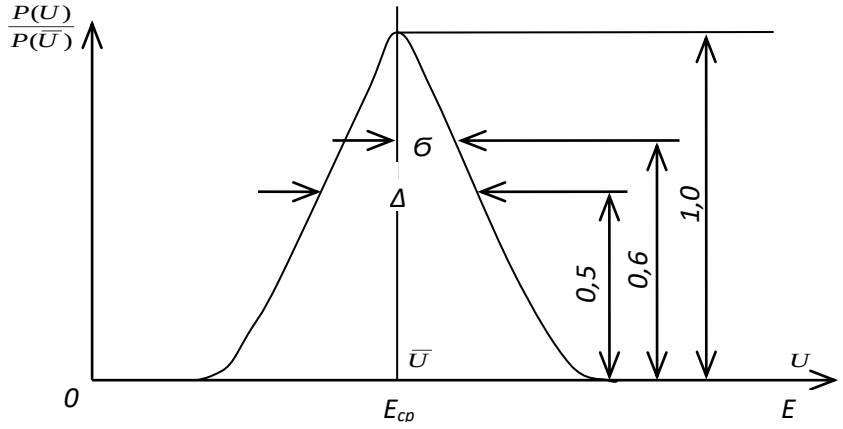


Figura 1 – Expansion of power line due to noise

The absolute value of the capacitance of the C_D, as well as of the parasitic capacitance C_S, largely determines the noise level, and with it the energy resolution of the charge-sensitive preamplifier. The current flowing through the leakage resistance R_L is another source of noise, which also leads to poor energy resolution.

For the subsequent devices of the detector to work - an amplitude analyzer, discriminator, coincidence circuit - an amplifier with a large gain is required. Usually the amplifier consists of two separate blocks: the preamplifier and the main amplifier. This separation is due to the desire to minimize input capacitance *C*, which affects the resolution, while preamplifier is located near sensor. The signal, amplified by first unit to a level at which the noise of subsequent amplifier practically does not affect, is transmitted to second unit via a matched cable. Particular attention should be paid to obtaining a minimum of noise in the preamplifier [5-7].

For noise analysis, let us consider in more detail the equivalent circuit of preamplifier. Noise, like a signal, can be expressed numerically in terms of voltage, charge, or energy. With energy losses *E*, electron-hole pairs are formed $N = \frac{E}{\overline{W_p}}$, giving a charge *Q* at the total input capacitance *C*. If $\tau_{вх} = RC$ it is large compared to the time of charge collection, then signal amplitude $U' = \frac{Q}{C}$. For further consideration, we will take into account the action of the forming chains. As a result of passing through the differentiating and integrating circuits $\tau_u = \tau_\partial = \tau$ (this case is often used in practice), the signal will decrease by a factor of *e* = 2.72, i.e. number $U = \frac{Q}{C \cdot e}$ of charge carriers $Q_ш = U_ш C \cdot e$ and, finally $N_ш = \frac{Q_ш}{q}$, to the equivalent noise energy [8]:

$$E_ш = \frac{U_ш C \cdot e \overline{W_p}}{q} .$$

Often when evaluating noise properties of amplifiers, the ratio signal to noise $\eta = \frac{U}{U_{uu}}$.

Knowing η signal and, it is not difficult to determine U_{uu} and $\frac{1}{2}\Delta$.

The spectral density of the parallel noise current is:

$$\frac{i_p^{-2}}{\Delta f} = 2qI + \left(\frac{4kT}{R_p}\right), \tag{3}$$

where I – is the sum (modulo) of all currents acting in parallel to the sensor; R_p – resistance of all resistors connected in parallel with the sensor; Δf – fragment of the spectral characteristics; T – absolute temperature.

This spectral density can be expressed by one equivalent noise impedance R_p, the value of which is determined by the ratio:

$$\frac{1}{R_p} = \frac{qI}{2kT} + \frac{1}{R_S}. \tag{4}$$

Parallel noise is frequency independent, but the voltage it creates at input capacitance C, as well as the input signal, depends on the frequency in inverse proportion:

$$\frac{\bar{u}_p^2}{\Delta f} = 4kT \frac{1}{R_p} \frac{1}{(\omega C)^2}. \tag{5}$$

Another source of noise in the input stage is determined by input amplifier, principle of its amplification. This noise does not depend on the input elements, so it is convenient to take it into account by the equivalent noise impedance R_S connected in series with the amplifier input. For a field effect transistor, the series equivalent noise impedance is $R_S \approx \frac{1}{S}$, where S – is the slope of the transistor's input characteristic. The sequential noise intensity is also frequency-independent and amounts to:

$$\frac{\bar{u}_s^2}{\Delta f} = 4kTR_S. \tag{6}$$

In some cases, especially when registering X-ray radiation, the noise component of transistors of the type $\frac{1}{f}$ plays a significant role. This noise can be determined by the formula:

$$\frac{\bar{u}_s^2}{\Delta f} = \frac{A_f}{f^{\alpha}}, \tag{7}$$

where A_f – is a constant coefficient depending on the manufacturing technology of transistor; $\alpha \approx 1$.

The total noise voltage of noise sources at the amplifier input is:

$$\overline{U_{uu}^2} = (4kT\frac{1}{R_p}\frac{1}{\omega^2 C^2} + 4kTR_s + \frac{A_f}{f})\Delta f = N(\omega)\Delta f, \quad (8)$$

where $N(\omega)$ – is the spectral density of input noise; Δf – narrow differential frequency bandwidth; $f = \frac{\omega}{2\pi}$.

In (8) $N(\omega)$ is the spectral density of the input noise Δf – narrow differential bandwidth of frequencies around the frequency $f = \frac{\omega}{2\pi}$. Narrowband amplifiers are only suitable for amplifying sinusoidal signals. The frequency response $K(\omega)$ of spectrometric amplifiers extends from low to high frequencies and the noise level U_{uu} at amplifier output is determined by the integral expression:

$$\overline{U}_{uu}^2 = \frac{1}{2\pi}\int_0^{+\infty} \left|N(\omega)\right\| K(\omega)\Big|^2 d\omega. \quad (9)$$

The limiting effect of $K(\omega)$ amplifier bandwidth also affects the waveform. The dependence of amplifier output signal on time can be determined by inverse Fourier transform formula:

$$S_2(t) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} S(\omega)K(\omega)e^{j\omega t}d\omega.$$

The choice of the best frequency response of spectrometric channel in order to obtain the maximum signal-to-noise ratio is essence of optimal filtering [9, 10].

The purpose of spectrometric amplifier is undistorted transmission and amplification of the amplitude of input signal, and not of its shape or rising edge. Therefore, with the appropriate circuits, it is necessary to select such a form of frequency response amplifier, at which the main spectrum of signal frequencies passes, but the noise spectrum is limited as much as possible. These requirements are contradictory, since maximum signal amplification requires widening the bandwidth, while bandwidth must be narrow to suppress noise. It is possible to find the best shaping circuits if we use some conclusions of theory of optimal methods radio reception, developed by V.A. Kotelnikov et al. [1, 10].

According to this theory, the square of maximum possible signal-to-noise ratio is [11]:

$$(\eta_{макс}^{\infty})^2 = \frac{2}{\pi}\int_0^{\infty}\frac{U^2(\omega)}{U_{uu}^2(\omega)},$$

where $U(\omega)$ and $U_{uu}(\omega)$ – are signal and noise spectrum at amplifier input, respectively.

It is shown theoretically that the maximum signal-to-noise ratio in this case is achieved at equal integration and differentiation time constants $\tau_{CR} = \tau_{RC} = \tau$. In this case, the noise level is minimal at some optimal time constant τ_0:

$$\tau_0 = C\sqrt{R_S R_P}. \quad (10)$$

Then the noise level at amplifier output is determined by integral expression:

$$\overline{U_{ш}^2} = \frac{1}{2\pi}\int_0^\infty N(\omega)\frac{\omega^2\tau^2}{(1+\omega^2\tau^2)^2}d\omega = 4kT\frac{R_S}{8\tau} + \frac{4kT\tau}{8C^2R_P} + \frac{A_f}{2}. \quad (11)$$

As can be seen from (11), serial noise depends inversely, parallel one is proportional, and type noise $\frac{1}{f}$ does not depend at all on τ. Minimum noise value at $\tau=\tau_0$ equals $\overline{U_{ш.мин}^2} = \frac{kT}{C}\sqrt{\frac{R_S}{R_P}}$ (excluding $\frac{1}{f}$ type noise). Considering that with CR-RC shaping, the amplitude of the output signal does not depend on τ, the minimum noise corresponds to maximum signal-to-noise ratio:

$$\eta_{макс}^{RC} = \frac{S_{2макс}}{U_{ш.мин}} = (\frac{2}{e})\frac{Q}{\sqrt{4kTC}}\sqrt[4]{\frac{R_P}{R_S}} = (\frac{2}{e})\eta_\infty. \quad (12)$$

This formula shows ratio of amplitude output voltage to the RMS voltage of output noise. The input signal to the spectrometric amplifier is charge *Q* or energy *E* released by the ionizing radiation in the sensor, therefore, in practice, it is customary to express the noise level also in terms of charge or energy. Having accepted $\eta_{макс}^{RC}=1$, we find the equivalent rms noise charge for CR-RC formation:

$$\sigma_q^{RC} = (\frac{e}{2})\sqrt{4kTC}\sqrt[4]{\frac{R_S}{R_P}} = 1{,}36\sigma_q, \quad (13)$$

where σ_q is minimum possible noise charge.

To determine the energy equivalent of input noise δ_E, it is sufficient to multiply the equivalent noise charge δ_q by energy of formation an electron-hole pair ε:

$$\sigma_E(эВ) = \sigma_q(eiectron)\varepsilon(eV/pair).$$

In spectrometric practice, to estimate the noise of amplifiers, it is more often not standard σ_E deviation that is used, but the distribution width at level of 0.5 of the maximum value. This value in the domestic literature is called the energy resolution:

$$\frac{1}{2}\Delta_E = 2{,}35\sigma_E. \quad (14)$$

In practice, one more way of expressing the noise properties of spectrometric amplifiers is widely used - in form of the dependence energy resolution (or equivalent noise charge) on the external capacitance at the input of amplifier *C*. Indeed, the total noise contribution to the energy resolution can be approximately represented in the form of two terms:

$$\Delta_E = \sqrt{\varepsilon^2 (C_{П.Т.}^2 \frac{R_S}{\tau}) + \varepsilon^2 \frac{R_S}{\tau} C_Д^2} \approx (\Delta_E)_0 + \varepsilon \sqrt{\frac{R_S}{\tau}} C_Д . \quad (15)$$

The first term $(\Delta_E)_0$ does not depend on the external capacitance and represents initial noise contribution of amplifier at zero capacitance of the sensor, it is determined by parallel noise and partially serial. The second term grows with an increase in the sensor capacitance. The multiplier here represents the slope of the dependence noise characteristic on external capacitance.

Consider the shape of the output signal at optimal shaping. It is known that the frequency response of an amplifier with optimal shaping can be represented as a result of the action of two linear filters $\Phi_1(\omega)$ and $\Phi_2(\omega)$. In this case, the linear filter $\Phi_1(\omega)$ converts noise so that it becomes white at filter output, i.e. with a uniform spectrum:

$$\left|\Phi_1(\omega)\right|^2 = \frac{1}{U_ш^2(\omega)} = \frac{\omega^2 C^2}{4kTR_S\omega^2 C^2 + 2qI_c + C_Д} . \quad (16)$$

Thus, modified signal and white noise will enter the input of the second filter. As a result, i.e. the frequency response of filter repeats (in modulus) the spectrum of signal supplied to it. The multiplier means that the filter is delayed by a time equal to duration of input pulse. At the moment, amplitude is measured, since it is at this moment that the output signal reaches its maximum. In this case, pulse is infinite and is determined by the maximum allowable delay in the moment of amplitude measurement.

$$U'(t) = \frac{Q}{C} \cdot e^{-\frac{t}{\tau_{опт}}} . \quad (17)$$

The frequency response and uniquely determine the transient response of the filters, and therefore the overall amplifier. The transient response of the first filter matches the waveform at the input of the other filter. The transient response of the second filter, where $h_2(t)$ – is the impulse response to a unit δ-function equal to the mirror image of the signal.

In the case of simple RC-RC shaping, maximum voltage corresponds $t_м = \tau_{опт}$, so it is interesting to know what gives optimal shaping for the same $t_м$:

$$\eta_{макс}^t = \sqrt{1 - e^{-2}}\,\eta_{макс}^\infty = 0{,}93\eta_{макс}^\infty . \quad (18)$$

It is known that $\eta_{макс}^t = 0{,}74\eta_{макс}^\infty$. Consequently, the gain compared to simple formation is 26%.

The presented model of the primary converter allows, taking into account the real properties of the crystal, to calculate dependences of energy equivalent noise on the time constant of the input stage preamplifier.

Conclusions. In the work, a model of primary transducer - gamma radiation sensor has been created. The model allows calculating the dependence of energy equivalent of noise on the properties preamplifier input stage, taking into account the real properties of crystal. It is shown that:

- increasing the crystal volume, bias voltage and sensor capacitance increases the noise level;

- results of the analysis applied to CdZnTe crystals used in this work indicate the possibility of the sensor operation without cooling.

In the work, a model of a gamma radiation detector has been created as a single system of primary and secondary converters. It contains physical analysis and analytical presentation of the processes occurring in the CdZnTe sensor and electronic preamplifier. It is shown that the charge collection in sensor differs in time, which leads to a spread of signal pulses in duration and amplitude. In this regard, the model shows need to use charge-sensitive preamplifier.

The main advantage of model is solution to problem of optimizing the signal-to-noise ratio in the detector. It is shown that:

- energy resolution of a charge-sensitive preamplifier is determined by the level of noise, which depends on capacitance of sensor, and therefore on the bias voltage and crystal quality;

- in order to obtain the maximum signal-to-noise ratio, it is necessary to select the frequency response of spectrometric path according to the theory of optimal filtering by V.A. Kotelnikov; for this, filters of both low and high frequencies must be included in the path; thus, simplest driver of a spectrometric amplifier should consist of a CR-RC filter; optimal shaping gives a 26% signal-to-noise ratio gain over simple shaping.

REFERENCES:

1. Vavilov V.S. Effect of radiation on semiconductors / V.S. Vavilov, N.P. Kekelidze, L.S. Smirnov. - M .: Science, 1988. - 192 p.

2. Lenkov S.V. Physico-technical basis of radiation technology semiconductors / S.V. Lenkov, V.A. Mokritsky, D.A. Peregudov, G.T. Tarielashvili. - Monograph. - Odessa: Astroprint, 2002. - 297 p.

3. Garkavenko A.C. Radiation modification of the physical properties of wide-gap semiconductors and the creation of high-power lasers on their basis / Lviv: ZUKTS, 2012. - 258 p.

4. Bansak O.V. Semiconductor detectors of new generation for radiation monitoring and dosimetry of ionizing radiation / OV Banzak, O.V. Maslov, V.A. Mokritsky: Ed. V.A. Mokritskogo, O.V. Maslova. - Monograph. - Odessa, 2013. - Publishing House "WWII". - 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, – Pp. 507-513.

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. – Pp. 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. – Pp. 12-87.

11. Masuruk K. Dopant incorporation during liquid phase epitaxy / K. Masuruk, T.Bryskewicz // J. Appl. Phys., 1981. – V. 52. – N3. – part 1. – Pp. 1347–1350.

12. 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. – Pp. 114-116.

д.т.н., доц. Банзак О.В., д.т.н., доц. Маслов О.В.,
д.т.н., проф. Мокрицький В.А., к.т.н., доц. Лещенко О.І.

МОДЕЛЮВАННЯ ДЕТЕКТОРА ДЛЯ СИСТЕМ РАДІАЦІЙНОГО КОНТРОЛЮ

У роботі створена модель первинного перетворювача - датчика гамма-випромінювання. Вона заснована на наступних властивостях кристала напівпровідника: максимальна квантова ефективність; максимальна рухливість; мінімальна щільність дефектів структури; максимальні значення питомої опору і щільності. Поєднання перерахованих властивостей забезпечує значну чутливість датчика при мінімальних розмірах кристала. Суперечливість такого поєднання необхідно усувати як в процесі виготовлення кристала (наприклад, високоомний кристал отримувати одночасним застосуванням очищення, компонентів і компенсуючого легування), так і подальшою обробкою запропонованими в даній роботі методами (термополевий метод, іонізаційний отжиг).

Для реєстрації малих по величині сигналів необхідно мати мінімальні струми втрат при досить великих напругах, доданих до датчика. Це означає, що напівпровідниковий матеріал повинен бути високоомним.

Серед відомих матеріалів для датчиків гамма-випромінювання оптимальним поєднанням перерахованих вище властивостей і можливостями їх отримання мають монокристали твердих розчинів $Cd_xZn_{1-x}Te$.

Розглядається створення моделі детектора гамма-випромінювання як єдиної системи первинного та вторинного перетворювачів. Вона містить фізичний аналіз і аналітичне уявлення процесів, що відбуваються в CdZnTe-датчику і електронному зовнішньому підсилювачу. Показано, що в датчику збір зарядів різниться в часі, що призводить до розкиду імпульсів сигналу по тривалості і амплітуді. У зв'язку з цим в моделі показана необхідність використання зарядово-чутливого попереднього підсилювача.

Ключові слова: модель первинного перетворювача, датчик гамма-випромінювання, детектор, максимальна квантова ефективність, монокристали твердих розчинів.

UDC 681.3(07)

Ph.D. **Tolok I.V.** (MIKNU)
Ph.D. **Banzak G.V.** (OSATRQ)
Ph.D. **Lenkov E.S.** (CSRI AME OF Ukraine)
Vozikova L.M. (OSATRQ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-02

COMPARATIVE STUDY OF DIFFERENT MAINTENANCE STRATEGIES

A characteristic feature of complex technical objects for special purposes is the presence in their composition of a large number (tens, hundreds of thousands) of various types component parts, which have different levels of reliability, different patterns of their wear and tear processes. This feature requires a more subtle approach to the organization and planning of maintenance in course of their operation.

The problem is that in the development of such facilities, all issues related to maintainability and maintenance should be addressed already at the early stages of facility design. If you do not provide in advance the necessary hardware and software for the built-in monitoring of technical condition (TC) of the object, do not develop and "build" the maintenance technology into the object, then it will not be possible to realize in the future a possible gain in the reliability of the object due to maintenance. Since all these issues must be resolved at the stage of object creation (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 the facility due to maintenance, to estimate the cost costs required for this. Then, on the basis of 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 acceptable maintenance strategy, and determine its optimal parameters.

The article shows that the optimal parameters of various maintenance strategies significantly depend on both the reliability and cost structure of the facility and specified requirements for the facility's reliability $T_0^{\text{тр}}$***. The higher the specified value*** $T_0^{\text{тр}}$***, the more serviced items should be included in the optimal maintenance strategy.***

It has also been proven that the effectiveness of various maintenance strategies depends significantly on the reliability and cost structure of object. If the distribution of cost restored (including serviced) elements is closely correlated with the distribution of their reliability indicators, difference in effectiveness of different maintenance strategies is reduced. This is clearly seen in the example of Test-2 object, for which the least reliable elements are also the most expensive.

Keywords: maintance strategy, components, reliability level, facility structure.

Introduction. Complex technical objects in modern society are extremely important. We are talking primarily about various radio-electronic systems for military and special purposes, radar stations, automated control systems (air traffic, energy facilities, etc.). The state's defense capacity, economic security, and the lives of hundreds and thousands of people depend on the level of reliability of such facilities.

Such objects belong to the class of recoverable objects of long-term repeated use. They are usually expensive and costly to operate. To ensure the required level of reliability during their operation, maintenance is usually carried out, the essence of which is timely preventive replacement of elements in a pre-failure state.

Analysis of recent research. The “surge” in number of theoretical works on the maintenance of complex systems falls on 70s of the last century, which can be explained by the mass production of complex radio-electronic equipment for military and special purposes at that time [1-4]. Currently, there is a decline in the number of scientific publications devoted to the maintenance of complex technical objects. One of reasons for this, in our opinion, is the sharp increase in the level of integration and reliability of components. Thanks to this, the developers of complex equipment were able to solve the issues of ensuring required level of reliability without significant maintenance costs (or without maintenance at all). However, the same reason (high integration and reliability of component parts) opened up the possibility of implementing more and more complex technology with new functions, which was impossible with the old element base. This again leads objectively to the

problems of ensuring reliability and, therefore, question of the need for maintenance and the choice of optimal strategy for its implementation again becomes relevant.

Formulation of the problem. Unfortunately, the currently known mathematical models and methods for calculating the optimal parameters of MC 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 an object at all, or it is possible to take into account only some of the simplest structures [5, 6]. In [7], a comparative analysis of the problems arising in solving the problems of maintenance "by resource" and "by state" is made. An overview of the latest work in the field of maintenance and repair of complex systems for that period is given. In [8], a theoretical generalization of the known mathematical models of MC processes is made. However, these models do not allow constructing methods suitable for practical use on their basis.

In our opinion, the situation is even worse with mathematical models of MC processes "by state". Only a small number of scientific works are devoted to this area of research [9-11].

Thus, the work solves the urgent scientific problem of developing methods and tools (software) to determine the optimal parameters of the maintenance strategy "by state" of complex technical objects.

Main part. The complexity of maintenance processes and the variety of factors influencing them significantly complicate the choice between different maintenance strategies. For an objective comparison of the advantages and disadvantages of various maintenance strategies, it is necessary to ensure the approximate equality (sameness) of the conditions in which they are applied.

When comparing different maintenance strategies, we will be guided by the following principles:

- it is possible to compare different maintenance strategies only by the results of their application to the same object;

- test objects (on which the comparison of maintenance strategies is made) should be comparable in terms of the structure time and cost costs for maintenance and maintenance;

- indicators of the quality maintenance process (objective functions), according to which the comparison of various maintenance strategies is made, should be evaluated at the same intervals of the object's operation and with the same parameters of modeling process (if the comparison of maintenance strategies is made based on the simulation results);

- characteristics of maintenance process obtained with the optimal parameters of maintenance strategies should be compared, that is, the potential capabilities of various maintenance strategies should be compared.

In this study, 4 test objects are used that differ in their reliability and structural characteristics. This, among other things, makes it possible to check and simultaneously demonstrate the "performance" of developed methods for determining the optimal parameters of various maintenance strategies for different initial data.

To ensure the comparability of the structure of time and cost costs for maintenance and current repairs, the characteristics of maintainability and cost that are the same for all elements and objects were set:

- average recovery time of an element $\tau_{\text{в}i}$ = 1 h;

- average duration of maintenance $\tau_{\text{то}i}$ = 1 h;

- item cost C_i = 10 c. u.;

- cost of operation current repair (replacement) of the element $C_{\text{тр}i}$ = 1 c. u.;

- cost of the maintenance operation of element $C_{\text{то}i}$ = 1 c. u.;

STD characteristics for test objects are set as follows:

- duration of diagnostics at MC $\tau_{\text{д}}$ = 0.5 h;

- cost of the diagnostic operation at MC $C_{\text{д}}$ = 1 c.u.

The same for all test objects are also set the indicators depending on the purpose of object - the specific cost losses incurred by the external system (in which this object is used) in the object failure state $c_{отк}$ = 10 c.u. / h, and in the MC state $c_{то}$ = 1 c .u. / h.

For all test objects, using the developed methods, optimal parameters for three maintenance strategies were determined. For brevity, as before, we will call them: “MC by state”, “adaptive MC” and “MC by resource”.

All calculations were made for the duration of operation $T_э$ = 20 years with continuous operation of the facilities.

The optimal parameters of various maintenance strategies were determined under the idealized assumption of the existence for test objects of measurable determining parameters for the least reliable elements $E_{то}$ related to the set of recoverable elements $E_в$. The subsets of potentially serviced items were specified in such a way that they included all the least reliable items. There are no elements in test objects, reliability of which would be lower than the reliability of any elements $E_{то}$ ($E_{то} \subset E_в$). Obviously, under this condition, with the optimal parameters of maintenance strategies, maximum, potentially possible efficiency of maintenance is provided, which is most likely unattainable in practice.

Table 1 - 4 presents the final results of calculating optimal parameters of various maintenance strategies. In fig. 1 - 4 shows the graphs of the mean time T_0 between failures and the unit cost of operation $c_{уд}$ from the number of serviced elements, obtained with the optimal parameters of the corresponding maintenance strategies.

Table 1

Comparative evaluation of indicators, T_0, $c_{уд}$ and $K_{ти}$ for object Test-1 with different maintenance strategies

Maintenance strategy		Maintenance condition	Adaptive maintenance	Maintenance by resource	Without maintenance
Indicators (target functions)	T_0, h	1660	1662	1609	1236
	$c_{уд}$, c.u./h	0,01461	0,01408	0,01695	0,02187
	$K_{ти}$	0,99851	0,99877	0,99689	0,99919
	ε	0,180	0,179	0,184	0,085
Optimal maintenance strategy parameters ($T_0^{тр}$ = 1500 h)		$\lvert E_{то}^* \rvert$ =3 $U_{то}^*$ ={0,5;0,4;0,5} $T_к^*$ = 1200 h	$\lvert E_{то}^* \rvert$ =3 $U_{то}^*$ ={0,5;0,4;0,5} γ^* = 0,45; β = 0,5	$N_{то}^*$ = 1 $\lvert E_{то1}^* \rvert$ =3 $T_{то}^*$ = 1400 h	-

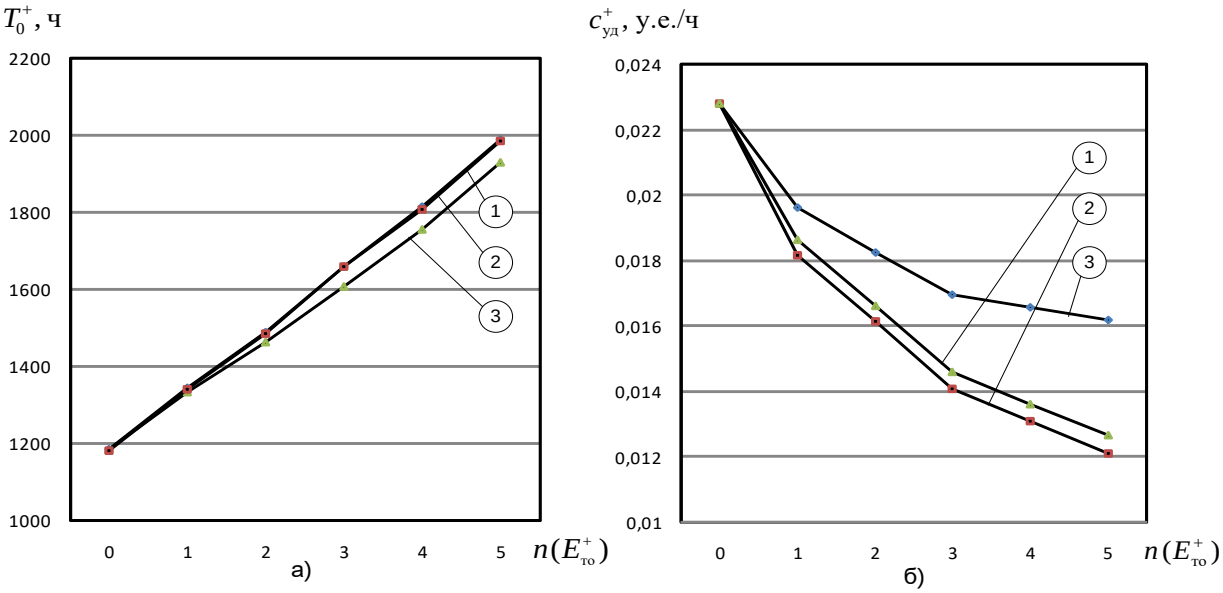


Figure 1 – Graphs dependence indicators T_0^+ and $c_{уд}^+$ on the number of serviced elements for various maintenance strategies (object Test-1):
1 - maintenance by condition; 2 - adaptive maintenance; 3 - maintenance by resource

Table 2

Comparative assessment of indicators T_0, $c_{уд}$ and $K_{ти}$ for the object Test-2 with different maintenance strategies

Maintenance strategy		Maintenance strategy condition	Adaptive maintenance	Maintenance by resource	Without maintenance
Indicators(target functions)	T_0, h	695	702	676	294
	$c_{уд}$, c. u./h	0,09852	0,08801	0,12009	0,66572
	$K_{ти}$	0,98610	0,99374	0,97564	0,99708
	ε	0,111	0,112	0,113	0,069
Optimal maintenance strategy parameters ($T_0^{тр}$ = 600 h)		$\lvert E_{то}^* \rvert = 5$ $U_{то}^* = \{0,55;0,45;$ $0,25;0,6;0,5\}$ $T_к^* = 250$ h	$\lvert E_{то}^* \rvert = 5$ $U_{то}^* = \{0,6;0,55;0,6,$ $0,5;0,6\}$ $\gamma^* = 0,45;\ \beta = 0,5$	$N_{то}^* = 1$ $\lvert E_{то1}^* \rvert = 5$ $T_{то}^* = 240$ h	-

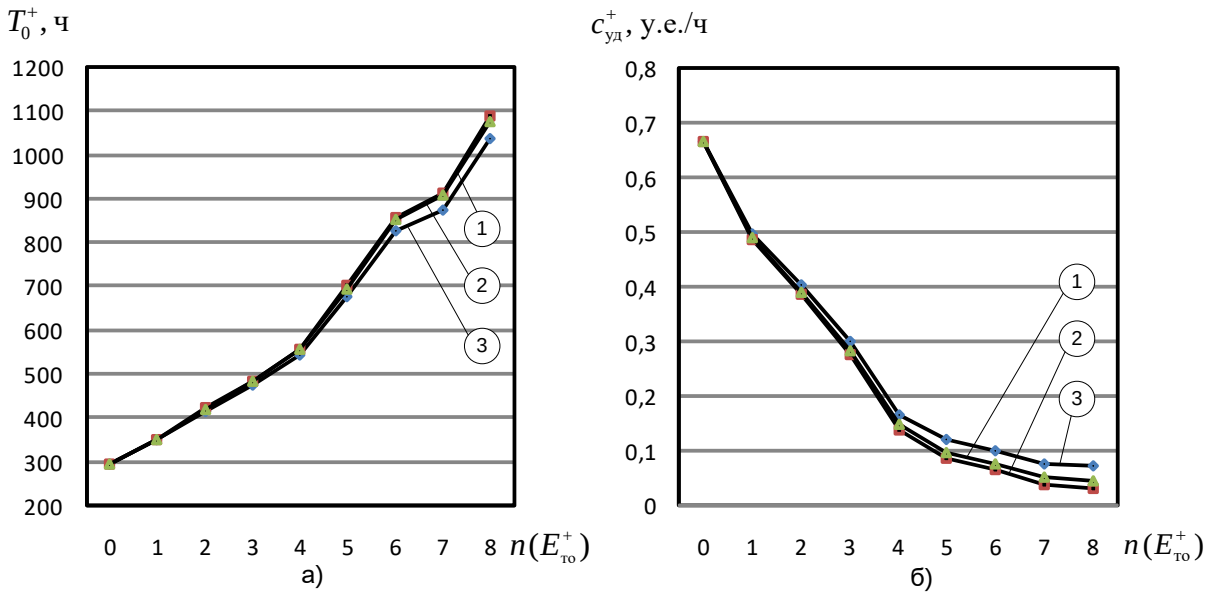


Figure 2 – Graphs of dependence indicators T_0^+ and $c_{уд}^+$ on number of serviced elements for various maintenance strategies (object Test-2):
1 - maintenance by condition; 2 - adaptive maintenance; 3 - maintenance by resource

Table 2

Comparative assessment of indicators T_0, $c_{уд}$ and $K_{ти}$ for object Test-3 with different maintenance strategies

Maintenance strategy		Maintenance condition	Adaptive maintenance	Maintenance by resource	Without maintenance
Indicators (target functions)	T_0, h	15194	15136	15009	9458
	$c_{уд}$, c.u../h	0,00154	0,00151	0,00169	0,00232
	$K_{ти}$	0,99982	0,99984	0,99967	0,99978
	ε	0,487	0,448	0,493	0,367
Optimal maintenance strategy parameters ($T_0^{тр}$ = 15000 h)		$\lvert E_{то}^* \rvert = 3$ $U_{то}^* = \{0,5;0,5;0,5\}$ $T_к^* = 10500$ h	$\lvert E_{то}^* \rvert = 3$ $U_{то}^* = \{0,7;0,6;0,5\}$ $\gamma^* = 0,4$; $\beta = 0,5$	$N_{то}^* = 1$ $\lvert E_{то1}^* \rvert = 4$ $T_{то}^* = 16000$ h	-

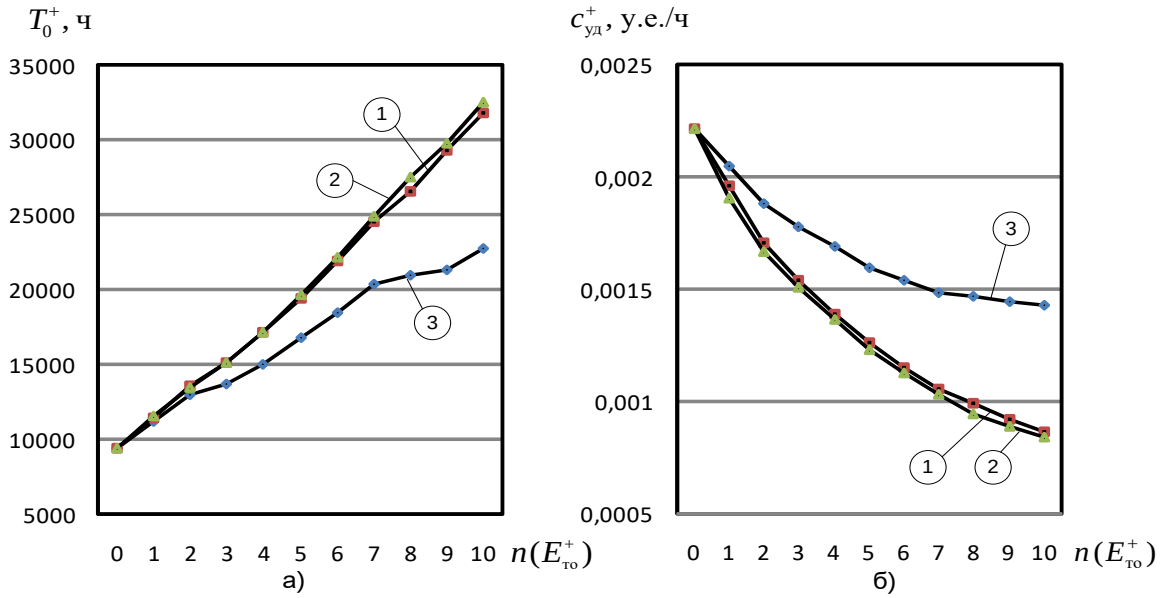


Figure 3 – Graphs of dependence indicators T_0^+ and $c_{уд}^+$ on number of serviced elements for various maintenance strategies (object Test-3):
1 - maintenance by condition; 2 - adaptive maintenance; 3 - maintenance by resource

Table 3

Comparative evaluation of indicators T_0, $c_{уд}$ and $K_{ти}$ for object Test-4 with different maintenance strategies

Maintenance strategy		Maintenance condition	Adaptive maintenance	Maintenance by resource	Without maintenance
Indicators (target functions)	T_0, h	6575	5566	4879	914
	$c_{уд}$, c.u./h	0,00668	0,00637	0,01180	0,02296
	$K_{ти}$	0,99736	0,99776	0,99323	0,99890
	ε	0,268	0,209	0,311	0,113
Optimal maintenance strategy parameters ($T_0^{тр}$ = 5000 h)		$\lvert E_{то}^* \rvert = 4$ $U_{то}^* = \{0,5;0,55;$ $0,65;0,85\}$ $T_к^* = 500$ h	$\lvert E_{то}^* \rvert = 3$ $U_{то}^* = \{0,55;0,55;$ $0,55\}$ $\gamma^* = 0,5;\ \beta = 0,5$	$N_{то}^* = 3$ $\lvert E_{то1}^* \rvert = 3$ $T_{то1}^* = 600$ h $\lvert E_{то2}^* \rvert = 3$ $T_{то2}^* = 6000$ h $\lvert E_{то3}^* \rvert = 4$ $T_{то3}^* = 22000$ h	-

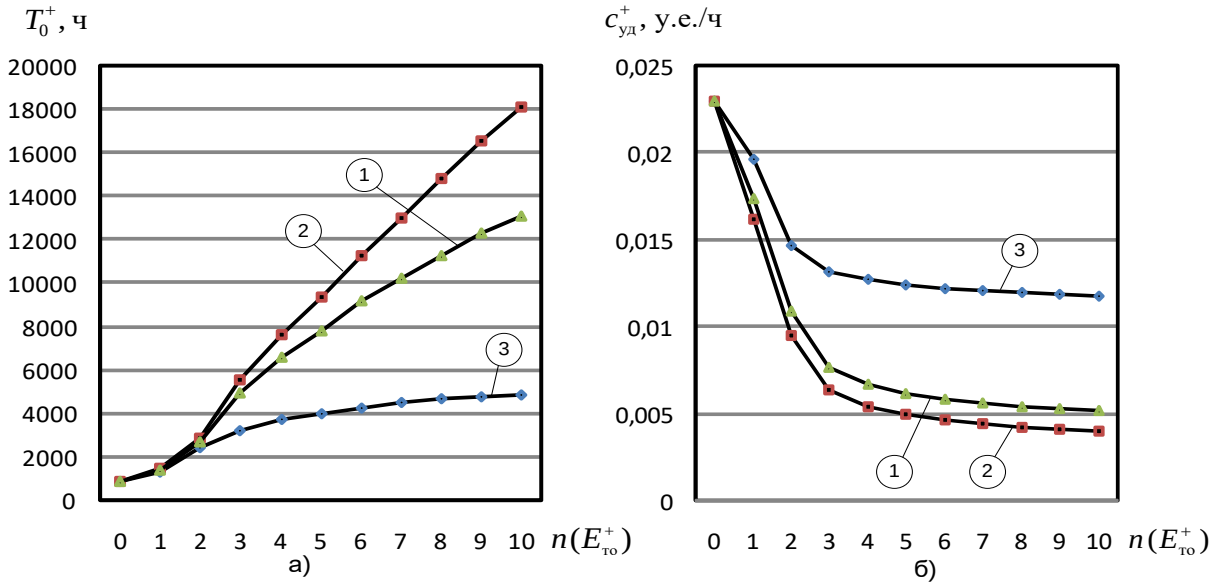


Figure 4 – Graphs of dependence indicators T_0^+ and $c_{уд}^+$ on number of serviced elements for various maintenance strategies (object Test-4):
1 - maintenance by condition; 2 - adaptive maintenance; 3 - maintenance by resource

For Test-4 object specified requirement $T_0^{тр}$ = 5000 h with the optimal “maintenance by resource” strategy is not ensured (despite the fact that all potentially serviced elements have been used).

The “adaptive maintenance” strategy has not been studied separately. The adaptive MC parameter β (exponential smoothing constant) was set equal to 0.5 for all test objects. This corresponds to a neutral situation, when the “weight” of the initial data on reliability indicators of elements (priori information) and data on the actual measured values of determining parameters (a posteriori information) is approximately the same.

Without delving into the study strategy of "adaptive maintenance", it can be assumed that adaptive maintenance is more profitable in the case of unreliable initial information about the indicators of reliability elements of object. We will check this assumption as follows.

Let us calculate indicators T_0 and $c_{уд}$ for test objects in the case when mean time to failure of all recoverable elements $T_{срi}$ is 2 times less than the indicators for which the parameters of the optimal maintenance strategy were calculated.

Obviously, indicators T_0' and $c_{уд}'$ obtained in this case should be worse in comparison with the indicators T_0 and $c_{уд}$ obtained with the initial values. Table 3 and 4 show the values coefficients of relative losses in the level of reliability δ_{T_0} and in unit cost of operation $\delta_{C_{уд}}$, which were determined by formulas:

$$\delta_{T_0} = \frac{T_0 - T_0'}{T_0} \cdot 100; \quad \delta_{C_{уд}} = \frac{c_{уд}' - c_{уд}}{c_{уд}} \cdot 100,$$

where T_0 ($c_{уд}$) - is mean time between failures (unit cost of operation) obtained at optimal parameters $T_{срi}$, provided that the indicators correspond to the values specified for test objects in test examples;

T_0' ($c_{\text{уд}}'$) - same indicators obtained with optimal parameters, but under the condition that the indicators $T_{\text{ср}i}$ in initial data are reduced by 2 times.

Based on the results obtained, the following **conclusions** can be drawn:

1. The best in terms of mean time between failures T_0 and unit cost of operation $c_{\text{уд}}$ is the "adaptive maintenance" strategy. This is followed by the "maintenance by condition" strategy. The worst is "MC by resource" strategy. The maintenance strategy is considered the best if the function graph T_0^+ is located higher (for function $c_{\text{уд}}^+$ – lower) in relation to corresponding graph for the compared strategy. The maintenance strategy, best in terms T_0^+ of performance, is usually the best in terms $c_{\text{уд}}^+$ of performance, and vice versa.

2. The strategies "maintenance by condition" and "adaptive maintenance" are very similar in terms of the obtained indicators. This is due to their common nature - during maintenance, information about the actual current state of the object is used.

3. The effectiveness of various maintenance strategies depends significantly on the reliability and cost structure of object. If distribution of the cost restored (including serviced) elements is closely correlated with the distribution of their reliability indicators, difference in effectiveness of different maintenance strategies is reduced. This is clearly seen in the example of Test-2 object, for which the least reliable elements are also the most expensive.

4. The optimal parameters of various maintenance strategies substantially depend on both the reliability and cost structure of the facility and the specified requirement for the facility's reliability $T_0^{\text{тр}}$. The higher the specified value $T_0^{\text{тр}}$, more serviced items should be included in the optimal maintenance strategy.

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 of periodicity technical maintenance of machines engineering armament during operation // Collection of scientific works of MIKNU named after T. Shevchenko. Issue 2. K .: MIKNU, 2005. - Pp. 29-32.

6. Boryak K.F. Reliability model of a complex restored object of radio-electronic equipment // Collection of scientific works of MIKNU named after T. Shevchenko. - K .: 2009. - № 21. - Pp. 33-41.

7. Reliability and efficiency in technology. Directory. T.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 .: The science, 1982. - 286 p.

9. Brown V.O., Boryak K.F., Lantvoit O.B., Tsytsarev V.N. Modeling of maintenance processes complex reconstructed objects of radio-electronic equipment // Bulletin of the Engineering Academy of Ukraine. - K., 2008. - №1. - Pp. 47 - 52.

10. Boryak K.F. Pre-service to process of technical service foldable radioelectronic equipment for additional and statistical statistical model // Bulletin of Engineering Academy of Ukraine. - K., 2008. - No. 2. - Pp. 85 - 91.

11. Banzak G.V. Database on the reliability of complex objects of radio-electronic equipment / G.V.

Banzak, K.F.Boryak, V.N. Tsytsarev // Collection of scientific works of MIKNU named after T. Shevchenko. - 2010. - No. 27. - Pp.89 - 97.

к.пед.н., доц. Толок І.В., к.т.н. Банзак Г.В., к.т.н. Лєнков Є.С., Возікова Л.М.

ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ РІЗНИХ СТРАТЕГІЙ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ

Характерною особливістю складних технічних об'єктів спеціального призначення є наявність в їх складі великої кількості (десятки, сотні тисяч) різнотипних комплектуючих елементів, які мають різний рівень надійності, різні закономірності процесів їх зносу і старіння. Ця особливість вимагає більш тонкого підходу до організації і планування ТО в процесі їх експлуатації.

Проблема полягає в тому, що при розробці таких об'єктів всі питання, пов'язані з ремонтопридатністю і технічним обслуговуванням повинні вирішуватися вже на ранніх етапах проектування об'єкта. Якщо не передбачити заздалегідь необхідні апаратні і програмні засоби вбудованого контролю технічного стану (ТС) об'єкта, що не розробити і не "вбудувати" в об'єкт технологію проведення ТО, то реалізувати в майбутньому можливий виграш в 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 в рівні безвідмовності об'єкта за рахунок проведення ТО, оцінити необхідні для цього 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 найбільш прийнятну стратегію ТО, визначити її оптимальні параметри.

У статті показано, що оптимальні параметри різних стратегій ТО істотно залежать як від надійно-вартісної структури об'єкта, так і від заданого вимоги до рівня безвідмовності об'єкта. Чим більше задане значення, тим більша кількість обслуговуваних елементів має включатися в оптимальну стратегію ТО.

Також доведено, що ефективність різних стратегій ТО істотно залежить від надійно-вартісної структури об'єкта. Якщо розподіл вартості елементів, що відновлюються (в тому числі і обслуговуються) близько корелюється з розподілом їх показників безвідмовності, відмінність в ефективності різних стратегій ТО скорочується. Це добре видно на прикладі об'єкта Test-2, для якого найменш надійні елементи одночасно є і найбільш дорогими.

Ключові слова: стратегія технічного обслуговування, комплектуючі елементи, рівень надійності, структура об'єкта.

УДК 004.056.5

к.т.н. **Ахмаметьєва Г.В.** (ОНПУ)
Баранюк Г.А. (ОНПУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-03

РОЗРОБКА СИСТЕМИ ВБУДОВИ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В ЗОБРАЖЕННЯ НА ОСНОВІ DCT-LWT-SVD

Захист авторського права на цифровий контент – досить актуальна проблема людства у XXI столітті, оскільки випадки неправомірного використання мультимедійного контенту спостерігаються дуже часто, і їх кількість постійно зростає. Одним із видів захисту авторської власності є вбудовування цифрового водяного знаку (ЦВЗ) у контент.

У роботі запропоновано новий метод вбудовування цифрового водяного знаку у зображення-контейнер з використанням дискретного косинусного перетворення (DCT), ліфтингового вейвлет-перетворення (LWT) з материнським вейвлетом «Добеші-8» та сингулярного розкладу матриці (SVD). Вбудовування здійснюється у перше сингулярне число, отримане сингулярним розкладанням області низьких частот вейвлет-перетворення. В якості цифрового водяного знаку використовуємо полутонове зображення, нормоване в діапазон від нуля до десяти для забезпечення високого показника пікового відношення сигнал/шум (PSNR).

В дослідженні проведено аналіз розробленого методу: алгоритмічна реалізація вбудовування та детектування інформації перевірена на стійкість до різних видів атак, а саме: накладання шумів (Гаусів та мультиплікативний шуми, «сіль та перець»), застосування фільтру «unsharp» та медіанного фільтру, атака стисненням (з коефіцієнтами якості для заповненого контейнеру від 60 до 100). В результаті проведеного тестування, встановлено, що метод є досить стійким до усіх аналізованих атак, окрім фільтрації «unsharp» (результуючі показники не є задовільними).

Метод показав гарні результати по піковому відношенню сигнал/шум – середнє значення PSNR дорівнює 50,5 дБ, а також високі показники вилучення вбудованого ЦВЗ – точність детектування складає від 77% до 97,6 % при збереженні заповненого контейнеру у форматі без втрат.

Ключові слова: стеганографія, цифровий водяний знак, дискретне косинусне перетворення, ліфтингове вейвлет-перетворення, сингулярне розкладання матриць, цифрове зображення.

Вступ та аналіз останніх досліджень. У наш час – вік цифрових технологій – інформація має певну ціну та цінність, тому з кожним моментом часу конфіденційна та таємна інформація знаходиться у зоні ризику. Ризики являють собою ряд факторів, що будуть впливати на властивості захищених даних. Одним з таких ризиків є отримання зловмисником або порушником незаконним шляхом необхідної інформації. Особливо цікавим є питання захисту авторського права цифрових даних. Саме тому у сфері інформаційних технологій було створено такий вид захисту інформації як цифровий водяний знак.

Цифровий водяний знак - це сигнал, що є вбудованим на постійній основі у цифрові дані (аудіо, зображення, відео та текст), який можна виявити або витягти за допомогою обчислювальних операцій для підтвердження їх наявності. ЦВЗ - це спеціальна мітка, вбудована в цифровий контент з метою захисту авторських прав і підтвердження цілісності самого документа. ЦВЗ приховується у даних контейнеру таким чином, що він стає невіддільним від них, цим самим забезпечуючи стійкість до багатьох операцій, що не погіршують контейнер [1].

Останнім часом дослідження в області цифрових водяних знаків, порівняно із іншими напрямами, стрімко зростають, адже тема захисту секретної/конфіденційної інформації стає дедалі актуальнішою. З кожним роком кількість робіт, присвячених даній темі збільшується, а методи, що існували до сьогоднішнього дня – вдосконалюються.

Серед стеганографічних методів вбудови інформації в область ДКП можна виділити роботи [2-4]. В роботах [2, 3] забезпечується висока пропускна здатність прихованого каналу зв’язку, однак візуальна цілісність заповненого контейнеру досить низька – показник пікового відношення сигнал/шум (PSNR) складає від 33 до 40 дБ. В роботі [4] навпаки забезпечуються

високі значення PSNR (від 55 до 68 дБ) за рахунок вбудови повідомлення малої довжини, що декілька обмежує область застосування запропонованого методу, особливо за необхідності вбудувати текст значного об'єму або ЦВЗ-зображення.

Щодо області вейвлет-перетворення, слід відрекомендувати роботи [5-6]. Ці алгоритми забезпечують високий рівень PSNR та об'єм інформації, що можна передати, проте головним їх недоліком є складність реалізації. Крім того, в роботі [5], незважаючи на високу стійкість до атак, пропонується система ЦВЗ напівзакритого типу [1], що не передбачає вилучення ЦВЗ.

Стаття [7] порівнює показники спотворень у заповнених контейнерах в порівнянні з оригінальним та вилучення ЦВЗ при використанні методів на основі DCT і DWT-перетворень, де перевага надається методу на основі дискретного косинусного перетворення.

Розглядаючи методи [8-12], у яких йде мова про спільне використання дискретного косинусного та дискретного вейвлет-перетворень, необхідно акцентувати на тому, що застосування цих двох перетворень в комплексі дають кращі результати, аніж їх використання окремо.

Статті [8-10] присвячені розробці закритих систем ЦВЗ, для яких характерним є використання оригінального контейнеру для вилучення ЦВЗ. В роботі [8] запропоновано систему ЦВЗ з використанням дискретного косинусного перетворення (DCT – Discrete Cosine Transform), дискретного вейвлет-перетворення (DWT – Discrete Wavelet Transform) та сингулярного розкладу матриць (SVD – Singular Value Decomposition), що дозволило отримати значення PSNR близько 52 дБ. Стаття [9] використовує комбінацію DWT і DCT-перетворень для вбудови бінарного ЦВЗ-зображення. При високих показниках PSNR та стійкості до атак візуально спостерігається посилення контрасту заповненого контейнера в порівнянні з оригіналом, що підкреслює наявність ЦВЗ в зображенні або його обробку.

В статті [11] запропонований стійкий до атак метод вбудови ЦВЗ на основі DWT-DCT-перетворень. При малих значеннях пропускної здатності забезпечуються високі показники PSNR, однак точність вилучення ЦВЗ досить низька. Однак при збільшенні об'єму повідомлення зростає точність детектування, але порівняння пустого і заповненого контейнерів дає значення PSNR с середньому 45 дБ. Робота [12] пропонує використання комбінації DWT-DCT-SVD-перетворень для методу, стійкого до атак. Однак основним недоліком методу є низькі значення PSNR (від 32 до 41 дБ).

Отже, аналіз досліджень, присвячених захисту зображень за допомогою ЦВЗ, виявив ряд протиріч між візуальною цілісністю заповнених контейнерів і точністю вилучення вбудованого ЦВЗ. Тому метою роботи є розробка методу вбудови ЦВЗ в зображення, що забезпечує високу якість заповненого контейнеру.

Основна частина. В якості контейнеру будемо використовувати кольорове цифрове зображення (ЦЗ), представлене в схемі RGB. Цифровий водяний знак представляє собою полутонове зображення або кольорове зображення, перетворене в ЦЗ в градаціях сірого. Значення яскравості ЦВЗ в діапазоні $[0,255]$ нормуються в діапазон $[0,10]$ у відповідності з формулою:

$$M' = \frac{M}{255} \cdot 10, \tag{1}$$

де M – полутонове зображення ЦВЗ, M' – нормований ЦВЗ.

Для методу, що розробляється, будемо використовувати поетапне застосування дискретного косинусного перетворення, ліфтінгового вейвлет-перетворення (LWT) та сингулярного розкладу матриці подібно методу [8], але на відміну від запропонованої в [8] системи вилучення ЦВЗ реалізується «в сліпу», тобто без використання оригінального контейнеру.

Вбудова інформації здійснюється наступним чином. Матриця контейнера поділяється на блоки 8×8, що не перетинаються. До кожного блоку застосовується дискретне косинусне перетворення. Для матриці отриманих коефіцієнтів DCT обчислюється ліфтингове вейвлет-перетворення. В свою чергу до матриці низьких частот (LL) застосовується сингулярний

розклад та виділяються сингулярні числа. В один блок матриці контейнеру можна помістити один елемент ЦВЗ. Процес вбудовування ЦВЗ здійснюється перше сингулярне число у відповідності з формулою:

$$s_1' = \begin{cases} \lfloor s_1/10 \rfloor + m', \; s_1 \geq 20, \\ 1.8m', \; m' \geq 5, \\ m' + 4, \; m' < 5, \end{cases} \tag{2}$$

де s_1 – значення першого сингулярного числа (СНЧ), s_1' – модифіковане значення першого СНЧ, $m', m' \in M'$ – нормоване значення яскравості ЦВЗ.

Аналіз сингулярних чисел матриці низьких частот LWT-перетворення показав, що в більшості випадків друге, третє і четверте сингулярні числа найбільш схильні до округлень. Тому для вбудови використовується перше СНЧ. При цьому значення m' поділяються на два піддіапазони: $[0,5)$ і $[5,10]$, до яких застосовуються різні формули модифікації першого СНЧ (2). В результаті піддіаназон m' $[0,5)$ дає значення першого СНЧ, що належать $[0,9)$, а піддіапазон $[5,10]$ - значення першого СНЧ, що належать $[9,18]$.

Вилучення ЦВЗ з заповненого контейнеру відбувається аналогічними послідовними DCT-LWT-SVD-перетвореннями блоків 8×8 за формулою:

$$w = \begin{cases} s_1' - \lfloor s_1'/10 \rfloor \cdot 10, \; s_1' \geq 20, \\ s_1'/1.8, \; s_1' \geq 9, \\ s_1' - 4, \; s_1' < 9, \end{cases} \tag{3}$$

після чого отримане значення повертається в діапазон $[0,255]$:

$$w = \left\lfloor \frac{w}{10} \cdot 255 \right\rfloor, \tag{4}$$

де w – детектований ЦВЗ, s_1' – перше сингулярне число SVD-розкладання матриці низьких частот LWT-перетворення DCT-коефіцієнтів блоку заповненого контейнеру, $\lfloor \ldots \rfloor$ - операція округлення до найближчого цілого.

В ході експериментального тестування вбудови і вилучення ЦВЗ при використанні різних колірних складових контейнеру помічено, що результати вилучення ЦВЗ різні: в одному випадку спостерігається мінімальна кількість помилок з точки зору візуальної цілісності ЦВЗ, в інших – значні візуально помітні спотворення, аналіз яких буде проведено нижче.

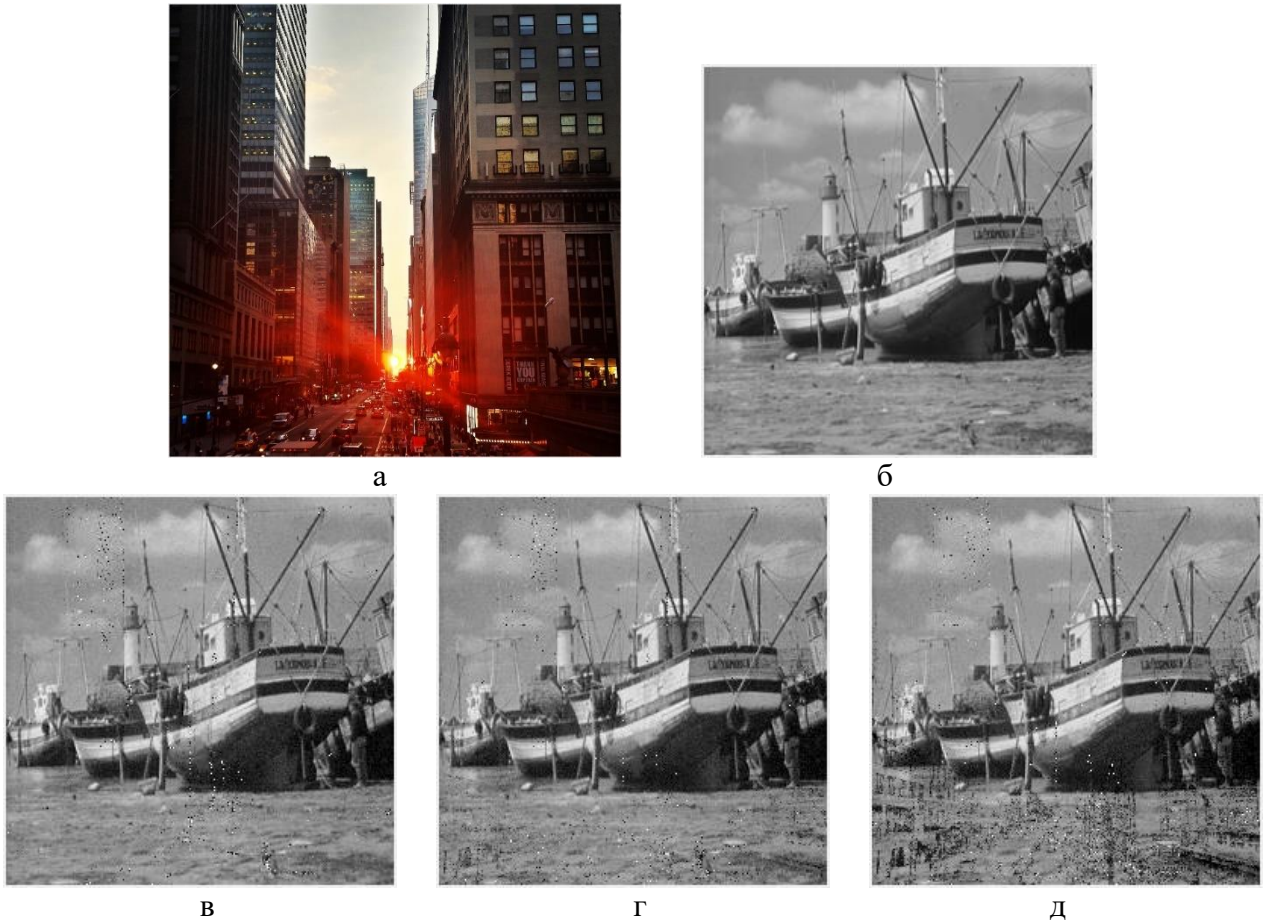
Слід зазначити, що у зв'язку з вбудовою ЦВЗ в область перетворень, яка передбачає округлення коефіцієнтів як DCT-перетворення, так і LWT-перетворення і сингулярного розкладання, а також представлення ЦВЗ в діапазоні $[0,10]$, визначення точності вилучення ЦВЗ стандартними показниками, що аналізують бітову послідовність, такими як NCC [13], SIM [7], BCR [11] може дати незадовільні результати, оскільки значення яскравості оригінального і вилученого ЦВЗ можуть відрізнятися на 5-10 одиниць, що призведе до низьких значень зазначених показників при збереженні візуальної цілісності вилученого ЦВЗ. У зв'язку з цим точність вилучення вбудованого ЦВЗ будемо оцінювати ступенем подібності, що визначається за наступним алгоритмом.

Обчислення ступеню подібності вбудованого і вилученого ЦВЗ.

Крок 1. Якщо $\left| m_{i,j} - m_{i,j}' \right| \leq 10$, то $count = count + 1$, де $m_{i,j}, m_{i,j}'$ - значення яскравості вбудованого і вилученого ЦВЗ відповідно, $i = \overline{1,H}$, $j = \overline{1,W}$, $H \times W$ - розмір ЦВЗ.

Крок 2. Обчислити $SD = \dfrac{count}{H \cdot W}$.

На рис. 1 наведено приклад вбудовування ЦВЗ (рис.1, б) в контейнер (рис.1, а) лише в червону, зелену та синю колірні складові. Результати вилучення ЦВЗ наведені на рис.1, в-д.



а б в г д

Рисунок 1 – Результати детектування ЦВЗ: а – контейнер розміром 2048×2048; б – оригінальний ЦВЗ розміром 256×256; в – ЦВЗ, вилучений з червоної колірної складової (SD=0.9408, NCC=0.3788, SIM=0.6724, BCR=0.6894); г – ЦВЗ, вилучений з зеленої колірної складової (SD=0.9142, NCC=0.3651, SIM=0.6657, BCR=0.6825); д – ЦВЗ, вилучений з синьої колірної складової (SD=0.8205, NCC=0.3270, SIM=0.6438, BCR=0.6635)

Як видно з рис. 1, навіть при деяких спотвореннях ЦВЗ зберігається його візуальна цілісність, проте показники NCC, SIM і BCR дають низькі значення, крім того найбільші спотворення характерні для ЦВЗ, вилученого з синьої колірної складової.

Аналіз причин помилок при вилученні ЦВЗ показав, що в більшості випадків некоректне детектування значень ЦВЗ відбувається в блоках, які містять більшість значень, що прагнуть до 0 або 255. У зв'язку з чим запропоновано наступний алгоритм для визначення колірної складової, найбільш придатної для вбудови ЦВЗ.

Вибір колірної складової зображення для вбудови/вилучення ЦВЗ.

Крок 1. Розбити колірну складову I^y, $y\in\{R,G,B\}$ розміром $M\times N$ цифрового зображення на блоки B^y розміром 8×8, що не перетинаються.

Крок 2. Для кожного блоку B^y:

2.1. Обчислити $R=\sum_{i,j=1}^{8} b_{i,j}\Big/\left(255\cdot64\right)$.

2.2. Якщо $R<0.1$, то $E_1^y=E_1^y+1$, де E_1^y - кількість блоків зі значеннями яскравості, що наближаються до 0, y-ої колірної складової.

2.3. Якщо $R > 0.9$, то $E_2^y = E_2^y + 1$, де E_2^y - кількість блоків зі значеннями яскравості, що наближаються до 255, y -ої колірної складової.

Крок 3. Обчислити $P^y = \left(E_1^y + E_2^y\right) / k$, де $k = \left\lfloor \frac{M}{8} \right\rfloor \cdot \left\lfloor \frac{N}{8} \right\rfloor$ - кількість блоків 8×8 колірної складової I^y, $\lfloor \ldots \rfloor$ - округлення до меншого цілого.

Крок 4. Для вбудови/вилучення ЦВЗ обирається колірна складова з мінімальним значенням P.

Необхідно акцентувати увагу на вейвлет-функції, що використовується в при обчисленні LWT-перетворення. В результаті проведення чисельних експериментів, було визначено, що найефективнішими материнськими вейвлетами є функції «Добеші-8» та «Хаара». Однак при використанні вейвлету «Хаара» спотворення ЦВЗ є більш помітними, тому найоптимальнішим варіантом є використання вейвлету «Добеші-8».

З урахуванням проведених експериментів сформулюємо основні кроки системи ЦВЗ.

Вбудова ЦВЗ в контейнер.

Крок 1. Визначити колірну складову для вбудови ЦВЗ.

Крок 2. Нормалізувати ЦВЗ у відповідності з формулою (1).

Крок 3. Обрану колірну складову ЦЗ I розміром $M \times N$ розбити на блоки B розміром 8×8, що не перетинаються.

Для кожного блоку B (кроки 4-10):

Крок 4. Виконати дискретне косинусне перетворення. Результат - B_{dct}.

Крок 5. До коефіцієнтів DCT B_{dct} застосувати ліфтінгове вейвлет перетворення. Результат – матриці LL, LH, HL, HH розміром 4×4.

Крок 6. Для матриці LL виконати сингулярне розкладання. Результат - S - матриця СНЧ, U, V - матриці сингулярних векторів.

Крок 7. Замінити перше СНЧ у відповідності з формулою (2).

Крок 8. Відновити матрицю низьких частот LL': $LL' = U \cdot S' \cdot V$, де S' - модифікована матриця СНЧ.

Крок 9. Застосувати обернене ліфтінгове вейвлет перетворення. Результат - $B_{dct}{}'$.

Крок 10. Виконати обернене дискретне косинусне перетворення. Результат - B'.

Крок 11. Зберегти заповнений контейнер.

Вилучення ЦВЗ з заповненого контейнеру.

Крок 1. Визначити колірну складову для вбудови ЦВЗ.

Крок 2. Обрану колірну складову ЦЗ I' розміром $M \times N$ розбити на блоки B' розміром 8×8, що не перетинаються.

Для кожного блоку B' (кроки 3-7):

Крок 3. Виконати дискретне косинусне перетворення. Результат - $B_{dct}{}'$.

Крок 4. До коефіцієнтів DCT $B_{dct}{}'$ застосувати ліфтінгове вейвлет перетворення. Результат – матриці LL', LH', HL', HH' розміром 4×4.

Крок 5. Для матриці LL' виконати сингулярне розкладання. Результат - S' - матриця СНЧ, U', V' - матриці сингулярних векторів.

Крок 6. Обчислити нормалізоване значення ЦВЗ у відповідності з формулою (3).

Крок 7. Перевести нормалізоване значення до діапазону $[0, 255]$ у відповідності з формулою (4).

Крок 8. З отриманих значень яскравості сформувати ЦВЗ.

Для оцінки ефективності запропонованого методу був проведений обчислювальний експеримент на основі 200 кольорових ЦЗ при використанні різних ЦВЗ. Ефективність стеганографічного методу будемо оцінювати визначенням показника PSNR, порівнюючи оригінальний і заповнений контейнери, та ступенем подібності вилученого ЦВЗ та вбудованого ЦВЗ. До заповнених контейнерів були накладені певні атаки, такі як зашумлення, підвищення різкості і медіанна фільтрація. В даному експерименті заповнені контейнери були збережені в форматі без втрат. Результати обчислювального експерименту наведені в табл. 1.

Таблиця 1

Ефективність вилучення ЦВЗ із заповненого контейнеру

Атака	Параметр	Середнє значення PSNR, дБ	Середнє значення ступеню подібності, %
Без атаки		50.45	93.85
Гаусів шум	$m = 0.0001,$ $d = 0.0000005$	48.67	93.44
	$m = 0.001,$ $d = 0.00005$	50.40	81.86
Мультиплікативний шум	$d = 0.0001$	50.45	81.76
	$d = 0.00001$	41.96	85.73
	$d = 0.000001$	48.62	93.72
Шум «Сіль та перець»	$d = 0.0001$	44.01	93.50
Фільтр підвищення різкості «Unsharp»		41.79	35.20
Медіанний фільтр		39.50	50.47

З табл. 1 видно, що запропонований метод забезпечує високі значення PSNR при збереженні заповненого контейнера в форматі без втрат – значення коливаються в межах 45 дБ до 56 дБ при забезпеченні високої пропускної здатності прихованого каналу зв'язку, що перевищує результати існуючих аналогів. Також метод є стійким до зашумлення – середні значення ступеню подібності перевищують 80%, причому у всіх зображень мінімальні значення ступеню подібності не нижче 70%. Однак запропонований метод виявився нестійким до медіанної фільтрації і підвищення різкості.

В табл. 2 наведені результати вилучення ЦВЗ з заповненого контейнеру, що зазнав атаку JPEG-стисненням.

Таблиця 2

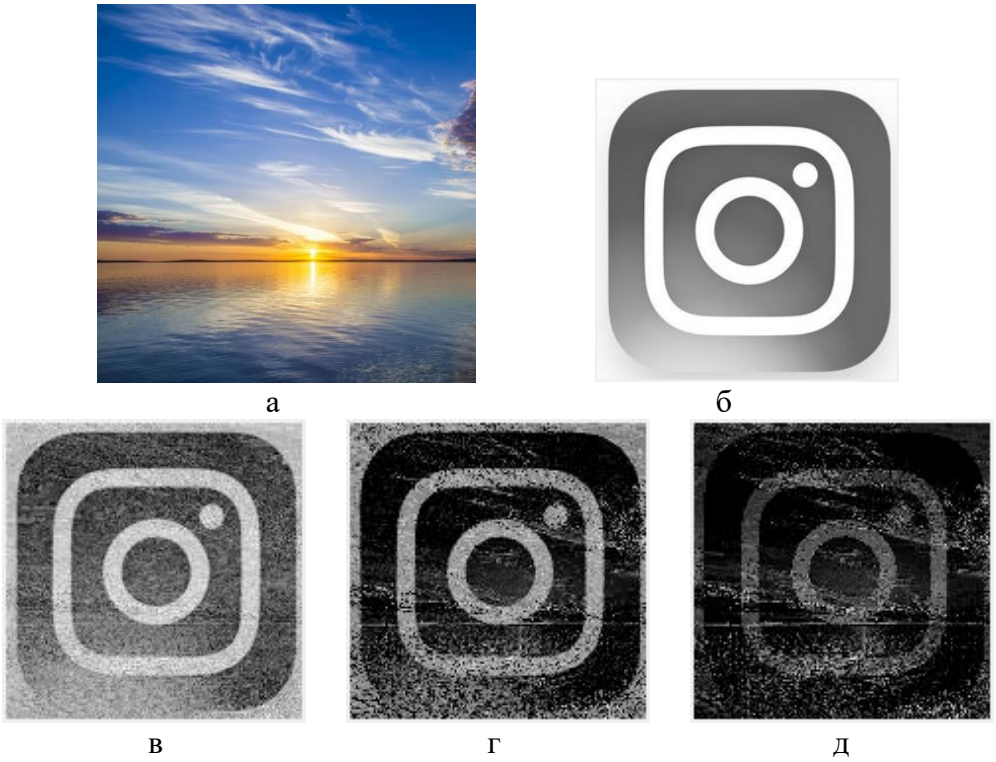
Ефективність вилучення ЦВЗ із заповненого контейнеру після JPEG-стиснення

Показник якості		*QF*								
		60	65	70	75	80	85	90	95	100
Середнє значення PSNR, дБ		38.86	40.72	42.93	47.93	44.47	43.64	45.99	47.07	47.77
	Подібність ЦВЗ									
Ступень подібності, %	Максимальне значення	87.50	89.16	88.14	88.90	87.88	87.76	87.76	89.16	91.96
	Мінімальне значення	1.78	1.89	1.80	2.15	2.49	2.53	1.57	1.46	2.24
	Середнє значення	28.88	26.76	26.78	24.06	25.01	26.65	27.90	29.22	34.23

З табл. 2 видно, що стиснення значно погіршує показники подібності вбудованого та вилученого ЦВЗ, які охоплюють широкий діапазон значень від 1,5% до 90%, причому тільки в 26% заповнених контейнерів при стисненні з $QF = 100$ ступень подібності перевищує 50%.

Однак, незважаючи на погіршення показників при стисненні, вилучений ЦВЗ залишається візуально помітним і зберігає можливість визначення авторства.

На рис. 2 наведений оригінальний ЦВЗ (рис. 2, б), вбудований в контейнер (рис. 2, а), та ЦВЗ, вилучені з заповнених контейнерів після атаки стиском (рис. 2, в-д). Незважаючи на наявність шумів, що повторюють контури контейнера і зростають зі зменшенням QF, цифровий водяний знак можна ідентифікувати при $QF \geq 80$.



а б в г д

Рисунок 2 – Результати детектування ЦВЗ після атаки стисненням: а – контейнер розміром 1200×1200; б – оригінальний ЦВЗ розміром 150×150; в – вилучений ЦВЗ зі стиснутого з $QF = 100$ заповненого контейнеру(SD=15.72%); г – вилучений ЦВЗ зі стиснутого з $QF = 90$ заповненого контейнеру(SD=1.88%); д – вилучений ЦВЗ зі стиснутого з $QF = 80$ заповненого контейнеру(SD=1.52%)

Висновки. В роботі розроблений новий метод вбудовування цифрового водяного знаку у зображення з послідовним використанням DCT-LWT-SVD-перетворень. Перед вбудовою ЦВЗ зображення-контейнер аналізується для вибору колірної складової, найбільш придатної для вбудови додаткової інформації, що веде до мінімізації помилок вилучення ЦВЗ.

В результаті проведених обчислюваних експериментів, спрямованих на визначення якості отриманих заповнених контейнерів, а також їх стійкості до атак, встановлено, що забезпечуються високі значення PSNR, які в середньому складають 50.45 дБ, при збереженні високої пропускної здатності прихованого каналу зв'язку. Експериментально доказана стійкість запропонованого методу до атак, зокрема до зашумлення зображення та стиснення ЦЗ при $QF \geq 80$. При накладанні шумів зберігається висока ступень подібності між оригінальним і вилученим ЦВЗ. У випадку стиснення ЦЗ при досить низьких значеннях ступеню подібності вилучений ЦВЗ піддається ідентифікації.

ЛІТЕРАТУРА:

1. Грибунин, В.Г. Цифровая стеганография / В. Грибунин, И. Оков, И. Туринцев. – Москва. : СОЛОН-Пресс, 2017. -262 с.

2. Senthooran V. DCT Coefficient Dependent Quantization Table. Modification Steganographic Algorithm / V.Senthooran, L.Ranathunga // First International Conference on Networks & Soft Computing. – 2014. – С. 432-436.

3. Alwan I. Image Hiding Using Discrete Cosine Transform / I. Alwan, F. Mohammed // J. Of College Of Education For Women. – 2016. - №27. – С. 393-399.

4. Nagpal C. Modified quantization based steganography for color images / C. NAGPAL, R. GOEL // International Journal of Electrical and Electronics Engineering. – 2013. - №2. – С. 9-17.

5. Ахмаметьєва Г. Модифікація стеганографічного методу вбудови цифрового водяного знаку в зображення на основі вейвлет-перетворення / Г.В. Ахмаметьєва, Г.А. Баранюк // Інформатика та мамематичні методи в моделюванні. – 2019. - №1. – С. 76-87.

6. Singh B. Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR / B. Singh // International Journal of Emerging Research in Management &Technology. – 2017. - №8. – С. 230-234.

7. Jabbar K. Compare Between DCT and DWT for Digital Watermarking in Color Image / K. Jabbar, B. Tuieb // Information and Knowledge Management. – 2015. - №5(7). – С. 22-31.

8. Singh N. High PSNR based Image Steganography / N. Singh // International Journal of Advanced Engineering Research and Science. – 2019. - №1. – С. 109-115.

9. Al-Haj A. Combined DWT-DCT Digital Image Watermarking / A. Al-Haj // Journal of Computer Science. – 2007. - №3(9). – С. 740-746.

10. Akter A. Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm / A. Akter, N. Tajnina, M. International Conference on Informatics, Electronics & Vision (ICIEV). – 2014. - № 10. – С. 1-6.

11. Benoraira A. Blind image watermarking technique based on differential embedding in DWT and DCT domains / A. Benoraira, K. Benmahammed, N. Boucenna // Benoraira et al. EURASIP Journal on Advances in Signal Processing. – 2017. - №55. – С. 1-11.

12. Rahman M. A DWT, DCT AND SVD BASED WATERMARKING TECHNIQUE TO PROTECT THE IMAGE PIRACY / M. Rahman // International Journal of Managing Public Sector Information and Communication Technologies. – 2013. - №4(2). – С. 1-12.

13. Мельник, М.А. Методика оценки устойчивости стеганоалгоритма к сжатию / М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. - 2013. - Вип. 44. - С. 121-128.

REFERENCES:

1. Gribunin V.G. (2017), “Cyfrovaya steganographiya” [Digital steganography], SOLON-Pres, 262 p.

2. Senthooran V., Ranathunga L. (2014), “DCT Coefficient Dependent Quantization Table. Modification Steganographic Algorithm”, First International Conference on Networks & Soft Computing, pp. 432-436.

3. Alwan I., Mohammed F. (2016), “Image Hiding Using Discrete Cosine Transform”, J. Of College Of Education For Women, №27, pp. 393-399.

4. Nagpal C., Goel R. (2013), “Modified quantization based steganography for color images”, International Journal of Electrical and Electronics Engineering, №2, pp. 9-17.

5. Akhmametieva A.V, Baraniuk A.A. (2019), “Modification of the steganographic method of embedding a digital watermark into image based on a wavelet transform”, Informatika ta matematichni metody v modelyvanny [Informatics and mathematical methods in modelling], №1, pp. 76-87.

6. Singh B. (2017), “Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR”, Journal of Emerging Research in Management &Technology, №8, pp. 230-234.

7. Jabbar K., Tuieb B. (2015), “Compare Between DCT and DWT for Digital Watermarking in Color Image”, Information and Knowledge Management, №5 (7), pp. 22-31.

8. Singh N. (2019), “High PSNR based Image Steganography”, International Journal of Advanced Engineering Research and Science, №1, pp. 109-115.

9. Al-Haj A. (2007), “Combined DWT-DCT Digital Image Watermarking”, Journal of Computer Science, №3 (9), pp. 740-746.

10. Akter A., Tajnina N. (2014), “Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm”, International Conference on Informatics, Electronics & Vision (ICIEV), №10, pp.1-6.
11. Benoraira A., Benmahammed K., Boucenna N. (2017), “Blind image watermarking technique based on differential embedding in DWT and DCT domains”, Benoraira et al. EURASIP Journal on Advances in Signal Processing, №55. – pp. 1-11.
12. Rahman M. (2013), “A dwt, dct and svd based watermarking technique to protect the image piracy”, International Journal of Managing Public Sector Information and Communication Technologies, №4 (2), pp. 1-12.
13. Melnyk M. (2014) “Method of estimation of steganographic algorithm stability to compression attacks”, Zbirnyk naukovykh prats’ Viys’kovoho instytutu Kyyivs’koho natsional’noho universytetu imeni Tarasa Shevchenka [Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv], № 44, pp. 121-128.

Ph.D. Akhmametieva A.V., Baraniuk A.A.

DEVELOPMENT OF A SYSTEM FOR DIGITAL WATERMARKS EMBEDDING INTO IMAGES BASED ON DCT-LWT-SVD

Copyright protection of digital content is a rather actual problem of humanity in the 21st century. Misuses of multimedia content is very common, and their number is growing with each passing day. One type of copyright protection is the embedding of digital watermark (DW) in the content.

In this paper a new method of embedding digital watermark into image using discrete cosine transform, lifting wavelet transform (LWT) with maternal wavelet "Dobeshi-8" and singular coefficients decomposition is proposed. Embedding is performed into the first singular number of the low frequency wavelet transform region. As a digital watermark, we will use a grayscale image normalized to a range from zero to ten to provide a high peak signal-to-noise ratio (PSNR).

The research analyzed the developed method: the method of embedding and detecting information was tested for its resistance to various types of attacks, namely: application of noise overlay (Gauss and pulse noise, "salt and pepper"), "unsharp" filter and median filter, and compression attack (with quality coefficients for a complete container from 60 to 100). As a result of the conducted testing, it was established that the method is quite resistant to all the attacks, except for the "unsharp" filtering (the resulting performance is not satisfactory).

The method showed good results in peak signal-to-noise ratio - the average PSNR value is 50.5 dB, as well as high rates of similarity between the embedded DW and the extracted one - from 77% to 97.6% while saving the full container in a lossless format, and up to 53, 05 dB and 91.96% while saving the image in a lossless format (JPEG).

Keywords: steganography, digital watermark, discrete cosine transform, lifting wavelet transform, singular value decomposition, digital image.

УДК 004.9: 681.3

д.т.н., проф. **Дружинін В.А.** (КНУ)
д.т.н., с.н.с. **Степанов М.М.** (КНУ)
к.т.н., с.н.с. **Жиров Г.Б.** (КНУ)
Трофимчук В.М. (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-04

ТЕХНОЛОГІЧНІ ПІДХОДИ ЩОДО ФОРМУВАННЯ ЦИФРОВОГО ЗОБРАЖЕННЯ ОБ'ЄКТІВ МІСЦЕВОСТІ ПРИ ДИСТАНЦІЙНОМУ ЗОНДУВАННЮ ЗЕМЛІ ІЗ ФОТО ТА РАДІОЛОКАЦІЙНІХ СИСТЕМ

Робота присвячена розгляду сучасного стану та тенденції застосування імітаційного моделювання для проведення математичного моделювання даних про місцевість отриманих із обробки цифрових знімків, як від фото так і радіолокаційних систем авіаційно-космічного базування. Актуальність розгляду стану та тенденцій розвитку технологічних підходів в моделюючих системах обумовлена практичною необхідністю отримання даних від фото та радіолокаційних зображень об'єктів зоні огляду системи з урахуванням зростаючих вимог до оперативності й точності визначення (виявлення) зображень об'єктів спостереження в реальному масштабі часу в складних умовах.

Наведена загальна структура побудови технології які застосовуються для імітаційного моделювання об'єктів місцевості визначені основні перспективи практичного застосування цих технологій при вирішенні завдань класифікації та моніторингу об'єктів місцевості.

Наведено оцінки основних технологічних підходів щодо зображень об'єктів при застосуванні розглянутих систем та оцінки точності визначення координат місцевості. Розглянуто канали передачі інформації в процесі отримання та обробки даних від фото та радіолокаційних систем дистанційного зондування землі.

Також як приклад приведено ланцюгово-вузлову модель просторових даних про об'єкти, які отримано в ході дистанційного зондування Землі і представляються лінійними і точковими. Для створення географічної основи щодо подальшого моделювання різноманітних телекомунікаційних систем та систем зв'язку. Це дозволить більш точно розробляти телекомунікаційні системи та перш за все системи зв'язку, враховуючи географічні дані і враховувати кути закриття при формуванні стільникового зв'язку.

Ключові слова: імітаційне моделювання, імітаційна система, модельований процес, векторна модель, провідні лінії зв'язку, канали передачі, шифрування.

Вступ. Останніми роками основні досягнення в різних галузях науки і техніки нерозривно пов'язані з процесом удосконалення ЕОМ. Сфера експлуатації ЕОМ – бурхлива галузь людської практики, яка стимулює розвиток нових теоретичних і прикладних напрямків [1]. Ресурси сучасної інформаційно-обчислювальної техніки дають можливість ставити і вирішувати математичні завдання такої складності, які в недавньому минулому здавалися нереалізованими, наприклад, моделювання великих систем.

Історично першим вважається аналітичний підхід – дослідження систем, де ЕОМ використовувалася в якості обчислювача за аналітичними співвідношеннями. Аналіз характеристик процесів функціонування великих систем за допомогою тільки аналітичних методів досліджень наштовхується зазвичай на значні труднощі, що призводять до необхідності істотного спрощення моделей або на етапі їх побудови, або в процесі роботи з моделлю, що може викликати отримання недостовірних результатів. Тому з'явилось математичне моделювання – процес встановлення співвідношення реального об'єкту та деякої математичної моделі і дослідження цієї моделі для отримання характеристик об'єкта.

Основна частина. Розглянемо види моделювання та моделі. За приклад візьмемо математичну модель.

Математична модель процесу як система співвідношень виду

$$\begin{cases} y_1(t) = f_1(x_1, x_2, \dots, x_{nX}; V_1, V_2, \dots, V_{nV}; h_1, h_2, \dots, h_{nH}; t) \\ y_2(t) = f_2(x_1, x_2, \dots, x_{nX}; V_1, V_2, \dots, V_{nV}; h_1, h_2, \dots, h_{nH}; t) \\ \dots \\ y_{ny}(t) = f_m(x_1, x_2, \dots, x_{nX}; V_1, V_2, \dots, V_{nV}; h_1, h_2, \dots, h_{nH}; t) \end{cases}, \quad (1)$$

де m – підсистеми, $y_1(t), y_2(t), \dots, y_{nY}(t)$ – характеристики підсистем, $x_1, x_2, \dots, x_{nX}$ – параметри підсистеми, $h_1, h_2, \dots, h_{nH}$ – вхідні дії на підсистеми, $\nu_1, \nu_2, \dots, \nu_{nV}$ – вплив зовнішнього середовища на підсистеми.

Математичне моделювання ділиться на аналітичне, імітаційне і комбіноване.

При аналітичному моделюванні співвідношення процеси об'єкта описуються у вигляді функціональних співвідношень (алгебраїчних, інтегро-диференціальних, різницевих тощо) або логічних умов, які вирішуються або в загальному вигляді, або за конкретними початковими даними (численними методами на ЕОМ), або якісно (наприклад, оцінка стійкості рішення).

Імітаційне моделювання у світовій практиці набуває все більшого використання при розробці та перевірці [2].

Імітаційне моделювання зводиться до проведення експериментів з моделлю шляхом багаторазового прогону програми з деякою множиною даних – середовищем системи [3]. Під час імітаційного моделювання можуть бути задіяні не тільки програмні засоби, але й технічні, люди та реальні системи. З математичної точки зору імітаційну модель можна розглядати як сукупність рівнянь, які розв’язуються з використанням численних методів у разі кожної зміни модельного часу. Цінність імітаційного моделювання полягає в тому, що воно ґрунтується на методології системного аналізу і дає змогу досліджувати проектовану систему з використанням технології операційного дослідження.

Імітаційна система реалізується на ЕОМ і дозволяє досліджувати імітаційну модель *M*, що задається у вигляді певної сукупності окремих блокових моделей і зв'язків між ними в їх взаємодії у просторі та часі при реалізації якого-небудь процесу. Можна виділити три основні групи блоків: блоки, що характеризують модельований процес функціонування системи *S*; блоки, які відображають зовнішнє середовище *E* і його вплив на реалізований процес; блоки, що грають службову, допоміжну роль, забезпечуючи взаємодію перших двох, а також виконують додаткові функції з отримання та обробки результатів моделювання. Крім того, імітаційна система характеризується набором змінних, за допомогою яких вдається управляти досліджуваним процесом, і набором початкових умов, які можна змінювати під час проведення машинного експерименту.

Забезпечення імітаційного моделювання.

Імітаційна система реалізується на ЕОМ і дозволяє досліджувати імітаційну модель *M*, що задається у вигляді певної сукупності окремих блокових моделей і зв'язків між ними в їхній взаємодії у просторі та часі при реалізації якого-небудь процесу. Можна виділити три основні групи блоків:

- блоки, що характеризують модельований процес функціонування системи *S*;
- блоки, що відображають зовнішнє середовище *E* і його вплив на реалізований процес;
- блоки, що грають службову, допоміжну роль, забезпечуючи взаємодію перших двох, а також виконують додаткові функції з отримання та обробки результатів моделювання.

Крім того, імітаційна система характеризується набором змінних, за допомогою яких з’являється можливість керувати досліджуваним процесом, і набором початкових умов, коли можна змінювати умови (план) проведення машинного експерименту.

Математичне забезпечення імітаційної системи – сукупність математичних співвідношень, що описують поведінку реального об'єкта, сукупність алгоритмів, що забезпечують як підготовку (введення вихідних даних), так і роботу з моделлю (імітація, висновок, обробка результатів).

Програмне забезпечення – сукупність програм: планування експерименту, імітаційної моделі, проведення експерименту, обробки та інтерпретації результатів, синхронізації процесів у моделі (псевдопаралельне виконання процесів у моделі).

Інформаційне забезпечення – засоби та технологія організації та реорганізації бази даних моделювання, методи логічної і фізичної організації масивів, форми документів, що описують процес моделювання і його результати.

Технічне забезпечення – засоби обчислювальної техніки, зв'язку та обміну між оператором і мережею ЕОМ, введення і виведення інформації, керування проведенням експерименту.

Ергономічне забезпечення – сукупність наукових і прикладних методик та методів, а також нормативно-технічних і організаційно-методичних документів, що створюють оптимальні умови для високопродуктивної діяльності людини у взаємодії з моделювальним комплексом.

Модель об'єкта моделювання, системи *S*, можна представити у вигляді безлічі величин, що описують процес функціонування реальної системи і утворюють в загальному випадку наступні підмножини: сукупність вхідних впливів на систему

$$x_1 \in X, i = \overline{1, n_x}\ . \tag{2}$$

Процес функціонування системи *S* описується в часі оператором F_s, який в загальному випадку перетворює екзогенні змінні в ендогенні відповідно до співвідношеннями виду

$$\vec{y}(t) = F_s(\vec{x}, \vec{v}, \vec{h}, t). \tag{3}$$

Основні переваги імітаційного моделювання при дослідженні систем:

- можливість дослідити особливості процесу функціонування системи *S* за будь-яких умов;
- за рахунок застосування ЕОМ істотно скорочується тривалість випробувань у порівнянні з натурним експериментом;
- результати випробувань реальної системи або її частин можна використовувати для проведення імітаційного моделювання;
- гнучкість варіювання структури, алгоритмів і параметрів модельованої системи під час пошуку оптимального варіанта системи;
- для складних систем – це єдиний практично реалізований метод дослідження процесу функціонування систем.

Основні недоліки імітаційного моделювання:

- для повного аналізу характеристик процесу функціонування систем і пошуку оптимального варіанта потрібно багато разів відтворювати імітаційний експеримент, варіюючи вихідні дані завдання;
- великі витрати машинного часу.

На зорі розвитку геоінформаційних систем найпопулярнішими були растрові ГІС. З комп’ютерами малої потужності виконувати обробку просторової інформації було зручно саме в растровому вигляді.

У растрових ГІС дані зберігаються у вигляді таблиць – сіток з осередками, що нагадують за внутрішньої організації растрові файли форматів BMP, BIL і інших форматів без стиснення.

Кожен прямокутник має унікальний номер, що складається з позицій у стовпчику (*I*) і рядку (*J*) матриці, що задає його положення щодо суміжних осередків. З рис. 1 видно, що, знаючи координати першого осередку і користуючись *I* та *J*, можна легко перейти до координат будь-якого іншого осередку матриці:

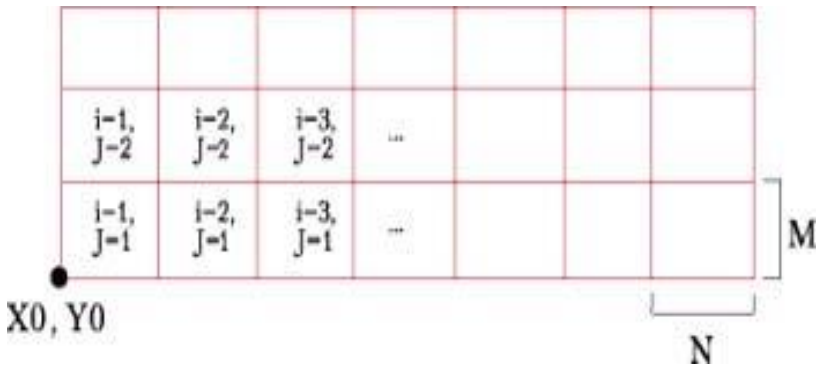


Рисунок 1 – Координати комірок у «сітці» растрової моделі

Векторна модель даних призначена для зберігання інформації про просторові об'єкти, межі яких описуються за допомогою координат. Кордон просторового об'єкта формується за допомогою геодезичних або картометричних вимірювань шляхом апроксимації контуру об'єкта і «перетворюється» на послідовність координат поворотних точок ділянок кордону. У загальному випадку об'єкт може мати як зовнішній, так і внутрішній кордон. Наприклад, водна поверхня озера матиме кілька кордонів, якщо посеред нього розташовані острова.

Контур або набір контурів просторового об'єкта є неподільною одиницею зберігання просторової інформації, з якою пов'язані атрибути об'єкта. У векторній моделі в якості єдиного і неподільного може бути представлений тільки той просторовий об'єкт, який характеризується однаковим набором атрибутів і їхніх значень.

Особливості зберігання топологічної інформації

Навіщо потрібна топологічна інформація? Справа в тому, що будь-які вимірювання координат об'єктів, виконані геодезичними або картометричними методами, мають певну точність. Знання точності визначення координат необхідно для практичної роботи з цифровими картами і геоінформаційними системами, в іншому випадку не уникнути серйозних помилок.

Наприклад, маючи карту з річками, відображеними лініями, і населеними пунктами, відображеними точками, потрібно за допомогою ГІС виявити, з якого боку річки знаходиться населений пункт. На рис. 2 показана ситуація, коли невисока точність карти перешкоджає встановленню правильної відповіді на це питання.

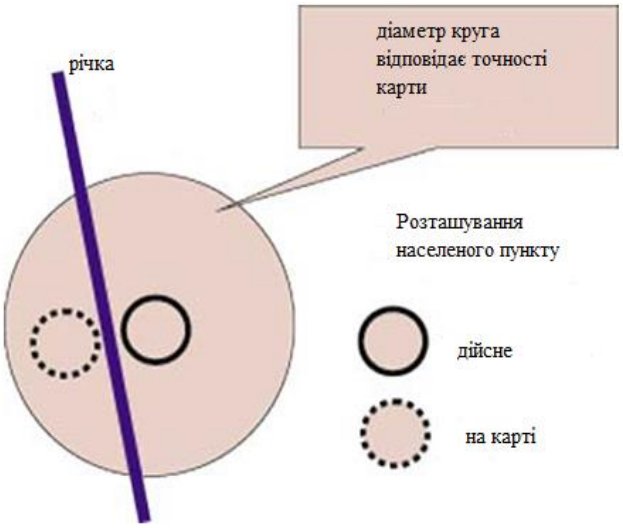


Рисунок 2 – Спотворення взаємного просторового положення об'єктів через високу точність карти

При створенні цифрових карт необхідно уважно стежити за дотриманням топологічних співвідношень між об'єктами: розташування праворуч-ліворуч, зверху-знизу, всередині-зовні, примикання одного об'єкта до іншого тощо.

Фахівці ESRI Inc. (США) розробили спеціальну ланцюгово-вузлову модель даних, яка заснована на використанні реляційної моделі даних і дозволяє уникати помилок в топологічних відносинах між об'єктами.

В рамках ланцюгово-вузлової моделі просторові дані про об'єкти представляються: лінійними і точковими. Лінійні примітиви використовуються для відображення кордонів лінійних і площових об'єктів, точкові - для відображення точкових об'єктів і внутрішніх областей площових об'єктів. Також використовуються спеціальні примітиви - вузли, які вказують точки примикань кордонів один до одного. Інформація про об'єкти зберігається у двох службових реляційних таблицях - AAT (Arc Attribute Table - таблиця атрибутів дуг) і PAT (Point Attribute Table - таблиця атрибутів точок) [5]. Поєднання елементів ланцюгово-вузлової моделі і структури таблиць AAT і PAT наведено на рис. 3.

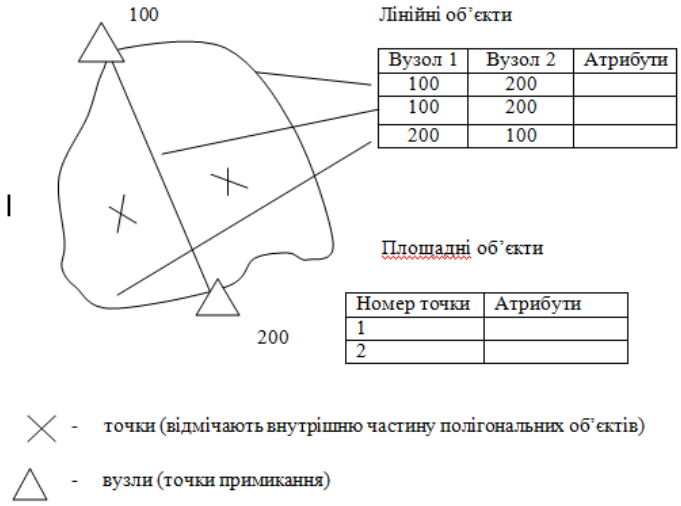


Рисунок 3 – Елементи ланцюгово-вузлової моделі і структури таблиць AAT і PAT

В основі концепції сховищ даних лежать такі основоположні ідеї:

- інтеграція раніше роз'єднаних деталізованих даних (історичні архіви, дані з традиційних систем обробки документів, розрізнених баз даних, дані із зовнішніх джерел) в єдиному сховищі даних;
- тематичне і часове структурування, узгодження і агрегування;
- поділ наборів даних, що використовуються для операційної (виробничої) обробки, і наборів даних, що використовуються для вирішення завдань аналізу.

Передача інформації каналами зв'язку

За видом сигналів, які передаються у фізичному середовищі розповсюдження (лініях зв'язку), системи передачі поділяються на аналогові і цифрові. В аналогових системах сигнали, які переносять інформацію по середовищу поширення, є безперервними функціями безперервного часу. У цифрових системах сигнали, які переносять інформацію по середовищу поширення, є дискретними функціями безперервного часу і являють собою в більшості випадків двійкові послідовності імпульсів.

При цьому вхідні сигнали системи передачі, що містять корисну інформацію, можуть бути будь-якого виду (наприклад, аналогові при передачі голосу або дискретні при передачі даних).

В основі побудови аналогових систем передачі лежить принцип частотного ущільнення каналів, який називають мультиплексовим з частотним поділом каналів. Цей принцип, в свою чергу, базується на тому, що ширина спектра переданих сигналів зазвичай істотно нижча, ніж

смуга пропускання фізичного середовища поширення. З цієї причини передавати тільки один сигнал по лінії зв'язку невигідно, оскільки загальна смуга пропускання каналу буде використана незначно. Наприклад, смуга частот (спектр) мовного сигналу, що забезпечує рівень розбірливості слів 90%, становить 3100 Гц і розміщується в смузі стандартного телефонного каналу зв'язку в діапазоні 300 ... 3400 Гц.

Для виключення впливу сусідніх каналів один на одного через накладення спектрів, викликаних неідеальністю смугових фільтрів, в якості розрахункової ширини смуги телефонного каналу приймається величина 4 кГц. При цьому захисна смуга частот між двома сусідніми каналами становить 900 Гц.

Разом із тим смуга пропускання кабельної лінії зв'язку (спектр ефективно переданих частот) може становити кілька мегагерц, що дозволяє передавати по даній лінії зв'язку сотні і тисячі мовних сигналів. Для реалізації такої багатоканальної системи передачі частотні спектри різних сигналів повинні бути зрушені відносно один одного так, щоб вони займали неперекриваючі частотні смуги. Це досягається застосуванням в аналогових системах передачі високочастотних несучих синусоїдальних коливань, параметри яких (амплітуда, частота і фаза) змінюються (модулюються) пропорційно величині переданих корисних сигналів.

Провідні (повітряні) лінії зв'язку використовуються для передачі телефонних і телеграфних сигналів, а також для передачі комп'ютерних даних. Ці лінії зв'язку застосовуються як магістральні.

По провідних лініях зв'язку можуть бути організовані аналогові і цифрові канали передачі даних. Швидкість передачі по провідних лініях, "простій старій телефонної лінії" (POST - Primitive Old Telephone System) є дуже низькою. Крім того, до недоліків цих ліній належать перешкодозахищеність і можливість простого несанкціонованого підключення до мережі.

Кабельні лінії зв'язку мають досить складну структуру. Кабель складається з провідників, укладених в кілька шарів ізоляції. У комп'ютерних мережах використовуються три типи кабелів.

Вита пара (twisted pair) - кабель зв'язку, який являє собою виту пару мідних проводів (або декілька пар проводів), укладених в екрановану оболонку. Пари проводів скручуються між собою з метою зменшення наведень. Вита пара є досить перешкодостійкою. Існує два типи цього кабелю: неекранована кручена пара UTP і екранована кручена пара STP.

Характерним для цього кабелю є простота монтажу. Даний кабель є найдешевшим і поширеним видом зв'язку, який знайшов широке застосування в найпоширеніших локальних мережах з архітектурою Ethernet, побудованих за топологією типу "зірка". Кабель підключається до мережевих пристроїв за допомогою з'єднувача RJ45.

Кабель використовується для передачі даних на швидкості 10 Мбіт / с і 100 Мбіт / с. Вита пара зазвичай використовується для зв'язку на відстані не більше декількох сотень метрів. До недоліків кабелю "вита пара" можна віднести можливість простого несанкціонованого підключення до мережі.

Коаксіальний кабель (coaxial cable) - це кабель з центральним мідним дротом, який оточений шаром ізолювального матеріалу для того, щоб відокремити центральний провідник від зовнішнього провідного екрана (мідного обплетення або шару алюмінієвої фольги). Зовнішній провідний екран кабелю покривається ізоляцією.

Існує два типи коаксіального кабелю: тонкий коаксіальний кабель діаметром 5 мм і товстий коаксіальний кабель діаметром 10 мм. У товстого коаксіального кабелю загасання менше, ніж у тонкого. Вартість коаксіального кабелю вище вартості крученої пари; і виконання монтажу мережі складніше, ніж крученою парою.

Коаксіальний кабель застосовується, наприклад, в локальних мережах з архітектурою Ethernet, побудованих по топології типу "загальна шина". Коаксіальний кабель більш перешкодозахищений, ніж кручена пара і знижує власне випромінювання. Пропускна здатність - 50-100 Мбіт/с. Допустима довжина лінії зв'язку - кілька кілометрів. Несанкціоноване підключення до коаксіального кабелю складніше, ніж до крученої пари.

Кабельні оптоволоконні канали зв'язку. Оптоволоконний кабель (fiber optic) - це оптичне волокно на кремнієвій або пластмасовій основі, укладене в матеріал з низьким коефіцієнтом заломлення світла, який вкритий зовнішньою оболонкою.

Оптичне волокно передає сигнали тільки в одному напрямку, тому кабель складається з двох волокон. На передавальному кінці оптоволоконного кабелю потрібно перетворення електричного сигналу в світловий, а на приймальному кінці зворотне перетворення.

Основна перевага цього типу кабелю - надзвичайно високий рівень перешкодозахищеності і відсутність випромінювання. Несанкціоноване підключення дуже складно. Швидкість передачі даних 3Гбіт/с. Основні недоліки оптоволоконного кабелю - це складність його монтажу, невелика механічна міцність і чутливість до іонізуючих випромінювань.

Радіоканали наземного (радіорелейного і стільникового) та супутникового зв'язку утворюються за допомогою передавача і приймача радіохвиль і належать до технології бездротової передачі даних.

Радіорелейні канали зв'язку складаються з послідовних станцій, які є ретрансляторами. Зв'язок здійснюється в межах прямої видимості, дальності між сусідніми станціями - до 50 км. Цифрові радіорелейні лінії зв'язку (ЦРРС) застосовуються в якості регіональних і місцевих систем зв'язку і передачі даних, а також для зв'язку між базовими станціями стільникового зв'язку.

У супутникових системах використовуються антени СВЧ-діапазону частот для прийому радіосигналів від наземних станцій і ретрансляції цих сигналів назад на наземні станції. У супутникових мережах використовуються три основні типи супутників, які знаходяться на геостаціонарних орбітах, середніх або низьких орбітах. Супутники запускаються, як правило, групами. Рознесені один від одного вони можуть забезпечити охоплення майже усієї поверхні Землі. Робота супутникового каналу передачі даних представлена на рис.4.

Організація багатоканальної аналогової системи передачі здійснюється шляхом модуляції корисними сигналами амплітуди або частоти несучих синусоїдальних коливань, що мають різні несучі частоти. При цьому відбувається перенесення спектра корисних сигналів на величину несучих частот.

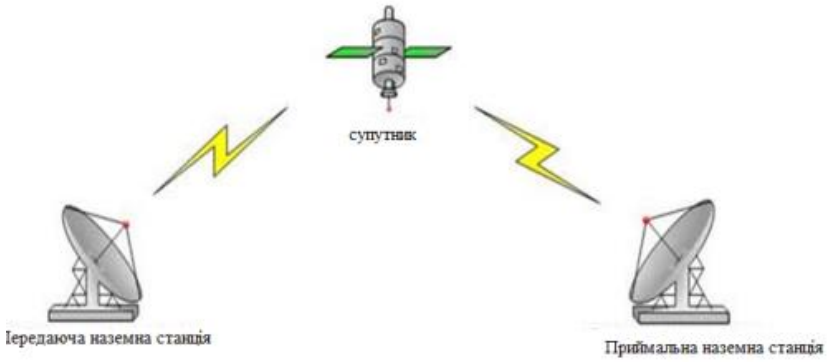


Рисунок 4 – Канали передачі

Доцільніше використовувати супутниковий зв'язок для організації каналу зв'язку між станціями, розташованими на значних відстанях, і можливості обслуговування абонентів у найбільш важкодоступних точках. Пропускна здатність висока - кілька десятків Мбіт/с.

Радіоканали стільникового зв'язку будуються за тими самими принципами, що і стільникові телефонні мережі. Стільниковий зв'язок - це бездротова телекомунікаційна система, що складається з мережі наземних базових приймально-передавальних станцій і стільникового комутатора (або центру комутації мобільного зв'язку).

Базові станції підключаються до центру комутації, який забезпечує зв'язок як між базовими станціями, так і з іншими телефонними мережами, а також з глобальною мережею

Інтернет. Під час виконання функцій центр комутації аналогічний звичайної АТС провідного зв'язку.

LMDS (Local Multipoint Distribution System) - це стандарт стільникових мереж безпровідної передачі інформації для фіксованих абонентів. Система будується за стільниковим принципом, одна базова станція дозволяє охопити район радіусом кілька кілометрів (до 10 км) і підключити декілька тисяч абонентів. Самі БС об'єднуються один з одним високошвидкісними наземними каналами зв'язку або радіоканалами. Швидкість передачі даних до 45 Мбіт/с.

Радіоканали передачі даних WiMAX (Worldwide Interoperability for Microwave Access) аналогічні Wi-Fi. WiMAX, на відміну від традиційних технологій радіодоступу, працює і на відбитому сигналі, поза прямої видимості базової станції. Експерти вважають, що мобільні мережі WiMAX відкривають набагато цікавіші перспективи для користувачів, ніж фіксований WiMAX, призначений для корпоративних замовників. Інформацію можна передавати на відстані до 50 км зі швидкістю до 70 Мбіт/с.

Радіоканали передачі даних MMDS (Multichannel Multipoint Distribution System). Ці системи здатна обслуговувати територію в радіусі 50-60 км, при цьому пряма видимість передавача оператора є необов'язковою. Середня гарантована швидкість передачі даних складає 500 Кбіт/с - 1 Мбіт/с, але можна забезпечити до 56 Мбіт/с на один канал.

Стандартом бездротового зв'язку для локальних мереж є технологія Wi-Fi. Вона забезпечує підключення у двох режимах: точка-точка (для підключення двох ПК) та інфраструктурне з'єднання (для підключення кількох ПК до однієї точки доступу). Швидкість обміну даними до 11 Мбіт/с при підключенні точка-точка і до 54 Мбіт/с при інфраструктурному з'єднанні.

Радіоканали передачі даних Bluetooth - це технологія передачі даних на короткі відстані (не більше 10 м) і може бути використана для створення домашніх мереж. Швидкість передачі даних не перевищує 1 Мбіт/с.

Підсистема зв'язку вважається найбільш вразливою підсистемою ІС, тому потрібно приділяти особливу увагу питанням її захисту.

Такий захист здійснюється:

1. З метою захисту інформації при передачі одиничних повідомлень (пакетів), які можуть стати об'єктами пасивних і активних вторгнень. При пасивних вторгненнях користувачам, що не мають повноважень, лише спостерігають за повідомленнями, які передаються лініями зв’язку, не змінюючи цих повідомлень. При активних вторгненнях регулярні повідомлення можуть бути видалені, модифіковані, відстрочені, перенаправлені, захищені повторно або спотворені. Проблеми, які при цьому виникають, обумовлені непередбаченими ситуаціями, апаратними збоями, перешкодами в лініях зв'язку, програмними помилками і т.п.

2. Для забезпечення захисту і секретності операцій, виконуваних над повідомленнями при передачі по обчислювальній мережі. Об'єктами вторгнень і джерелами труднощів у цьому випадку є проблеми організації зв'язку між двома і більше користувачами, протоколи передачі, пристрої передачі та програмне забезпечення систем передачі тощо. Механізми, що забезпечують захист операцій в обчислювальній мережі, проектуються так, щоб гарантувати цілісність та захист даних при передачі по мережі.

Забезпечення конфіденційності повідомлення - одна з функцій захисту від несанкціонованого перегляду вмісту повідомлення, що гарантує його скритність.

Забезпечення цілісності - функція захисту від несанкціонованих або випадкових модифікацій, що гарантує правильність передачі вмісту повідомлення.

Для захисту окремих повідомлень ці функції можна використовувати як спільно, інтегровано, так і роздільно.

Справжність повідомлення можна забезпечувати різними способами, не вдаючись до його шифрування. Такий підхід придатний у багатьох випадках, коли цілісність даних відіграє винятково важливу роль, а конфіденційність не потрібна.

Він використовується при реалізації фінансових операцій і розподілі відкритих ключів між об'єктами мережі. Широко поширені такі методи забезпечення автентичності повідомлення.

Існує низка цілісності шифрування повідомлення:

- побітове шифрування потоку даних;
- побітове шифрування потоку зі зворотним зв'язком щодо шифрування;
- побітове шифрування зі зворотним зв'язком за вихідним тексту;
- поблочних шифрування потоку даних;
- поблочних шифрування потоку зі зворотним зв'язком (ОС);
- шифрування блоками;
- шифрування блоками зі зворотним зв'язком.

Криптографічний засіб захист називають спеціальні методи і засоби перетворення інформації, в результаті яких маскується її зміст. Основними видами криптографічного закриття є шифрування і кодування даних, що захищаються. При цьому в шифруванні є такий вид закриття, при якому самостійному перетворенню підлягає кожен символ даних, які закриваються. Підчас кодування дані діляться на блоки, що мають смислове значення, і кожний такий блок замінюється цифровим, літерним або комбінованим кодом. Для криптографічного закриття інформації в системах обробки даних найбільшого поширення набуло шифрування. Використовується кілька систем шифрування: заміна (підстановка), перестановка, гамування, аналітичне перетворення шифрувальних даних. Широке поширення набули комбіновані шифри, коли початковий текст перетворюється з використанням двох або навіть трьох різних шифрів. Наприклад, комбіноване застосування заміни і гамування або перестановки та гамування тощо.

Важлива характеристика системи шифрування є її продуктивність. Продуктивність шифрування залежить як від використовуваної системи шифру, так і від способу реалізації апаратного або програмного шифрування. З погляду трудомісткості шифрування найменших витрат вимагають шифри заміни, а найбільших - шифри, основані на аналітичному перетворенні даних. З точки зору способу реалізації продуктивність апаратного шифрування в кілька разів перевищує виробництво програмного шифрування.

Висновки. Імітаційне моделювання відтворює алгоритми процесів функціонування систем в часі. Імітуються елементарні явища, що становлять процес, зі збереженням їх логічної структури і послідовності протікання в часі.

Для відтворення в цифровому вигляді даних про місцевість, які отриманні із дешифрування інформації із фотографічних та радіолокаційних даних імітаційне моделювання є найкращим застосуванням за допомогою яких можна проводити моделювання побудови різноманітних систем і процесів. Для створення географічної основи щодо подальшого моделювання різноманітних телекомунікаційних систем та систем зв’язку. Це дозволить більш точно розробляти телекомунікаційні системи та системи зв’язку враховуючи географічні дані. Враховувати кути закриття при формуванні стільникового зв’язку.

Основною перевагою імітаційних моделей у порівнянні з аналітичними є можливість вирішення більш складних завдань. Імітаційні моделі дозволяють легко враховувати наявність дискретних або безперервних елементів, нелінійні характеристики, випадкові впливи та ін. Тому цей метод широко застосовується на етапі проектування складних систем. Основним засобом реалізації імітаційного моделювання служить ЕОМ, що дозволяє здійснювати цифрове моделювання систем і сигналів.

Було розроблено ряд ефективних сховищ для збереження даних. За основу були взяті розробки фахівців ESRI Inc. (США), які розробили спеціальну ланцюгово-вузлову модель даних, яка заснована на використанні реляційної моделі даних і дозволяє уникати помилок в топологічних відносинах між об'єктами.

Для захисту даних при створенні моделі існує криптографічний засіб. Основними видами криптографічного закриття є шифрування і кодування даних, що захищаються. При

цьому в шифруванні використовується такий вид захисту, при якому самостійному перетворенню підлягає кожен символ даних, які закриваються. Підчас кодування дані діляться на блоки, що мають смислове значення, і кожний блок замінюється цифровим, літерним або комбінованим кодом.

ЛІТЕРАТУРА:

1. Геоинформационные системы /Журкин И. Г., Шайтура С. В. – М.: КУДИЦ, 2009. – 272 с.
2. Геоинформатика: учебное пособие / Лайкин В.И., Упоров Г.А. – Комсомольск-на-Амуре: Изд-во АмГПГУ, 2010. – 162 с.
3. Имитационное моделирование: Теория и технологи / Ю.И. Рыжиков. С-П.: 2004. – 529 с.
4. Інтернет ресурси: http://www.gisa.ru/; http://resources.arcgis.com/.
5. Иванов В.Г. Основы формирования единого геоинформационного пространства специального назначения с использованием Webтехнологий / В.Г. Иванов, Н.Д. Бородин // САПР и графика. - № 3. - 2016. - С. 18-20.
6. Горбунов А.А., Пономорчук А.Ю., Иванов В.Г. Использование геоинформационных систем при принятии управленческих решений в единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций // Научноаналитический журнал «Вестник СанктПетербургского университета Государственной противопожарной службы МЧС России». – 2015. – № 2. –С. 71-76.
7. Шелухин О.И. / Моделирование информационных систем / О.И. Шелухин // Учебное пособие для вузов, 2-е изд., перераб. и доп., Научно-техническое издательство «Горячая линия – Телеком», 2018, 536с.
8. Флегонтов А.В., Матюшичев И.Ю. /Моделирование информационных систем. Unified Modeling Language. Учебное пособие / А.В. Флегонтов, И.Ю. Матюшичев. - М., 2019. – 112 с.
9. А.А. Светличный, А.В. Пяткова / Геоинформационное моделирование водной эрозии почв / Светличный А.А., Пяткова А.В.// Збірник наукових статей “Проблеми безперервної географічної освіти і картографії” - 2014. – Випуск 1 - С. 83-87.
10. Светличный А.А. Проблема верификации пространственно-распределенных математических моделей водной эро зии почв / А. А. Светличный, А. В. Пяткова, С. В. Плотницкий [и др.]// Вестник Одесского национального университета им. И. И. Мечникова. Географические и геологические науки. – [Том 18, вып. 3]. – 2013. – С. 78-90.
11. Светличный А. А. Математическое моделирование водной эрозии: проблема классификации / Светличный А. А. // Вісник ОНУ. Серія географічні та геологічні науки. – Том 15, вип. 13. – 2010. – С. 32-39.
12. Цветков В.Я., Буравцев В.А. Метрики сложной детерминированной системы // Онтология проектирования. 2017. Т. 7. № 3(25). С. 334-346. DOI: 10.18287/2223-9537-2017-7-3-334-346
13. Раев В.К. Дихотомический метод уменьшения информационной неопределенности // Перспективы науки и образования. - 2017. - № 2(26). - С. 7-11.
14. РозенбергИ.Н. Топосемантическое информационное соответствие в пространственном моделировании // Науки о Земле. - 2017. - № 3. - С. 64-73.
15. Christopher B. Oneal, John D. Stuart, Steven J. Steinberg, Geographic analysis of natural fire rotation in the California redwood forest during the suppression era [Електронний ресурс] // Fire Ecology, Volume02, Issue01, Spring, 2016. – Режим доступу: http://fireecology.org/docs/Journal/pdf/Volume02/Issue01/073.pdf
16. Radmila Jovanovic, Zeljko Bjeljac, Olgica Miljkovic, Aleksandra Terzic Spatial analysis and mapping of fire risk zones and vulnerability assessment — case study mt. Stara Planina [Електронний ресурс] // Prevention and Education in Natural Disasters, 2018. – Режим доступу: http://www.doiserbia.nb.rs/img/doi/0350-7599/2013/0350-75991303213J.pdf
17. Atlas of natural hazards & risks of Georgia // Caucasus Environmental NGO Network, 2019 [Електронний ресурс]. – Режим доступу: http://drm.cenn.org/index.php/en/
18. Svetlitchnyi A. A. Spatial distribution of soil moisture convent within catchments and its modeling on the basis of topographic data / A. A. Svetlitchnyi, S. V. Plotnitskiy, O. Y. Stepovaya // Journal of Hydrology [V. 277]. – 2013. – P. 50-60.
19. Mordechai Ben-Ari. Mathematical Logic for Computer Science/ Third Edition. Springer London Heidelberg New York Dordrecht, 2012. 364 p. ISBN 978-1-4471-4128-0
20. Victor Raizer / Optical Remote Sensing of Ocean Hydrodynamics / Copyright Year 2019, ISBN 9780815360148

21. William Emery Adriano Camps / Introduction to Satellite Remote Sensing, 1st Edition, Atmosphere, Ocean, Land and Cryosphere Applications / 2017, ISBN: 9780128092590

22. Savinykh V.P., Tsvetkov V.Ya. Geodata As a Systemic Information Resource. Herald of the Russian Academy of Sciences. 2014. Vol. 84. No. 5. P. 365-368. DOI: 10.1134/S1019331614050049.

REFERENCES:

1.*Geoinformation systems*. / Zhurkin I. G., Shaitura S. V. M.:KUDIT, 2009. – 272 p.

2.*Geoinformatika*: uchebnoe posobie [Geoinformatika: uchebnoe posobie] / Laikin V. I., Uporov G. A. – Komsomolsk-on-Amur: publishing house of Amspu, 2010. – 162 p.

3.*Imitation modeling: theory and technologies* /Yu. I.Ryzhikov – S-P, 2004. – 529 p.

4. Online resources: http://www.gisa.ru/; http://resources.arcgis.com/

5.Ivanov V. G., Borodin N. D. Osnovy formirovaniya United Geoinformation space of special purpose with the use of Webtechnologies // *CAD and graphics*, No. 3, 2016, pp.18-20.

6. Gorbunov A. A., Ponomorchuk A. Yu., Ivanov V. G. use of Geoinformation systems in the adoption of managerial decisions in the United State System of prevention and elimination of emergency situations // *scientific and analytical journal "Bulletin of the St. Petersburg University State Fire Protection Service of the Ministry of emergency situations Russia*", 2015, № 2, pp. 71-76.

7.Shelukhin O. I. / *Modeling of Information Systems* / O. I. Shelukhin // textbook for universities, 2nd ed., rework. and add., Scientific and technical publication "hot line – telecom", 2018., 536 p.

8.Phlegontov A.V., Matyushichev I. Yu./*Modeling of Information Systems. Unified Modeling Language. Textbook* / A.V. Phlegontov, I. Yu. Matyushichev / Lan, Moscow, 2019, 112 p.

9.A. A. Svetlichny, A.V. Pyatkova / Geoinformation modeling of water erosion of soils / Svetlichny A. A., Pyatkova A.V.// Collection of scientific works. - Kharkiv, 2014 . - Issue 19, p. 24.

10. Svetlichny A. A., Pyatkova A.V., Plotnitsky S. V. Problema verifikatsii spatially distributed mathematical models of water erosion of soils [the problem of verification of spatial distribution of mathematical models].] / / Bulletin of the Odessa National University им. I. I. Mechnikov. Geographical and geological sciences. - [Volume 18, Ed. 3]. -2013. - pp. 78-90.

11. Svetlichny A. A. Matematicheskoe modelirovanie vodnoi erosii: problema klassifikatsii [mathematical modeling of water erosion: a problem of classification]. Geographical and geological sciences series. - [Volume 15, issue 13]. -2010. - pp. 32-39.

12.Tsvetkov V. Ya., Buravtsev V. A. metrics of a complex deterministic system. 2017. Vol. 7. № 3 (25). P. 334-346. DOI: 10.18287/2223-9537-2017-7-3-334-346

13. the Rosenbergs.N. Toposemantic information correspondence in spatial modeling. 2017. № 3. С. 64-73.

14. Christopher B. Oneal, John D. Stuart, Steven J. Steinberg, Geographic analysis of natural fire rotation in the California redwood forest during the suppression [[electronic resource] // Fire Ecology, Volume02, Issue01, Spring, 2016. - Access mode : http://fireecology.org/docs/Journal/pdf/Volume02/Issue01/073.pdf

15. Radmila Jovanovic, Zeljko Bjeljac,. Olgica Miljkovic, Aleksandra Terzic Spatial analysis and mapping of fire risk zones and vulnerability assessment – case study mt. Stara Planina [electronic resource] // Prevention and Education in Natural Disasters, 2018. - Access mode : http://www.doiserbia.nb.rs/img/doi/0350-7599/2013/0350-75991303213J.pdf

16.Atlas of natural hazards & risks of Georgia // Caucasus Environmental NGO Network, 2019 [electronic resource]. - Access mode : http://drm.cenn.org/index.php/en/

17. Svetlitchnyi A. A. Spatial distribution of soil moisture convent within catchments and its modeling on the basis of topographic data / A. A. Svetlitchnyi, S. V. Plotnitskiy, O. Y. Stepovaya // Journal of Hydrology [V. 277]. – 2013. – Pp. 50-60.

18. Mordechai Ben-Ari. Mathematical Logic for Computer Science/ Third Edition. Springer London Heidelberg New York Dordrecht, 2012. 364 p. ISBN 978-1-4471-4128-0

19. Victor Raizer / Optical Remote Sensing of Ocean Hydrodynamics / Copyright Year 2019, ISBN 9780815360148

20. William Emery Adriano Camps / Introduction to Satellite Remote Sensing, 1st Edition, Atmosphere, Ocean, Land and Cryosphere Applications / 2017, ISBN: 9780128092590

D.Sc. Druzhynin V., D.Sc. Stepanov M., Ph.D. Zhyrov G, Trofimchuk V.

TECHNOLOGICAL APPROACHES TO THE FORMATION OF DIGITAL IMAGES OF TERRAIN OBJECTS DURING REMOTE SENSING OF THE EARTH FROM PHOTO AND RADAR SYSTEMS

The paper is devoted to the consideration of the current state and trends in the use of simulation modeling for mathematical modeling of terrain data obtained from the processing of digital images, both from photos and radar systems of Aerospace-based aircraft. The relevance of considering the state and trends in the development of technological approaches in modeling systems is due to the practical need to obtain data from photo and radar images of objects in the system's viewing area, taking into account the growing requirements for the efficiency and accuracy of determining (detecting) images of observation objects in real time in difficult conditions. The general structure of the construction of technologies used for simulation modeling of terrain objects is given the main prospects for practical application of these technologies in solving problems of classification and monitoring of terrain objects are determined.

Estimates of the main technological approaches to images of objects in the application of the considered systems and assessment of the accuracy of determining terrain coordinates are given. Channels of information transmission in the process of receiving and processing data from photo and radar systems of remote sensing of the earth are considered.

Also, as an example, a chain-node model of spatial data about objects that are obtained during remote sensing of the Earth and are represented as linear and point-based. To create a geographical basis for further modeling of various telecommunications and communication systems. This will allow for more accurate development of telecommunications and communication systems based on geographical data. Take into account the closing angles when forming a cellular connection.

Keywords: simulation modeling, simulation system, simulated process, vector model, wired communication lines, transmission channels, encryption.

УДК 629.015.4

Комаров В.О. (ЦНДІ ОВТ ЗСУ)
к.т.н., доц. **Пампуха І.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-05

ПОРІВНЯННЯ МОЖЛИВОСТЕЙ МЕТОДІВ НЕРУЙНІВНОГО КОНТРОЛЮ ДЛЯ ЕФЕКТИВНОГО ВИЯВЛЕННЯ ПОШКОДЖЕНЬ У СИЛОВИХ ЕЛЕМЕНТАХ КОНСОЛЬНО ЗАКРІПЛЕНИХ КОНСТРУКЦІЙ ПЛАНЕРА ЛІТАКА

У статті розглядається економічний ефект від застосування методу контролю частоти власних коливань при технічному обслуговуванні авіаційної техніки та порівняння ефективності виявлення тріщин методами: рентгенографічним, візуальним і контролю частоти власних коливань.

Метод контролю ЧВК досить простий у експлуатації. Він відрізняється від інших МНК незначним терміном перевірки, великою точністю одержання результатів. Цей метод повинен суттєво доповнити спектр методів неруйнівного контролю, що широко застосовуються у цей час, таких як контроль за допомогою проникаючих випромінювань (рентгено й гаммаграфії). Метод контролю ЧВК, що пропонується, не вимагає узгодження з виконанням іншого виду регламентних робіт на літаку. Необхідно виконання лише деяких умов: об'єкт контролю не повинен бути підданим зовнішнім впливам (не допускається ходіння по об'єкту контролю, збільшення його маси сторонніми предметами). Таким чином метод контролю ЧВК, забезпечуючи отримання об'єктивної інформації про стан закритих обшивкою елементів конструкції, при значному виграші в часі, що витрачається на контроль, дає значний економічний ефект при його використанні.

Метод контролю ЧВК, забезпечуючи одержання об'єктивної інформації про стан закритих елементів конструкції, при значному виграшу в часі, що витрачається на контроль, дає значний економічний ефект при використанні порівняно дешевої контрольно-записуючої та діагностичної апаратури. Правильна оцінка надійності і якості ЛА з урахуванням інформації, отриманої при діагностичному контролі, має велике значення як з точки зору економічної доцільності їх використання в подальшій експлуатації, так і, як наслідок, для забезпечення безпеки польотів.

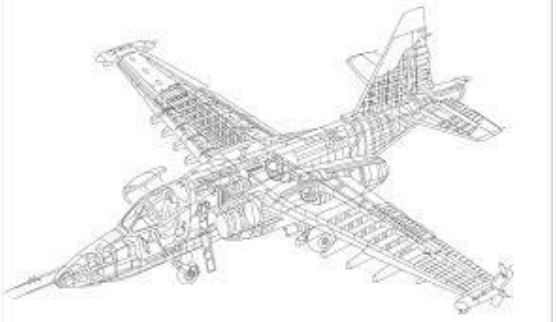
Ключові слова: метод контролю, дефектоскопія, неруйнівний контроль, дефекти, частота власних коливань

Вступ. З розвитком авіації та при переході системи експлуатації за технічним станом суттєвих змін зазнали й методи та форми технічного обслуговування літальних апаратів (ЛА). У теперішній час, технічне обслуговування літаків розвивається в напрямах більш гнучких форм, щоб уникнути зайвих дорогих зупинок експлуатації техніки й гарантувати виявлення виниклих схованих дефектів, розвиток яких може привести до виходу ЛА з ладу. Можливість переходу до прогресивної системи обслуговування за технічним станом багато в чому визначається рівнем розвитку неруйнівних методів контролю (НМК) [1].

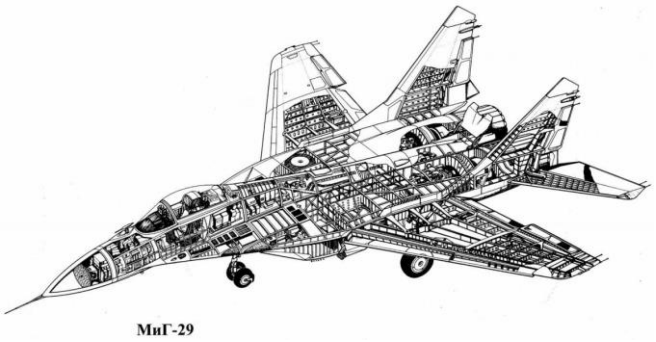
Аналіз останніх досліджень та публікацій. Силова конструкція літаків типу Су-17, Су-24, Су-25, МіГ-29 та інших, що знаходяться на озброєнні Збройних Сил України, досить надійна навіть при наявності експлуатаційних та бойових уражень основних силових елементів планера літака.

Планер зазначених типів літаків є достатньо ремонтопридатним, тобто пристосованим до усунення наслідків щодо появи експлуатаційних чи бойових пошкоджень, що підтверджено досвідом виконання ремонту.

Су-17М2



Су-25



Але ремонт після отримання бойових пошкоджень спрямований лише на відновлення пошкодженої ділянки і не враховує наявність втомленої пошкодженості елементів, яку накопичено за весь терміном служби планера. Крім того, виконання ремонту бойового пошкодження конструктивного елементу не передбачає оцінку технічного стану сполучених силових елементів конструкції. Ці особливості на сучасному етапі експлуатації ЛА необхідно враховувати при ремонті експлуатаційних й бойових пошкоджень [2]. Тому для забезпечення умов безпечної експлуатації силової конструкції з експлуатаційними й бойовими ураженнями необхідно здійснювати контроль їх технічного стану. В експлуатації авіаційної техніки використовуються різні системи контролю у залежності від прийнятих методів експлуатації - по ресурсу, за технічним станом і суміщений.

Основна частина. При експлуатації за встановленим ресурсом контроль конструкцій виконується після досягнення обмежень їх ресурсу, але разом з тим перевірки можуть проводитися вибірково там, де вони можливі та ефективні. Такі початкові інтервали контролю встановлюються виробником техніки.

При експлуатації за технічним станом плануються періодичні контрольно-перевірочні роботи, за результатами яких приймається рішення про подальшу експлуатацію. Інтервали контролю при цьому базуються на досвіді експлуатації і рекомендаціях виробників, а також на припустимості пошкоджень. Повністю перевести авіаційну техніку на експлуатацію за технічним станом не вдається (тільки від 60 до 75 % агрегатів і систем сучасної авіатехніки експлуатуються за станом), тому основним методом експлуатації є суміщений метод.

Перехід на експлуатацію по технічному стану і на суміщений метод експлуатації сприяє підвищенню рівня надійності техніки завдяки впровадженню найбільш ретельного контролю значно більшого числа деталей об’єкта в умовах експлуатації і ремонту. Більша увага при цьому повинна приділятися визначенню стану матеріалу деталей методами дефектоскопії.

Порядок проведення робіт по технічному обслуговуванню і контролю визначається типом техніки і може бути різним. Однак, в програмах технічного обслуговування різних об’єктів АТ здійснюються деякі загальні принципи використання засобів дефектоскопії

Так, часті перевірки передбачається виконувати візуально. Перевірки з більшою

періодичністю виконують з використанням інструментальних засобів контролю. Найбільш часто перевіряються високо навантажені і відповідальні деталі та вузли. При великому напрацюванні з появою втомних тріщин і корозії передбачається збільшення кількості деталей, що контролюють, ретельності і частоти перевірок засобами дефектоскопії, використання комплексного контролю.

Вибір методів контролю для кожної деталі здійснюється у два етапи. На першому етапі враховують вид і характер очікуваних дефектів, матеріал об'єкта контролю та інші фактори. На другому етапі по спеціальній програмі визначають найбільш ефективний метод. За результатами вибору методу неруйнівного контролю в деяких випадках необхідне доопрацювання конструкцій для забезпечення контролепридатності.

Надійність контролю залежить від застосовуваних методів і засобів контролю, чутливості засобів контролю, обумовлюється режимами контролю та характером впливу зовнішніх факторів. Чутливість основних методів неруйнівного контролю, що застосовуються для дефектації ЛА, до величини пошкодження, представлена в табл. 1.

Таблиця 1

Вимоги до граничної чутливості приладів (мм., мм ^{2})

Метод контролю	За шириною	За глибиною	За протяжністю
магнітопорошковий	0,001-0,01	0,01-0,05	0,3
вихрестумовий	0,0005-0,001	0,15-0,2	0,6-,2,0
ультразвуковий	0,001-0,03	0,3	мін. площа 2
імпедансний	-	-	мін. площа 15
капілярний	0,001-0,03	0,01-0,1	0,1
оптичний	0,005-0,01	-	0,1
рентгенівський	0,1	1-2%	-

Загальний ефект від використання НМК при технічному обслуговуванні авіаційної техніки (АТ) складається з переваг, отриманих в основному в результаті скорочення часу простою АТ при виконанні на ній регламентних робіт, пов'язаних з повним або частковим розбиранням для пошуку дефектів і несправностей, і одержання більш об'єктивних відомостей про технічний стан конструкції.

Зазвичай, профілактичний контроль пов'язаний з повним або частковим розбиранням АТ для доступу до систем і агрегатів, що цікавлять, на предмет появи ушкоджень у силових елементах конструкції. Це суттєво підвищує вартість контролю, збільшує трудовитрати. Профілактичні контрольні операції на новій АТ призначаються, як правило, у великому об'ємі й більш частіше, ніж це дійсно необхідно, із залученням великого числа обслуговуючого персоналу. Забезпечення надійності таким шляхом стає усе більш затратним [3].

До експлуатаційних факторів, що впливають на надійність АТ, відносяться, в більшій мірі, методи контролю (діагностики) та профілактики, що застосовуються при її технічному обслуговуванні і ремонті, об'єктивність і своєчасність отримання інформації про стан АТ при її експлуатації та ремонті.

Однією з найважливіших умов підтримки АТ в справному стані в процесі експлуатації є забезпечення інформацією про кількісні та якісні характеристики стану, динаміці їх змін. Зазначені завдання інформаційного забезпечення та визначення характеристик станів вирішуються в експлуатації за допомогою технічної діагностики з використанням методів неруйнівного контролю, зазначених в таблиці 1.

Технічна діагностика конструктивних елементів планера ЛА, з використанням зазначених методів неруйнівного контролю, дозволяє виявляти дефекти до виникнення відмови і планувати профілактичні або ремонтні роботи. Технічна діагностика також дозволяє

встановити початок появи небезпечного дефекту або тріщини задовго до того, коли буде потрібно негайне зняття ЛА з експлуатації.

Методи діагностування, що зазначені в табл. 1, спираються на вирішення наступних завдань:

- за прийнятим від конструкції, яка діагностується, сигналу, визначити ступінь її справності - справна вона чи ні;

- шляхом вимірювання параметрів конструкції визначити величину параметрів стану не розбираючи конструкції (отримання поточної інформації про технічний стан конструкції в процесі її діагностування та контролю).

Всі методи неруйнівного контролю, що використовуються в процесі експлуатації АТ, переслідують рішення комплексної задачі, важливої для бойової частини - зменшити час контролю (діагностування) ЛА і знизити його собівартість шляхом застосування недорогого обладнання та мінімальної кількості обслуговуючого персоналу [4].

Ефективним засобом зниження вартості технічного обслуговування літаків можна вважати широке застосування в дефектоскопії методу контролю частот власних коливань (ЧВК), заснованого на контролі в процесі експлуатації ЛА зміни динамічних характеристик конструкції при появі тріщин або іншого типу пошкоджень силових елементів конструкції.

Застосовуваний для частотних випробувань (для діагностики конструкції) метод контролю ЧВК, заснований на застосуванні фізичних коливань із власною частотою, що збуджуються або виникають в об'єкті контролю (крилі або інших консольно закріплених конструкціях планера ЛА), і класифікується за ДСТУ 23829-85 та ДСТУ 15467-79 і по керівному документу РД 25.002-80 як резонансний МНК. Резонансний МНК заснований на порушенні авторезонансних пружних коливань в об'єкті контролю або його частини й аналізі параметрів коливань динамічної системи. При застосуванні резонансного МНК реєструються такі параметри авторезонансних коливань, як частота власних (авторезонансних) коливань і амплітуда коливань.

Іспитове устаткування, яке застосовується при цьому методі, повинно забезпечувати:

- стабільність підтримки частоти власних коливань і задану точність випробувань;

- виключити вплив повторних експлуатаційних факторів, що знижують чутливість устаткування;

- можливість ручного й автоматичного керування процесом випробувань;

- можливість оперативного (негайного) одержання інформації під час проведення частотних випробувань;

- можливість багаторазового використання й повторення.

Суть вказаного методу полягає в тому, що поведінка конструкції при вільних коливаннях (з частотою власних коливань) характеризує її «динамічну індивідуальність», що полягає у властивому їй розподілі масових і жорсткісних характеристик. Втомні і інші пошкодження (включаючи бойові) знижують жорсткість динамічної системи.

Якщо відомо початкове значення частоти власних коливань для нової конструкції (завідомо неушкодженої конструкції або для конструкції, яка пройшла належний діагностичний контроль методами неруйнівного контролю), то, виявляючи зміну динамічних параметрів цієї конструкції в процесі експлуатації, можна завчасно виявити пошкодження в силовому наборі (закритому обшивкою) і вжити заходів до їх усунення.

Таким чином, завдання діагностування формулюється при цьому як зворотна пружна динамічна задача - ідентифікація масово-інерційних, частотних і дисипативних параметрів конструкції за відомими характеристиками коливального руху.

Чутливість методу контролю ЧВК до пошкоджень з конкретним місцем його розташування залежить від напруженого стану пошкодженого силового елемента. Пошкодження таких елементів продольного силового набору (зокрема, крила) як стрингери, обшивка, пояси лонжеронів значно зменшують лише вигинну жорсткість конструкції по осі Y, а поява пошкоджень в поясах бортових нервюр, поздовжніх тріщин в стінках лонжеронів і

в обшивці практично не призводить до зниження ЧВК вигинних тонів. У той же час зазначені ушкодження істотно знижують жорсткість конструкції на крутіння [5].

Отже, на реальних консольно закріплених конструкціях літака, таких як крило, стабілізатор і кіль, з метою отримання більш об'єктивної інформації для повного діагностичного аналізу, доцільно порушувати не тільки вигинні, але і крутильні форми коливань [6-8].

Метод контролю ЧВК досить простий у експлуатації. Він відрізняється від інших МНК незначним терміном перевірки, великою точністю одержання результатів.

Так, застосування методу контролю ЧВК для літака дозволить збільшувати її ресурс із одночасним зниженням працевитрат, що було б не можливим при дорогому й частому контролі вузлів і елементів конструкції ЛА, пов’язаних з повним або частковим розбиранням літака [9].

Час перебування АТ у неробочому стані значно скорочується, що особливо важливо для об’єктів бойової авіаційної техніки.

Метод контролю ЧВК повинен суттєво доповнити спектр методів, що широко застосовуються у цей час такі, як контроль за допомогою випромінювань, що проникають (рентгено- й гаммаграфії). Візуальний контроль із застосуванням радіографічних методів слід проводити при дотриманні необхідних застережень. Обслуговуючий персонал не повинен находитися близько літака, що контролюється, щоб виключити біологічний вплив на організм людини. Це призводить до збільшення загального часу простою літака. Метод контролю ЧВК, що пропонується, не вимагає узгодження з виконанням іншого виду регламентних робіт на літаку. Необхідно виконання лише деяких умов: об’єкт контролю не повинен бути підданим зовнішнім впливам (не допускається ходіння по об’єкту контролю, збільшення його маси сторонніми предметами).

У табл. 2 наведені порівняльні дані щодо працезатрат на контроль основних елементів ЛА двох типів при візуальному, рентгенівському й методі контролю ЧВК з метою виявлення тріщин.

Таблиця 2

Порівняльні дані щодо працезатрат на контроль основних елементів ЛА двох типів при візуальному, рентгенівському й методі контролю ЧВК

Об’єкт контролю	Трудовитрати, години, хвилини					
	Візуальний контроль		Рентгенографія		Метод контролю ЧВК	
	Перший ЛА	Другий ЛА	Перший ЛА	Другий ЛА	Перший ЛА	Другий ЛА
Стерно висоти	24	40	3 г.	5 г.10 хв.	20	20
Стерно повороту	25	32	1 г.	4 г. 45 хв.	30	35
Закрилки	24	40	2 г.	3 г.	20	20
Елерон	20	23	1 г.	3 г. 10 хв.	20	20
Крило	1 г.	1г.30хв	до 10 г.	До 10 г.	30	30

Апаратуру для контролю ЧВК можуть обслуговувати два-три фахівці, що мають середній рівень підготовки. Для двох інших, зазначених вище методів, необхідно мати висококваліфікований обслуговуючий персонал з великим досвідом експлуатації.

У табл. 3 показані порівняльні характеристики трудовитрат існуючих МНК і перспективного МНК (методу контролю ЧВК), заснованого на контролі динамічних властивостей конструкції.

Таблиця 3

Порівняльні характеристики трудовитрат існуючих МНК і перспективного МНК (методу контролю ЧВК)

Об'єкт контролю	Мета контролю	Трудовитрати, людино/год		
		Візуальний	Рентгенографія	Метод ЧВК
Стерно висоти	Стан обшивки і силового набору	80	14	2-3
Стерно повороту		15	4	2-3
Закрилки		75	15	до 2
Елерон		20	7	до 2
Крило	Наявність пошкоджень	90	12	до 2

З табл. 3 видно, що метод контролю ЧВК, забезпечуючи одержання об'єктивної інформації про стан закритих елементів конструкції, при значному виграшу в часі, що витрачається на контроль, дає значний економічний ефект при використанні порівняно дешевої контрольно-записуючої та діагностичної апаратури (зразок якої показано на рис. 1), де, відповідно, на лівій консолі крила літака показано схему закріплення обладнання 1 для збудження у комплексі вигинних і крутильних коливань по першому тону коливань, а на правій консолі – обладнання 2 для збудження у комплексі вигинних і крутильних коливань по другому та третьому тону коливань (обладнання конструктивно не відрізняється між собою).

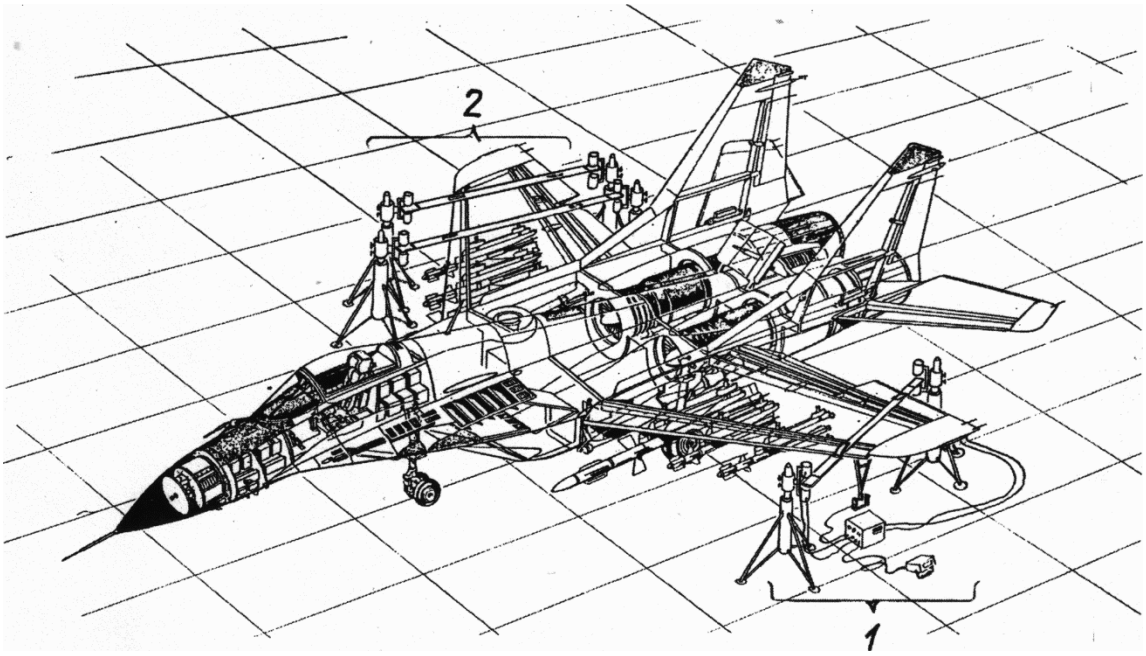


Рисунок 1 – Схема розміщення діагностичної апаратури на крилі літака

Загальна економія працезатрат при контролі методом ЧВК становить 90-95% працезатрат, при візуальному огляді й до 80%, при рентгенівському контролі. При цьому обладнання можуть обслуговувати 1-2 фахівця.

Метод контролю ЧВК досить простий в експлуатації. Він відрізняється від інших МНК незначним терміном проведення перевірки, великою точністю одержаних результатів [10].

Так, застосування відносно дешевого методу контролю ЧВК для системи технічного обслуговування літака дозволить збільшувати періоди до чергових перевірок літака з одночасним зниженням працевитрат, що було б не можливим при дорогому й частому контролі вузлів і елементів конструкції ЛА, пов’язаних з повним або частковим розбиранням літака.

Час перебування АТ у неробочому стані значно скорочується, що особливо важливо для об’єктів авіаційної техніки, насамперед, в період ведення інтенсивних бойових дій.

Правильна оцінка надійності і якості ЛА з урахуванням інформації, отриманої при діагностичному контролі, має велике значення як з точки зору економічної доцільності їх використання в подальшій експлуатації, так і, як наслідок, для забезпечення безпеки польотів. Важливе значення в цьому питанні набуває також можливість за фактичними характеристиками технічного стану конструкції встановити її ресурс (й залишкову міцність) [11].

До теперішнього часу ресурс конструкцій ЛА встановлювався, як правило, на підставі стендових і експлуатаційних іспитів. Однак експлуатаційні та стендові випробування не завжди дозволяють в повному обсязі виявити порушення працездатності конструкції і, тим самим, оцінити її ресурс, що, в основному, залежить від міцності, зносостійкості конструктивних елементів об'єкту контролю, досконалості технології ремонту [12,13].

Тому, для більш ефективного отримання діагностичної інформації, необхідно провести наукове обгрунтування робіт по збільшенню ресурсу АТ, періодичності її технічного обслуговування і визначення обсягу регламентних робіт відповідно до вимог льотної придатності. Все це надасть можливість розробити заходи щодо вдосконалення технічного обслуговування, методів діагностування (нових методів неруйнівного контролю), ремонту та льотної експлуатації.

Висновки. Метод контролю ЧВК повинен суттєво доповнити спектр методів неруйнівного контролю, що широко застосовуються у цей час, таких як контроль за допомогою проникаючих випромінювань (рентгено- й гаммаграфії). Візуальний контроль при застосуванні радіографічних методів слід проводити при дотриманні необхідних застережень. Обслуговуючий персонал не повинен находитися близько літака, що контролюється, щоб виключити біологічний вплив на організм людини. Це призводить до збільшення загального часу простою літака. Метод контролю ЧВК, що пропонується, не вимагає узгодження з виконанням іншого виду регламентних робіт на літаку. Необхідно виконання лише деяких умов: об’єкт контролю не повинен бути підданим зовнішнім впливам (не допускається ходіння по об’єкту контролю, збільшення його маси сторонніми предметами). Таким чином метод контролю ЧВК, забезпечуючи отримання об'єктивної інформації про стан закритих обшивкою елементів конструкції, при значному виграші в часі, що витрачається на контроль, дає значний економічний ефект при його використанні. Загальна економія трудовитрат при діагностичному контролі крила літака (а також інших консольно закріплених конструкцій планера літального апарату - горизонтального оперення і кіля) методом ЧВК становить 2-3 чол/години трудовитрат, в той час, як на візуальний контроль піде до 80-90 чол/годин, а на контроль методом рентгенографії - 10-15 чол/годин (в залежності від об'єкта контролю і його розташування відносно поверхні землі).

ЛІТЕРАТУРА:

1. ГОСТ 23146-78 Система технического обслуживания и ремонта техники. Выбор и задание показателей ремонтопригодности. Общие требования. – М.: Изд-во стандартов, 1978. – 10 с.

2. ДСТУ 3004-95. Надійність техніки. Методи оцінки показників надійності за експериментальними даними. – К.: Держстандарт України, 1995. – 123 с.

3. Арепьев А.Н., Громов М.С., Шапкин В.С. Вопросы эксплуатационной живучести авиаконструкций. – М.: Воздушный транспорт, 2002. – 424 с.

4. Пестов М.Д. Боевая эффективность и надежность летательных аппаратов: Методы расчетов: учебн. Пособие для лабораторных работ/ М.Д. Пестов. – М.: Изд-во МАИ, 2002. – 100 с. Библиогр.: с. 97. – 150 экз.

5. Комаров, В.О. Про використання методу контролю частоти власних коливань при виборі методу відновлення авіаційної техніки [Текст] / В. О. Комаров, О. О. Растригін // Проблеми координації військово-технічної та оборонно промислової політики в Україні. Перспективи розвитку озброєння та військової техніки : тези доповідей на VII науково-практичній конференції / Міністерство оборони України. Міністерство освіти і науки України. Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України. – Київ, 2019. – С. 350-352.

6. Комаров, В.О. Використання форм власних коливань елементів конструкції літального апарату для діагностування їх залишкової міцності [Текст] / В. О. Комаров, ММ. Мітрахович, О.О. Расстригін. Створення та модернізація озброєння і військової техніки в сучасних умовах : Збірник XIX науково-технічної конференції 5-6 вересня 2019 року / Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки. – Чернігів, 2019. - С. 136-137.

7. Пат. 127849 Україна, МПК (2018.01) B 64 C 3/00, G 01 M 7/00, G 01 B 11/26. Пристрій для визначення просторово-частотних характеристик коливань консольно закріплених елементів літальних апаратів при їхніх випробуваннях на утомлену міцність [Текст] / Комаров В. О. ; заявники і патентовласники Комаров В. О., Расстригін О. О. – № u 2018 02126 ; заявл. 01.03.18 ; опубл. 27.08.18, Бюл. № 16. – 4 с. : іл.

8. Пат. 109226 Україна, МПК (2016) G 01 M 5/00, G 01 N 3/00. Спосіб визначення характеристик жорсткості крила літака неруйнівним методом в умовах експлуатації та ведення бойових дій [Текст] / Комаров В. О. ; заявники і патентовласники Комаров В. О., Ткаченко В. А., Галушка В. І. – № u 2016 02602 ; заявл. 16.03.16 ; опубл. 10.08.16, Бюл. № 15. – 6 с. : іл..

9. Комаров, В. О. Використання форм власних коливань елементів конструкції літального апарату для діагностування їх залишкової міцності [Текст] / В. О. Комаров, М. М. Мітрахович, О. О. Расстригін. Створення та модернізація озброєння і військової техніки в сучасних умовах : Збірник XIX науково-технічної конференції 5-6 вересня 2019 року / Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки. – Чернігів, 2019. - С. 136-137.

10. Комаров, В. О. Підвищення точності частотних випробувань авіаційних конструкцій [Текст] / В. О. Комаров, М. П. Яременко. Створення та модернізація озброєння і військової техніки в сучасних умовах : Збірник XIX науково-технічної конференції 5-6 вересня 2019 року / Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки. – Чернігів, 2019, - С. 137-138.

11.Когге Ю.К. Основы надежности авиационной техники: ученик для студ. авиацион. техникумов / Ю.К. Когге, Р.А. Майский. – М.: Машиностроение, 1993. – 176 с. – Библиогр.: с. 165. – 1900 екз. – ISBN5-217-01363-X.

12. Ицкович А.А. Надежность летательных аппаратов и авиадвигателей: учеб. пособие для вузов / А. А. Ицкович; Моск. Ин-т инженеров гражд. Авиации. – М.: МНИИГА, 1990. – 104 с. – Библиогр.: с. 104. – 500 экз

13. Пампуха І.В., Нікіфоров М.М., Комаров В.О. Розробка методики визначення запасу міцності бойових літаків на основі аналізу динамічних характеристик з урахуванням експлуатаційних факторів. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2020. № 67. С. 30-39.

REFERENCES:

1. GOST 23146-78 Systema tehnycheskogo obsluzhyvanyja y remonta tehnyky. Vыbor y zadanye pokazatelej remontoprygodnosty. Obshhye trebovanyja. M.: Yzd-vo standartov, 1978. 10 p.

2. DSTU 3004-95. Nadijnist' tehniky. Metody ocinky pokaznykiv nadijnosti za eksperymental'nymy danymy. K.: Derzhstandart Ukrai'ny, 1995. 123 p.

3. Arep'ev A.N., Gromov M.S. and Shapkin V.S. (2002). Voprosy jekspluatacionnoj zhivuchesti aviakonstrukcij. Moscow: Vozdushnyj transport, 424 p.

4. Pestov M.D. (2002). Boevaja jeffektivnost' i nadezhnost' letatel'nyh apparatov: Metody raschetov: uchebn. Posobie dlja laboratornyh rabot. Moscow: Izd-vo MAI, 100 p. ISBN 5-7035-1275-1.

5. Komarov, V.O. and Rastrygin O.O. (2019). Pro vykorystannja metodu kontrolju chastoty vlasnyh kolyvan' pry vybori metodu vidnovlennja aviacijnoi' tehniky. Problemy koordynacii' vijs'kovo-tehnichnoi' ta oboronno promyslovoi' polityky v Ukrai'ni. Perspektyvy rozvytku ozbrojennja ta vijs'kovoi' tehniky : tezy dopovidej na VII naukovo-praktychnij konferencii' / Ministerstvo oborony Ukrai'ny. Ministerstvo osvity i nauky Ukrai'ny. Central'nyj naukovo-doslidnyj instytut ozbrojennja ta vijs'kovoi' tehniky Zbrojnyh Syl Ukrai'ny. Kyi'v, pp. 350-352.

6. Komarov V.O., Mitrahovych M.M. and Rasstrygin O.O. Vykorystannja form vlasnyh kolyvan' elementiv konstrukcii' lital'nogo aparatu dlja diagnostuvannja i'h zalyshkovoi' micnosti. Stvorennja ta modernizacija ozbrojennja i vijs'kovoi' tehniky v suchasnyh umovah : Zbirnyk HIH naukovo-tehnichnoi' konferencii' 5-6 veresnja 2019 roku. Derzhavnyj naukovo-doslidnyj instytut vyprobuvan' i sertyfikacii' ozbrojennja ta vijs'kovoi' tehniky. Chernigiv, pp. 136-137.

7. Komarov V.O., Rasstrygin O.O. (2018). Prystrij dlja vyznachennja prostorovo-chastotnyh harakterystyk kolyvan' konsol'no zakriplenyh elementiv lital'nyh aparativ pry i'hnih vyprobuvannjah na utomlenu micnist' Ukrainian patent, no. 127849.

8. Komarov V.O., Tkachenko V.A., Galushka V.I. (2016). Sposib vyznachennja harakterystyk zhorstkosti kryla litaka nerujnivnym metodom v umovah ekspluatacii' ta vedennja bojovyh dij. Ukrainian patent, no. 109226.

9. Komarov V.O., Mitrahovych M.M., and Rasstrygin O.O. (2019). Vykorystannja form vlasnyh kolyvan' elementiv konstrukcii' lital'nogo aparatu dlja diagnostuvannja i'h zalyshkovoi' micnosti. Rasstrygin. Stvorennja ta modernizacija ozbrojennja i vijs'kovoi' tehniky v suchasnyh umovah *: Zbirnyk HIH naukovo-tehnichnoi' konferencii' 5-6 veresnja 2019 roku.* Derzhavnyj naukovo-doslidnyj instytut vyprobuvan' i sertyfikacii' ozbrojennja ta vijs'kovoi' tehniky. Chernigiv, pp. 136-137.

10. Komarov V.O. and Jaremenko M.P. (2019). Pidvyshhennja tochnosti chastotnyh vyprobuvan' aviacijnyh konstrukcij. Stvorennja ta modernizacija ozbrojennja i vijs'kovoi' tehniky v suchasnyh umovah : *Zbirnyk HIH naukovo-tehnichnoi' konferencii' 5-6 veresnja 2019 roku*. Derzhavnyj naukovo-doslidnyj instytut vyprobuvan' i sertyfikacii' ozbrojennja ta vijs'kovoi' tehniky. Chernigiv, pp. 137-138.

11.Kogge Ju.K .and Majskij R.A. (1993.) Osnovy nadezhnosti aviacionnoj tehniki: uchenik dlja stud. aviacion. Tehnikumov. Moscow: Mashinostroenie, 176 p., ISBN5-217-01363-H.

12. Ickovich A.A. (1990). Nadezhnost' letatel'nyh apparatov i aviadvigatelej: ucheb. posobie dlja vuzov Mosk. In-t inzhenerov grazhd. Aviacii. Moscow: MNIIGA, 104 p.

13. Pampuha I.V., Nikiforov M.M., Komarov V.O. (2020) Rozrobka metodyky vyznachennja zapasu micnosti bojovyh litakiv na osnovi analizu dynamichnyh harakterystyk z urahuvannjam ekspluatacijnyh faktoriv. *Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka*. K.: VIKNU, no 67. Pp. 30-39.

Komarov V.O., Ph.D. Pampukha I.V.

THE COMPARISON OF CAPABILITIES OF METHODS OF THE NON-DESTRUCTIVE CONTROL FOR THE EFFECTIVE IDENTIFICATION OF DAMAGES IN THE FORCE ELEMENTS OF THE CONSOLE FORTIFIED CONSTRUCTIONS OF THE AIR PLANE PLANNER

The article describes the economic effect of applying the method of frequency control of the natural oscillations whilst providing technical service to aviation hardware and the comparison of the effectiveness of identifying splits with the aid of the following methods: x-ray graphic, visual and the control of frequency of natural oscillations. The method of control of the frequency of natural oscillations is quite simple in terms of application. It differentiates from the other methods of scientific control due to an insignificant period of checking, and a high precision of the results achieved. This method is to significantly increase the spectrum of non-damage control that is widely applied nowadays, such as control with the aid of piercing radiation (x-ray and gammagraphy). The method of control of the frequency of natural oscillations, which is suggested doesn't require cohesion with the exercise of other types of technical activities on a plane. It is only considered necessary to fulfil a certain number of requirements: the object of control is not to be subjected to external influences (it is prohibited to step on the object of control, the increase of its mass by side objects). Thus, the method of control of the frequency of natural oscillations, assuring the reception of objective information about the state of the concealed elements of constructions, whilst spending less time on control provides a significant economic effect when used. The method of control of the frequencies of natural oscillations, whilst assuring the reception of objective information on the hidden and concealed elements of the construction when providing additional time which is spent on control, provides a significant economic effect when using the comparatively cheap control-fixating and other hardware for diagnosis.

The correct assessment of the sustainability and the quality of the flying device taken into account the information received in the course of diagnosis control has a significant meaning both in terms of economic effect of their implementation in the course of further exploitation, and as well as the assurance of security of flights.

Keywords: method of control, defectoscopia, non-damage control, frequency of natural oscillations.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Джулій В.М.** (ХмНУ)
д.т.н., с.н.с. **Сєлюков О.В.** («Укрспецконсалтинг»)
к.т.н., доц. **Орленко В.С.** (ХмНУ)
Атаманюк А.В. (ХмКК ХКТЕ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-06

МОДЕЛЬ БЕЗПЕКИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

У статті запропоновано підхід до визначення моделі безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу. Інформаційно-телекомунікаційні мережі є великомасштабними мережами з постійно зростаючим числом абонентів. З бурхливим зростанням кількості користувачів ІТКМ виникають проблеми інформаційної безпеки і захисту інформації в них. Проведений аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту.

Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даної задачі. Проведений аналіз публікацій з даної тематики показує, що існуючі рішення малоефективні. Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Розроблено алгоритм реалізації ЗПЗІ (загрози поширення забороненої інформації) в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Запропонована імітаційна модель ЗПЗІ в ІТКМ, яка враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі. Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

Ключові слова: інформаційна безпека, аналітична модель, імітаційна модель, поширення загроз, інформаційна взаємодія, модель мережі.

Вступ. Інформаційно-телекомунікаційні мережі (ІТКМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. Сучасною проблемою таких систем є їх низький рівень інформаційної безпеки. Ефективного захисту абонентів від загрози поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій (SOAP, CORBA, REST тощо), не існує. Серед безлічі функцій захисту принциповою в відношенні даних систем є функція попередження прояву забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози поширення і

розсилання повідомлень з попередженнями про наслідки дій зі забороненим контентом. Використання інших функцій (попередження, виявлення, локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в реальних умовах неможливо.

Інформаційно-телекомунікаційна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярними з них є соціальні мережі. З бурхливим ростом кількості користувачів інформаційно-телекомунікаційних мереж виникають і проблеми безпеки в них. Узагальнена структурна схема інформаційно-телекомунікаційних мереж (ІТКМ) приведена на рис. 1. Її склад в загальному випадку утворюють такі функціональні елементи:

- абоненти (А). Під абонентом розуміється людино-машинна система, що складається з пристрою, через який здійснюється доступ до мережі, і безпосередньо користувача ІТКМ. Абоненти можуть бути окремими вузлами мережі (якщо користувач використовує свій домашній комп'ютер), або можуть бути об'єднані в корпоративну обчислювальну мережу (КОМ) (якщо абонент використовує робочий комп'ютер), включають в себе модулі (інформаційного) захисту (МЗ) і програмне забезпечення (браузер) для взаємодії з керуючим елементом;

- мобільні абоненти (МА). Користувачі, які використовують мобільні пристрої (смартфони, планшети тощо), для доступу до мережі. Також використовують програмне забезпечення (спеціальний додаток) і модулі захисту (МЗ);

- сервери (С). У КОМ знаходяться інформаційні сервери різного функціонального призначення, які беруть участь в інформаційній взаємодії (наприклад, проксі-сервера);

- КОМ містить крім абонентів і серверів, також засоби маршрутизації, комутації та адміністрування (МКА), систему безпеки (СБ), що включає механізми захисту для всієї корпоративної мережі;

- засоби телекомунікації, що забезпечують взаємодію абонентів між собою;

- керуючий елемент технічно є сукупністю комутуючого і серверного устаткування, що реалізує основні функції системи. Включає в себе сервери, які містять в загальному випадку: балансувальник навантаження (БН), елемент бізнес-логіки (БЛ), бази даних (БД), інфраструктурні системи (ІС) (системи статистики, конфігурації, моніторингу тощо).

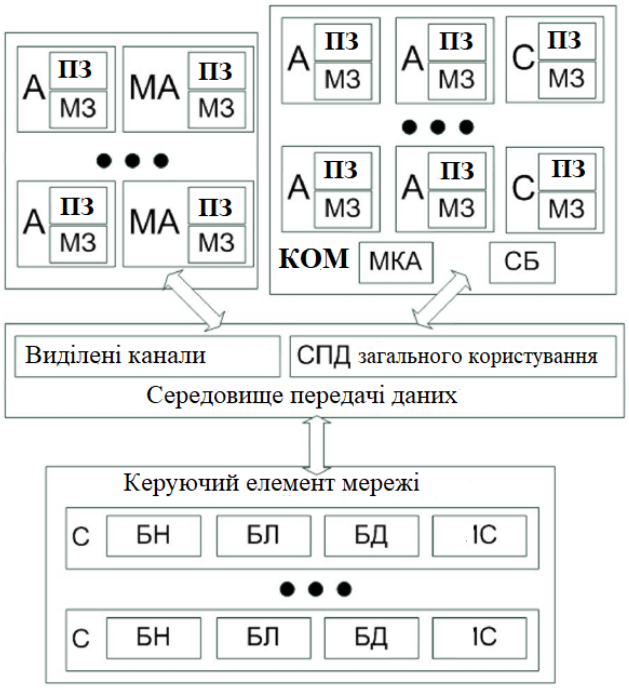


Рисунок 1 – Структурна схема ІТКМ

Розглянемо існуючі проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах, які актуальні для даного дослідження:

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи. Найбільш вразливими компонентами системи, що часто атакуються, є: сервери; робочі станції; середовище передачі інформації; вузли комутації. Типові інформаційні впливи зловмисників:

Прослуховування мережевого трафіку. Щоб прослухати трафік (sniffing) мережевий адаптер переводиться в «безладний» режим. У цьому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, як в нормальному режимі функціонування-технології – ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating. Перехоплення здійснюється з використанням мережевих моніторів, з яких найбільш функціональними є Sniffer Pro від компанії Sniffer Technologies, IRIS Network Traffic Analyzer від компанії EYE і TCP Dump.

Наслідки. Сучасні мережеві протоколи (TCP / IP, ARP, HTTP, FTP, SMTP, POP3 тощо) не мають механізмів захисту (дані передаються у відкритому вигляді). Зловмисник, що перехоплює трафік між сервером і будь-яким вузлом мережі, може заволодіти аутентифікаційними даними користувача (отримати пароль).

Протидія. Відомо ряд методів визначення наявності запущеного сніфера в мережі, наприклад метод пінга, метод ARP, метод DNS і метод пастки.

Сканування вразливостей. Результатом роботи сканера є інформація про систему, що містить список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПЗ (а отже і вразливостей, властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаку. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосереднього НСД.

Виявлення. Само по собі сканування не є незаконним. Однак, якщо сканування з боку зовнішньої, по відношенню до системи, мережі звичайне явище, то сканування комп'ютерів з внутрішньої мережі – безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора. Виявити кроки сканування можна, вивчаючи журнали реєстрації міжмережевих екранів (МЕ). Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ і системи виявлення вторгнень СВВ мають модулі (plug-in), що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють здійснювати сканування максимально приховано. Наприклад, в Nmap існують можливості, що дозволяють значно ускладнити виявлення сканування для СВВ.

Протидія. Використання мережевих СВВ, або періодичне вивчення журналів реєстрації МЕ.

Мережеві атаки. Мережеві атаки можна розділити на: атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями; атаки, спрямовані на відмову в обслуговуванні (Denial Of Service attacks). Атаки не обов'язково використовують вразливості в ПЗ системи, що атакується. Порушення працездатності системи відбувається через те, що дані, що їй посилають, призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Суть її в наступному: на комп'ютер жертви надсилається сильно фрагментований ICMP-пакет великого розміру. Реакцією ОС Windows на отримання такого пакету є повне зависання.

Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків – експлойти (exploit). Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти є шкідливими програмами, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання НСД до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій подавлення антивірусних програм і МЕ. Наслідки застосування

експлойтів можуть бути самими критичними. У випадку отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути такими: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких та зовнішніх носіїв інформації, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлів з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СОВ, встановлені на системі, що атакується, в деяких випадків не в змозі відобразити дію експлойтів. Для успішного відображення атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча є розробки, здатні за завіреннями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

Шкідливі програми. Шкідливі програми – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якого іншого впливу, що перешкоджає нормальному функціонуванню мережі. До шкідливих програми відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки тощо.

Протидія. Типовим методом протидії є застосування антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване програмне забезпечення.

2. Проблема забороненого контенту. Залежно від законодавства країни різні матеріали можуть вважатися нелегальними. У більшості країн заборонені: матеріали сексуального характеру за участю дітей і підлітків, порнографічний контент, описи насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті. В українському законодавстві кілька законів регулюють питання надання інформації про фізичних та юридичних осіб, а саме: Закон України «Про інформацію» від 02.10.92, що регулює відносини щодо одержання і поширення інформації; Закон України «Про захист персональних даних» від 01.06.2010, що визначає захист і обробку персональних даних; Закон України «Про доступ до публічної інформації» від 13.01.2011, який надає право на отримання інформації, що знаходиться у володінні розпорядників.

Аналогічно з концепцією забезпечення комплексного захисту об'єкта інформатизації, можна сформувати повну множину функцій захисту від забороненої інформації. Під функцією захисту (ФЗ) розуміється сукупність однорідних в функціональному відношенні заходів, що регулярно здійснюються в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік повної множини функцій захисту від забороненої інформації в соціальних мережах:

1. Попередження умов виникнення забороненої інформації. Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу поширення забороненої інформації в соціальних мережах, так як в цілому ситуація з дотриманням законів незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2. Попередження безпосередньої прояви забороненої інформації. Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі.

3. Виявлення забороненої інформації, яка проявилася. Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даного захисту використовується різні СОРМ (система оперативно-розшукових заходів). Дана ФЗ пов'язана з проблемами контекстного пошуку, а також необхідністю контролю над всією системою.

4. Попередження впливу на абонентів забороненої інформації, яка проявилася. Функція може бути реалізована за допомогою автоматичного пересилання повідомлення з попередженням про відповідальність за розповсюдження забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до керування системи та нелегітимними – при його відсутності (зламання акаунта). ФЗ ділиться на дві функції. Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним одержувачам забороненої інформації.

5. Виявлення впливу забороненої інформації на абонентів. Функція пов'язана безпосередньо з фіксацією процесу поширення забороненої інформації, може бути реалізована через контекстний аналіз повідомлень.

6. Локалізація, обмеження впливу забороненої інформації на абонентів. Функція реалізується через блокування абонентів, що поширюють заборонену інформацію, або абонентів – потенційних розповсюджувачів. Дана ФЗ опирається на попередні функції і для її ефективної реалізації необхідний контроль над системою.

7. Ліквідація наслідків виявленого впливу забороненої інформації на абонентів. Функція пов'язана з видаленням забороненої інформації з системи. Для реалізації даної функції також необхідний контроль над системою.

На основі проведеного аналізу функцій захисту видно, що найбільш ефективні функції – це перші функції, оскільки вони забезпечують захист на початкових етапах. Наведені функції захисту мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є $ФЗ_2$. На даному етапі, маючи інформацію про топології ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Постановка задачі. Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗПЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження. Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в межах цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування загрози поширення забороненої інформації більше 30%. Крім того, дані підходи мають в основному теоретичний характер, практика їх використання не виходить за межі експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів загрози поширення забороненої інформації, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Створення моделей та алгоритмів поширення загрози забороненої інформації – одна з ключових задач в даному напрямку. При її вирішенні виникають проблеми, пов'язані з властивостями розглянутої інформаційно-телекомунікаційної системи, а саме:

1. Відсутність перевірки достовірності даних про вузол системи. Дуже часто абоненти ІТКМ вказують недостовірну інформацію про себе.

2. Закритість системи. Структура та інформація про управління системою є конфіденційною інформацією.

3. Проблема збору інформації. Неможливо отримати повну інформацію про топологію ІТКМ. Існує можливість для звичайного абонента збору інформації про структуру мережі (функції API), але ця можливість має багато обмежень (налаштування приватності, часовий інтервал).

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу.

Прведений аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту, існуючі рішення малоефективні.

Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відбивається SF мережею. При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Основна частина. За результатами проведеного дослідження предметної області вставлено необхідність розробки імітаційної і аналітичної моделей поширення загрози забороненої інформації в ІТКМ. Імітаційна модель необхідна для отримання експериментальних результатів для синтезування аналітичної моделі. Необхідність створення аналітичної моделі обґрунтовується тим, що для імітаційного моделювання на топології існуючих ІТКМ (десятки мільйонів вузлів) необхідні великі витрати часу. Не враховуючи час на збір інформації про топології мережі, який може становити близько тижня, безпосередньо моделювання загрози поширення забороненої інформації (ЗПЗІ) займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз загрозі поширення забороненої інформації майже миттєво. З її допомогою можна отримати актуальні дані (до того моменту, коли кількість атакуючих абонентів буде максимальним) за динамікою ЗПЗІ.

Процес ЗПЗІ характеризується наступними особливостями. У мережі існують вузли трьох типів. Перший тип – атакуючі вузли, це вузли, які розповсюджують заборонену інформацію. Другий тип – захищені вузли, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися. Третій тип – потенційно вразливі. Вузли такого типу не беруть участі в процесі поширення загрози, але можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію.

Аналітична модель динаміки атаки $I(t)$ та модель ахисту вузлів $R(t)$ представлені наступним чином (1):

$$\begin{cases} I(t) = f(N, \beta, \gamma, \varphi, t) \\ R(t) = g(N, \beta, \gamma, \varphi, t) \end{cases} \quad (1)$$

де, N – кількість вузлів, яка дорівнює кількості абонентів мережі, β – параметр, що відображає силу загрози, ймовірність здійснення атаки, γ – параметр, що відображає ступінь протидії загрозі, ймовірність захисту абонента (β і γ в даному дослідженні визначено як константи, але можуть бути виражені як функції, що залежать від психосемантичних профілів абонентів ІТКМ), φ – коефіцієнт топологічної вразливості мережі, що відображає внутрішню властивість ІТКМ, засновану на характеристиках її топології, яке сприяє поширенню забороненої інформації , t – час процесу (в умовних одиницях часу).

Розробка аналітичної моделі включає в себе послідовність наступних дій:

- формування імітаційної моделі для дослідження характеру і параметрів процесу ЗПЗІ;
- синтез аналітичних залежностей параметрів процесу;
- проведення експериментів з метою перевірки точності (адекватності) моделі.

Наведемо алгоритм реалізації ЗПЗІ, грунтуючись на описі процесів, що відбуваються в реальних ІТКМ. Схема реалізації загрози зображена на рис. 2.

Алгоритм загрози поширення забороненої інформації в ІТКМ

1. Поширення забороненої інформації (ЗІ) (далі процес «атаки») ініціює будь-який абонент-зловмисник (на рис. 2 – вузол 1), поширюючи повідомлення з ЗІ (реалізує загрозу) за його списком контактів. Атаку може починати один зловмисник або група.

2. Абоненти-одержувачі (вузли 2, 3, 4), прийнявши повідомлення з ЗІ, читають його і включаються в процес атаки, поширюючи її далі по своєму списку контактів (вузол 3), або ігнорують або взагалі видаляють повідомлення (вузол 2) , тобто в атаці не беруть участь. Процес атаки зазвичай йде лавиноподібно. Атакуючі абоненти не закінчують атаку, одного разу передавши повідомлення із забороненою інформацією. Вікно атаки, як правило, триває протягом досить значного проміжку часу і залежить від типу подачі ЗІ в повідомленні, зацікавленості абонента тощо.

3. Абоненти можуть перестати сприймати і, відповідно, поширювати ЗІ (вузол 5) (далі процес «захисту»), внаслідок впливу механізмів захисту (наприклад, попередження про неї), тому повідомлення з ЗІ від атакуючих абонентів будуть постійно відхилятися.

4. Процес триває поки в мережі є абоненти-зловмисники, або є потенційно вразливі вузли, якщо відсутній процес захисту.

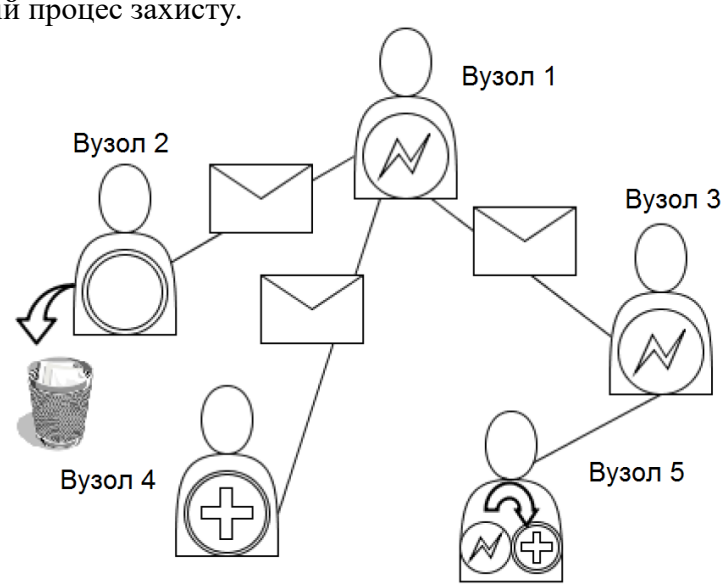


Рисунок 2 – Схема реалізації загрози поширення забороненої інформації в ІТКМ

Таким чином, ЗПЗІ в ІТКМ є складним динамічним процесом, що складається з двох протидіючих підпроцесів атаки і захисту вузлів мережі.

На основі описаного алгоритму побудована імітаційна модель ЗПЗІ в ІТКМ:

Вхідні дані: N, k – середній ступінь зв'язності вузлів, a – параметр, що відображає середню довжину шляху і рівень мережевої кластеризації, β, γ (в моделі вважається, що β та γ однакові для кожного абонента), I_0 - кількість абонентів-зловмисників - початкових джерел загроз, R_0 - кількість абонентів спочатку несприйнятливих до атакуючих дій.

Вихідні дані: $I(t), R(t), S(t)$ – чисельні масиви даних, що описують динамічний процес реалізації ЗПЗІ (кількості атакуючих, захищених і потенційно вразливих вузлів у кожну умовну одиницю часу відповідно).

1. Створення топології ІТКМ – графа $G_{SW} = \langle V, E \rangle$, де G_{SW} – граф small-world мережі (на основі моделі Watts-Strogatz), $V = \{v_i\}$ – множина вершин, $E = \{e_{ij}\}$ – множина ребер, $i = \overline{1, N}$, $j = \overline{1, N}$. Даний крок здійснюється з використанням програми Pajek, адаптованої під цю задачу, за рахунок заданих топологічних параметрів *N, k, a*.

2. Сформувати множину $V = \{V^I, V^S, V^R\}$, де $V^I = \{v_i^I\}$ – множина атакуючих вузлів $\left(\left|V^I\right| = I_0\right)$, $V^R = \{v_i^R\}$ – множина захищених вузлів $\left(\left|V^R\right| = R_0\right)$, $V^S = \{v_i^S\}$ – множина потенційно вразливих вузлів $\left(\left|V^S\right| = N - I_0 - R_0\right)$.

3. $\forall v_i^I$, якщо $\exists e_{ij}$ та $v_j \in V^S$, $j = \overline{1,N}$, то з ймовірністю β виконати: $V^S \setminus v_j$ та $V^I \bigcup v_j$; з ймовірністю γ виконати: $V^I \setminus v_i, V^R \bigcup v_i$.

4. Якщо $V^I = \varnothing$ або $\gamma = 0$ та $V^S = \varnothing$, то кінець алгоритму, інакше перейти до п. 3.

Аналізуючи процес інформаційної взаємодії абонентів при поширенні забороненої інформації в ІТКМ, можна зробити наступні висновки. Маємо справу з трьома типами абонентів: атакуючі абоненти, які поширюють заборонену інформацію, захищені абоненти, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися, і потенційно вразливі абоненти, які можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію. При цьому ми спостерігаємо два протиборчих підпроцеси атаки і захисту абонентів мережі. Для моделювання таких явищ часто застосовують епідеміологічні моделі , зокрема нашому опису відповідає SIR-модель Кермак-Маккендріка. Характер графіків, отриманих у результаті імітаційного моделювання (рис. 3), подібний з результатами, що дає дана модель. Виходячи з вищесказаного, приходимо до висновку, що дана модель є найбільш релевантною для цього дослідження

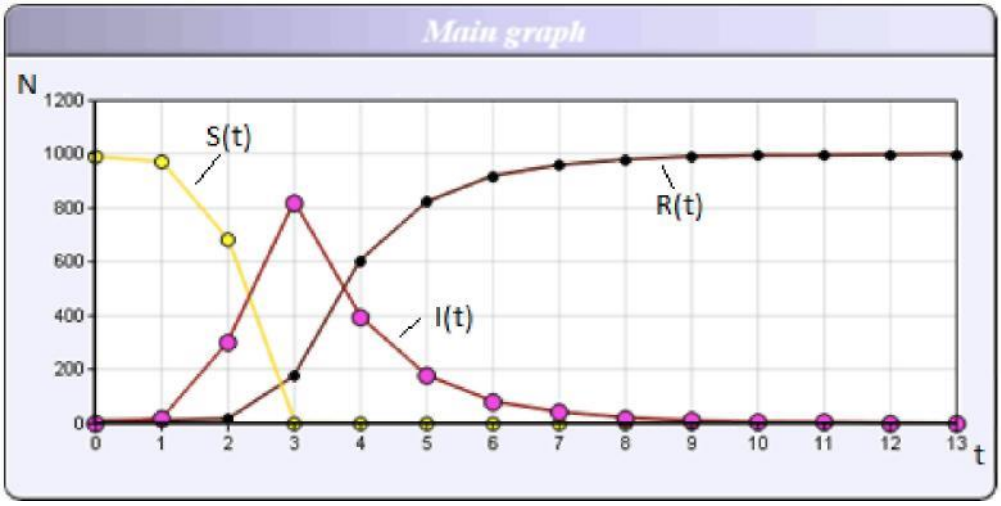


Рисунок 3 – Імітаційне моделювання
($N = 1000$, $\varphi = 20$, $I_0 = 1$, $\beta = 0.5$, $\gamma = 0.5$, $R_0 = 10$), $S(t)$ – кількість схильних до атаки вузлів

SIR–епідеміологічна модель, що спрощено описує поширення захворювання, які передаються від одного індивіда до іншого, яка розглядає суб'єктів з точки зору трьох можливих станів: сприйнятливий, інфікований, імунізований.

Система диференціальних рівнянь, що описують SIR-модель, має вигляд:

$$\begin{cases} \dfrac{\partial I}{\partial t} = \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -\beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (2)$$

де, $I(t)$ – кількість заражених (інфікованих) особин, $S(t)$ – кількість сприятливих особин, $R(t)$ – кількість «виключених з імунізацією» особин, $N = I(t) + S(t) + R(t)$ – кількість особин у популяції, γ – коефіцієнт відновлення / смерті, β – коефіцієнт зараження (інфікування), t – час.

При використанні системи (2) для аналізу ЗПЗІ в ІТКМ отримуємо результати, які хоча і адекватно описують характер процесу, але не дають потрібної точності прогнозу.

На основі проведенго аналізу даних, отриманих за результатами імітаційного моделювання та аналітичного рішення системи (2), і простеживши фізичний зміст рівнянь в даній системі, можна прийти до наступного висновку: процес атаки залежить від структури зв'язків між абонентами в мережі. Параметр топологічної вразливості φ може впливати на $I(t)$ через коефіцієнт β. У загальному вигляді адаптовану систему (2) можна представити в наступному вигляді

$$\begin{cases} \dfrac{\partial I}{\partial t} = 2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (3)$$

Система диференціальних рівнянь (3) дозволяє отримати прогноз ЗПЗІ у великомасштабної ІТКМ ($N = 10^5..10^8$) з похибкою до 18%.

Висновки. Інформаційно-телекомунікаційні мережі є великомасштабними мережами з постійно зростаючим числом абонентів. З бурхливим зростанням кількості користувачів ІТКМ виникають проблеми інформаційної безпеки і захисту інформації в них.

Аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту.

Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даної задачі. Проведений аналіз публікацій з даної тематики показує, що існуючі рішення малоефективні. Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відбивається SF мережею. При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Розроблено алгоритм реалізації ЗПЗІ в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Запропонована імітаційна модель ЗПЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

ЛІТЕРАТУРА:

1. Кримінальний кодекс України від 05.04.2001 № 2341-III. Дата оновлення: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (дата звернення: 02.09.2020).

2. Про інформацію: Закон України від 02.10.1992 №2657-XII. Дата оновлення: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (дата звернення: 02.09.2020).

3. Про науково-технічну інформацію: Закон України від 25.06.1993 № 3322-XII. Дата оновлення: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (дата звернення: 02.09.2020).

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.09.2020).

5. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.09.2020).

6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 02.09.2020).

7. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Дата оновлення: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 02.09.2020).

8. Концепція розвитку системи електронних послуг в Україні. Розпорядження Кабінету Міністрів України від 16.11.2016 р. № 918-р. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (дата звернення: 02.09.2020).

9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 02.09.2020).

10. Аналізатор Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (дата звернення: 02.09.2020).

11. Аналіз та візуалізація дуже великих мереж. URL: http://mrvar.fdv.uni-lj.si/pajek/ (дата звернення: 02.09.2020).

12. Биячуев, Т.А. Безопасность корпоративных сетей: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2016. – 161 с.

13. Брэгг, Р., Родс-Оусли, М., Страссберг, К. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг; – М : Эком, 2006. – 912 с.

14. Завдада А.А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А.А. Завада, О.В. Самчишин, В.В. Охрімчук // Збірник наукових праць ЖВІ НАУ «Інформаційні системи'12», 2012. – Випуск 6. – С. 97 – 106.

15. Загальні рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи. URL:

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (дата звернення: 02.09.2020).

16. Kolotov, A. Мониторинг сети с помощью tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (дата звернення: 02.09.2020).

17. Лукацький, А.В. Предотвращение сетевых атак: технологии и решения / А.В. Лукацкий. – СПб. : Экспрес Электроника, 2006. – 268 с.

18. Столлингс, В. Основы защиты сетей. Приложения и стандарты / В. Столлингс. – М.: Издательский дом "Вильямс", 2002. – 432 с.

19. Тропіна М. Дослідження соціальних мереж як нового феномену сучасного світу / М. Тропіна // Наукові записки Малої академії наук України. Серія «Педагогічні науки» : [зб. наук. праць; редкол. : С.О. Довгий (голова), О.Є. Стрижак, О.В. Лісовий, І.М. Савченко та ін.]. – Київ : Національний центр «Мала академія наук України», 2019. – Вип. 16. – С. 57-63 (76 с.)

REFERENCES:

1. Kryminal′nyy kodeks Ukrayiny vid [The Crimean Code of Ukraine from] 05.04.2001 № 2341-III. Data onovlennya: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (data zvernennya: 02.09.2020).

2. Pro informatsiyu : Zakon Ukrayiny vid [About information : Law of Ukraine from] 02.10.1992 №2657-XII. Data onovlennya: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (data zvernennya: 02.09.2020).

3. Pro naukovo-tekhnichnu informatsiyu : Zakon Ukrayiny vid [About scientific and technical information : Law of Ukraine from] 25.06.1993 № 3322-XII. Data onovlennya: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (data zvernennya: 02.09.2020).

4. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh : Zakon Ukrayiny vid [On information protection in information and telecommunication systems : Law of Ukraine from] 05.07.1994 № 80/94-VR. Data onovlennya: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (data zvernennya: 02.09.2020).

5. Pro elektronni dovirchi posluhy : Zakon Ukrayiny vid [About electronic trust services : Law of Ukraine from] 05.10.2017 № 2155-VIII. Data onovlennya: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (data zvernennya: 02.09.2020).
6. Pro zakhyst personal′nykh danykh : Zakon Ukrayiny vid [On personal data protection : Law of Ukraine from] 01.06.2010 № 2297-VI. Data onovlennya: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (data zvernennya: 02.09.2020).
7. Pro dostup do publichnoyi informatsiyi : Zakon Ukrayiny vid [On access to public information : Law of Ukraine from 13.01.2011] 13.01.2011 № 2939-VI. Data onovlennya: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (data zvernennya: 02.09.2020).
8. Kontseptsiya rozvytku systemy elektronnykh posluh v Ukrayini. Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid [The concept of development of the electronic services system in Ukraine. Order of the Cabinet of Ministers of Ukraine from] 16.11.2016 p. № 918-p. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (data zvernennya: 02.09.2020).
9. Pro zatverdzhennya Zahal′nykh vymoh do kiberzakhystu ob″yektiv krytychnoyi infrastruktury. Postanova Kabinetu Ministriv Ukrayiny vid [On approval of the General requirements for cyber protection of critical infrastructure. Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019] 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (data zvernennya: 02.09.2020).
10. Analizator Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (data zvernennya: ата звернення: 02.09.2020).
11. Analysis and visualization of very large networks. URL: http://mrvar.fdv.uni-lj.si/pajek/ (data zvernennya: ата звернення: 02.09.2020).
12. Biyachuyev, T.A. (2016), “Bezopasnost' korporativnykh setey” [Security of corporate networks] : ucheb. posobiye / T.A. Biyachuyev; pod red. Osovetskogo L.G. – SPb.: SPbGU ITMO, 161 p.
13. Bregg, R., Rods-Ousli, M., Strassberg, K. (2006) “Bezopasnost' setey. Polnoye rukovodstvo” [Network Security. Complete Guide] / R. Bregg, M. Rods-Ousli, K. Strassberg; – M : Ekom, 912 p.
14. Zavdada A.A. “Analiz suchasnykh system vyyavlennya atak i zapobihannya vtorhnennyam” [Analysis of of modern detection of attacks and prevention of invasions of systems] / A.A. Zavada, O.V. Samchyshyn, V.V. Okhrimchuk // Zbirnyk naukovykh prats′ ZHVI NAU «Informatsiyni systemy″12», 2012. – Vypusk 6, pp. 97 – 106.
15. Zahal′ni rekomendatsiyi shchodo pidvyshchennya rivnya zakhyshchenosti informatsiynykh resursiv pry viddaleniy roboti spivrobitnykiv ustanovy [General recommendations for improving the level of security of information resources in the remote work of employees of the institution] URL:
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (date of application: 02.09.2020).
16. Kolotov, A. Network monitoring with tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (date of application: 02.09.2020).
17. Lukats'kiy, A.V. (2006), “Predotvrashcheniye setevykh atak: tekhnologii i resheniya” [Prevention of network attacks: technologies and solutions] / A.V. Lukatskiy. – SPb. : Ekspres Elektronika, p. 268.
18. Stollings, V. (2002), “Osnovy zashchity setey. Prilozheniya i standarty” [Fundamentals of Network Security. Applications and standards] / V. Stollings. – M.: Izdatel'skiy dom "Vil'yams", p.432.
19. Tropina M. Doslidzhennya sotsial′nykh merezh yak novoho fenomenu suchasnoho svitu [Research of social networks as a new phenomenon of the modern world] / M. Tropina // Naukovi zapysky Maloyi akademiyi nauk Ukrayiny. Seriya «Pedahohichni nauky» : [zb. nauk. prats′ ; redkol. : S.O. Dovhyy (holova), O.YE. Stryzhak, O.V. Lisovyy, I.M. Savchenko ta in.]. – Kyiv: Natsional′nyy tsentr «Mala akademiya nauk Ukrayiny», 2019. — Vyp. 16. – Pp. 57-63 (p. 76)

D.Sc. Lienkov S.V., Ph.D. Dzhulij V.M., D.Sc. Sieliykov O.V.,
Ph.D. Orlenko V.S., Atamaniuk A.V.

SECURITY MODEL DISSEMINATION OF FORBIDDEN INFORMATION IN INFORMATION AND TELECOMMUNICATION NETWORKS

The article proposes an approach to defining a security model for the dissemination of prohibited information in information and telecommunication networks.

The most effective prediction of the spread of the prohibited information threat is carried out by modeling this process. Information and telecommunication networks are large-scale networks with an ever-

growing number of subscribers. With the rapid growth in the number of ITKS users, there are problems of information security and information protection in them.

The analysis of information security problems proved that apart from the problems associated with the use of the global Internet as a distributed information and telecommunication system, it is well known and can be solved, there is a poorly studied problem of prohibited content.

Creation of models and algorithms for the spread of the threat of prohibited information is one of the key approaches to solving this problem. The analysis of publications on this topic shows that existing solutions are ineffective. Usually, when modeling the propagation of a threat of prohibited information, the ITKS topology (the network model is a fully connected graph) is not taken into account. When modeling the threat of the spread of prohibited information, it is important to have a topology that reflects the structure of connections in a real network, as well as to use an adequate model of information interaction between nodes. Another important problem is the large-scale ITCS, which makes it difficult to obtain data from the simulation model in a reasonable time. The solution to this problem is to create an analytical model of the threat of the spread of prohibited information in the ITCS.

An algorithm has been developed for the implementation of TSPI (threat of the spread of prohibited information) in the ITKS, based on the nature of the processes occurring in real conditions.

The simulation model of TSPI in ITKS has been proposed, which takes into account the topological characteristics of the network, as well as the features of information interaction of subscribers as man-machine systems. With its help, experiments have been carried out, the results of which have shown the dependence of the implementation of the RFID on the topological vulnerability of the network.

An analytical model of the TSPI has been developed, taking into account the topological vulnerability of the network. The relevance of the results of the analytical solution was confirmed by a series of experiments on the topology of a real network using simulation modeling. In this case, the error for the protection process was no more than 10%, for the attack process - no more than 15%.

Keywords: information security, analytical model, simulation model, threat propagation, information interaction, network model.

УДК 004.94

Петрівський В.Я. (КНУ)
д.т.н., проф. **Шевченко В.Л.** (КНУ)
д.т.н., доц. **Бичков О.С.** (КНУ)
к.т.н. **Лоза В.М.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-07

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПОКРИТТЯ ТЕРИТОРІЇ ДАТЧИКАМИ ІЗ ЗАДАНИМ РІВНЕМ ПЕРЕТИНУ ТА МІНІМІЗАЦІЄЮ ВИТРАТ

Завдяки стрімкому розвитку технологій, зокрема інформаційних, сенсори набули широкого розповсюдження та застосування у всіх галузях людської діяльності. Особливого використання сенсори та сенсорні мережі набули під час виконання збору та обробки даних різного типу. При проведенні моніторингу певної території виникає проблема максимального її покриття для збільшення інформативності та повноти накопичених даних. Одночасно з перевагою автономного використання датчиків виникає проблема тривалості роботи датчику. Дана величина залежить від ємності акумулятора. В свою чергу перед інженерами стоїть задача мінімізації конструкції датчиків, наслідком чого є зменшення об'єму акумулятора одночасно із всіма іншими компонентами. Також очевидним є факт того, що при збільшенні радіусу охоплення сенсору збільшуються енерговитрати, що в свою чергу скорочує термін використання сенсору. Крім енерговитрат, у статті до розгляду беруться витрати на обслуговування та придбання датчиків. Таким чином, крім максимізації відсотку покриття досліджуваної території виникає проблема мінімізації сумарних витрат. Очевидно, що для забезпечення передачі даних між датчиками необхідною умовою є наявність перетину зон покриття сенсорів. У даному випадку розглядається константне значення даного параметру. У матеріалах запропоновано підхід вирішення проблеми максимізації покриття території з мінімізацією витрат із заданим рівнем перетину зон покриття датчиків. Запропонований підхід ґрунтується на розв'язанні багатокритеріальної задачі нелінійного програмування. Також одним із варіантів вирішення описаної проблеми запропоновано зведення цільових функцій до однієї шляхом використання зваженої згортки критеріїв. Крім того у статті запропоновано ітераційний підхід вирішення описаної проблеми. Проведено ряд комп'ютерних експериментів. Результати проведених обчислювальних експериментів підтверджують можливість використання запропонованої інформаційної технології як у вигляді оптимізаційної проблеми так і у вигляді ітераційного процесу.

Ключові слова: датчик, покриття території, інформаційна технологія, багатокритеріальна оптимізація, нелінійна оптимізація.

Вступ. Завдяки широкому спектру застосування сенсори та сенсорні мережі набули широкого розповсюдження. Серед основних переваг сенсорів можна виділити можливість автономної роботи у поєднанні із варіативністю досліджуваної величини. Дані переваги дозволяють широко застосовувати сенсори та сенсорні мережі для виконання задач збору та обробки інформації. Під час здійснення моніторингу ключовим аспектом є максимальне покриття досліджуваної території. Автономність роботи датчиків залежить від обєму акумулятора. Таким чином виникає проблема збільшення терміну використання сенсорів. Для передачі даних необхідною умовою є наявність перетину зон покриття елементів сенсорної мережі. Таким чином, розглядається задача максимального покриття території датчиками із заданим рівнем перетину та мінімізацією витрат.

Метою статті є створення інформаційної технології вирішення задачі максимального покриття території сенсорами із заданим рівнем перетину та мінімізацією енерговитрат.

Аналіз останніх досліджень та публікацій. У наш час датчики набули значного застосування завдяки ряду переваг: розмір, автономність, доступність, мобільність [1, 2]. Також датчики використовують для виконання ряду певних задач, що пов'язані із збором та обробкою інформації [3], серед яких поширеною є задача моніторингу, тобто задача оптимального покриття території заданим числом датчиків з відповідними характеристиками [4]. У роботі [5] представлено розгляд технології екологічного моніторингу, а також

вирішення задачі розміщення сенсорів в багатокутній зоні спостереження з наявністю перешкод. Також у роботі наведено порівняльний аналіз використаних евристик SC, BC та HC. У працях [6, 7] описано алгоритми та методи розв'язання задачі моніторингу та оптимального розташування сенсорів. Алгоритм оптимального розташування сенсорів для визначення структурних пошкоджень різних видів техніки представлено у [8]. У [7, 9] представлено оптимальну стратегію розміщення датчиків для моніторингу навколишнього середовища за допомогою бездротових сенсорних мереж. Оптимізація розміщення датчиків з використанням градієнтного спуску та імовірнісного покриття представлена у роботі [10]. В свою чергу, у праці [11] представлено підхід зменшення енерговитрат сенсорної мережі шляхом регуляції зон покриття датчиків.

Виклад основного матеріалу. Розглянемо двовимірну прямокутну територію з розмірами a та b, позначимо її A. Нехай дано датчики, що мають однакову величину вимірювання та змінний радіус покриття r з максимальним значенням r^{max}. Під зоною покриття сенсору будемо вважати коло з центром у певній точці зони A з координатами (x, y) та радіусом r. Враховуючи, що коло з радіусом r можна вписати у квадрат зі стороною $2r$, задачу покриття прямокутної області A розглянемо як задачу квадратної однорідної упаковки [12], що схематично може бути представлена наступним чином (рис. 1):

Рисунок 1 – Покриття території датчиками без перетину зон покриття

Очевидно, що під час вимірювання, можливою є ситуація наявності зон перетину покриття сенсорів, позначимо дану величину c [11]. Схематично дану величину можна зобразити наступним чином (рис. 2).

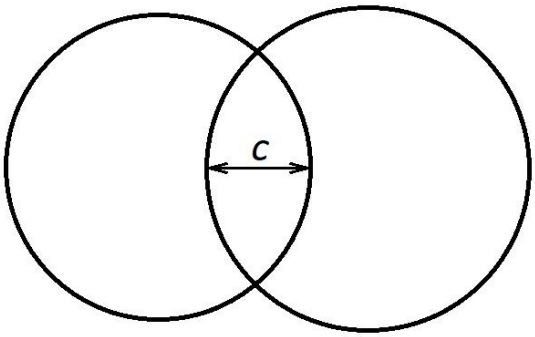


Рисунок 2 – Значення величини c

З урахуванням величини перетину зон покриття датчиків та еквівалентності радіусів покриття територію, що представлена на рис. 1 можна покрити наступним чином (рис. 3):

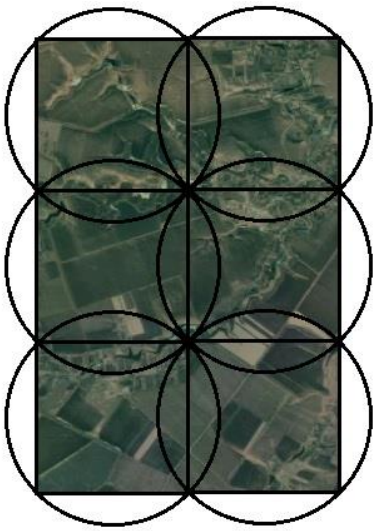


Рисунок 3 – Покриття території з урахуванням зон перетину

У описаному вище випадку досягається повне покриття території. Візьмемо до розгляду енерговитрати сенсору, що впливають на термін його використання та на період активного покриття території. Розглянемо обчислення витрат згідно з [11]:

$$Bc_i = \frac{r_i}{r_i^{max}} Bc_i^{max}, \tag{1}$$

де r_i – поточний радіус охоплення датчику, r_i^{max}– максимальний радіус охоплення датчику, Bc_i^{max}– витрати енергії при максимальному радіусу охоплення.

Очевидно, що при максимальному покритті термін використання сенсору є мінімальним. Враховуючи даний факт та наявність перетину зон покриття сформулюємо задачу максимального покриття території датчиками із заданим рівнем перетину та мінімізацією витрат у наступному вигляді:

$$\begin{matrix} Z(r,c) \to max \\ E(r,c) \to min' \end{matrix} \tag{2}$$

де $E(r,c) = nBc$, $n = \left[\frac{ab}{(2r-c)^2}\right]$, Bc – енерговитрати сенсору (1), r – радіус покриття сенсору, c – величина зони перетину датчиків, a та b – розміри зони.

У рівнянні (2) величина зони покриття $Z(r,c)$ обчислюється як різниця між загальною покритою територією та площею перетинів зон покриття сенсорів у наступному вигляді:

$$Z(r,c) = Z_{covered}(r,c) - Z_{intersected}(r,c). \tag{3}$$

Враховуючи припущення, що зоною покриття датчику є коло з центром у певній точці (x,y) та радіусом r, величина $Z_{covered}(r,c)$ буде рівною:

$$Z_{covered}(r,c) = N(r,c)\pi r^2, \tag{4}$$

де $N(r,c) = \left[\frac{ab}{(2r-c)^2}\right]$, a, b – розмір зони.

Значення площі перетину зон покриття сенсорів обчислимо використовуючи [13] з урахування рівності радіусів у наступному вигляді:

$$Z_{intersected}(r,c) = m\frac{r}{2}(K(r,c) - \sin(K(r,c))), \tag{5}$$

де $K(r,c) = 2\arcsin\left(\frac{\sqrt{r^2-(r-\frac{c}{2})^2}}{r}\right)$, m – кількість перетинів.

Будемо вважати, що зона покриття кожного сенсору перетинається або виходить за межі зони з 4 сторін, тобто $m = 4n$.

Очевидно, площа покрита сенсорами не повинна перевищувати площі досліджуваної зони. Для виконання даної умови перетворимо функцію (3) у наступному вигляді:

$$Z(r,c) = ab - Z_{covered}(r,c) + Z_{intersected}(r,c). \quad (6)$$

Згідно з перетворенням (6), функція (2) набуде наступного вигляду:

$$\begin{matrix} Z(r,c) \to min \\ E(r,c) \to min \end{matrix}. \quad (7)$$

Будемо вимагати виконання наступних обмежень:

$$0 \le r \le r^{max}, \quad (8)$$

$$0 \le c \le r^{max}. \quad (9)$$

Отримана задача (7)-(9) є багатокритеріальною задачею нелінійного програмування.

Використавши метод згортки критеріїв [14] отримаємо задачу нелінійного програмування у наступному вигляді:

$$F(r,c) = \alpha_1 Z(r,c) + \alpha_2 E(r,c) \to min, \quad (10)$$

$$0 \le r \le r^{max}, \quad (11)$$

$$0 \le \alpha_1 \le 1, 0 \le \alpha_2 \le 1, \quad (12)$$

$$0 \le c \le r^{max}. \quad (13)$$

Розв’язком задачі (10)-(13) є певне значення радіусу покриття сенсору r^* за якого досягається максимізація покриття з заданим рівнем перетину зон покриття датчиків c при мінімізації енерговитрат. Положення сенсорів будуть рівновіддаленими один від одного на величину $2r^*$.

У випадку зони довільної форми запропонований підхід можна застосувати за умови доповнення зони до прямокутної (рис. 4).

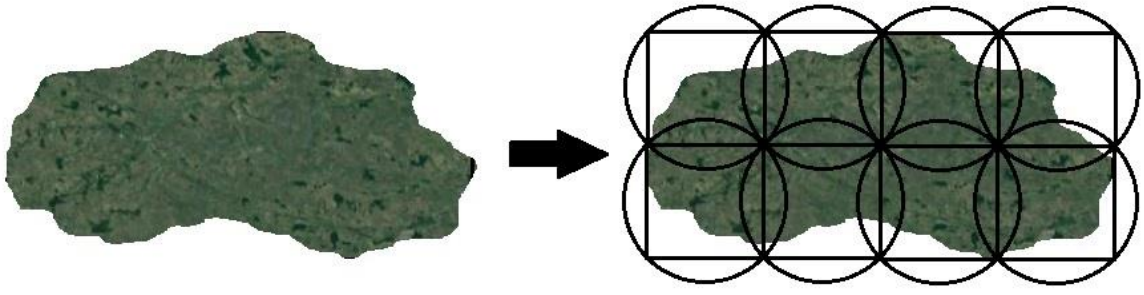


Рисунок 4 – Отримання прямокутної зони

Після отримання розв'язку задачі (10) – (13) необхідно відкинути сенсори покриття яких знаходиться за межами зони або зона покриття сенсору покриває зону менше ніж на β%.

Також для розв’язання описаної вище проблеми запропонуємо ітераційний підхід, що може бути описаний наступними кроками:

1. Формуємо за необхідності прямокутну зону;

2. Заповнюємо отриману зону сенсорами з радіусами покриття $r = r^{max}$;

3. Відкидаємо сенсори, що покривають зону менше ніж на β%.

4. Обчислюємо значення $Z_i(r_i, c)$, $E_i(r_i, c)$ для кроку i.

5. Перевіряємо умову $r_i \leq r_{min}$ та у разі невиконання зменшуємо значення радіусу на величину Δr та переходимо до кроку 3;

6. Серед отриманих значень покриття та витрат обираємо оптимальні за Парето.

Результати обчислювальних експериментів. У даному розділі представлені результати комп'ютерного моделювання з використанням відомих та запропонованого підходів при розв'язанні описаної проблеми. Нехай необхідно знайти оптимальне співвідношення між радіусом покриття та величиною зони перетину при покритті заданої території (рис. 5). Після використання запропонованого підходу отримали зону з розмірами 200x100 умовних одиниць. Відомо, що радіус покриття сенсорів $r^{max} = 10$ умовних одиниць. Розв'язавши задачу у вигляді (7)-(9) або у вигляді (10)-(12) із урахуванням даних параметрів отримаємо множину Парето-оптимальних рішень. Розв'язок можна зобразити наступним чином (рис. 6).

Рисунок 5 – Зона для покриття

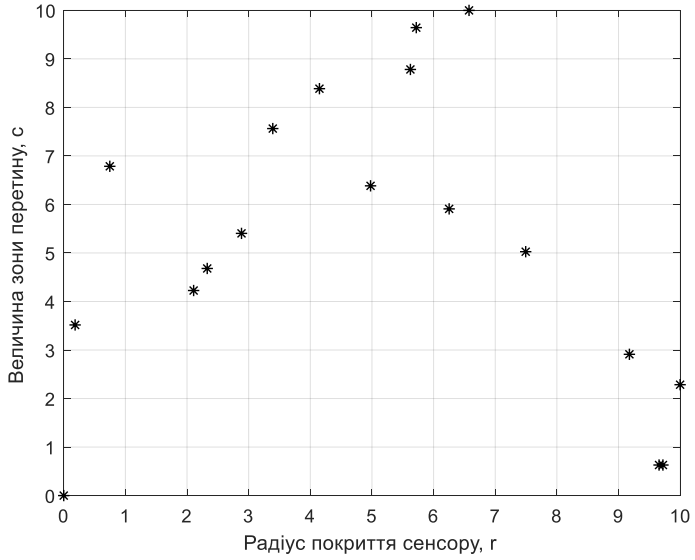


Рисунок 6 – Множина оптимальних співвідношень радіусу покриття та величини зони перетину

Розглянемо задачу оптимального покриття території (рис. 7) датчиками з сталим рівнем перетину зон покриття $c = 3$ та параметрами $r^{max} = 15$, $Bc^{max} = 10000$. Використавши описаний вище підхід отримаємо наступне значення радіусу при розв'язанні задачі у формі (7)-(9) $r^* = 7.048$. Під час розв'язання задачі у вигляді (10)-(13) при значеннях $\alpha_1 = \alpha_2 = 1$ оптимальне значення радіусу буде рівним $r^* = 7.065$. Результатом використання

запропонованого ітераційного алгоритму є значення $r^* = 7$. Відповідно до отриманих результатів розташування сенсорів схематично можна зобразити наступним чином (рис. 7):

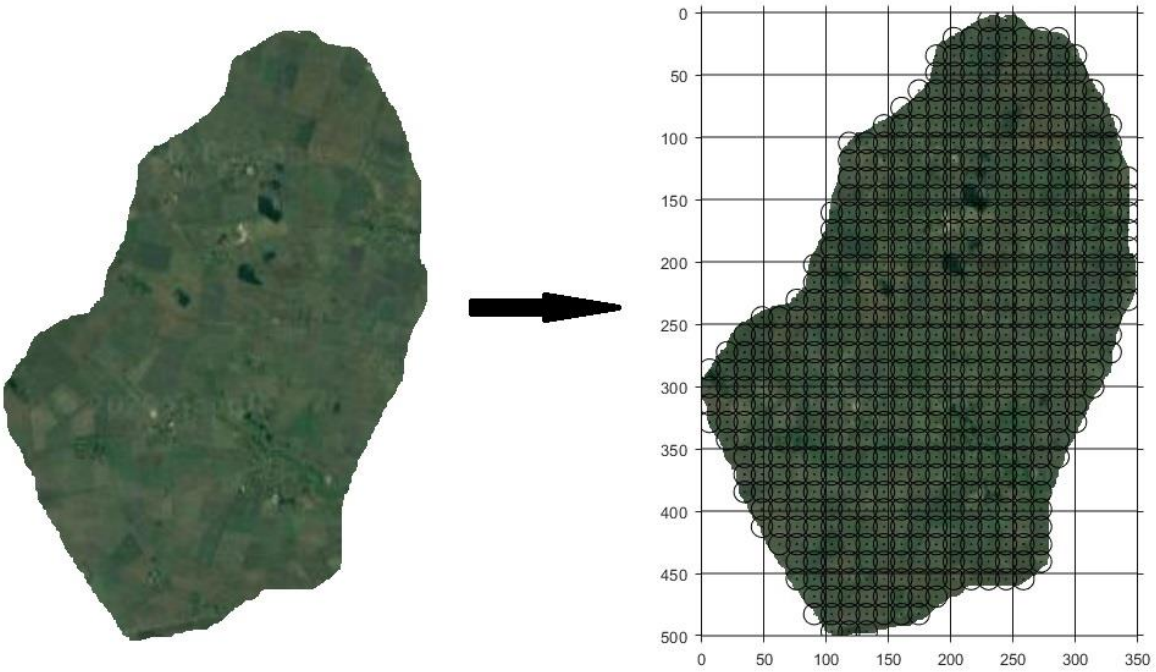


Рисунок 7 – Покриття обраної зони з допустимим рівнем перетину $c = 3$

Висновки. У статті представлено підхід вирішення задачі максимізації покриття території сенсорами із заданим рівнем перетину зон покриття та мінімізацією витрат. Під витратами мається на увазі енерговитрати, що можуть бути поєднані із витратами на обслуговування датчиків. Величина перетину зон покриття розглядалася як стала величина для всіх сенсорів. Представлена задача описана як багатокритеріальна задача нелінійного програмування. Одним із запропонованих підходів вирішення поставленої задачі є використання методу згортки цільових функцій. Також запропоновано ітераційний алгоритм розвязання описаної проблеми. Представлені результати обчислювальних експериментів підтверджують доцільність використання запропонованих підходів.

ЛІТЕРАТУРА:

1. Pandey, M., Mishra, G. Types of Sensor and Their Applications, Advantages, and Disadvantages. / Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing. 2019 № 814. Springer, Singapore. Pp. 791-804.

2. Michalaki, P., Quddus, M., Pitfield, D., Mageean, M., Huetson, A. A Sensor-based System for Monitoring Hard-shoulder Incursions: Review of Technologies and Selection Criteria / MATEC Web of Conferences. 2016. № 81. C. 1-8.

3. Argyriou, A. Data Collection from Resource-Limited Wireless Sensors for Cloud-Based Applications. / GLOBECOM 2015 - 2015 IEEE Global Communications Conference. 2014.

4. Геоматика в моніторингу довкілля та оцінці загрозливих ситуацій : монографія / [О. Л. Дорожинський та ін.] ; за ред. проф. Олександра Дорожинського ; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2016. - 399 с. : рис. - ISBN 978-617-607-923-1.

5. Данилюк С. Л. Концептуальні підходи до вирішення задачі оптимального розміщення сенсорів в області екологічного моніторингу / С. Л. Данилюк. // Сучасні інформаційнітехнології у сфері безпекита оборони. 2016. №26. С. 45–48.

6. Кочкаров, А.А., Яцкин, Д.В. Алгоритм поиска оптимального расположения сенсоров для решения задачи мониторинга пространства // Программные продукты и системы. 2016. №3 (115).

7. Krishnamurthy, P., Khorrami, F. Optimal Sensor Placement for Monitoring of Spatial Networks / IEEE Transactions on Automation Science and Engineering. 2017. № 1(15). С. 33-44.

8. Li, C.H., Yang, Q.W. Optimal Sensor Placement Algorithm for Structural Damage Identification / Recent Patents on Engineering. 2020. № 14(69). Pp. 69-81.

9. Castello, C., Fan, J., Davari, A., Chen, R-X. Optimal sensor placement strategy for environmental monitoring using Wireless Sensor Networks / Proceedings of the Annual Southeastern Symposium on System Theory. 2010. Pp. 275 - 279.

10. Akbarzadeh, V., Lévesque, J., Gagne, C., Parize, M. Efficient sensor placement optimization using gradient descent and probabilistic coverage [Електронний ресурс] Sensors (Basel), 2014. № 8(14). Режим доступу до журн.:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4179027/.

11. Петрівський, В.Я., Шевченко, В.Л., Бражиненко, М.Г. Збільшення часу роботи датчиків шляхом регулювання енерговитрат / Системи обробки інформації. 2019. № 3(158). С. 36-41.

12. Stoyan, Y.G., Yaskov, G.N. Packing identical spheres into a cylinder / International Transactions in Operational Research. 2010. № 17. С. 51–70.

13. Petrivskyi, V., Shevchenko, V., Bychkov, O., Brazhenenko, M. Information technology of the increasing sensors term of use considering their movement / 2020 IEEE 16-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). 2020. Pp.86-89.

14. Wesner, N. Multiobjective Optimization via Visualization / Economics Bulletin, 2017. № 2(37). Pp. 1226–1233.

REFERENCES:

1. Pandey, M., Mishra, G. (2019), “Types of Sensor and Their Applications, Advantages, and Disadvantages”, Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing, No. 814. Springer, Singapore. pp. 791-804.

2. Michalaki, P., Quddus, M., Pitfield, D., Mageean, M., Huetson, A. (2016), “A Sensor-based System for Monitoring Hard-shoulder Incursions: Review of Technologies and Selection Criteria”, MATEC Web of Conferences. No. 81. pp. 1-8.

3. Argyriou, A. (2015), “Data Collection from Resource-Limited Wireless Sensors for Cloud-Based Applications”, GLOBECOM 2015 - 2015 IEEE Global Communications Conference.

4. Dorozhynskyi, O.L. (2016), “Geomantyka v monitoryngu dovkillya ta ocinci zagrozlyvyh ssytuacii: monografiia” [Geomatics in environmental monitoring and threat assessment], Lviv, 399 p.

5. Danyliuk, S.L. (2016), “Konceptyalni pidhody do vyrishennya zadachi optymalnogo rozmishchennya sensoriv v oblasti ekologichnogo monitoryngu” [Conceptual approaches to solving the problem of optimal placement of sensors in the field of environmental monitoring], Modern information technologies in the field of security and defense, No. 26, pp. 45–48.

6. Kocharov, A.A., Yackin, D.V. (2016) “Algoritm poiska optimalnogo razpolozeniya sensorov dla resheniya zadachi monitoringa prostranstva” [Algorithm for finding the optimal location of sensors for solving the problem of monitoring space], Software products and systems, No. 3(115).

7. Krishnamurthy, P., Khorrami, F. (2017), “Optimal Sensor Placement for Monitoring of Spatial Networks”, IEEE Transactions on Automation Science and Engineering, No. 1(15), pp. 33-44.

8. Li, C.H., Yang, Q.W. (2020), “Optimal Sensor Placement Algorithm for Structural Damage Identification”, Recent Patents on Engineering, No. 14(69), pp. 69-81.

9. Castello, C., Fan, J., Davari, A., Chen, R-X. (2010), “Optimal sensor placement strategy for environmental monitoring using Wireless Sensor Networks”, Proceedings of the Annual Southeastern Symposium on System Theory, pp. 275 - 279.

10. Akbarzadeh, V., Lévesque, J., Gagne, C., Parize, M. (2014), “Efficient sensor placement optimization using gradient descent and probabilistic coverage”, Sensors (Basel), No. 8(14), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4179027/.

11. Petrivskyi, V.Y., Shevchenko, V.L., Brazhenenko, M.G. (2019), “Increase the operation time of sensors by regulating power consumption,” Information processing systems, No. 3(158), pp. 36-41.

12. Stoyan, Y.G., Yaskov, G.N. (2010), “Packing identical spheres into a cylinder”, International Transactions in Operational Research, No. 17, pp. 51–70.

13. Petrivskyi, V., Shevchenko, V., Bychkov, O., Brazhenenko, M. (2020) “Information technology of the increasing sensors term of use considering their movement”, 2020 IEEE 16-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). pp.86-89.

14. Wesner, N. (2017), “Multiobjective Optimization via Visualization”, Economics Bulletin, No. 2(37), pp. 1226–1233.

Petrivskyi V.Y., Dr. Eng. Sc. Shevchenko V.L., Dr. Eng. Sc. Bychkov O.S., Ph.D. Loza V.M.

INFORMATION TECHNOLOGY OF TERRITORY COVERING BY SENSORS WITH THE CONSTANT INTERSECTION LEVEL AND COST MINIMIZATION

Thanks to the rapid development of technologies, in particular information, sensors have become widespread and used in all areas of human activity. Sensors and sensor networks have received special use during the collection and processing of data of various types. When monitoring a certain territory, the problem arises of its maximum coverage in order to increase the information content and completeness of the accumulated data. Simultaneously with the predominance of autonomous use of sensors, the problem of the duration of the sensor operation arises. This value depends on the capacity of the battery. In turn, engineers are faced with the task of minimizing the design of the sensors, which results in a decrease in the volume of the battery simultaneously with all other components. It is also obvious that as the sensor coverage radius increases, the energy consumption increases, which in turn shortens the sensor life. In addition to energy costs, the article considers the costs of servicing and purchasing sensors. Thus, in addition to maximizing the percentage of coverage of the study area, the problem of minimizing the total costs arises. Obviously, to ensure data transfer between sensors, a necessary condition is the presence of the intersection of the sensor coverage areas. In this case, the constant value of this parameter is considered. The materials propose an approach to solving the problem of maximizing the coverage of the territory with minimizing costs for a given level of intersection of the coverage areas of the sensors. The proposed approach is based on solving a nonlinear multiobjective optimization problem. Also, one of the options for solving the described problem is proposed to reduce the objective functions in one by using a weighted convolution of criteria. In addition, the article proposes an iterative approach to solving the described problem. A number of computer experiments have been carried out. The results of the performed computational experiments confirm the possibility of using the proposed information technology both in the form of an optimization problem and in the form of an iterative process.

Keywords: sensor, territory coverage, information technology, multicriteria optimization, nonlinear optimization.

УДК 621.391.3
Сушин І.О. (НТУУ «КПІ ім. Ігоря Сікорського»)
к.т.н., с.н.с. **Міночкін Д.А.** (НТУУ «КПІ ім. Ігоря Сікорського»)

DOI: https://doi.org/10.17721/2519-481X/2020/68-08

ПРИМАНКА ІОТ З ВИКОРИСТАННЯМ БЕЗПЕЧНОЇ АУТЕНТИФІКАЦІЇ

У статті було розглянуто метод підвищення безпеки технологій Інтернету-речей. Користувачі побоюються наслідків порушень безпеки Інтернету-речей. Тому цифрова безпека повинна бути спроектована з нуля і у всіх точках системи для того щоб вразливості в певній частині не ставили під загрозу усю систему в цілому. Ризик повинен бути зменшений протягом всього життєвого циклу, особливо з урахуванням його масштабування і географічного розширення. Мережа Інтернету-речей складається з великої кількості недорогих пристроїв. Пристрої Інтернету-речей зазвичай мають обмежену пам'ять і живляться. від батареї, що дає дуже обмежені можливості в плані обчислень і зв'язку. Використання алгоритмів шифрування/дешифрування не повинно вимагати великих ресурсів, а діапазон частот, що використовується обмежений. Також це великомасштабна мережа, що підтримує масові з'єднання. Щоб задовольнити цей попит, протоколи мережевої передачі повинні включати в себе безліч нових функцій, таких як багатоперехідна маршрутизація, спільна ретрансляція, динамічний доступ та інше. При такому налаштуванні мережі вкрай складно керувати секретними ключами і поширювати їх. Різноманітність сценаріїв використання вимагають різних QoS та рівнів безпеки. На сьогоднішній день Інтернет-речей відіграє важливу роль у багатьох сценаріях і має великі перспективи для подальшого розповсюдження. Існує потреба в збільшенні ефективності роботи того чи іншого підприємства, процесів, тому збільшується кількість інтерактивних речей, що створюють розумні осередки (будинки, офіси, склади, міста). Реалізація даного напрямку досягається різноманітними технологіями, які з часом страждають від знайдених вразливостей, що призводить до значних втрат, як даних так і часу. Можна зустріти багато пропозицій, які направленні на вирішення тої чи іншої проблеми після знаходження певної вразливості, але це може бути недостатньо дієвим. Тому було запропоновано створити метод, який може вирішити комплекс проблем одночасно шляхом поєднання безпечної аутентифікації PKI та приманок. Він дозволить не лише виявляти нові вразливості та атаки швидше, але і марнувати ресурси атакуючих (всі захоплені атаки будуть ідентифікуватися і створюватись профілі атакуючих).

Ключові слова: PKI, Інтернет-речей, приманки, атаки, вразливості.

Вступ. Розповсюдженість технологій в нашому повсякденному житті означає, що світ навколо нас також стає «розумнішим». Цифрові пристрої знаходяться не тільки в наших кишенях або офісах, але все частіше в наших будинках, різноманітних будівлях, а також в багатьох місцях і містах. Граючи ключову роль в зборі, аналізі та моніторингу даних і інформації про навколишнє середовище, ці пристрої можуть зв'язуватися один з одним через величезну переплетену мережу, відому як «Інтернет-речей» (IoT). Вона дозволяє пристроям підключатися і «спілкуватися» один з одним, а також з нами, надаючи безліч даних і поглиблений аналіз, який покращить та розширить світ навколо нас. IoT все ще в стадії розробки, але налаштований на революцію в тому, як ми живемо і зробить найбільший технологічний вплив з часу хмарних обчислень.

Переваги IoT неможливо заперечувати, але успіх залежить від цілісності та конфіденційності рішень і даних разом із зниженням ризиків кібербезпеки. Кінцеві користувачі побоюються наслідків порушень безпеки IoT. Дослідження 2019-го року [1] показують що у багатьох аспектах 50 і більше відсотків опитаних не впевнені у безпеці пристроїв IoT. Мережа IoT складається з великої кількості недорогих пристроїв. Пристрої IoT, зазвичай, мають обмежену пам'ять і живляться від батареї, що дає дуже обмежені можливості в плані обчислень і зв'язку. Використання алгоритмів шифрування/дешифрування, зазвичай, заборонено, а діапазон частот, що використовується обмежений. Також це великомасштабна

мережа, що підтримує масові з'єднання. Щоб задовольнити цей попит, протоколи мережевої передачі повинні включати в себе безліч нових функцій, таких як багато перехідна маршрутизація, спільна ретрансляція, динамічний доступ та інше. При такому налаштуванні мережі вкрай складно керувати секретними ключами і поширювати їх. Різноманітність сценаріїв використання вимагають різних QoS та рівнів безпеки. Але попри усі вдосконалення описані вище проблеми лишаються через те, що з часом в будь-якому рішенні знаходять недоліки та пробіли завдяки яким можна відтворити ті чи інші атаки.

Аналіз останніх досліджень та публікацій. В літературі та дослідженнях пояснюються різні уразливості і можливі атаки на IoT [2-7]. Проте присвячені вони в більшості цих документів тільки певним типам загроз, заснованим на конкретних цілях безпеки. Актуальним лишається створення методу, який би протистояв декільком загрозам одночасно зважаючи на обмеження пристроїв та архітектури Інтернету-речей. Пропонується використовувати існуючий спосіб раннього виявлення атак на основі приманок [8-9] разом із безпечною аутентифікацією PKI, яка пристосована для пристроїв Інтернету-речей [10-11].

Мета статті. Метою статті є наведення методу підвищення безпеки технологій Інтернету-речей.

Виклад основного матеріалу. Приманка (honeypot) – це інструмент з окремою і відокремленою мережею, що імітує реальну цінну мережу або реальний пристрій, що буде корисним для зловмисників. Його можна розглядати як підроблену систему, яка виглядає як справжня, з метою привернути зловмисників, щоб вони могли потрапити в неї і, таким чином, відстежувати взаємодію між зловмисниками і зараженим пристроєм. Згодом приманка стала одним з важливих предметів для дослідників в області інформаційної безпеки для виявлення атак і інструментарію обману. В даний час розглядаються можливість впровадження приманки в IoT, оскільки пристрої IoT стали на меті зловмисників, до того ж це одна з популярних платформ в цьому столітті. З швидким розвитком комп'ютерів та Інтернету, приманка може надати нам інформацію про атаки зловмисних програм або навіть про шаблони атак.

Приманку можна розділити на два типи [12]: комерційну приманку і дослідницьку приманку. Зазвичай, комерційна приманка часто використовується для допомоги організації в захисті внутрішньої IT-інфраструктури. Оскільки у такої приманки менше функцій, її часто легко реалізувати. Можна сказати, що комерційна приманка вимагає компромісу між простотою експлуатації і кількістю інформації, що збирається. Антагоністом виробничої приманки є дослідницька приманка. Ця приманка дуже складна, оскільки призначена для максимального збору вичерпної інформації про зловмисника, тому її складніше розгорнути. Зібрана інформація допоможе експертам-криміналістам мережі краще зрозуміти шаблони атакуючих.

Згідно іншої класифікації [13] приманки поділені на рівні взаємодії: приманка з низьким рівнем взаємодії (LIH), приманка із середнім взаємодією (MIH) та приманка з високим рівнем взаємодії (HIH). *Приманка LIH* має невеликий набір служб, таких як SSH, Telnet і FTP, і, як правило, не надає зловмисникові доступу до операційної системи, так як на цій приманці не встановлена операційна система. Тому взаємодія зловмисника обмежується спробою входу в систему, наприклад вгадування пароля. LIH дає мінімальну відповідь, яка в основному використовується для статистичної оцінки. По суті, ця приманка є комерційною приманкою, оскільки її легко встановити і з великою ймовірністю зламати. *Приманка MIH* також не має операційної системи, але забезпечує більш високий рівень змодельованих послуг, щоб заінтригувати зловмисника. В результаті ця приманка видає розумну відповідь як каталізатор для запуску наступної атаки. Ризик компрометації відповідний рівню можливостей взаємодії. З іншого боку, *приманка HIH* являє собою складну і витончену приманку. Її складніше реалізувати і підтримувати, ніж попередні, оскільки він надає зловмисникові необмежену середу операційної системи з встановленим величезним набором сервісів. Іншими словами, HIH не просто емулює службу в операційній системі, а запускає саму операційну систему. Це

дозволяє збирати і вивчати поведінку зловмисника в повному обсязі. Ця приманка, зазвичай, використовується в якості приманки для досліджень.

Ґрунтуючись на цих спостереженнях, можна запропонувати гібридну платформу-приманку (рис. 1) для Інтернету-речей, яка дозволяє збирати більш повні зразки зловмисних програм, націлених на пристрої Інтернету-речей. Ключове нововведення складається з двох частин: використання HIH та LIH, що працюють у віртуальному середовищі. На відміну від певних LIH [14], які аналізують тільки сімейства зловмисних зразків, відбуватиметься аналіз подібності зловмисних зразків. І обидва вони використовуються для збору зловмисних зразків на пристроях Інтернету речей. Компонент з низьким рівнем інтерактивності імітує процедуру входу в систему служби Telnet/SSH на пристроях IoT. Після входу в систему зловмисники отримають конкретну банерну інформацію, яку зібрано від виробників пристроїв Інтернету-речей, таких як Huawei, Dahua, D-Link і тощо. Високоінтерактівний компонент відображає реальні вразливі служби на пристроях IoT в загальнодоступну мережу з допомогою методу, що має назву переадресація трафіку, і хакери можуть безпосередньо звертатися до цих служб в загальнодоступній мережі. Можна відстежувати трафік процесу зв'язку, щоб виявляти зловмисну поведінку, таку як завантаження двійкових файлів зловмисних програм.

Для полегшення розробки та розгортання даної приманки, конкретний код реалізації безпосередньо розгортається в Docker. Docker – це cgroup, простір імен та подібна до AUFS технологія UnionFS на основі Linux, яка інкапсулює та ізолює процеси. Це технологія віртуалізації на рівні операційної системи, яка значно підвищує ефективність розробки для розробників [15].

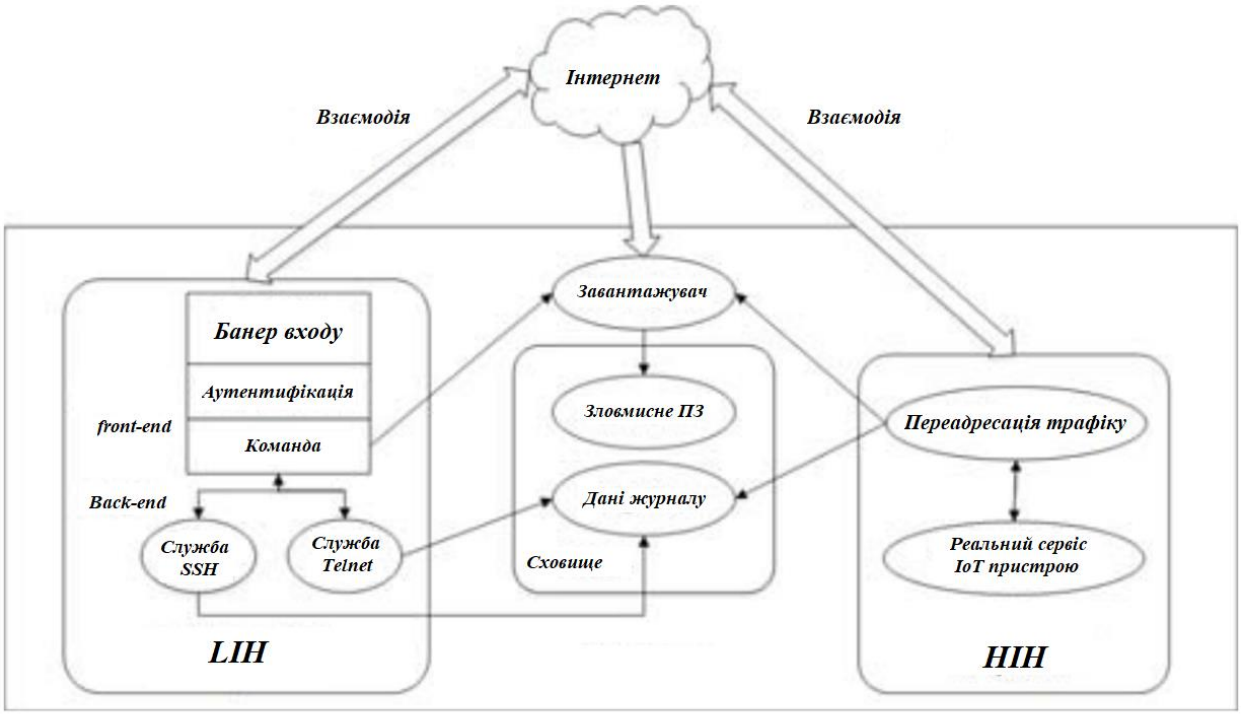


Рисунок 1 – Гібридна платформа-приманка

PKI (Public Key Infrastructure) – це ефективний підхід до розподіленого управління аутентифікацією для підтримки шифрування даних, тим самим підтримуючи засіб для безпечного і конфіденційного обміну даними через потенційно небезпечну інфраструктуру, яка, зазвичай, використовується IoT. PKI широко відомий і використовує пару ключів, відомих як відкритий ключ і закритий ключ. Ці ключі пов'язані і є похідними. Відкритий ключ надається безкоштовно для шифрування, а закритий ключ, як випливає з назви, зберігається в секреті і використовується для дешифрування. Знання відкритого ключа не дозволяє отримати закритий ключ з використанням сучасних обчислювальних методів [10]. Крім того, закритий

ключ можна використовувати для підпису повідомлень, відправлених користувачам, які можуть використовувати відкритий ключ для перевірки справжності повідомлення. Деякі криптографічні схеми, такі як RSA, дозволяють використовувати ключову пару як для шифрування, так і для підпису.

Як правило, цифрова сертифікація PKI використовує довірений сторонній об'єкт, який видає сертифікат після законної аутентифікації. Ці органи відомі як CA (Центр сертифікації), які генерують, видають і підписують цифровий сертифікат. RA (центр реєстрації) перевіряє ідентичність органів, які запитують цифрові сертифікати для видачі з CA, а механізм централізованого управління використовується для зберігання і індексації ключів сертифікатів для управління доступом до збережених цифрових сертифікатів [68]. RA вводиться для поліпшення масштабованості PKI, а також забезпечує високий ступінь захисту первинних ключів CA.

Розглянемо безпечну структуру аутентифікації IoT з використанням механізму цифрового сертифікату PKI. Ця структура заснована на тристоронньому зв'язку між користувачем, пристроєм IoT і хмарою. У цій структурі хмара аутентифікує як користувача, так і пристрій IoT, використовуючи їх цифровий сертифікат. Передбачається, що користувач не спілкується регулярно безпосередньо з пристроєм IoT, за винятком початкового завантаження. Таким чином, користувач повинен пройти через шлюз і хмарну систему, щоб обмінюватися даними з пристроєм IoT. Тобто, якщо пристрій IoT довіряє CA і користувач довіряє CA, то вони довіряють один одному. Це звичайна архітектура Інтернету речей в домашніх умовах, але не єдина модель. Передбачається, що інфраструктура хмарних обчислень забезпечує зручний спосіб надання обчислювальних ресурсів для спільної групи, наприклад мереж, служб, серверів і застосунків зберігання. Хмарні сервіси можуть надавати основні компоненти для шифрування, дешифрування і управління ключами PKI [11]. На рисунку 2 наведена безпечна структура, яка може надати можливість для реєстрації пристрою IoT з використанням цифрового сертифіката, а також користувача на хмарному сервері. Після завершення процесу реєстрації тільки справжній зареєстрований користувач може мати доступ для використання IoT пристрою, доступного в мережі.

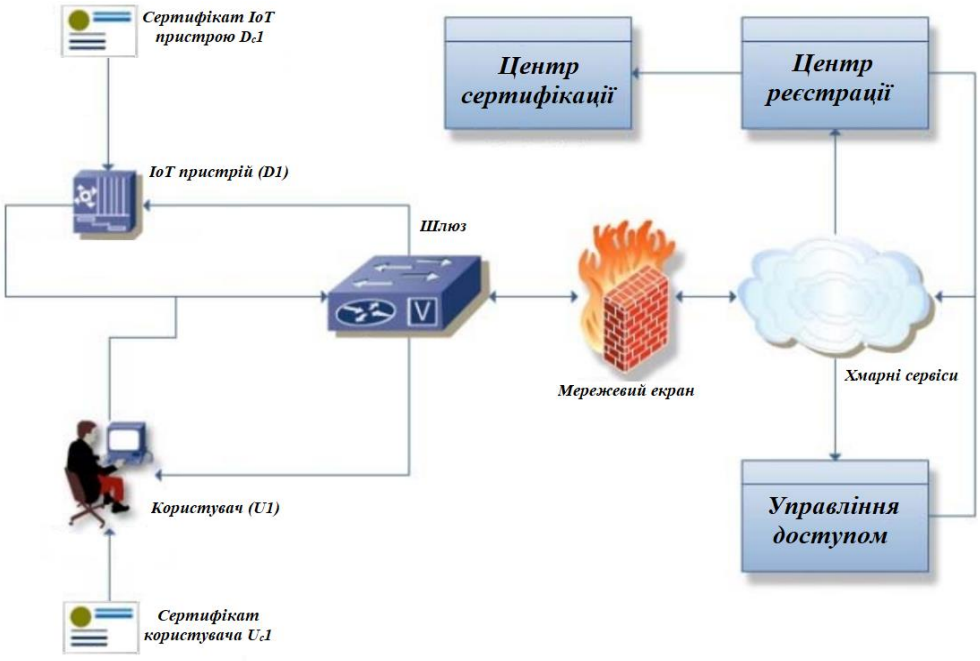


Рисунок 2 – Структура системи аутентифікації PKI для IoT

Виходячи з того що технології, що розглядалися вище ефективно допомагають підвищити безпеку та зрозуміти напрямки розвитку атак на технології Інтернету-речей, можливо поєднати їх для підвищення безпеки. Пропонується використовувати

аутентифікацію PKI замість протоколів telnet та SSH. При цьому приманка допоможе записати та зібрати логи зловмисників, які змогли обійти аутентифікацію чи використовують вразливості (нульового дня) сервісів Інтернету-речей, які ще не встигли закрити. Алгоритм роботи вдосконаленої гібридної приманки зображений на рис. 3.

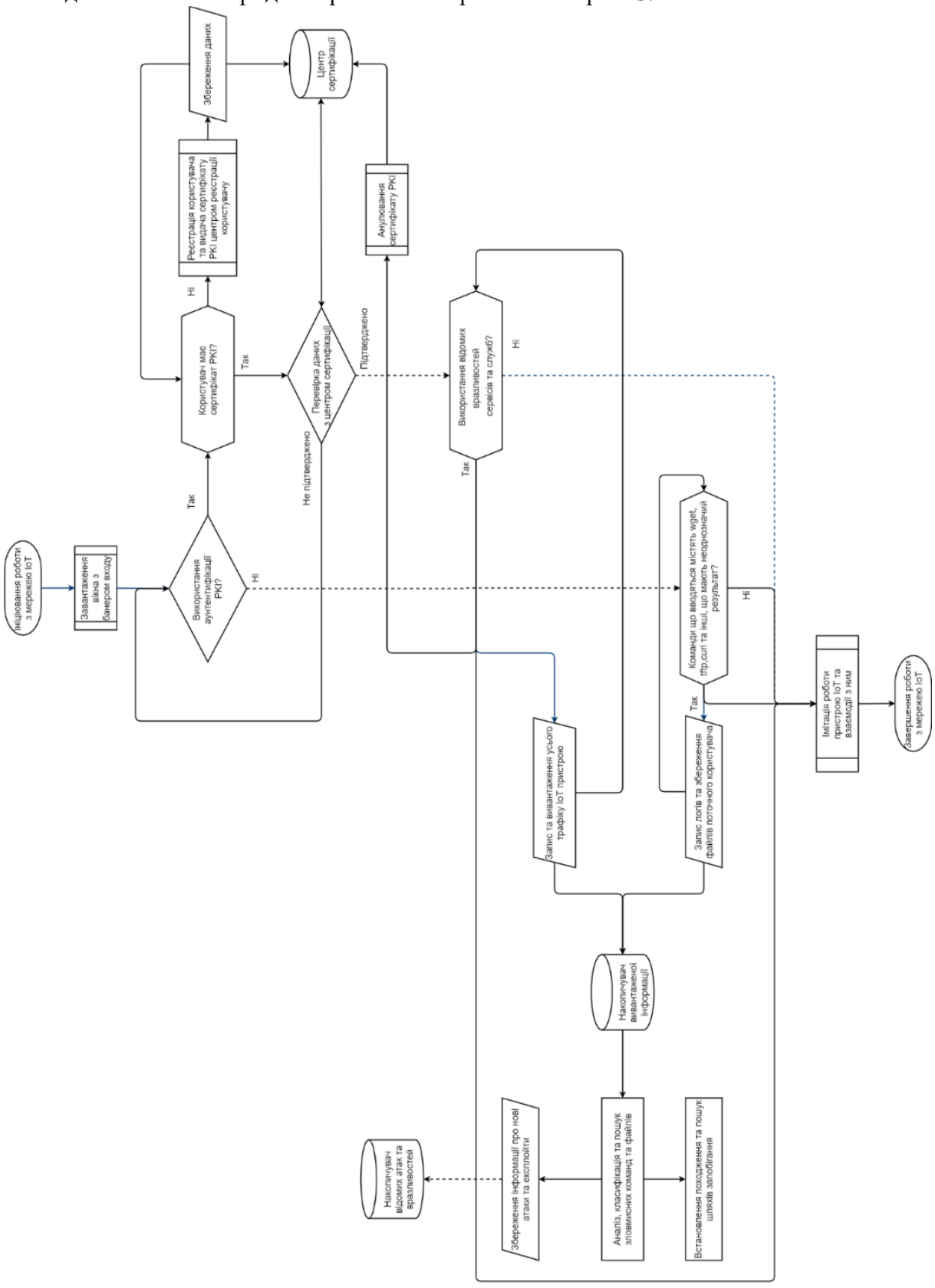


Рисунок 3 – Алгоритм роботи вдосконаленої гібридної приманки

Використовуючи дане рішення можливо зменшити кількість атак, але при цьому вони стануть більш якісними. Тобто, успішна атака на приманку дасть можливість та розуміння того як необхідно покращувати аутентифікацію PKI або цільові сервіси IoT.

Основними перевагами PKI є:

- Технологія у основі якої лежить стандарт X.509. Його підтримують більшість відомих сервісів, тому використання PKI можливого легко реалізувати змінивши стандартну конфігурацію за необхідності для використання під той чи інший сервіс;
- Масштабованість. Користувачі підтримують свої власні сертифікати, а перевірка справжності сертифіката включає обмін даними тільки між клієнтом і сервером. Це означає, що сторонній сервер аутентифікації не повинен бути в мережі. Таким чином, немає обмежень на кількість користувачів, яких можна підтримувати за допомогою PKI;
- Уповноважена довіра. Тобто користувач, який отримав сертифікат від визнаного і довіреного центру сертифікації, може аутентифікувати себе на сервері в найперший раз, коли він підключається до цього сервера, без попередньої реєстрації в системі.

Основними перевагами приманок є:

- Спостереження за хакерами у дії та вивчення їх поведінки;
- Збереження інформацію про вектори атак, зловмисне програмне забезпечення та експлойти;
- Створення профілів хакерів, які намагаються отримати доступ до цільових систем;
- Марнування часових та інших ресурсів хакерів.

Отже, виходячи з даних переваг, можна побачити загальні переваги вдосконаленої приманки (див. табл. 1)

Таблиця 1

Переваги вдосконаленої приманки

Перевага	*PKI*	*Honeypot*	*PKI + Honeypot*
Стандарт X.509	+		+
Масштабованість	+		+
Уповноважена довіра	+		+
Спостереження за атакуючими		+	+
Збереження логів та встановлення закономірностей		+	+
Марнування ресурсів атакуючих		+	+
Створення профілів атакуючих		+	+

Висновки і перспективи подальших досліджень. Було запропоновано використовувати безпечну аутентифікацію PKI у приманках, наведений алгоритм роботи вдосконаленої приманки. Це дозволило виявити дуже цінні нові атаки, які націлені безпосередньо на даний тип аутентифікації. Також існують вразливості у сервісах Інтернету-речей, які не встигають швидко виправити і проходить певний час. Якщо за цей час приманка буде реєструвати збіг використовуваної вразливості з тою що знаходиться в базі даних, то буде можливість анулювати сертифікат виданий поточному користувачу та замінити скомпрометовані, а також отримати інформацію про те, що на даний тип атаки необхідно звернути більше уваги. Вдосконалена приманка з використанням безпечної аутентифікації дозволить зменшити час на виправлення вразливостей, кількість атак, але, при цьому, вони стануть більш якісними. Тобто, успішна атака на приманку дасть можливість та розуміння того, як необхідно покращувати аутентифікацію PKI або сервіси IoT, які використовуються у діючих елементах мережі.

ЛІТЕРАТУРА:

1. Internet Society (2019), “The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things”. Available at: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-

consumer-attitudes-to-iot/.

2. Fan K., Gong Y., Liang C., Li H., Yang Y. (2015) “Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G”. Security and Communication Networks 9(16), pp. 3095–3104.

3. I. Andrea, C. Chrysostomou and G. Hadjichristofi (2015), “Internet of Things: Security vulnerabilities and challenges”, IEEE Symposium on Computers and Communication (ISCC), pp.180-187.

4. Wahid, Abdul, P. Kumar (2015), “A Survey on attacks, Challenges and Security Mechanism in Wireless Sensor Network”, JIRST- International Journal for Research in Science & Technology, Volume 1, Issue 8, pp. 189-196.

5. S.N Uke, A.R Mahajan, R.C Thool (2013), “UML Modeling of Physical and Data Link Layer Security Attacks in WSN”, International Journal of Computer Applications, Volume 70– No.11.

6. Li, Hong, Y. Chen, and Z. He (2012), "The Survey of RFID Attacks and Defenses." 8th International Conference on IEEE Wireless Communications, Networking and Mobile Computing (WiCOM).

7. Kandah, Farah, Y. Singh, and C. Wang (2011), “Colluding injected attack in mobile ad-hoc networks”, IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPS).

8. M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder (2016), “A Survey on Honeypot Software and Data Analysis”.

9. C. H. Malin et al. (2017), “Sweet Deception: Honeypots,” Decept. Digit. Age, pp. 227–239.

10. Z. A. Alizai, N. F. Tareen, and I. Jadoon (2018), “Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures,” in 2018 International Conference on Applied and Engineering Mathematics (ICAEM), pp. 1–5.

11. J. Xu, W.-T. Zhu, and D.-G. Feng (2009), “An improved smart card-based password authentication scheme with provable security,” Comput. Stand. Interfaces, vol. 31, no. 4, pp. 723–728.

12. C. Seifert, I. Welch, and P. Komisarczuk (2006), “HoneyC-The LowInteraction Client Honeypot”

13. I. Mokube and M. Adams (2007), “Honeypots: Concepts, Approaches, and Challenges,” Proc. 45th Annu. southeast Reg. Conf. - ACM-SE 45, pp. 321–326.

14. Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow (2016), “Iotpot: A novel honeypot for revealing current iot threats,” Journal of Information Processing, vol. 24, no. 3, pp. 522–533.

15. C. Anderson (2015), “Docker [software engineering],” IEEE Software, vol. 32, no. 3, pp. 102–c3.

Sushyn I.O., Ph.D. Minochkin D.A.

IOT HONEYPOT WITH USING SECURE AUTHENTICATION

The article considers the method of increasing the security of Internet of Things technologies. Users fear the consequences of Internet security violations. Therefore, digital security must be designed from zero and at all points of the system so vulnerabilities do not jeopardize the whole system in a certain part. The risk must be reduced throughout the life cycle, especially in view of its scaling and geographical expansion. The Internet of Things consists of a large number of inexpensive devices. IoT devices usually have limited memory and battery power, which gives very limited computing and communication capabilities. The use of encryption/decryption algorithms should not require large resources, and the frequency range is limited. It is also a large-scale network that supports mass connections. Network transmission protocols must include many new features, such as multi-transient routing, shared relay, dynamic access, and other to meet this demand. It is extremely difficult to manage and distribute private keys with this network setup. A variety of usage scenarios require different QoS and security levels. Nowadays IoT plays an important role in many scenarios and has great potential for further dissemination. There is a need to increase the efficiency of a particular enterprise, processes, so the number of interactive things that create smart areas (houses, offices, warehouses, cities) is growing. The implementation of this areas reaches a variety of technologies, which vulnerable from the found attacks over time, leading to significant losses, as data and time. There are many suggestions that address target issue after finding a vulnerability, but this may not be effective enough. Therefore, it was proposed to create a method that can solve a set of problems simultaneously by combining PKI secure authentication and honeypots. It will not only detect new vulnerabilities and attacks faster, but also waste attackers' resources (all captured attacks will be identified and attacker profiles created).

Keywords: PKI, IoT, Honeypot, attacks, vulnerabilities.

УДК 004.056.21

д.т.н., проф. **Толюпа С.В.** (КНУ)
к.т.н., доц. **Плющ О.Г.** (ДУТ)
к.т.н., доц. **Пархоменко І.І.** (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-09

ПОБУДОВА СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ НА ОСНОВІ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО РОЗПОДІЛУ ДАНИХ

У статті запропонована комбінаторна побудова системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних та проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі. Проведені експерименти з програмним прототипом показали високу якість виявлення мережевих атак і довели правильність вибору методів інтелектуального аналізу даних і застосовність вироблених методик.

Проаналізовано стан захищеності інформаційно-телекомунікаційних систем по протидії від кібератак, що дало можливість зробити висновки, шо для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме систем: розмежування доступу користувачів; міжмережного екранування; криптографічного захисту інформації; віртуальні приватні мережі; антивірусного захисту елементів ІТС; виявлення і запобігання вторгнень; автентифікації, авторизації і аудиту; попередження втрати даних; управління безпекою та подіями; управління захищеності.

Проведено аналіз публікацій вітчизняних та іноземних фахівців, в яких узагальнюється:

досвід побудови систем виявлення атак, їх недоліки та переваги; побудова систем виявлення атак та вторгнень на основі застосування інтелектуальних систем.

За результатами розгляду сформовано пропозиції щодо:

побудови систем виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних та проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі.

Ключові слова: кіберпростір, атака, нейромережа, інформаційно-телекомунікаційна мережа, системи виявлення атак, методи інтелектуального аналізу даних, тренувальна база.

Вступ та аналіз останніх досліджень. Інтенсивний розвиток інформаційно-телекомунікаційних мереж (ІТС) та технологій всебічно впливає на всі сфери діяльності суспільства. Переважна кількість сучасних державних та приватних підприємств використовує ІТС для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо. Це забезпечує їм низку переваг, пов'язаних з: підвищенням продуктивності праці і мобільності працівників; високою оперативністю доступу до інформації та послуг; можливостями віддаленого управління ресурсами і процесами тощо.

Низка нещодавно реалізованих кібератак, які завдали шкоди багатьом державним установам та приватним підприємствам і організаціям в 2017 році (Ощадбанк, Укргазбанк, Укрпошта, Укрзалізниця, Укренерго, ДТЕК, Київенерго, Київводоканал, Міжнародні аеропорти «Бориспіль» і «Київ», Rozetka, Київстар, Vodafone Україна, Lifecell, Київський метрополітен, телеканали СТБ і ICTV, Нова пошта, мережа магазинів «Епіцентр», автозаправки WOG і ТНК тощо [1]) показали неготовність та недосконалість їх власних систем безпеки до раніше невідомих вторгнень.

У 2020 році в Україні зафіксували близько 1 мільйон випадків кіберзагроз. Серед них - мережеві атаки, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення. З метою попередження можливих атак, Національний координаційний центр кібербезпеки (НКЦК) посилив співпрацю з приватними компаніями. Вони передбачають обмін інформацією про кіберзагрози та інциденти в сфері кіберзахисту для оперативного інформування, реагування, попередження можливих атак і взаємодопомоги [2].

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи [3-7], моделі [8, 9], засоби [10-12], ПЗ [13] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [14,15], які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому, системи виявлення вторгнень (СВВ) повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

На сьогодні вирішення питань забезпечення безпеки в ІТС та управління станом їх захищеності описується в роботах вітчизняних та закордонних дослідників, а саме: Бурячка В.Л., Гнатюка С.О., Корченко О.Г., Кузнецова О.О., Субача І.Ю., Юдіна О.К., Бучика С.С., Євсеєва С.П., Дудикевича В.Б., Казмирчук С.В., T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІТС з боку неавторизованої сторони (НАС). Також слід наголосити, що атаки на ІТС з кожним роком стають все досконалішими, глобальнішими та частішими.

Основна частина. На сьогоднішній день ІТС дозволяє вирішувати найбільш актуальні завдання: надання користувачам можливості обміну інформаційними повідомленнями різного типу (мова, відео, дані); швидке та якісне отримання необхідної інформації з будь-якого віддаленого джерела в мережі; автоматизацію процесів обробки, накопичення, зберігання великих обсягів інформації в мережі, самого процесу виробництва інформації.

Для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме систем: розмежування доступу користувачів; міжмережного екранування; криптографічного захисту інформації; віртуальні приватні мережі; антивірусного захисту елементів ІТС; виявлення і запобігання вторгнень; автентифікації, авторизації і аудиту; попередження втрати даних; управління безпекою та подіями; управління захищеності.

Системи виявлення вторгнень є одним з ключових компонентів комплексу засобів захисту інформації. Всі існуючі промислові СВВ і наукові розробки мають ті чи інші недоліки: обмежений спектр виявляються атак або підтримуваної програмно-апаратної середовища, складність адміністрування або створення профілю, висока обчислювальна складність.

Системи виявлення атак (СВА) являють собою окремий клас програмних засобів (ПЗ), під яким розуміють програми, процедури, правила, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування системи обробки інформації. Повна назва СВА – це системи виявлення і запобігання атак, так як саме в можливості автоматизованої протидії атакам полягає одна з основних переваг таких систем, у порівнянні, наприклад, із засобами, заснованими на людському факторі. Проте надалі буде використовуватися найбільш усталена назва - система виявлення атак. Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей інформаційної безпеки [16].

Системи виявлення мережевих атак збирають інформацію з пакетів мережевого трафіку, системних журналів і показників функціонування системи. Традиційні системи виявлення мережевих атак будуються на сигнатурному підході: за допомогою набору правил або сигнатур, що формуються експертами і розміщені в базу вирішальних правил, описуються всі можливі сценарії і особливості атак. У цього підходу існує безліч відомих недоліків. За допомогою аналізу сигнатур неможливо виявити нові види атак, тому що база вирішальних правил не містить інформації про відповідну атаці. Процес аналізу сигнатур для розподілених атак є вкрай складним завданням. Крім того, бази вирішальних правил популярних систем

виявлення вторгнень практично є загальнодоступними, тому порушник може протестувати можливості приховування атаки [18-19].

Перераховані проблеми підходу пошуку сигнатур змушують фахівців шукати альтернативні шляхи для організації захисту від мережевих атак. Одним з популярних напрямків досліджень є застосування різних методів інтелектуального аналізу даних (ІАД) в системах виявлення мережевих атак. В основі даних методів лежить припущення, що вся легітимна активність в системі може бути представлена у вигляді математичної моделі [20-22].

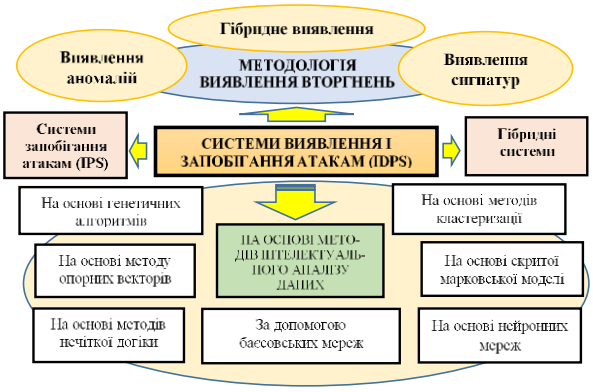


Рисунок 1 - Кваліфікаційні ознаки СВА на основі інтелектуальних методів аналізу даних

В останні десятиліття методи інтелектуального аналізу даних отримали широке застосування в багатьох наукових напрямах, і проблема виявлення мережевих атак не є винятком з цієї тенденції. Існують кілька сотень наукових досліджень щодо застосування різних методів інтелектуального аналізу даних для виявлення мережевих атак і для вирішення пов'язаних з виявленням підзадач.

Аналіз методів інтелектуального розподілу даних детально представлений в [23].

Описані в статті методики дозволяють використовувати всі вибрані методи інтелектуального аналізу даних для вирішення відповідних підзадач, пов'язаних з виявленням мережевих атак. У представлених методиках присутня значна кількість внутрішніх налаштувань. Для більшості налаштувань описані алгоритми по автоматичному вибору. Для інших видані рекомендації по ручному застосування при експериментальній побудові модулів виявлення для конкретних мережевих атак.

Рисунок 2 - Інтелектуальна система виявлення вторгнень

Звичайно протидіяти вторгненням і атакам основуючись тільки на одному з методів інтелектуального аналізу даних малоефективно, тому необхідно підійти до цього питання комплексно і побудувати інтелектуальну систему протидії вторгненням (рис. 2). При побудові такої інтелектуальної (експертної) системи пропонується вибрати нечітку модель. Це пов’язано з тим, що значна частина інформації про причини і джерела атак може бути отримана тільки експертним шляхом або у вигляді евристичних описів процесів. Для визначення джерел атак система безпеки має бути представлена моделлю тієї інформаційної мережі на яку вона орієнтується.

Данна модель ділить завдання переміщення інформації між комп’ютерами через середовище мережі на кількість рівнів менш великих і легше вирішуваних підзадач. Кожна з цих підзадач вирішується за допомогою одного рівня мережі. Тому первинне завдання для фахівця безпеки може бути представлене декомпозицією завдань безпеки по окремих рівнів мережі [24].

Аналіз останніх публікацій свідчить про те, що існуючі атаки, які застосовуються для проведення вторгнень в ІТС поділяються на 5 категорій. Кожна з категорій містить множину типів атак, які використовуються для реалізації мети вторгнення. В свою чергу кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію, щодо здійснення деструктивного впливу на мережу.

Серед лідерів детектування вразливостей можливо зазначити наступних розробників відповідних баз даних вразливостей: компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE); National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD); United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND), компанія IBM та база вразливостей X-Force та інші.

Питання вибору тренувальної бази з атаками не має простого рішення, тому що широко поширені бази даних містять багато в чому застарілі типи атак, а більш сучасні бази мають специфічну структуру, що вимагає складної попередньої обробки, і використовуються тільки окремими дослідниками, що перешкоджає порівнянні якісних показників результатів роботи.

При розробці та проведенні досліджень систем виявлення вторгнень однією з ключових завдань є вибір масивів даних, на яких буде проводитися тестування. Великі компанії-розробники в першу чергу орієнтуються на власні бази даних, спеціалізовані під конкретні завдання і область застосування.

На сьогоднішній день можна виділити дві найбільш поширені тренувальні бази даних з відомими атаками - DARPA і KDD.

Тренувальна база даних DARPA (Defense Advanced Research Project Agency) була сформована в рамках досліджень лабораторії Лінкольна Массачусетського технологічного інституту (MIT Lincoln Laboratory) в рамках дослідження можливостей різних систем виявлення вторгнень. Під час цього дослідження використовувалися дані мережевого трафіку і відомості від файлової системи для можливості ідентифікації змодельованих вторгнень, проведених фахівцями під час запису мережевих дампов. Тренувальні дані містять як реальний потік мережевого трафіку, так і спеціально змодельований фоновий трафік. Всі атаки були спрямовані на реальні обчислювальні системи.

В даний час тренувальні бази доступні всім дослідникам, тому значна частина публікацій у науковій літературі, пов'язаних з пропозицією нових методів і підходів з виявлення мережевих атак або аномалій, спираються на ці тестові дані. Використання даної бази даних дозволяє дослідникам по-рівняти основні характеристики якості виявлення: ймовірності помилок пропуску (false negative) і помилкового спрацьовування (false positive).

Загальна кількість типів атак, включених в тестові дані DARPA, склало 32 атаки. З точки зору атакуючого ці атаки можна розділити на чотири категорії: атаки відмови в обслуговуванні (Denial of Service, DoS); атаки переходу від віддаленого використання до локального (Remote to Local); атаки отримання користувачами прав суперкористувача (User to Root); атаки сканування або проб (Probing/surveillance).

Інформація про атаки DARPA зберігається у вигляді текстового опису, в якому вказується час початку атаки, тривалість, адреса жертви, назва атаки, категорія атаки та інші параметри.

На відміну від тренувальних даних DARPA, база даних KDD містить не дампи мережевого трафіку, а оброблені відомості у вигляді масивів з 42 ключових значень. Дана база успішно застосовується багатьма дослідниками для аналізу застосування різних математичних методів в завданні виявлення мережевих атак, в основному через можливість використання масивів даних з більшості програмних засобів без виконання додаткової обробки.

Зміст 42 параметрів, що розглядаються в базі даних KDD, був обґрунтований науково, присвяченими виявлення аномалій в мережевому трафіку. Однак при дослідженні можливостей по виявленню конкретних мережевих атак виявляється недостатньо аналізувати тільки представлені параметри, але також необхідно розглядати корисне навантаження мережевих пакетів - вищі рівні стека про-токолів TCP / IP. Крім позначених тренувальних баз даних існує безліч більш вузько спеціалізованих, але вони не набули такого широкого поширення в науковому середовищі.

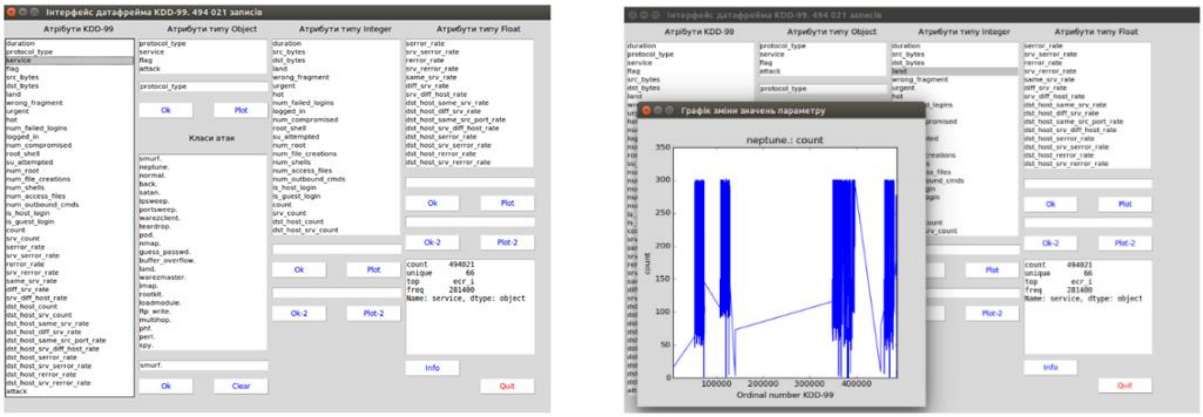


Рисунок 3 - Інтерфейс датафрейма KDD

Дослідниками пропонується безліч нестандартних рішень, що використовують конкретні особливості застосування даних методів. Формування СВВ на основі методів інтелектуального аналізу даних дозволяє позбутися від деяких відомих недоліків систем пошуку сигнатур і систем виявлення аномалій. Вибір конкретних методів і формування методик щодо застосування є складним завданням, що вимагає значних обсягів експериментів, і може сильно залежати від навчальної множини.

При розробці та проведенні досліджень систем виявлення вторгнень однією з ключових завдань є вибір масивів даних, на яких буде проводитися тестування. Великі компанії-розробники в першу чергу орієнтуються на власні бази даних, спеціалізовані під конкретні завдання і область застосування. Крім позначених тренувальних баз даних існує безліч більш вузько спеціалізованих, але вони не набули такого широкого поширення в науковому середовищі.

В рамках нашого дослідження були сформовані модулі виявлення для окремо взятих атак категорій User-to-Root і Remote-to-Local з тренувальних баз даних DARPA та KDD, які є найбільш складними для виявлення. Для більшості атак був отриманий результат в 100% правильно класифікованих пакетів. Для подібних атак отримані однакові набори «базових» параметрів. При об'єднанні кількох атак одного типу в класи також досягається 100% розпізнавання, при цьому збільшується кількість опорних векторів. Процес тестування складався з п'яти етапів. У першій частині тестування використовувалися багаторозрядні параметри трафіку, які добувають із заголовків IP і TCP пакетів. Всього використовувалося 14 базових параметрів, 6 для IP і 8 для TCP. Для значної частини атак було досягнуто 100% розпізнавання. На другому етапі, шляхом поділу багаторозрядних параметрів на кілька частин, кратних 8 бітам, число базових параметрів було збільшено до 24. В результаті аналогічного тестування для більшого числа атак було досягнуто 100% розпізнавання. У порівнянні з багаторозрядними параметрами збільшилася кількість опорних векторів, і велику роль став грати вибір даної матриці в методі головних компонент.

На третьому етапі тестування в набір розглянутих базових параметрів були включені статистичні параметри TCP-сеансів: час з'єднання, число переданих і прийнятих пакетів, байт і число пакетів з різними мітками - всього 49 базових параметрів. Для всіх розглянутих атак істотно збільшилася кількість опорних векторів в SVM-моделях, що викликано збільшенням розрядності простору. Для кількох атак так і не було отримано 100% результат. Для деяких атак виявилося досить від 2 до 5 нових параметрів з 49 для досягнення 100% розпізнавання та незначного збільшення числа опорних векторів. На четвертому етапі для атак, які не вдавалося виявити на попередніх етапах, була проведена кластеризація тренувальних даних і проведені процедури навчання нових модулів виявлення. В результаті майже для всіх розглянутих атак були побудовані кілька простих SVM-моделей, які дозволили класифікувати пакети зі 100% вірогідністю. Атаки, для яких не вдалося побудувати SVM-моделі, були проаналізовані та виявлено, що в складі тренувальних даних були присутні однакові пакети з різними мітками,

що призводило до неможливості побудови класифікатора. На п'ятому етапі було реалізовано розширення можливостей блоків кластеризації і класифікацій шляхом внесення нечіткості. В результаті побудовані пересічні кластери, однакові пакети з різними мітками були віднесені до класу атак з певною ймовірністю. Метод опорних векторів із застосуванням нечіткої логіки підвищив показники виявлення для окремих модулів. В результаті експериментального дослідження були отримані залежності числа опорних векторів від кількості нових параметрів для ряду атак. У всіх точках представлених залежностей досягнуто 100% розпізнавання. На на рис. 4 показані залежності при використанні тільки параметрів IP і TCP заголовків (всього 23 параметра).

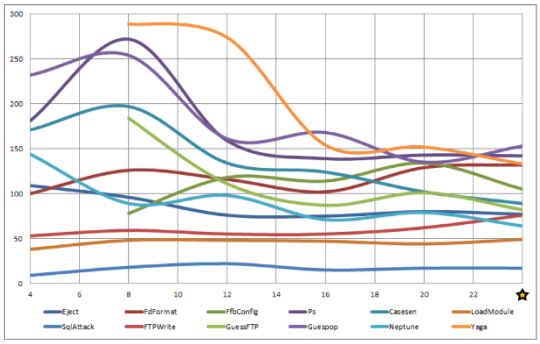


Рисунок 4 - Залежність числа опорних векторів від числа нових параметрів

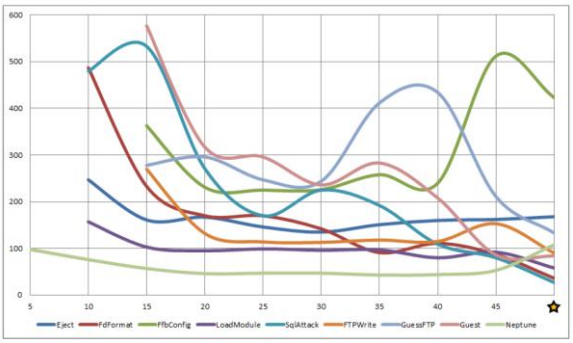


Рисунок 5 - Залежність числа опорних векторів від параметрів TCP-сеансів

На рис. 5 безліч параметрів доповнено параметрами TCP-сеансів (всього 49 параметрів). Зірочкою позначена робота без скорочення розмірності.

Для деяких атак, які не розпізнані програмним прототипом за допомогою одного модуля виявлення зі 100% ймовірністю, застосування декількох модулів виявлення з надмірною кількістю розглянутих «базових» і «нових» параметрів дозволяє скоротити число помилок другого роду до нуля. Проведені експерименти з окремими модулями виявлення показали хорошу працездатність системи та застосовність обраних інтелектуальних методів аналізу даних для поставленої мети. Метод опорних векторів дозволяє ідентифікувати значну частину розглянутих атак зі 100% ймовірністю, а в решті випадків помилка не перевищує декількох відсотків від числа всіх пакетів. Методи скорочення розмірності допомагають скоротити обсяг інформації, необхідної для класифікації мережевих пакетів й істотно підвищити продуктивність системи.

Проведене експериментальне дослідження підтвердило правильність запропонованої моделі та вибору безлічі методів інтелектуального розподілу даних, що лежать в її основі. Метод опорних векторів дозволив ідентифікувати більшість атак з результатом 98-100%. Метод головних компонент скоротив обсяг інформації, необхідної для класифікації мережевих пакетів, і підвищив швидкість формування модулів виявлення, але виявив проблему перенавчання. Методи кластеризації дозволили сформувати безліч модулів виявлення, виділивши типові фрагменти атак в окремі модулі виявлення та розбивши комплексні атаки на окремі модулі. Застосування нечіткої логіки підвищило результати роботи системи і дозволило класифікувати вектора, що мають різні мітки в навчальній вибірці.

На основі даного дослідження були детально опрацьовані сформульовані раніше методики по застосуванню методів інтелектуального розподілу даних по завданню виявлення мережевих атак [20]. Результати етапів експериментального дослідження наведені в таблиці 1.

Таблиця 1

Результати етапів експериментального дослідження

Метод анализу даних	Правильно розпізнано, %	Хибні сигнали, %
SVM (багаторозрядні параметри)	85	5
SVM	91	2
SVM + МГК	94	3
SVM + МГК + *k*-means	98	1
SVM + МГК + *k*-means + нечітка логіка	99	0,6

В табл. 2 представлені результати досліджень в сфері застосування методів інтелектуального розподілу даних в задачах виявлення мережевих атак.

Таблиця 2

Результати досліджень в сфері застосування методів інтелектуального розподілу даних в задачах виявлення мережевих атак

Метод анализа даних	Вірно розпізнано, %	Хибні сигнали, %
Quarter-sphere SVM	65	1
SVM	95,5	1
SVM + Генетичні алгоритми	99	-
SVM + Нечітка логіка	99,56	0,44
C4.5	95	1
C4.5 + МГК	92,16	-
C4.5 + Нейронні мережі	93,28	0,2
k-means кластеризація	65	1
Single leakage кластеризація	69	1
Y-means кластеризація	89,89	1
k-ближніх сусідів	92	1
Нейронні мережі + МГК	92,22	-
Багатошаровий персептрон	94,5	1
Генетичні алгоритми	97,47	0,69

Висновки. В статті запропоновано різні комбінаторні варіанти побудова системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних і проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі.

Проведені експерименти показали високу якість виявлення мережевих атак і довели правильність вибору методів інтелектуального аналізу даних і застосовність вироблених методик. Застосування різних методів, можливість настройки внутрішніх параметрів і порогових значень дозволяють домогтися оптимального співвідношення продуктивності системи і точності розпізнавання атак в розподіленої мережі.

ЛІТЕРАТУРА:

1. Хакерські атаки на Україну [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2017. URL: https://is.gd/6lkWHY.

2. Хакерські атаки в Україні. [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2020. https://glavcom.ua/topics/ rosijskikhakeru.html.

3. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс] / А. А. Корниенко, И. М. Слюсаренко // CIT forum : [сайт]. 2009.

4. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі [Електронний ресурс] / В. В. Литвинов [та ін.] // Математичні машини і системи. К : ІПММС НАН України, 2018. № 1. С. 31-40.

5. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, А. В. Котенко // Тр. СПИИРАН. 2016. № 2 (45). С. 207-244.

6. Сучасні методи виявлення аномалій в системах виявлення вторгнень / О.М. Колодчак // Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі. 2012. № 745. С. 98-104.

7. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д. О. Даниленко, О. А. Смірнов, Є. В. Мелешко // Системи озброєння і військова техніка. Х.: Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, 2012. № 1. С. 92-100.

8. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.

9. Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак / Г.Бекетова, Б. Ахметов, О. Корченко, В. Лахно // Безпека інформації. К: НАУ, 2016. Т. 22, № 3. С. 242-254.

10. Огляд систем виявлення атак в мережевому трафіку / К. М. Носенко, О. І. Півторак, Т. А. Ліхоузова // Адаптивні системи автоматичного управління. К: НТУУ КПІ, 2014. № 1 (24). С. 67-75.

11. Аналіз системи виявлення вторгнень та комп'ютерних атак / М. М. Радченко [та ін.] // Междисциплинарные исследования в науке и образовании. 2013. № 2.

12. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. Pp. 41-47.

13. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. А.Завада, О. В. Самчишин, В. В. Охрімчук // Інформаційні системи. Житомир: Збірник наукових праць ЖВІ НАУ, 2012. Т. 6, № 12. С. 97-106.

14. An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, No. 2. Pp. 109-120.

15. Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, No. 2. Pp. 169-184.

17. IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https://www.netgate. com/docs/pfsense/ids-ips/.

18. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Науково-технічний журнал "Сучасний захист інформації". – №1. 2019. С. 56-62.

19. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). С. 69-79.

20. Ghahramani, Z. An Introduction to hidden Markov models and Bayesian networks / Z. Ghahramani // International Journal of Pattern Recognition and Artificial Intelligence – 2001. –Vol. 15. – Pp. 9-42.

21. Barbara D. Detecting novel network intrusions using Bayes estimators / D. Barbara, J. Couto, S. Jajodia, N. Wu. // In: Proc. of the 1st SIAM International Conference on Data Mining. – 2001.

22. Kruegel, C. Bayesian event classification for intrusion detection / C. Kruegel, D. Mutz, W. Robertson, F. Valeur // In: Proc. of the 19th Annual Computer Security Applications Conference – 2003. – Pp. 14–23.

23. Толюпа С.В., Штаненко С.С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 3. 2018р. С. 56-66.

24. Toliupa S.1, Druzhynin V.2, Parkhomenko I Signature and statistical analyzers in the cyber attack detection system. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) September 2018. Pp. 47-53.

25. Valdes, A. Adaptive model-based monitoring for cyber attack detection / A. Valdes, K. Skinner // In: Proc. of the Recent Advances in Intrusion Detection (Toulouse, France, 2000) – 2000. – Pp. 80-92.

26. Portnoy, L. Intrusion detection with unlabeled data using clustering / L. Portnoy, E. Eskin, S. J. Stolfo // In: Proc. of ACM Workshop on Data Mining Applied to Security. – 2001. – Pp. 1-14.

REFERENCES:

1. Hacker attacks on Ukraine [Electronic resource] // Wikipedia: [site]. Kyiv, 2017. URL: https://is.gd/6lkWHY.

2. Hacker attacks in Ukraine. [Electronic resource] // Wikipedia: [site]. Kyiv, 2020. https://glavcom.ua/topics/ rosijskikhakeru.html.

3. Systems and methods of detection of intrusions: the current state and directions of improvement [Electronic resource] / A.A. Kornienko, I.M. Slyusarenko // CIT forum: [site]. 2009.

4. Analysis of systems and methods for detecting unauthorized intrusions into computer networks [Electronic resource] / V.V. Litvinov [etc.] // Mathematical Machines and Systems. K: IPMMS NAS of Ukraine, 2018. № 1. Pp. 31-40.

5. Analysis and classification of methods for detecting network attacks / A.A. Branitsky, A.V. Kotenko // Tr. SPIIRAN. 2016. № 2 (45). Pp. 207-244.

6. Modern methods of detecting anomalies in intrusion detection systems / O.M. Kolodchak // Bulletin of the National University "Lviv Polytechnic". Computer systems and networks. 2012. № 745. pp. 98–104.

7. Research of methods of detection of intrusions into telecommunication systems and networks / D.O. Danilenko, O.A. Smirnov, E.V. Meleshko // Weapons systems and military equipment. H .: Hark. nat. University of the Air Force. I. Kozheduba, 2012. № 1. Pp. 92-100.

8. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014.

9. Development of a model of intelligent recognition of anomalies and cyberattacks using logical procedures based on the coverage of feature matrices / G. Beketova, B. Akhmetov, O. Korchenko, V. Lakhno // Information Security. K: NAU, 2016. T. 22, № 3. Pp. 242-254.

10. Review of attack detection systems in network traffic / K.M. Nosenko, O.I. Pivtorak, T.A. Likhouzova // Adaptive automatic control systems. K: NTUU KPI, 2014. № 1 (24). Pp. 67-75.

11. Analysis of the system of detection of intrusions and computer attacks / M.M. Radchenko [etc.] // Interdisciplinary research in science and education. 2013. № 2.

12. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. Computer Network and Information Security, 2014. Vol. 8. Pp. 41-47.

13. Analysis of modern systems for detecting attacks and preventing invasion / A.A. Zavada, O.V. Samchyshyn, V.V. Okhrimchuk // Information systems. Zhytomyr: Collection of scientific works of ZhVI NAU, 2012. T. 6, №12. Pp. 97-106.

14. An implementation of intrusion detection system using genetic algorithm / Moham-mad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Net-work Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, no. 2. Pp. 109-120.

15. Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, no. 2. Pp. 169-184.

17. IDS / IPS. Netgate Documentation: [website]. Washington: Rubicon Communications LLC, 2017. [Electronic resource]. Online: https: //www.netgate. com / docs / pfsense / ids-ips /.

18. Dovbeshko S.V., Toliupa S.V., Shestak Y.V. Application of data mining methods to build attack detection systems. Scientific and technical journal "Modern information protection". - №1. 2019. Pp. 56-62.

19. Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection Volume 7, Issue 1 (12). with. 69-79.

20. Ghahramani, Z. An Introduction to hidden Markov models and Bayesian networks / Z. Ghahramani // International Journal of Pattern Recognition and Artificial Intelligence - 2001. - Vol. 15. - Pp. 9-42.

21. Barbara D. Detecting novel network intrusions using Bayes estimators / D. Barbara, J. Couto, S. Jajodia, N. Wu. // In: Proc. of the 1st SIAM International Conference on Data Min-ing. - 2001.

22. Kruegel, C. Bayesian event classification for intrusion detection / C. Kruegel, D. Mutz, W. Robertson, F. Valeur // In: Proc. of the 19th Annual Computer Security Applications Conference - 2003. - Pp. 14-23.

23. Toliupa S.V., Shtanenko S.S., Berestovenko G. Classification features of attack detection systems and directions of their construction. Collection of scientific works of the Military Institute of Telecommunications and Informatization named after Heroes of Kruty Issue № 3. 2018. with. Pp. 56-66.

24. Toliupa S.V., Druzhynin V.A., Parkhomenko I.I. Signature and statistical analyzers in the cyber attack detection system. Scientific and Practical Cyber Security Journal (SPCSJ) № 3 (02) September 2018. Pp. 47-53.

25. Valdes A. Adaptive model-based monitoring for cyber attack detection / A. Valdes, K. Skinner // In: Proc. of the Recent Advances in Intrusion Detection (Toulouse, France, 2000) - 2000. - Pp. 80-92.

26. Portnoy L. Intrusion detection with unlabeled data using clustering / L. Portnoy, E. Eskin, S. J. Stolfo // In: Proc. of ACM Workshop on Data Mining Applied to Security. - 2001. - Pp. 1-14.

Dr. Eng. Sc.Toliupa S., Ph.D. Pliushch O., Ph.D. Parhomenko I.

CONSTRUCTION OF SYSTEMS OF DETECTION OF INVASIONS INTO THE INFORMATI TON AND TELECOMMUNICATIONS NETWORK ON THE BASIS OF METHODS OF INTELLECTUAL DISTRIBUTION OF DATA

The article proposes a combinatorial construction of a network attack detection system based on selected methods of data mining and conducts experimental research that confirms the effectiveness of the created detection model to protect the distributed information network. Experiments with a software prototype showed the high quality of detection of network attacks and proved the correctness of the choice of methods of data mining and the applicability of the developed techniques.

The state of security of information and telecommunication systems against cyberattacks is analyzed, which allowed to draw conclusions that to ensure the security of cyberspace it is necessary to implement a set of systems and protection mechanisms, namely systems: delimitation of user access; firewall; cryptographic protection of information; virtual private networks; anti-virus protection of ITS elements; detection and prevention of intrusions; authentication, authorization and audit; data loss prevention; security and event management; security management.

An analysis of publications of domestic and foreign experts, which summarizes:

experience in building attack detection systems, their disadvantages and advantages;

construction of attack and intrusion detection systems based on the use of intelligent systems.

Based on the results of the review, proposals were formed on:

construction of network attack detection systems on the basis of selected methods of data mining and experimental research, which confirms the effectiveness of the created detection model for the protection of the distributed information network.

Keywords: cyberspace, attack, neural network, information and telecommunication network, attack detection systems, methods of data mining, training base.

УДК 004.771

д.т.н., проф. **Чернишев Д.О.** (КНУБА)
д.т.н., проф. **Хлапонін Ю.І.** (КНУБА)
к.т.н., доц. **Вишняков В.М.** (КНУБА)

DOI: https://doi.org/10.17721/2519-481X/2020/68-10

ДОСВІД ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ В ЗАКЛАДІ ВИШОЇ ОСВІТИ

Важливою проблемою на шляху розвитку електронної демократії є забезпечення довіри громадян до електронних систем голосування. Хоч існує чимало фактів впровадження таких систем, але у кожному разі виборці повинні приймати на віру, що персонал, який обслуговує систему, буде чесно і безпомилково виконувати роботу. Іншими словами, жодна з цих систем не надає виборцям достатніх і зрозумілих доказів про те, що таємниця їх голосів не може бути порушена, а результати підрахунку голосів не можуть бути сфальсифіковані. Відомо, що беззаперечною довірою виборців користуються системи, у яких громадяни виконують аудит усіх тих процедур, де можливі прояви шахрайства. Зараз такі системи є, але у них не використовується електронне голосування. Мета цієї роботи полягає у доведенні та практичному підтвердженні можливості побудови системи таємного електронного голосування у публічній мережі Інтернет з доступними для виборців засобами проведення аудиту усіх тих процесів, які можуть викликати недовіру під час проведення голосування. Проаналізовані принципи побудови систем електронного голосування з точки зору можливості забезпечення довіри громадян за рахунок повної відкритості для аудиту обраних програмно-апаратних рішень. Саме з використанням таких рішень побудована система, яку впроваджено у Київському національному університеті будівництва і архітектури для проведення виборів представників студентства до Ради студентського самоврядування. Також ця система використовується для проведення таємних голосувань на засіданнях Вченої Ради Університету у режимі online. Важливим практичним результатом даного впровадження є усунення обтяжливої процедури ручного підрахунку голосів, що у випадку засідання, яке відбулося 16 жовтня 2020 року, де кількість бюлетенів була 53, хоч з 85 членів Вченої Ради прийняли участь у голосуванні 53 (шестеро проголосували паперовими бюлетенями), полегшення було відчутним, бо в урні було на 2491 бюлетень менше. Крім того, комп'ютерний підрахунок є миттєвим і безпомилковим, а наявність автоматизованого аудиту усуває можливість для будь-яких підробок програмного забезпечення або позаштатного втручання персоналу у роботу сервера. Головна перевага звичайно та, що створюються умови для захисту від розповсюдження вірусної хвороби і не треба припиняти діяльність Вчених Рад під час карантину.

Ключові слова: електронна демократія, таємне електронне голосування у мережі Інтернет, довіра громадян до систем електронного голосування, прозорість побудови систем електронного голосування, автоматизований аудит системи електронного голосування.

Вступ. Однією з основних проблем на шляху розвитку електронної демократії є створення систем голосування, які б заслуговували на абсолютну довіру з боку громадян. Хоч існують факти впровадження подібних систем на рівні держав, але у кожному разі виборці повинні приймати на віру, що персонал, який обслуговує систему, буде чесно і безпомилково виконувати роботу. Іншими словами, жодна з цих систем не надає виборцям достатніх і зрозумілих доказів про те, що таємниця їх голосів не може бути порушена, а результати підрахунку голосів не можуть бути сфальсифіковані. Відомо, що беззаперечною довірою виборців користуються системи, у яких громадяни виконують аудит усіх тих процедур, де можливі прояви шахрайства. Наприклад, у громадян Італії не виникає підозр щодо чесності проведення виборів [1]. Слід зауважити, що там мова йде про голосування паперовими бюлетенями, де завдяки призначенню випадкових виборців для участі у підрахунку голосів і широкому доступі спостерігачів для аудиту усіх тих процесів, де можуть бути вчинені порушення, не виникає підстав для недовіри.

Метою цієї роботи є доведення та практичне підтвердження можливості побудови системи таємного електронного голосування у публічній мережі Інтернет з доступними для

виборців засобами проведення аудиту усіх тих процесів, які можуть викликати недовіру під час проведення голосування.

Аналіз опублікованих робіт. Метою цього аналізу є висвітлення шляхів щодо забезпечення довіри громадян до систем електронного голосування. Актуальність такого аналізу пояснюється тим, що наявність недовіри є фактором, який здатен завдати значну шкоду розвитку електронної демократії у цілому.

Кожна з робіт, яку ми проаналізуємо, висвітлює певну властивість системи електронного голосування, яка може претендувати на 100% довіру з боку громадян. Хоч не кожен громадянин зможе розібратись в особливостях електронних систем, але у сучасному суспільстві вже існує значна кількість фахівців яким це доступно. Важливо, що їх кількість зростає рік від року.

Перший крок у напрямку відкритості систем електронного голосування було зроблено відомим американським вченим Брюсом Шнайером, який у роботі [2] висловив рішучу заяву проти закритого програмного забезпечення машин для голосування. Він заявив: «Компанії, які виробляють ці машини, постійно стверджують, що вони повинні зберігати секретність свого програмного забезпечення з метою безпеки. Не вірте їм. У даному випадку секретність не має нічого спільного з безпекою.» Також у цій роботі Брюс Шнайер вказує на необхідність підвищення якості аудита програмного забезпечення систем електронного голосування і надає таку пораду щодо майбутніх розробок: «Якщо ми збираємось витрачати гроші на нові технології голосування, то є сенс витрачати їх на технології, які будуть спрощувати проблему, замість її ускладнення.» Фактично у цій роботі було закладено ідею створення простих і відкритих для аудиту систем електронного голосування, але ця ідея не була підтримана професійними розробниками, включаючи широко відому естонську систему електронного голосування [3]. Зрозуміло, що для професіоналів ідея спрощення не приваблива, бо це може негативно вплинути на їх фінансування. Як показує аналіз сучасних систем електронного голосування, їх продовжують ускладнювати [4]. Але ідею Брюса Шнайера було підтримано у студентській роботі «Відкрита система таємного голосування», яку опубліковано у 2014 у збірнику КНУБА (Київського національного університету будівництва і архітектури) [5]. У цій роботі обрано прості і досконалі рішення щодо забезпечення таємниці голосів виборців. По-перше, обрано серверну операційну систему *OpenBSD*, яка є єдиною сертифікованою в Україні для побудови систем захисту даних [6], а по-друге, для захисту персональних даних і голосів виборців обрано шифр Вернама, який забезпечує абсолютний захист даних від розкриття, що математично доведено в роботі [7]. Хоч використання цього шифру потребує виконання особливих умов, але перевагою є те, що виток даних під час передавання стає абсолютно неможливим, а це є важливою складовою для забезпечення довіри виборців. У таблиці надано перелік умов для абсолютного захисту даних під час передавання.

Таблиця

Умови забезпечення абсолютного захисту даних під час передавання

Умова	Опис виконання умови
Генерування випадкових бітових послідовностей (не псевдовипадкових)	Реалізовано метод генерування випадкових (не псевдовипадкових) бітів, який дозволяє генерувати випадкові послідовності на будь-якому комп'ютері, що описано у роботі [8].
Кожну випадкову бітову послідовність можна використовувати для шифрування тільки один раз	Для кожного сеансу зв'язку генеруються випадкові бітові послідовності незалежно одна від одної
Для обміну випадковими послідовностями бітів слід використовувати абсолютно захищений канал зв'язку	Обмін випадковими послідовностями бітів відбувається за алгоритмом Диффі- Хеллмана з такими параметрами, для яких у сучасних умовах не існує можливості розкриття даних.

У роботі [9] обґрунтовано вибір параметрів алгоритму Диффі-Хелмана для задачі електронного голосування, а у роботі [10] описано метод протидії атаці посередника, яка є можливою загрозою, у разі використання цього алгоритму.

Крім абсолютного захисту інформації від витоку під час передавання, для забезпечення 100% довіри щодо збереження таємниці голосів, слід також унеможливити виток інформації на сервері, де голоси розшифровуються і підраховуються. Це реалізовано завдяки операційній системі *OpenBSD*, яка дозволяє створювати захищену від будь-якого стороннього проникнення частину оперативної пам'яті, у якій підраховуються голоси. Ця технологія описана у роботі [11]. Таким чином, персональні дані виборців ніяк не можуть витікати зі сервера під час підрахунку голосів, бо їх розшифровка відбувається у захищеній частині оперативної пам'яті, де вони потрапляють на лічильник голосів, після чого ніякої інформації про те хто як голосував не залишається.

Крім збереження таємниці голосів для забезпечення повної довіри слід усунути можливість фальсифікації підрахунку голосів.

Зрозуміло, що у разі повної відкритості і багаторазового випробування програмного забезпечення, можна гарантувати відсутність помилок у підрахунку голосів, але не можна покладатись на чесність персоналу, який буде обслуговувати систему електронного голосування. Оскільки персонал, який зобов'язаний встановлювати і запускати програмне забезпечення, має можливість втручання у роботу сервера, то з метою недопущення з його боку позаштатних дій, у роботі [12] запропоновано проведення автоматизованого контролю усіх дій щодо управління сервером. При цьому кожен користувач мережі може проводити такий контроль. Але реалізація всього, що описано у перелічених роботах, може залишити привід для недовіри, бо потрібен ще контроль апаратних засобів, які розпізнають і підраховують голоси. У разі відсутності такого контролю може виникнути підозра, що зловмисник, з метою фальсифікації виборів, створив спеціалізоване обладнання, у якому закладено засоби імітації чесної роботи, а насправді є можливість втручання у процеси розпізнавання та підрахунку голосів. Усунути цю підозру дозволяє підхід, який описано у роботі [13], де запропоновано для серверів підрахунку голосів використовувати стандартні міні комп'ютери типу *Raspberry Pi* 3 з відкритим монтажем. При цьому, контролерам дозволено не тільки робити їх зовнішній огляд, але й підключати власні пристрої для копіювання файлів програмного забезпечення та виконання безпечних команд операційної системи. У таких умовах підробка серверного обладнання виходить за межі реальності через брак ресурсів для розміщення на цих міні комп'ютерах додаткового програмного забезпечення.

Усі перелічені технології реалізовані і надаються для голосування на серверах Державного підприємства ДНДІАСБ, яке є провайдером послуг у мережі Інтернет, про що свідчить інформація на їхньому сайті [14].

Електронне голосування у закладі вищої освіти. Згідно Плану заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019-2020, який затверджено КМУ 12 червня 2019 р. №450-р із змінами, внесеними згідно з Постановою КМ № 123 від 05.02.2020 року, в закладах вищої освіти слід впроваджувати інструменти електронного голосування в діяльність органів студентського самоврядування [15]. Крім того, 15 липня 2020 року Урядом України внесено зміни до Порядку присудження наукових ступенів. Ці зміни дозволяють проведення засідань в дистанційному режимі з використанням сучасних засобів відео зв'язку, але голосування повинно залишатись таємним і відбуватись з використанням програмного забезпечення, яке обирає сама рада [16].

Судячи з Плану заходів Уряду України, бачимо, що таке важливе питання розвитку електронної демократії, як впровадження електронного голосування, покладено в першу чергу на заклади вищої освіти (ЗВО). Цей підхід суттєво відрізняється від того, який існував довгий час у інших країнах, де повністю покладались на професійних розробників і отримали потік критики через неможливість забезпечення довіри громадян, що описано у багатьох роботах дослідників, наприклад у цих [1, 4, 17]. При цьому, крім робіт наших студентів та аспірантів,

немає жодної, де було б вказано про можливість забезпечення беззаперечної довіри виборців до е-голосування.

Проблема забезпечення довіри полягає у тому, що люди тільки у разі можливості безперервного аудиту від початку голосування до закінчення підрахунку голосів можуть позбутися недовіри. Оскілки аудит цих систем потребує спеціальних знань, то для досягнення довіри необхідно набуття знань у галузі ІТ. Тому План Уряду щодо першочергового впровадження засобів е-голосування у ЗВО є доцільним, бо потрібні знання набуваються саме у закладах вищої та середньої освіти. Крім того, якщо студенти самі активують і створюють розробки, то програмно-технічні рішення будуть простішими і зрозумілішими, а це іде на користь досягненню довіри. Саме з цих міркувань було прийнято наше рішення щодо обрання засобів таємного дистанційного голосування.

Для систем таємного електронного голосування у ЗВО не всі вимоги відповідають тим, що існують на рівні держав. Тому треба було внести зміни у програмне забезпечення, яке запропоновано нашими фахівцями для виборів на державному рівні. Слід було доповнити систему можливістю управління періодами голосування під час засідань або зборів у режимі *online*. Для цього створено спеціальний інтерфейс, через який представник лічильної комісії або секретар засідання може керувати процесом голосування. Цей інтерфейс показано на рис. 1.

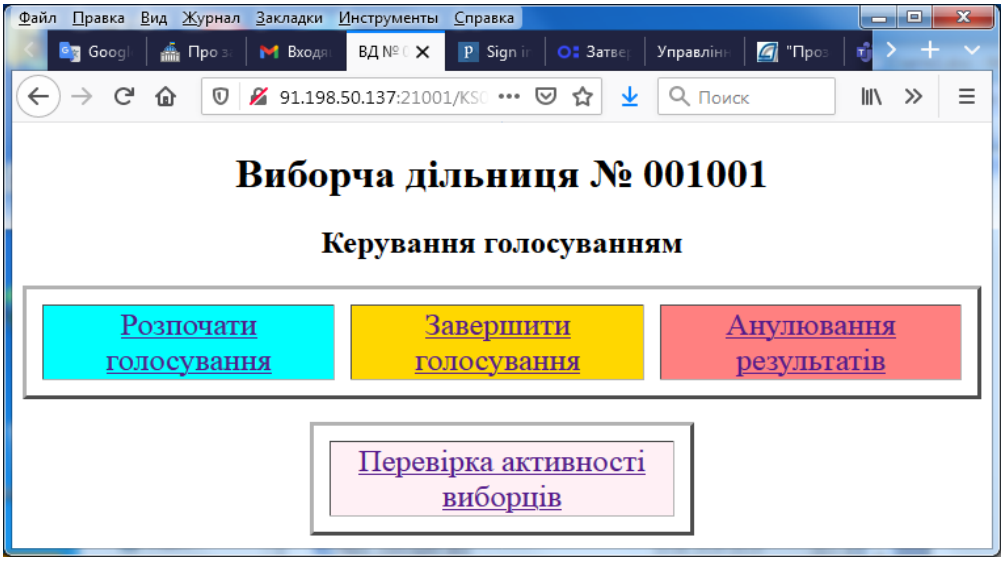


Рисунок 1 – Інтерфейс для управління процесом голосування

Через даний інтерфейс можна перевіряти активність виборців, що дозволяє у реальному часі дізнаватись хто вже проголосував. Це важливо у режимі *online*, бо можна нагадувати виборцям, які відволіклися, про необхідність проголосувати.

Поновлений інтерфейс виборців показано на рис. 2.

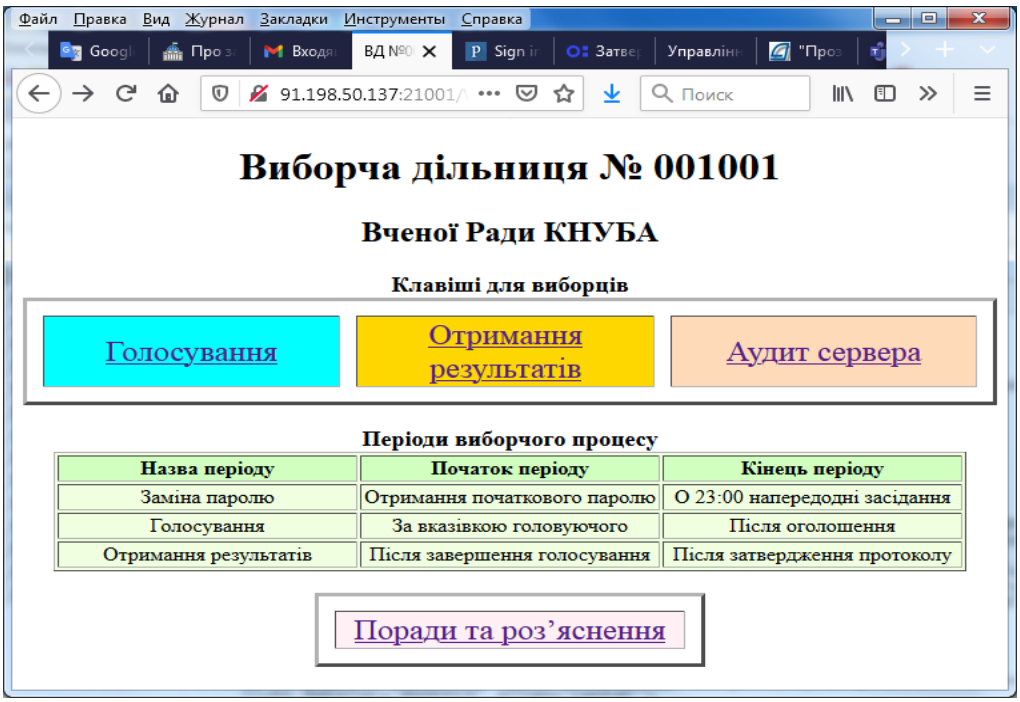


Рисунок 2 – Головний інтерфейс виборця

Вигляд бюлетенів для голосування на засіданні Вченої Ради показано на рис. 3, а сторінку з результатом голосування – на рис. 4.

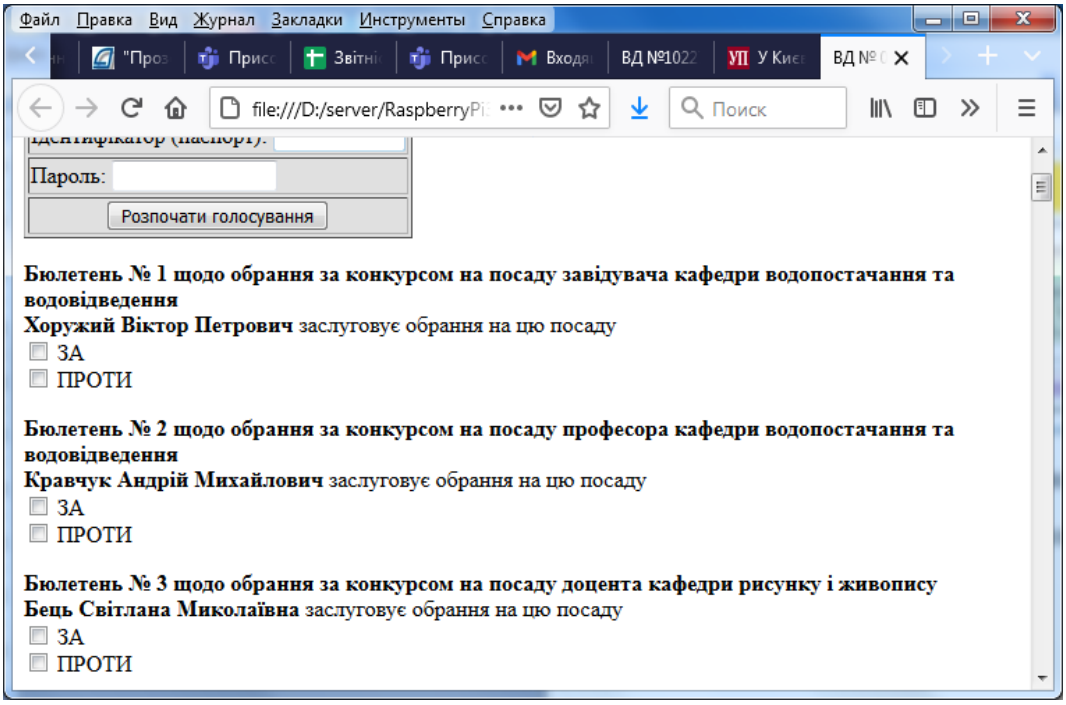


Рисунок 3 – Вигляд електронних бюлетенів на засіданні Вченої Ради

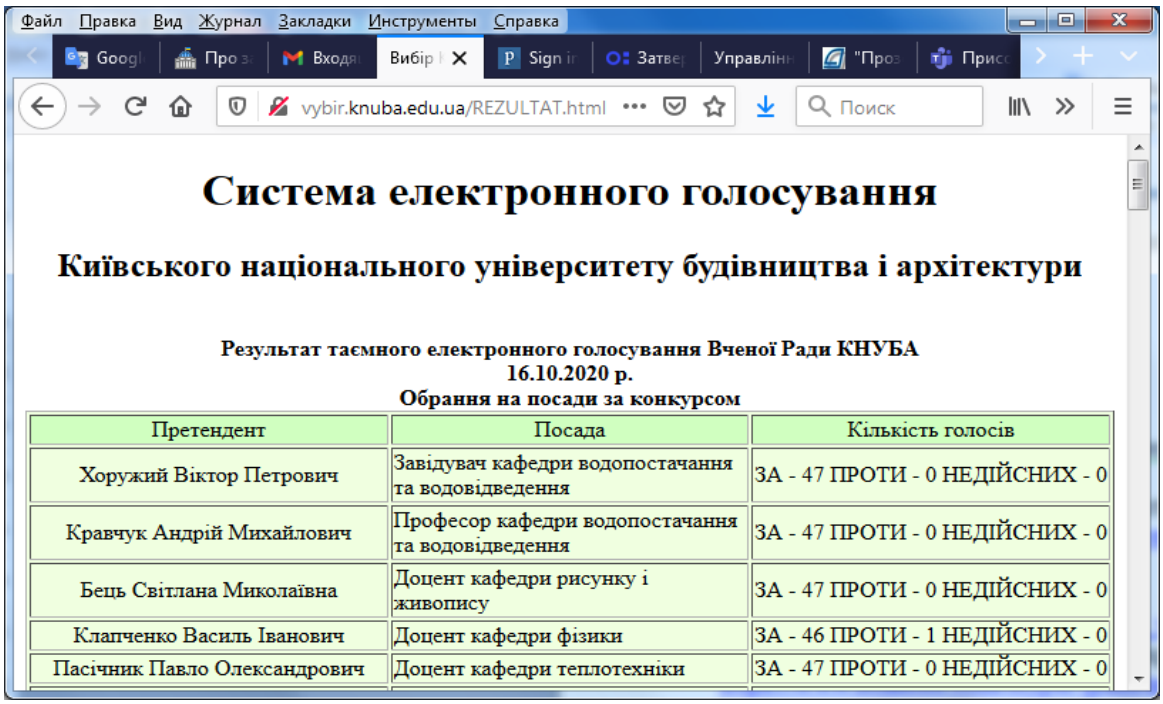


Рисунок 4 – Вигляд web сторінки з результатом голосування

Зміни у програмному забезпеченні з метою усунення зайвих перевірок, які не є доцільними у випадку проведення засідань або зборів у режимі *online*, були зроблені такі:

- усунено автентифікацію виборців по біологічним або іншим ознакам;
- усунено захист від впливу на виборців різними методами примусу.

При цьому в повному обсязі залишено такі властивості:

- абсолютну неможливість розкриття таємниці голосів;
- безперервний автоматизований контроль усіх програмно-апаратних засобів і процесів, які можуть стати приводом для недовіри виборців.

Слід зауважити, що аудит системи є доступним не тільки виборцям, а також і їх довіреним особам. Тому для проведення аудиту не обов'язково мати знання у галузі ІТ, а можна звернутись для цього до будь-яких фахівців.

Процедура підготовки до голосування полягає у тому, що реєстратор, якому адміністратор системи надає спеціальні повноваження, заповнює реєстр виборців по дільниці, яку він обслуговує. У цьому реєстрі, крім прізвища та ім'я слід вказати електронну пошту та унікальний ідентифікатор виборця, який є його початковим паролем. Ідентифікатори призначаються реєстратором за узгодженням з адміністратором таким чином, щоб не було повторень у межах установи. Для кожної групи голосуючих, наприклад, Вченої Ради, реєстр заповнюється одноразово, а перед кожним голосуванням слід лише вносити зміни та доповнення. Після занесення виборця до реєстру реєстратор відправляє йому повідомлення на електронну пошту. У цьому повідомленні надаються посилання для входу на web сторінку своєї виборчої дільниці та для заміни початкового паролю на свій постійний. Паролі виборці обирають і вводять самостійно від 8 до 16 символів на латинському регістрі. У будь-який момент до початку періоду голосування виборці можуть перевіряти та замінювати паролі. У разі, коли виборець не може пригадати пароль, реєстратор має можливість повернути йому початковий. Зауважимо, що реєстр виборців готується і зберігається на окремому комп'ютері, з якого на сервер голосування пересилається файл з паролями і ідентифікаторами у зашифрованому вигляді. Цей файл може пересилатись у відкритому вигляді, бо обраний шифр не підлягає розшифруванню. Таким чином на сервері голосування, де усі файли є відкритими для читання, не має персональних даних виборців, крім паролів і ідентифікаторів, які захищені шифром.

Процес голосування у переважній більшості випадків не викликає труднощів. Голосуючим, крім будь-якого пристрою з браузером і доступом до мережі Інтернет, нічого не потрібно. Усі процедури щодо управління системою голосування КНУБА, а також аудит серверів є у цілодобовому доступі за посиланням http://vybir.knuba.edu.ua/ через головну сторінку системи, що зображена на рис. 5, а сторінку для аудиту показано на рис. 6.

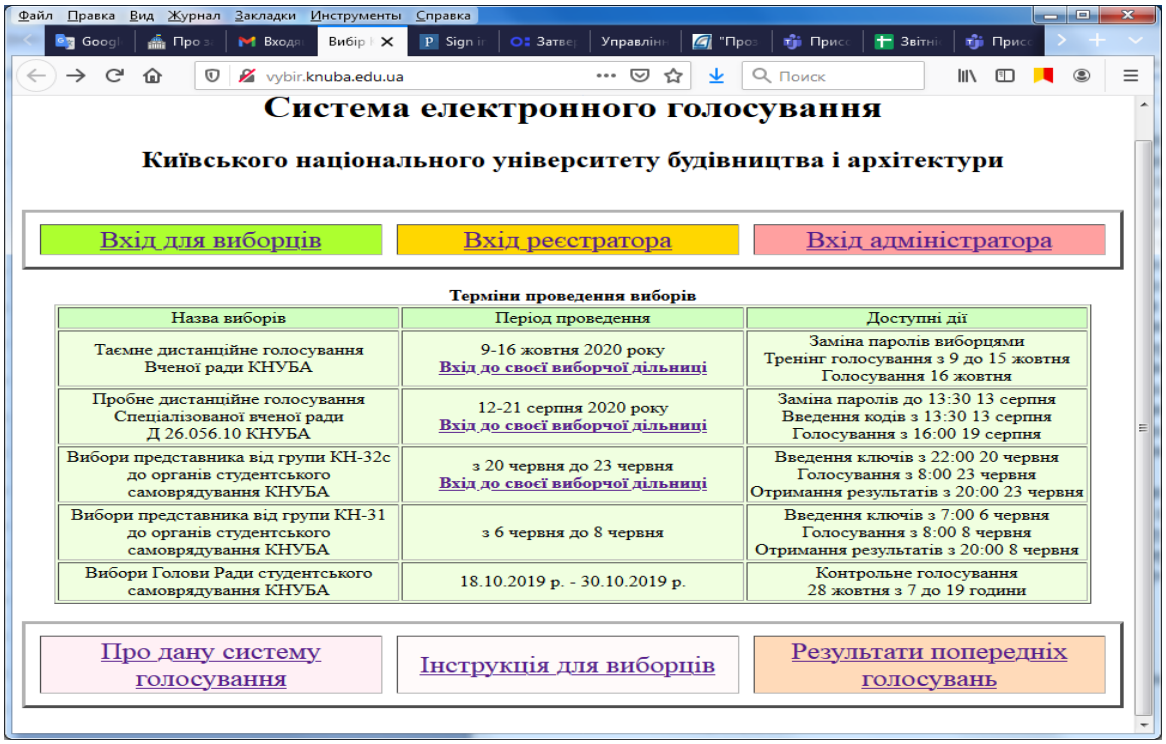


Рисунок 5 – Головна web сторінка Системи електронного голосування КНУБА

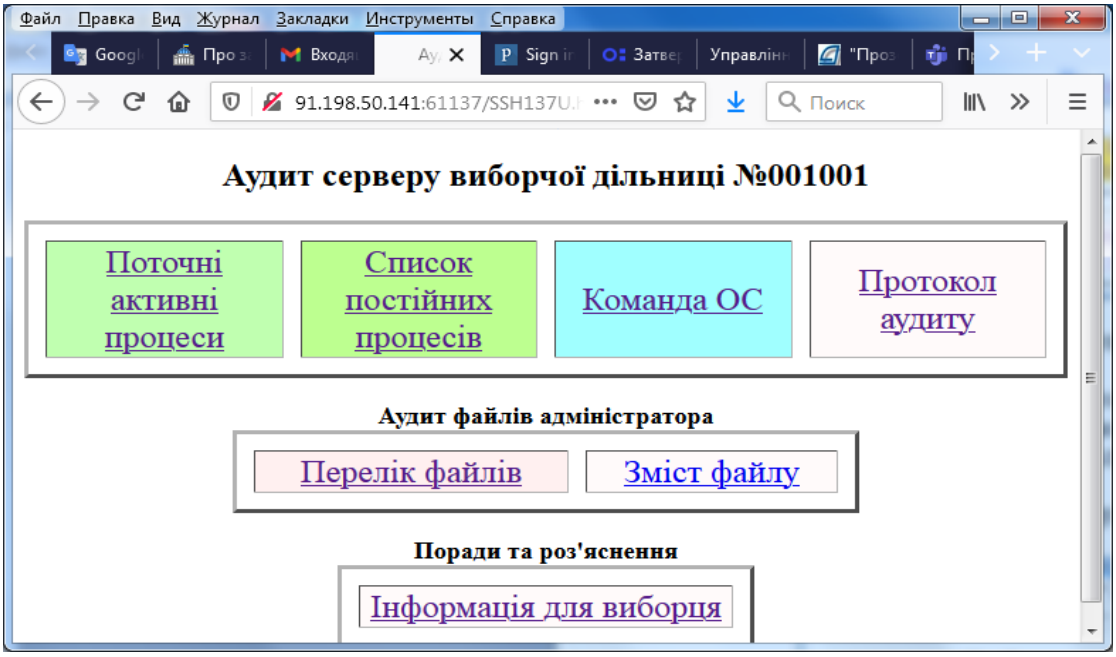


Рисунок 6 – Web сторінка для аудиту сервера Вченої Ради КНУБА

Важливою особливістю даної системи є повна відкритість і простота програмного забезпечення, яке створено з використанням лише двох широко відомих сучасних

комп'ютерних мов HTML і JavaScript. Це надає змогу її швидкого перетворення для різних застосувань, де необхідно збереження таємниці голосів і забезпечення захисту від шахрайства під час підрахунку.

Зовнішній вигляд серверного обладнання для голосування у режимі *online* представлено на рис. 7.

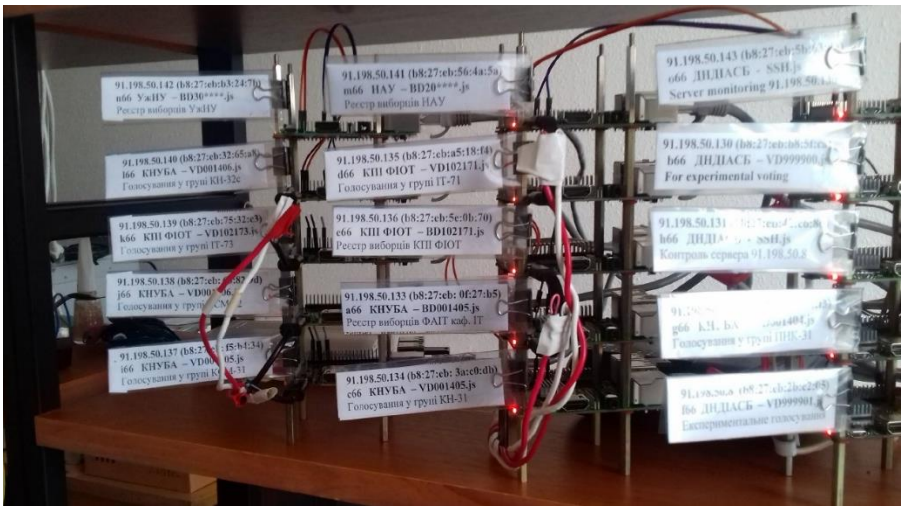


Рисунок 7 – Зовнішній вигляд серверного обладнання системи голосування

Для кожної виборчої дільниці за даною технологією *online* голосування призначається окремий сервер на міні комп'ютері типу *Raspberry Pi* 3 *B* з відкритим монтажем, що дозволяє аудиторам підключати свої контролюючі пристрої до потрібного сервера для повного контролю незалежно від інших серверів.

Також важливим практичним результатом є усунення обтяжливої процедури ручного підрахунку голосів, що у випадку засідання, яке відбулося 16 жовтня 2020 року, де кількість бюлетенів була 53, хоч з 85 членів Вченої Ради прийняли участь у голосуванні 53 (шестеро проголосували паперовими бюлетенями), полегшення було відчутним, бо в урні було на 2491 бюлетень менше. Крім того, комп'ютерний підрахунок є миттєвим і безпомилковим, а наявність автоматизованого аудиту усуває можливість для будь-яких підробок програмного забезпечення або позаштатного втручання персоналу у роботу сервера. Головна перевага звичайно та, що створюються умови для захисту від розповсюдження вірусної хвороби і не треба припиняти діяльність Вчених Рад під час карантину. З докладною інформацією щодо голосування на цьому засіданні Вченої Ради КНУБА у режимі *online* можна ознайомитись через наступне посилання http://www.knuba.edu.ua/?p=82428.

Висновки. Розглянуто принципи побудови та приклад впровадження системи таємного електронного голосування у закладі вищої освіти на засіданні Вченої Ради університету в режимі *online*.

Показано, що у цій системі забезпечено абсолютну таємницю голосів виборців за рахунок застосування досконалого методу шифрування під час пересилання даних по каналах мережі Інтернет та обробці даних у захищеній від будь-якого позаштатного втручання засобами операційної системи *OpenBSD* ділянці оперативної пам'яті сервера.

Описано можливості та методи проведення аудиту усіх програмних та апаратних засобів і процесів, які можуть викликати недовіру виборців під час проведення голосування, що дозволяє забезпечити повну довіру до даної системи за рахунок її 100% відкритості.

ЛІТЕРАТУРА:

1. Lombardi E. Electronic Vote & Democracy. May 2020. [Електронний ресурс] Режим доступу: http://www.electronic-vote.org.

2. Schneier B. What's Wrong With Electronic Voting Machines? November 2004. [Електронний ресурс] Режим доступу: https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html.

3. Electronic voting in Estonia. [Електронний ресурс] Режим доступу: https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia

4. Schneier B. Voatz Internet Voting App Is Insecure. March 15, 2020. [Електронний ресурс] Режим доступу: https://www.schneier.com/crypto-gram/archives/2020/0315.html

5. Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування. *Управління розвитком складних систем. Збірник наукових праць*, 2014, №20.- С. 110 – 115.

6. Первая и единственная UNIX-подобная защищённая операционная система в Украине. [Електронний ресурс] Режим доступу: https://www.atmnis.com

7. Shannon C. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949. 28 (4). Pp. 656-715.

8. Чуприн В.М. Генерування випадкових чисел штатними засобами хостів мережі Інтернет / В.М. Чуприн, В.М.Вишняков, М.П. Пригара // *Захист інформації*. – 2016. – Т. 18, №4. – С. 323-335.

9. Чуприн В.М., Вишняков В.М., Пригара М.П. Метод протидії незаконному впливу на виборців у системі Інтернет голосування. *Безпека інформації*. – 2017. – Том 23, №1. – С. 7–14.

10. Чуприн В.М., Вишняков В.М., Комарницький О.О., Метод протидії атакам посередника у транспарентній системі інтернет голосування, *Захист інформації, Ukrainian Information Security Research Journal*. - К.: НАУ, 2019. – Т.20. - №2. – С.172-182.

11. Чуприн В.М. Захист операційного середовища систем Інтернет голосування./ В.М. Чуприн, В.М.Вишняков, М.П. Пригара // *Захист інформації*. – 2017. – Т. 19, №1 – С. 56-66.

12. Вишняков В.М., Комарницький О.О., Жуковський А.О., Методи контролю керування системою Інтернет голосування, *Управління розвитком складних систем*. – 2019. - № 38 – С. 37-44.

13. Вышняков В.М., Комарницкий О.А. Транспарентные системы электронной демократии. Accent Graphics Communications & Publishing, Оттава, Канада. 2019. – 96 с.

14. Експериментальне голосування [Електронний ресурс] Режим доступу: http://www.asdev.com.ua/dndiasb/news/lates_news/eksperimentalne-golosuvannya.html

15. Про затвердження плану заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019-2020 роки. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/405-2019-%D1%80/sp:max10#Text

16. Про внесення змін до Порядку присудження наукових ступенів. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/607-2020-%D0%BF#n8

17. Голубицкий С. Мутная технология. Уроки московских выборов на блокчейне. 30 сентября 2019 г [Електронний ресурс] Режим доступу: https://новаягazeta.ru/articles/2019/09/30/82175-mutnaya-tehn o logiya.

REFERENCES:

1. Lombardi, E. (2020) *Electronic Vote & Democracy*. Available at: http://www.electronic-vote.org (Accessed: 23 November 2020).

2. Schneier, B. (2004) *What's Wrong With Electronic Voting Machines?* Available at: https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html (Accessed: 23 November 2020).

3. 'Electronic voting in Estonia' *Wikipedia*. Available at https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia (Accessed: 23 November 2020).

4. Schneier, B. (2020) Voatz *Internet Voting App Is Insecure. March 15, 2020*. Available at: https://www.schneier.com/crypto-gram/archives/2020/0315.html (Accessed: 23 November 2020).

5. Vyshniakov, V.M., Prygara, M.P. and Voronin O.V. (2014)," Vidkryta systema tayemnoho holosuvannya" [The system of secret ballot is open], Upravlinnya rozvytkom skladnykh system. Zbirnyk naukovyh prac', No. 20, pp. 110 – 115.

6. *First UNIX-like operating system in Ukraine*. (2017) Available at: https://www.atmnis.com . (Accessed: 23 November 2020).

7. Shannon, C. (1949) "Communication Theory of Secrecy Systems", Bell System Technical Journal, No. 28 (4), pp. 656–715.

8. Chupryn, V.M., Vyshniakov, V.M. and Prygara, M.P. (2016) Heneruvannya vypadkovykh chysel shtatnymy zasobamy khostiv merezhi Internet [Generation of random numbers by regular means of Internet hosts], Zakhyst informatsiyi, T. 18, No. 4, pp. 323-335.

9. Chupryn, V.M., Vyshniakov, V.M. and Prygara, M.P. (2017) Metod protydiyi nezakonnomu vplyvu na vybortsiv u systemi Internet holosuvannya [Method of counteracting illegal influence on voters in the Internet voting system], Bezpeka informatsiyi, T. 23 No. 1, pp. 7–14.

10. Chupryn, V.M., Vyshniakov, V.M. and Komarnitskiy, O.O. **(2019)** Metod protydiyi atakam poserednyka u transparentniy systemi internet holosuvannya [A method of counteracting the attacks of a mediator in a transparent Internet voting system], Zakhyst informatsiyi. *Ukrainian Information Security Research Journal*, T. 20, No. 2, pp. 172-182.

11. Chupryn, V.M., Vyshniakov, V.M. and Prygara, M.P. (2017) Zakhyst operatsiynoho seredovyshcha system Internet holosuvannya [Protection of the operating environment of Internet voting systems], Zakhyst informatsiyi, T. 19, No.14, pp. 56-66.

12. Vyshniakov, V.M., Komarnitskiy, O.O. and Zhukovs′kyy A.O. (2019) Metody kontrolyu keruvannya systemoyu Internet holosuvannya [Methods of control over the management of the Internet voting system], Upravlinnya rozvytkom skladnykh system. Zbirnyk naukovyh prac', No. 38, pp. 37-44.

13. Vyshniakov, V.M. and Komarnitskiy, O.O. (2019)**,** "Transparentnyye sistemy elektronnoy demokratii" [Transparent systems of e-democracy], Accent Graphics Communications & Publishing, Ottawa, Canada, 96 p.

14. *Eksperymental'ne holosuvannya.* (2020). Available at: http://www.asdev.com.ua/dndiasb/news/lates_news/eksperimentalne-golosuvannya.html. (Accessed: 23 November 2020)

15. *Pro zatverdzhennya planu zakhodiv shchodo realizatsiyi Kontseptsiyi rozvytku elektronnoyi demokratiyi v Ukrayini na 2019-2020 roky*. (2019). Available at: https://zakon.rada.gov.ua/laws/show/405-2019-%D1%80/sp:max10#Text. (Accessed: 23 November 2020)

16. *Pro vnesennya zmin do Poryadku prysudzhennya naukovykh stupeniv*. (2020). Available at: https://zakon.rada.gov.ua/laws/show/607-2020-%D0%BF#n8. (Accessed: 23 November 2020).

17. Golubitskiy, S. (2019). *Mutnaya tekhnologiya. Uroki moskovskikh vyborov na blokcheyne*. Available at: https://новаяgazeta.ru/articles/2019/09/30/82175-mutnaya-tehn o logiya. (Accessed: 23 November 2020).

Dr. Eng. Sc. Chernyshev D.O., Dr. Eng. Sc. Khlaponin Y.I., Ph.D. Vyshniakov V.M.

EXPERIENCE OF INTRODUCTION OF ELECTRONIC VOTING IN HIGHER EDUCATION INSTITUTIONS

An important problem on the way to the development of e-democracy is to ensure citizens' confidence in electronic voting systems. Although there are many cases of implementation of such systems, in all cases, voters must take it on faith that the personnel serving the system will honestly and accurately perform the work. In other words, none of these systems provide voters with sufficient and understandable evidence that the secret of their votes cannot be revealed and the results of the vote count cannot be falsified. It is known that the systems in which citizens perform audits of all those procedures where fraudulent manifestations are possible, enjoy the indisputable trust of voters. Now such systems exist, but they do not use electronic voting. The purpose of this work is to prove and practical confirmation of the possibility of building a system of secret electronic voting on the public Internet with means available to voters for auditing all those processes that may cause distrust during voting. The principles of constructing e-voting systems are analyzed from the point of view of the possibility of ensuring the trust of citizens through complete openness for auditing selected software and hardware solutions. It was with the use of such solutions that the system was built, which was implemented at the Kiev National University of Construction and Architecture for the election of student representatives to the Student Self-Government Council. Also, this system is used to conduct secret voting at meetings of the Academic Council of the University online. An important practical result of this implementation is the elimination of cumbersome manual counting procedures. In the case of the meeting that took place on October 16, 2020, where the number of ballots was 53, although 53 out of 85 members of the Academic Council took part in the vote (six voted with paper ballots), the relief was tangible, because there were 2,491 fewer ballots in the ballot box. In addition, computerized counting is instant and error-free, and the presence of automated auditing eliminates the possibility for any software tampering or unauthorized personnel interference with the server. The main advantage, of course, is that conditions are created to protect against the spread of a viral infection and there is no need to stop the activities of the Scientific Councils during quarantine.

Keywords: e-democracy, secret e-voting on the Internet, citizens' confidence in e-voting systems, transparency of building e-voting systems, automated audit of e-voting systems.

ЗАГАЛЬНІ ПИТАННЯ

УДК 355.211.3

к.військ.н. **Георгадзе О.А.** (НУОУ)
к.військ.н. **Шевчук В.В. (**НУОУ)
к.т.н., доц. **Пампуха І.В.** (ВІКНУ)
к.військ.н. **Нікіфоров М.М.** (ВІКНУ
Баргилевич А.В. (КСВ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-11

ОБҐРУНТУВАННЯ УЗАГАЛЬНЕНОГО ПОКАЗНИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПІДГОТОВКИ ОКРЕМОЇ БРИГАДИ ТЕРИТОРІАЛЬНОЇ ОБОРОНИ ЗБРОЙНИХ СИЛ УКРАЇНИ

За результатами аналізу командно-штабних тренувань підрозділів територіальної оборони, наукових досліджень з визначення підходів до оцінювання ефективності підготовки військових частин запропонована сукупність показників ефективності підготовки підрозділів територіальної оборони Збройних Сил України. Узагальненим показником оцінювання ефективності визначено досягнення визначених бойових спроможностей, що залежить від готовності до виконання завдань таких складових як управління кадру, організаційне ядро та підрозділів бригади територіальної оборони.

Показник, як інструмент вимірювання, має відображати рівень прояву певної властивості об'єкта. Визначення обґрунтованих показників оцінювання ефективності підготовки окремої бригади територіальної оборони має надзвичайно важливе теоретичне і практичне значення. Обґрунтування критерію та сукупності показників оцінювання ефективності підготовки окремої бригади територіальної оборони являється складним завданням дослідження. У практичному плані сукупність показників оцінювання ефективності підготовки окремої бригади територіальної оборони є наслідком діяльності відповідних соціально-технічних систем (структур, органів суб'єктів територіальної оборони), які створюються для виконання завдань. Для оцінювання ефективності підготовки окремої бригади територіальної оборони використовуються складні показники, які можуть узагальнювати певні обсяги інформації і разом з тим зберігатимуть об'єктивність оцінок, що в окремих випадках, зокрема при вирішенні нових завдань, може передбачати необхідність синтезу (об'єднання раніше розрізнених понять і цілей), формулювання нових показників та алгоритмів їх розрахунку. За результатами аналізу командно-штабних тренувань підрозділів територіальної оборони і наукових досліджень з визначення підходів до оцінювання ефективності підготовки військових частин запропонована сукупність показників ефективності підготовки підрозділів територіальної оборони Збройних Сил України. Узагальненим показником оцінювання ефективності визначено досягнення визначених бойових спроможностей, що залежить від готовності до виконання завдань таких складових як управління кадру, організаційне ядро та підрозділів бригади територіальної оборони та може бути використаним для розроблення часткової методики оцінювання ефективності підготовки організаційного ядра окремої бригади територіальної оборони.

Ключові слова: територіальна оборона, застосування, ефективність, оцінювання, показники.

Вступ. Визначення обґрунтованих показників оцінювання ефективності підготовки окремої бригади територіальної оборони (обр ТрО) має надзвичайно важливе теоретичне і практичне значення.

У теоретичному плані показники є ключовою ланкою в переході від теоретичних до методологічних засад дослідження об'єктів і визначають напрями збору й узагальнення емпіричної інформації про них а також здійснюють зворотній зв'язок через аналіз і тлумачення отриманих даних.

У практичному плані сукупність показників оцінювання ефективності підготовки обр ТрО є наслідком діяльності відповідних соціально-технічних систем (структур, органів

суб'єктів ТрО), які створюються для виконання завдань.

Аналіз попередніх досліджень та публікацій. Аналіз попередніх досліджень та публікацій з даного напряму [1-6] свідчить про те, що вони базуються на оцінюванні ефективності оперативної та бойової підготовки. Дослідники виходили з тих наукових завдань, які були породжені актуальними проблемами того часу, та застосовували критерії та показники, які найбільш повно відбивали процеси, що розглядалися. Детальний аналіз запропонованого в цих роботах науково-методичного апарату свідчить, що вони дозволяють оцінити окремі характеристики, але не у повній мірі спроможні врахувати зміни, які відбулися в системі підготовки ЗС України з впровадженням нових доктринальних документів [7-9] та не коректно оцінюють готовність бригад ТрО ЗС України до виконання завдань за призначенням.

Мета статті. Відповідно логічним буде визначити, що метою статті є обґрунтування ефективного стану необхідної системи, а саме обр ТрО. При цьому, така система повинна відповідати всім логічним послідовним складовим ефективності підготовки такої бригади для досягнення очікуваного результату.

Постановка проблеми. Показник, як інструмент вимірювання, має відображати рівень прояву певної властивості об'єкта. У найбільш загальному вигляді показник – це будь-яка реальна чи потенційна характеристика об'єкта, що може бути емпірично перевірена. Показники можуть бути якісними і кількісними. Якісні показники констатують наявність або відсутність певної характеристики об'єкта: виконано – не виконано, є – немає. Кількісні показники відображають рівень прояву властивості в чисельному значенні. Вони можуть бути дискретними (що можуть набувати лише певних значень) і безперервними (що набувають будь-яких значень). Існує низка класифікацій показників: вони можуть бути одиничними, груповими, абсолютними, відносними, порівняльними, контекстуальними, аналітичними, структурними, простими, складними, глобальними, тощо [10].

Прості типи показників порівняно легко розраховуються, але вимагають додаткового аналізу й інтерпретації, що досить часто невиправдано знижує об'єктивність дослідження. Крім того, опис об'єктів високої складності вимагає надзвичайно великої кількості простих показників, що може призвести до невиправданого зростання обсягів інформації, необхідної для аналізу та надмірних витрат часових і трудових ресурсів. Тому для оцінювання ефективності підготовки об ТрО доцільно використовувати складні показники, які можуть узагальнювати певні обсяги інформації і разом з тим зберігатимуть об'єктивність оцінок, що в окремих випадках, зокрема при вирішенні нових завдань, може передбачати необхідність синтезу (об'єднання раніше розрізнених понять і цілей), формулювання нових показників та алгоритмів їх розрахунку.

Виклад основного матеріалу. Обґрунтування критерію та сукупності показників оцінювання ефективності підготовки обр ТрО являється складним завданням дослідження. Такий критерій повинен бути презентабельним, обчислювальним та стійким до вхідних змін, окрім того – характеризувати вплив підготовки на готовність обр ТрО до виконання завдань за призначенням. Разом з тим, необхідно врахувати і те, що визначений критерій повинен відповідати основному завданню дослідження, його фізичний зміст підтверджувати ступінь досягнення мети дослідження.

За критерій ефективності підготовки обр ТрО приймаємо величину оцінки узагальненого показника, який відповідає меті функціонування та готовності до виконання завдань [11]. Він складається з сукупності кількісних (якісних) інтегральних показників, що відображають окремі властивості, які впливають на нього.

Враховувати необхідно і те, що підготовка обр ТрО це цілеспрямований процес навчання військовослужбовців управлінь кадру та резервістів, військовозобов'язаних, організаційного ядра а також злагодження підрозділів, який спрямований на досягнення їх готовності до виконання завдань за призначенням.

Для аналізу проведених заходів підготовки підрозділів ТрО було застосовано системний підхід, який дозволив визначити ієрархію її побудови та провести декомпозицію за елементами. Основними елементами підготовки обр ТрО у відповідності до [9] є: суб'єкти й

об’єкти підготовки, ресурси підготовки та навчальна матеріальна технічна база.

Виходячи з того, що підготовка обр ТрО являється комплексною категорією та багатошаровою, тож для отримання доцільного варіанту оцінки її ефективності потрібно застосувати системний підхід, який передбачає багатокритеріальне оцінювання, а отже, оцінка буде описана багатокритеріальною залежністю, яка характеризуватиметься найбільш істотними показниками, котрі можуть різнитися природою, вектором направленості та інтенсивністю впливу. Чим буде забезпечена її більша точність.

Під час підготовки обр ТрО вирішується низка завдань і реалізується значна кількість функцій, які на різних етапах діяльності мають відмінну значимість і тому неоднаково позначаються на узагальнений показник.

Таким чином, узагальнений показник оцінки ефективності підготовки обр ТрО повинен відповідати кінцевій меті дослідження, включати сукупність складових підготовки, а також бути адекватним. Фізичний зміст узагальненого показника повинен вказувати на ступінь досягнення кінцевої мети підготовки – готовності до виконання завдань за призначенням (набуття визначених бойових спроможностей).

Тому, основним критерієм ефективності підготовки обр ТрО доцільно вибрати безрозмірну величину $P_{ВБС}(t)$, якій надамо описані вище характеристики на фрагментарний час t. Обираємо її в якості узагальненого показника, за допомогою якого будемо визначати рівень готовності обр ТрО виконати завдання за призначенням.

Узагальнений показник, рівень готовності обр ТрО до виконання завдань за призначенням $P_{ВБС}(t)$, є безрозмірною величиною що перебуває діапазоні від 0 до 1, приймаюче таке значення математична залежність набуває виразу:

$$0 < P_{ВБС}(t) \le 1. \qquad (1)$$

Пропонується мати систему показників, яка буде складатися з узагальненого показника, інтегральних показників та часткових показників. Інтегральні показники, часткові показники також є безрозмірними величинами, тому їх значення також приймаються в межах від 0 до 1.

Ефективність складових підготовки обр ТрО пропонується оцінювати за інтегральними показниками, які здійснюють безпосередній вплив на рівень готовності обр ТрО до виконання завдань за призначенням. До таких показників відносяться: “готовність управлінь кадру” “готовність організаційного ядра” та “готовність підрозділів”, які характеризують готовність обр ТрО виконувати завдання за призначенням.

Така математична залежність матиме наступний вигляд:

$$P_{ВБС}(t) = f_{ВБС}\left\{ P_{ГУпК}(t); P_{ГОрЯ}(t); P_{Гп}(t) \right\}, \qquad (2)$$

де $P_{ГУпК}(t)$ – інтегральний показники “готовність управління кадру”, на фрагментарний момент часу;

$P_{ГОрЯ}(t)$ – інтегральний показники “готовність організаційного ядра”, на фрагментарний момент часу;

$P_{Гп}(t)$ – інтегральний показники “готовність підрозділів”, на фрагментарний момент часу.

Кожен з інтегральних показників складається із сукупності часткових показників, які характеризують і розкривають їх фізичний зміст та визначатимуть відповідний рівень у безрозмірній величині.

Фізичний зміст інтегрального показника “готовність управління кадру” $P_{ГУпК}(t)$ полягає в тому, що він характеризує спроможність управлінь кадру обр ТрО на час t здійснювати планування і проведення мобілізаційного розгортання, а також заходів бойового злагодження обр ТрО. Його пропонується розраховувати за функціональною залежністю, яка враховує спроможність t-го управління кадру обр ТрО (управління кадру обр ТрО та управлінь кадру обр ТрО тобто підрозділу бригади) до виконання завдань за призначенням:

$$P_{ГУпК}(t) = f_{ГУпК}\left\{ P_{ГУпКПi}(t) \right\}. \quad (3)$$

Рівень готовності t-го управління кадру обр ТрО залежить від організації підготовки t-го управління кадру обр ТрО, його укомплектованості і навченості. Тоді математична залежність набуває такий вигляд:

$$P_{ГУпКПi}(t) = f_{ГУпКПi}\left\{ M_{ОРi}(t); M_{Уi}(t); M_{Нi}(t) \right\}, \quad (4)$$

де $M_{ОРi}(t)$ – показник "організація підготовки t-го управління кадру підрозділу", на фрагментарний момент часу;

$M_{Уi}(t)$ – показник "укомплектованість t-го управління кадру підрозділу особовим складом" на фрагментарний момент часу;

$M_{Нi}(t)$ – показник "навченість t-го штабу" на фрагментарний момент часу.

Приймаємо, що на початок циклу підготовки управління кадру обр ТрО, укомплектовані особовим складом на 100%, тому показник $M_{Уi}(t)$ приймаємо рівним одиниці, тоді вираз (4) можна записати у такому вигляді:

$$P_{ГУпКПi}(t) = f_{ГУпКПi}\left\{ M_{ОРi}(t); M_{Нi}(t) \right\}. \quad (5)$$

Фізичний зміст інтегрального показника "готовність організаційного ядра" $P_{ГОрЯ}(t)$ на час t полягає в тому, що він характеризує спроможність резервістів та військовозобов'язаних, здійснювати першочергові мобілізаційні заходи підготовки до відмобілізування та приведення у бойову готовність підрозділів обр ТрО. Його пропонується розраховувати за функціональною залежністю, яка враховує спроможність t-го організаційного ядра обр ТрО до виконання завдань за призначенням:

$$P_{ГОрЯ}(t) = f_{ГОрЯ}\left\{ P_{ГОрЯ}(t) \right\}. \quad (6)$$

Рівень готовності g-го організаційного ядра обр ТрО залежить від організації його підготовки укомплектованості і Таким чином математичний вираз залежності набуває вигляд:

$$P_{ГОрЯ}(t) = f_{ГОрЯ}\left\{ M_{ОРg}(t); M_{Уg}(t); M_{Нg}(t) \right\}, \quad (7)$$

де $M_{ОРg}(t)$ – показник "організація підготовки g-го організаційного ядра", на фрагментарний момент часу;

$M_{Уg}(t)$ – показник "укомплектованість g-го організаційного ядра особовим складом" на фрагментарний момент часу;

$M_{Нg}(t)$ – показник "навченість g-го організаційного ядра" на фрагментарний момент часу.

Приймаємо, що на початок циклу організаційне ядро, укомплектовані особовим складом на 10% від укомплектованості бригади тобто 100 % організаційного ядра, тому показник $M_{Уg}(t)$ приймаємо рівним одиниці, тоді математичну залежність (7) можна записати у такому вигляді:

$$P_{ГОрЯ}(t) = f_{ГОрЯі}\left\{ M_{ОРg}(t); M_{Нg}(t) \right\}. \quad (8)$$

Фізичний зміст інтегрального показника "готовність підрозділів" $P_{Гп}(t)$ полягає в тому, що він характеризує спроможність підрозділів обр ТрО на час t виконати завдання за призначенням. Його пропонується розраховувати за функціональною залежністю, яка враховує спроможність k-го підрозділу обр ТрО виконати завдання за призначенням:

$$P_{Гп}(t) = f_{Гп}\left\{ P_{Гпk}(t) \right\}. \quad (9)$$

Рівень готовності k-го підрозділу обр ТрО залежить від організації підготовки k-го підрозділу, його укомплектованості і навченості. Тоді функціональна залежність матиме наступний вигляд:

$$P_{Гпk}(t) = f_{Пk}\left\{ M_{ОРk}(t); M_{Уk}(t); M_{Нk}(t) \right\}, \quad (10)$$

де $M_{ОРk}(t)$ – показник "організація підготовки k-го підрозділу", на фрагментарний момент часу;

$M_{Уk}(t)$ – показник "укомплектованість k-го підрозділу особовим складом" на фрагментарний момент часу;

$M_{Нk}(t)$ – показник "навченість k-го підрозділу" на фрагментарний момент часу.

Будемо вважати, що на початок циклу підготовки підрозділи обр ТрО укомплектовані особовим складом на 100%, тому показник $M_{Уk}(t)$ приймаємо рівним одиниці, тоді вираз (10) можна записати наступним чином:

$$P_{Гпk}(t) = f_{Пk}\left\{ M_{ОРk}(t); M_{Нk}(t) \right\}. \quad (11)$$

Для оцінювання організації підготовки суб'єктами підготовки і навченості об'єктів підготовки пропонується використовувати часткові показники.

Частковий показник "організація підготовки i-го управління кадру $M_{ОРi}(t)$ та g-го організаційного ядра $M_{ОРg}(t)$ (k-го підрозділу $M_{ОРk}(t)$)" залежить від повноти і якості планування підготовки i-го управління кадру та g-го організаційного ядра (k-го підрозділу), а також достатності ресурсного забезпечення заходів підготовки i-го управління кадру та g-го організаційного ядра (k-го підрозділу). Таким чином функціональна залежність набуває наступного математичного вигляду:

$$M_{ОРi}(t) = f_{ОРi}\left\{ C_{ПЛi}(t); C_{РЗi}(t) \right\}, \quad (12)$$

$$M_{ОРg}(t) = f_{ОРg}\left\{ C_{ПЛg}(t); C_{РЗg}(t) \right\} \quad (13)$$

$$M_{ОРk}(t) = f_{ОРk}\left\{ C_{ПЛk}(t); C_{РЗk}(t) \right\}, \quad (14)$$

де $C_{ПЛ}(t)$ – показник "планування підготовки i-го управління кадру, а також g-го організаційного ядра (k-го підрозділу)", на фрагментарний момент часу;

$C_{РЗ}(t)$ – показник "укомплектованість k-го підрозділу особовим складом" на фрагментарний момент часу;

Частковий показник "навченість i-го управління кадру $M_{Нi}(t)$ та g-го організаційного ядра $M_{Нg}(t)$ (k-го підрозділу $M_{Нk}(t)$)" залежить від сукупного рівня індивідуальних спроможностей кожного військовослужбовця, управління кадру та резервіста, військовозобов'язаного організаційного ядра (підрозділу) та їх злагодженості. Тоді функціональна залежність матиме наступний вигляд:

$$M_{Нi}(t) = f_{Нi}\left\{ C_{ICi}(t); C_{Зi}(t) \right\}, \quad (15)$$

$$M_{Нg}(t) = f_{Нg}\left\{ C_{ICg}(t); C_{Зg}(t) \right\}, \quad (16)$$

$$M_{Нk}(t) = f_{Нk}\left\{ C_{ICk}(t); C_{Зk}(t) \right\}, \quad (17)$$

де $C_{IC}(t)$ – показник "сукупний рівень індивідуальних спроможностей військовослужбовців i-го управління кадру, а також g-го резервістів, військовозобов'язаних організаційного ядра (k-го підрозділу)", на фрагментарний момент часу;

$C_з(t)$ – показник “укомплектованість k-го підрозділу особовим складом” на фрагментарний момент часу;

Система показників, яка використовується для оцінювання ефективності підготовки обр ТрО наведена на рис. 1.

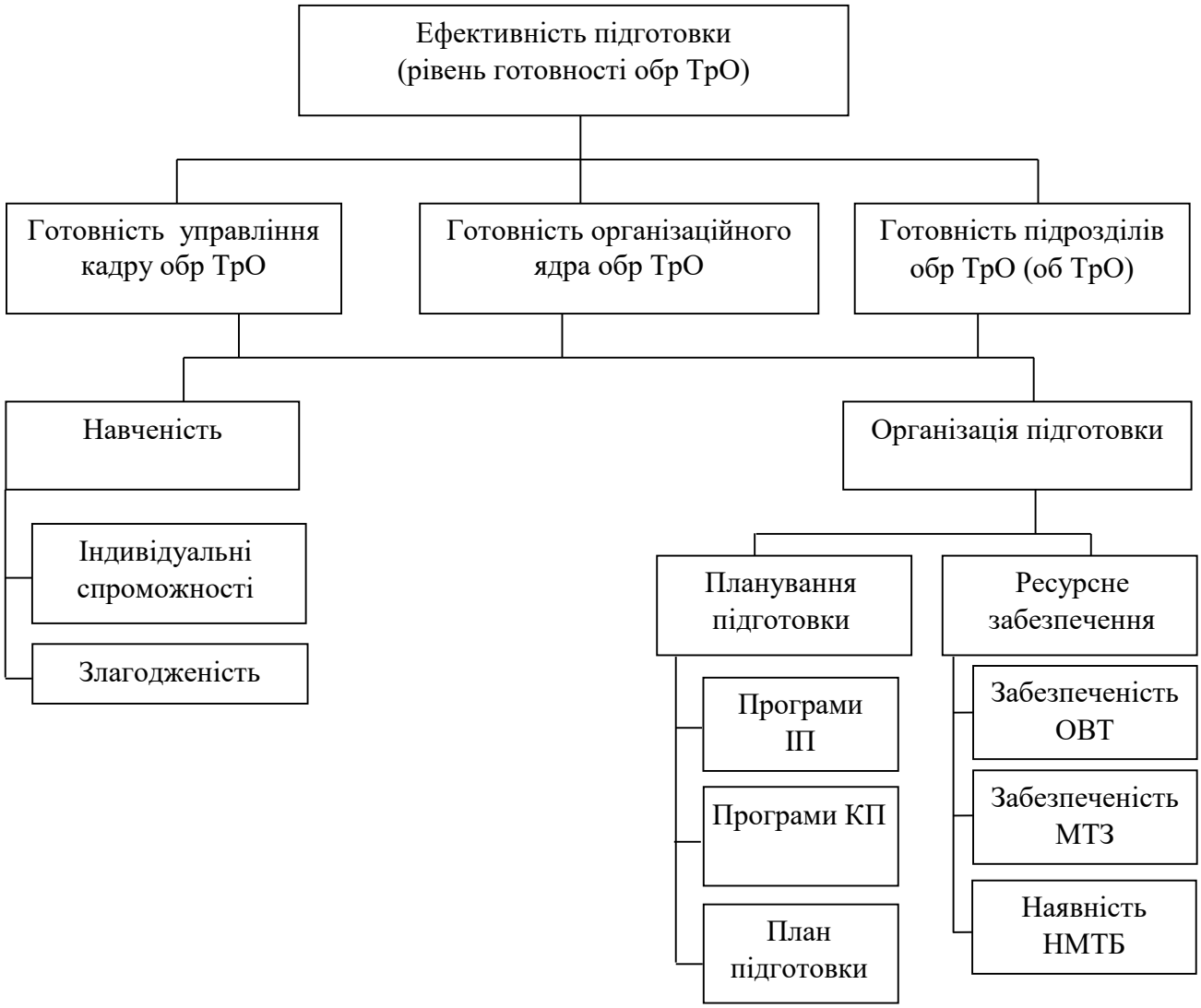


Рисунок 1 – Система показників оцінювання ефективності підготовки окремої бригади територіальної оборони

Виходячи з наведеного вище можна зробити висновок, що завдання оцінювання ефективності підготовки обр ТрО є багатокритеріальною задачею разом з тим описані математичні залежності перебувають в тісному фізичному взаємозв’язку, а отже доцільним буде використати метод згортки показників звести зазначене завдання до однокритеріальної задачі. Зазначені показники усіх рівнів можуть мати як рівну, так і різну значимість або вагомість. Тому під час їх проведення згортки необхідно застосовувати відповідні “вагові” коефіцієнти. Розрахунок яких проводиться методом експертного оцінювання.

Зважаючи на те, що інтегральні показники достатньо сильно корельовані, для визначення узагальненого показника $P_{ВБС}(t)$ пропонується використовувати нормовану мультиплікативну згортку [12]:

$$P_{ВБС}(t) = P_{ГУпК}(t)^{q_i} \cdot P_{ГОрЯ}(t)^{q_g} \cdot P_{Гп}(t)^{q_k}, \qquad (18)$$

де $P_{ГУпК}(t)$ – значення інтегрального показника “готовність управління кадру”, на час t;

$P_{ГОрЯ}(t)$ – значення інтегрального показника “готовність організаційного ядра”, на час t;

$P_{Гп}(t)$ – значення інтегрального показника “готовність підрозділів”, на час t;.

q_i q_g q_k – вагові коефіцієнти інтегральних показників.

Відповідно до визначених концептуальними, нормативними та керівними документами вимог до системи оцінювання готовності військової частини виконувати завдання за призначенням [13-14], визначимо значення критеріїв до узагальненого показника $P_{ВБС}(t)$. Оцінка обр ТрО виставляється як НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ, або НЕ НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ виконати завдання за призначенням.

Для визначення числового значення узагальненого показника рівня готовності до виконання завдань за призначенням $P_{ВБС}(t)$ використовується універсальна шкала Харрінгтона [15], яку наведено у табл. 1. Запропонована шкала дає змогу переводити отриману кількісну оцінку в якісну у певних межах.

Таблиця 1

Універсальна шкала Харінгтона

Оцінка за чотирибальною шкалою	Оцінка за шкалою Харінгтона	Порогові значення		Відповідність критерію
		min	max	
“відмінно”	“дуже добре”	0,8	1	НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ
“добре”	“добре”	0,63	0,8	
“задовільно”	“задовільно”	0,37	0,63	НЕ НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ
“незадовільно”	“погано”	0,2	0,37	
	“дуже погано”	0	0,2	

Проведемо порівняння якісних оцінок з відповідними їх пороговими значеннями $P_{ВБС}(t)$. Можемо визначити, що, ефективність підготовки обр ТрО на оцінку НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ матиме величину в межах $0{,}63 \le P_{ВБС}(t) \le 1$; НЕ НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ $-P_{ВБС}(t) < 0{,}63$.

Відповідність критерію оцінці НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ визначено в межах від 0,63 до 1 тому, що відповідно до нормативних документів з оцінювання за стандартами підготовки [13], об’єкт підготовки оцінюється як СПРОМОЖНИЙ, коли безрозмірна оцінка за виконання стандартів підготовки не нижче 0,7. Але, як було зазначено вище, на ефективність підготовки обр ТрО крім навченості об’єктів підготовки впливає також її організації власне суб’єктами підготовки. Тому, безрозмірна оцінка ефективності підготовки обр ТрО буде нижче 0,7.

Таким чином, за критерій готовності до виконання завдань за призначенням обр ТрО доцільно вибрати умову $P_{ВБС}(t) \ge 0{,}63$, яка відповідає оцінці НАБУЛА ВИЗНАЧЕНИХ БОЙОВИХ СПРОМОЖНОСТЕЙ.

Висновки і перспективи подальших досліджень. Запропонований критерій та показники достатньо зрозумілі та можуть бути використані для дослідження ефективності підготовки окремої бригади територіальної оборони Збройних Сил України до готовності виконати завдання за призначенням, а наведена удосконалена сукупність показників дає змогу всебічно її оцінити. Перспективами подальших наукових досліджень у цьому напрямі може бути розроблення часткової методики оцінювання ефективності підготовки організаційного ядра окремої бригади територіальної оборони.

ЛІТЕРАТУРА:

1. Георгадзе О.А. Методичний підхід щодо оцінювання якості програми індивідуальної підготовки артилерійських підрозділів / О.А. Георгадзе, В.І. Харабара, С.В. Горбенко // Науковий журнал Харківського університету Повітряних Сил імені Івана Кожедуба "Системи озброєння і військова техніка". – 2015. – № 2 (42). – С. 68–70.
2. Георгадзе О.А. Комплексна методика оцінювання ефективності бойової підготовки артилерійської бригади / О.А. Георгадзе // Збірник наукових праць Національного університету оборони України "Труди університету". – 2015. – № 5 (132). – С. 47–53.
3. Казан П.І. Деякі підходи до розрахунку багатокритеріальної оцінки ефективності підготовки типової військової частини Збройних Сил України / П.І. Казан // Збірник наукових праць Національного університету оборони України "Труди університету". – 2013. – № 6 (120). – С. 48–54.
4. Шпанчук Г.В. Удосконалена методика оцінки рівня підготовки підрозділів окремої механізованої бригади, що укомплектована військовослужбовцями професійної служби / Г.В. Шпанчук // Збірник наукових праць Національного університету оборони України "Труди університету". – 2011. – № 4 (103). – С. 51–55.
5. Мальков М.І. Про деякі підходи до оцінки ефективності бойової підготовки військ / М.І. Мальков // Збірник наукових праць Національної академії оборони України "Труди академії". – 2000. – № 27. – С. 21–25.
6. Нурулін Р.Ш. Особливості методичного підходу до оцінювання ефективності організації оперативної підготовки органів управління / Р.Ш. Нурулін // Збірник наукових праць ЦНДІ ЗС України. – 2009. – № 2 (48). – С. 38–48.
7. Харабара В.І. Комплексна методика оцінювання ефективності бойової підготовки танкової бригади у ході відновлення боєздатності / В.І. Харабара, О.А. Георгадзе // Збірник наукових праць Національного університету оборони України "Труди університету". – 2019. – № 6 (156), С. 133–143.
8. Наказ Генерального штабу Збройних Сил України від 21.01.20 № 18 "Про затвердження Доктрини підготовки сил оборони держави".
9. Доктрина з організації підготовки у Збройних Силах України. Затверджено начальником Генерального штабу Збройних Сил України від 01.07.2020.
10. Доктрина з організації оцінювання (сертифікації) у Збройних Силах України. Затверджено начальником Генерального штабу Збройних Сил України від 30.06.2020.
11. Барабаш Ю.Л. Основи теорії оцінювання ефективності складних систем : навч. посібн. [для ад'юнктів та здобувачів наукового ступеня] / Ю.Л. Барабаш // – К. : НАОУ, 1999. – 39 с. – (Методологія військово-наукових досліджень).
12. Шевченко В.Л. Якісна схожість згорток в математичних моделях процесів розвитку складних систем / В.Л. Шевченко // Збірник наукових праць "Телекомунікаційні та інформаційні технології". – 2014. – № 3 . – С. 32–38.
13. Наказ Генерального штабу Збройних Сил України від 27.01.20 № 26 "Про порядок розроблення (розміщення) стандартів (каталогів завдань) з підготовки та проведення оцінювання за стандартами підготовки Збройних Сил України".
14. Наказ Міністерства оборони України та Генерального штабу Збройних Сил України "Про затвердження інструкції про порядок проведення оцінювання бойової, мобілізаційної готовності до реалізації функціональних завдань та визначення спроможності вести (підтримувати, забезпечувати) бойові дії військових організаційних структур Міністерства оборони України та Збройних Сил України" від 11.10.2019 р.
15. Харрингтон Д. Управление качеством в американских корпорациях: Сокр. пер. с англ. / Авт. вступ. ст. и науч. ред. Л.А. Конарева. — М. : Экономика, 1990. – 272 с.

REFERENCES:

1. Georgadze O.A., Harabara V.I. and Gorbenko S.V. (2015) Metodychnyj pidhid shhodo ocinjuvannja jakosti programy indyvidual'noi' pidgotovky artylerijs'kyh pidrozdiliv. *Systemy ozbrojennja i vijs'kova tehnika*. Kharkiv, no. 2 (42), pp. 68-70.
2. Georgadze O.A. (2015) Kompleksna metodyka ocinjuvannja efektyvnosti bojovoi' pidgotovky artylerijs'koi' brygady. *Trudy universytetu*. Kyi'v, no. 5 (132), pp. 47-53.
3. Kazan P.I. (2013). Dejaki pidhody do rozrahunku bagatokryterial'noi' ocinky efektyvnosti pidgotovky typovoi' vijs'kovoi' chastyny. *Trudy universytetu*. Kyi'v, no. 6 (120), pp. 48-54.
4. Shpanchuk G.V. (2011) Udoskonalena metodyka ocinky rivnja pidgotovky pidrozdiliv okremoi' mehanizovanoi' brygady, shho ukomplektovana vijs'kovosluzhbovcjamy profesijnoi' sluzhby. *Trudy universytetu*. Kyi'v, no. 4 (103), pp. 51-55.
5. Mal'kov M.I.(2000) Pro dejaki pidhody do ocinky efektyvnosti bojovoi' pidgotovky vijs'k. *Trudy universytetu*. Kyi'v, no. 27, pp. 21-25.
6. Nurulin R.Sh. (2009) Osoblyvosti metodychnogo pidhodu do ocinjuvannja efektyvnosti organizacii' operatyvnoi' pidgotovky organiv upravlinnja. Zbirnyk naukovyh prac' CNDI ZS Ukrai'ny. Kyi'v, no. 2 (48), pp. 38-48.
7. Harabara V.I. and Georgadze O.A. Kompleksna metodyka ocinjuvannja efektyvnosti bojovoi' pidgotovky tankovoi' brygady u hodi vidnovlennja bojezdatnosti. *Trudy universytetu*. Kyi'v, no.6 (156), pp. 133-143.
8. Nakaz General'nogo shtabu Zbrojnyh Syl Ukrai'ny vid 21.01.20 № 18 “Pro zatverdzhennja Doktryny pidgotovky syl oborony derzhavy”.
9. Doktryna z organizacii' pidgotovky u Zbrojnyh Sylah Ukrai'ny. Zatverdzheno nachal'nykom General'nogo shtabu Zbrojnyh Syl Ukrai'ny vid 01.07.2020.
10. Doktryna z organizacii' ocinjuvannja (sertyfikacii') u Zbrojnyh Sylah Ukrai'ny. Zatverdzheno nachal'nykom General'nogo shtabu Zbrojnyh Syl Ukrai'ny vid 30.06.2020
11. Barabash Ju.L. (1999) Osnovy teorii' ocinjuvannja efektyvnosti skladnyh system : navch. posibn. [dlja ad’junktiv ta zdobuvachiv naukovogo stupenja]. Kyi'v: NAOU, 39 p. – (Metodologija vijs'kovo-naukovyh doslidzhen').
12. Shevchenko V.L. (2014) Jakisna shozhist' zgortok v matematychnyh modeljah procesiv rozvytku skladnyh system. *Telekomunikacijni ta informacijni tehnologii'*. Kyi'v, no. 3, pp. 32-38.
13. Nakaz General'nogo shtabu Zbrojnyh Syl Ukrai'ny vid 27.01.20 № 26 “Pro porjadok rozroblennja (rozmishhennja) standartiv (katalogiv zavdan') z pidgotovky ta provedennja ocinjuvannja za standartamy pidgotovky Zbrojnyh Syl Ukrai'ny”.
14. Nakaz Ministerstva oborony Ukrai'ny ta General'nogo shtabu Zbrojnyh Syl Ukrai'ny “Pro zatverdzhennja instrukcii' pro porjadok provedennja ocinjuvannja bojovoi', mobilizacijnoi' gotovnosti do realizacii' funkcional'nyh zavdan' ta vyznachennja spromozhnosti vesty (pidtrymuvaty, zabezpechuvaty) bojovi dii' vijs'kovyh organizacijnyh struktur Ministerstva oborony Ukrai'ny ta Zbrojnyh Syl Ukrai'ny” vid 11.10.2019 r.
15. Harryngton D. (1990) Upravlenye kachestvom v amerykanskyh korporacyjah: Sokr. per. s angl. Avt. vstup. st. y nauch. red. L.A. Konareva. M. : Эkonomyka, 272 p.

Ph.D. Heorhadze O.A., Ph.D. Shevchuk V.V.,
Ph.D. Pampukha I.V., Ph.D. Nikiforov M.M., Bargilevich A.V.

JUSTIFICATION OF THE OVERALL INDICATOR FOR THE ESTIMATION OF EFFECTIVENESS OF TRAINING OF A SEPARATE TERRITORIAL DEFENSE BRIGADE OF THE ARMED FORCES OF UKRAINE

Based on the results of the analysis of command and staff training of the territorial defence units and scientific research conducted to determine approaches to the estimation of the effectiveness of military units training, a set of indicators required to estimate the effectiveness of training of territorial defence units of the Armed Forces of Ukraine has been suggested. The achievement of the designated combat capabilities has been defined as an overall indicator for the effectiveness estimation. This indicator depends on the readiness to perform tasks of such components as personnel management, organizational core and units of the territorial defence brigade.

Being a measuring tool the indicator should reflect the level of the item's specific property display. The definition of the well-grounded indicators required to estimate the separate territorial defence brigade training effectiveness is of great theoretical and practical importance. Justification of the criterion and a set of indicators required to estimate the effectiveness of training of a separate territorial defence brigade is a challenging task. In practical terms, a set of indicators required to estimate the effectiveness of training of a separate territorial defence brigade is a result of activities of the relevant social and technical systems (territorial defence structures and agencies) established to perform missions. Estimation of the effectiveness of training of a separate territorial defence brigade requires application of complex indicators which can generalise a certain amount of information and at the same time maintain the objectivity of estimation. In some cases, in particular, when dealing with new tasks, this may require synthesis (a combination of earlier identified concepts and goals), the formulation of new indicators and algorithms for their calculation. Based on the results of the analysis of command and staff training of territorial defence units and scientific research conducted to determine approaches to the estimation of the effectiveness of military units training, a set of indicators required to estimate the effectiveness of training of territorial defence units of the Armed Forces of Ukraine has been suggested. The achievement of the designated combat capabilities has been defined as an overall indicator for the effectiveness estimation. This indicator depends on the readiness to perform tasks of such components as personnel management, organizational core and units of the territorial defence brigade and can be used to develop a partial methodology for the estimation of effectiveness of training the territorial defence brigade organizational core.

Keywords: territorial defence, application, effectiveness, estimation, indicators.

УДК 62:930.8.71:06-9/13

д.іст.н., доц. **Машталір В.В.** (ГШ ЗСУ)
д.техн.н., проф. **Гріффен Л.О.** (НАНУ)
д.іст.н., проф. **Рижева Н.О.** (МНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-12

ПОГЛЯДИ НА ІСТОРИЧНІ ПРОЦЕСИ СТАНОВЛЕННЯ НАУКОВОЇ ПАРАДИГМИ

У статті досліджено історичний розвиток процесів накопичення знань, що в результаті призвели до становлення нинішньої наукової парадигми, яка є інформаційною основою сучасної життєдіяльності людства. Стаття базується на науково-критичному використанні попередніх досягнень у галузі історії науки.

Наукова новизна статті полягає в комплексному представлені історичного розвитку наукової парадигми як результату закономірної діалектичної зміни специфічних його етапів з відповідною систематизацією знань (міфологія, філософія, наука), що викликана зростанням обсягу знань і розвитком методів дослідження (пізнання в процесі практичної діяльності, «стороннього» споглядання, експерименту з наступним формуванням теоретичної моделі).

Матеріали, досліджені в статті дозволяють говорити про те, що нинішні тенденції про роль науки в сучасному суспільстві змушують повертатись до процесів становлення наукової парадигми. Останні були складними і нелінійними, а становлення наукових принципів пізнання стало їх закономірним результатом. Упродовж історії людства отримання й використання знань про об'єктивний світ здійснювалося в різних, історично необхідних формах – як у методології пізнання, так і у способі систематизації, що визначались рівнем їх накопичення.

У статті автори зазначають, що накопичення у суспільстві знань відбувалось у процесі безпосередньої практичної діяльності, на основі нібито «стороннього» споглядання і в результаті свідомого впливу на об'єкт вивчення (експерименту) з їх різною «питомою вагою» на різних історичних етапах. У такий спосіб, сьогодні наукова парадигма є закономірним результатом історичного розвитку форм пізнання та його вищим досягненням, і приниження її ролі об'єктивно веде до зниження ефективності суспільного розвитку.

Ключові слова: наукова парадигма, історія науки, методологія, міфологія, філософія, наука.

Постановка проблеми. Проблема становлення й розвитку наукового знання нерідко уявляється у вигляді кількісного зростання відомостей про природу, технічні прилади і суспільство, без урахування специфіки наукового знання, відмінного від будь-якого іншого. При цьому виникали й інші погляди, згідно з якими етапністю характеризувався не тільки суспільний розвиток, але й інтелектуальна еволюція, що була значною мірою визначальною для суспільних змін.

Сьогодні глобальні зміни в розвитку людської цивілізації, пов'язані зі швидким нарощуванням виробничих сил, супроводжуються, зокрема, переглядом фундаментальних уявлень про роль і місце науки. Загальною тенденцією стає своєрідне зміщення науки з центральних позицій світосприймання й фактична відмова від визнання наступництва в розвитку знання.

Аналіз останніх досліджень і публікацій. Розвиток процесів здобування та систематизації знань у суспільстві досі не став предметом комплексного наукового дослідженні. Існують поодинокі наукові роботи, які опосередковано висвітлюють подібні дослідження. Наприклад, деякими дослідниками [1, 2] висуваються припущення про початок стадії «закінчення» безроздільного домінування основних ментальних, світоглядних і культурних кліше «класичної науки», тобто того, що можна було б назвати науковою парадигмою. Ці гіпотези узгоджуються з висновками критиків наукового світогляду – таких як Р. Генон [3], М. Хайдеґґер [4], О. Шпенглер [5], М. Еліаде [6], К.-Г. Юнг [7]. Останні стверджують, що наука як нормативна інстанція втрачає фундаментальне значення у процесі вирішення соціальних, культурних, ідеологічних та історичних питань, у зв'язку з чим назріває необхідність нової інтерпретації сутності, функцій, меж і логіки еволюції науки на

основі тих парадигмальних зсувів в історичній свідомості, які тривають протягом усього розвитку цивілізації.

Авторами [8, 9] прийнято пов'язувати з наукою отримання, систематизацію й використання знань про навколишню дійсність. Однак не будь-яке знання є наукою – особливою галуззю людської діяльності, спеціально спрямованою на пошук, систематизацію й застосування відомостей про реальну дійсність. Така дійсність може полягати у фізичних, біологічних, технічних об'єктах, психічних і соціальних процесах, зокрема у процесах мислення. Відзначимо, наука – історично нещодавнє явище в житті людства. Водночас воно не могло виникнути й існувати без наявності певної системи відомостей про природу й суспільство, а тому «людина стала використовувати й підкорювати речовини і сили природи задовго до виникнення науки» [2, с. 42], застосовуючи й інші, «донаукові» форми знання. Сама ж наука стала результатом суспільного розвитку, становлення наукової парадигми опанування світу являло складний і довготривалий історичний процес, який нині, у зв'язку з появою нових уявлень про роль науки в суспільстві, викликає підвищений інтерес [10].

Огюст Конт, перший в історії філософії мислитель (засновник позитивізму), який мав базову технічну освіту, принципово по-новому підійшов до розуміння і тлумачення цілої низки наукових проблем. Він виділяв три форми мислення людини. На першій – теологічній, люди всі явища пояснюють дією надприродних сил. На другій – метафізичній, явища трактуються як результат дії певних «причин», що руйнує релігійні уявлення, готуючи становлення третьої форми, – позитивної, яка все мотивує науково [11, с. 26-26].

Наведені міркування, відповідно до конкретних реалій сьогодення, є результатом здогадки, але не наукового аналізу. Причини характеру пізнання, його історичної еволюції, очевидно, варто шукати у способі отримання й організації знань у суспільстві. Знання про природу, технічні пристрої й соціальні явища існують стільки ж, скільки є люди. При цьому суспільний характер знань, який виявляється тим визначеніше, чим вище їхнє кількісне зростання, для суспільства загалом і диференціації щодо окремого індивіда, вимагає все більш чіткої й ефективної їх організації в певну систему. Зазначене й обумовило актуальність та необхідність даної статті.

Мета статті полягає у висвітлені історичного розвитку процесів здобування та систематизації знань у суспільстві.

Виклад основного матеріалу. Системний характер суспільних знань на кожному етапі розвитку суспільства визначають два фактори. По-перше, необхідно враховувати, що знання про навколишнє середовище становлять більш чи менш повне і точне ідеальне відображення останнього, яке фактично є не простою сукупністю окремих предметів і явищ, а внутрішньо пов'язаною системою. Отже, її адекватне відображення також повинно носити системний характер. По-друге, важливо мати на увазі, що знання через його суспільне буття передбачає й «роздробленість» наявного обсягу «в головах» окремих індивідів. Тому цілісність знання може бути забезпечена тільки його системним характером. Це стосується всіх форм знань, і в найбільшій мірі – знання наукового, парадигмальне формування якого становить особливий інтерес.

У цьому контексті надзвичайно важливе загальне розуміння першого історичного етапу становлення систем суспільного знання. Саме в цей період простежується як поява його донаукових еквівалентів, так і формування наукових уявлень. В історичній літературі перший етап становлення й розвитку наукових знань пов'язують із «традиційними спільнотами», або періодом розвитку соціально-економічних, політичних структур, культурно-духовних систем держав «Давнього Світу», що їх розгорнута характеристика презентована в сучасній науковій літературі [1, 3, 8, 12]. Традиційними спільнотами «Давнього Світу» прийнято вважати цивілізації, головною прикметою яких є визнання центрального місця в основі всіх соціально-культурних і політичних інститутів за міфологічними й релігійними системами.

Знаковим складником традиційного суспільства була «міфологія», що й визначала систему поглядів. У ній окремі речі, істоти, події, природні й соціальні явища пов'язувалися

множинністю сюжетів, які були елементами загального міфу, або розвитком окремих його аспектів у цілому й забезпечували певну систему єдиних уявлень про світ.

Обмеженість знань і тривалість існування власне «традиційних спільнот» у практично незмінному вигляді приводила до переконання, що «істинна» ідея не може бути «новою», і взагалі істина не вважалася продуктом людського розуму. Вона існувала ніби незалежно від індивіда, тому єдине, що необхідно було зробити, – це намагатися її опанувати. Отже, істинна ідея належала всім, хто був здатний її осягнути.

Послідовне вивчення збереженого комплексу матеріальних артефактів, письмових джерел дозволяє зробити висновок, що в традиційних спільнотах технічна і практична діяльність, яка вимагала певних раціональних навичок (що нагадували окремі елементи сучасного наукового підходу), обов'язково мала також ірраціональні, зокрема магічні, складники. Додамо, що кожна цивілізація Давнього Світу мала власні різновиди основ традиційних наук, що виникали. Це пояснювалося як сукупністю природно-географічних, економічних особливостей, так і специфікою мислення, комплексом конкретних факторів життєдіяльності окремих народів, реаліями певного періоду в їхній історії. Деякі знання, отримані в галузі математики, астрономії, медицини, транслювалися всередині вищих каст за принципом виключної належності (від старшого до молодшого за віком і рангом).

Сформоване в такий спосіб упродовж довгого часу знання зберігалося практично в «застиглому» вигляді. Навчання будувалося за принципом передавання готових детермінованих алгоритмів на основі визначеності наперед причини і наслідку. Замкненість передачі знання всередині професійних і соціальних груп зумовила модель, де місце індивіда посідав колективний узагальнений хранитель (Давній Єгипет). У цілому знання давніх цивілізацій носили прикладний характер; відмінності між точними й наближеними рішеннями задач не вважалися принциповими – будь-яке рішення виявлялося прийнятним, якщо призводило до бажаного результату.

Першими елементами саме наукових знань стали досягнення в галузі математики. Найбільш ранні відомі математичні тексти залишили дві великі цивілізації давнини – Єгипет і Месопотамія, де вирішувалися перші математичні задачі, рішення яких вимагало повсякденне життя. З'явилась арифметика, значного розвитку досягла геометрія. Математика ж як наукова дисципліна виникла в Давній Греції, де була створена методологія математики, основою якої став дедуктивний метод [13, с. 225-438].

Елементи наукових даних, що формувалися, включалися до всезагальної міфологічної системи – астрології, нумерології й т. ін. Об'єктивні реалії розвитку суспільства свідчать, що знання про навколишнє середовище ніколи не існувало й не може існувати як конгломерат розрізнених відомостей, воно повинно мати цілісний характер. Систематизація знань у цілому – умова їх накопичення й суспільного функціювання, незалежно від того, яким чином це здійснюється. Поповнення знань про навколишній світ завжди передбачає два етапи: отримання даних безпосередньо з навколишньої дійсності та зведення їх у певну систему.

Упродовж накопичення знань спосіб досягнення й того, й іншого носив історично визначений характер. У різні періоди отримання даних безпосередньо з навколишнього середовища відбувалося з переважанням одного з трьох факторів. По-перше, відомості в процесі життєдіяльності або практики отримували завдяки безпосередньому оперуванню об'єктами. По-друге, здійснювалося «відсторонене» спостереження над даним й іншими процесами (споглядання). По-третє, тривав цілеспрямований вплив на об'єкти вивчення для отримання відомостей про них – експеримент.

На основі отриманих так відомостей відбувалася їх систематизація й організація в цілісну систему, де кількісні характеристики знань відігравали надзвичайно важливу роль. Первісно систематизація здійснювалася за рахунок «накладання» на природне середовище в його ідеальному відображенні як організаційного начала тих системних зв'язків, що були відомі людині в найближчому ареалі її існування, а в подальшому – у вигляді суспільних зв'язків. У розвиненому вигляді такого роду система, базована на образі як вихідному елементі, отримала найменування міфології. Наступним кроком стала філософія, що на основі

ніби апріорних елементів – категорій – ідеально конструювала світ у вигляді більш або менш цілісної системи визначених фрагментів, а ті своєрідною конструкцією «накладалися» на дійсність як певна картина. Проте тільки на третій, науковій, стадії – відображення світу з досягненням достатньо високого рівня знань – власне сам цей світ у всьому різноманітті став основою узагальнень у систематично пов'язаних поняттях. Тому становлення наукової парадигми пройшло значний шлях історичного розвитку, що розпочався з міфології.

Міфологія, як спосіб отримання й організації відомостей про світ, принципово не могла – через малий обсяг раціональних даних – повністю на них базуватися. З огляду на незначний обсяг знань, для отримання цілісної картини світу взагалі або тієї чи іншої його «підсистеми» зокрема, люди змушені були, поряд із раціональними відомостями, використовувати «дані» міфологічні, що в цілому формувало химерну картину. Саме такою «теоретичною концепцією» керувалася людина у практичній діяльності. Створена картина світу була тим ближче до реальності, чим більшого числа повсякденних речей стосувалася, проте вона незмінно відображалася на всій діяльності людини.

Стосовно проблем розвитку й функціювання техніки міфологічна «модель світу» неминуче передбачала ірраціональний – з нашого сьогоденного погляду – компонент практично будь-якої технології. Прагнучи реалізації тої чи іншої мети, людина робила вчинки, не тільки визначені її безпосереднім життєвим досвідом, але й такі, що витікали з більш загальних уявлень про навколишні об'єкти та їх взаємодію, визначувані сформованим досвідом, як дійсним, так і уявним. Це означає, що дії людини, зокрема, не були – знов-таки згідно з сучасними уявленнями – раціональними, закономірно необхідними для досягнення поставленої мети. Вона діяла так не тому, що сподівалася привернути на допомогу «вищі сили», а тому, що, з її точки зору, світ був так улаштований. Певні дії включалися в комплекс практично корисних технологічних прийомів, що вели до заданої мети, попри відсутність розуміння процесів, що відбувалися.

Людина неухильно розширювала раціональні знання про світ, замінюючи недостатні ланки магічними уявленнями, які іноді відбивали справжню, але невідому картину світу, поступово збільшуючи обсяг об'єктивних відомостей.

На певному ступені розвитку людства в духовно-релігійну парадигму привноситься ідея вищої істоти, яка стояла над реальним світом. Це також створювало віру в певну єдність світу, оскільки, «якщо існує світобудова, значить – існує її єдність. ... Богопізнання – пошук реальності, в якій усі ми складаємо єдине ціле» [14, с. 107].

У подальшому це стає методологічною базою в процесі становлення нового способу отримання й організації знань про світ – філософії, засади якої первісно вироблялися в межах релігійної форми свідомості.

Загальне уявлення про єдність світу дозволило філософії з часом відмовитися від акцентів на «дію божественних сил» і виробити нові методи пізнання. З'являється більш детальне розуміння відомостей, що відкривалися в різноманітних явищах, належних до різних систем образів. Вичленовування ряду подібних рис дозволяло припускати наявність у них певних спільностей структур та елементів, як і певної ізоморфності законів, яким вони підкорені, відповідно організуючі системне узагальнення наявних даних.

В античний період поступовий розвиток цивілізації фіксує виникнення низки уявлень, які в межах міфологічної парадигми передбачають використання певних елементів наукового підходу. Найбільш переконливо це проявилося в математиці («Начала» Євкліда), а також, в окремих випадках, – у галузі природничих наук. У сфері механіки Архімедом було встановлено ряд законів статики і гідростатики, які стали основою подальшого вдосконалення системи знань і пізніше ввійшли до складу наукової картини світу [15].

В обговорюваний період найбільш перспективною системою формування знань стає філософія, яка презентувала світ у вигляді певної комбінації обмеженої кількості вихідних елементів. Ідеальне відображення цих елементів, принципи їх сполучення становлять філософські категорії. Аристотель уважав, що в філософії категорії відіграють роль універсальних визначень, через які розум пізнає речі: «за їхньою допомогою й на їх основі

пізнається все інше…» [16, с. 91]. Категорії, як базові структуранти, не мають чітко визначених дефініцій, уявлення про них формуються на основі досвіду інтуїтивно й розвиваються в процесі застосування до конкретних явищ. Саме система категорій складала основу всезагальної структури знань.

Завдяки використанню основного методу філософії, який полягав у накладанні на дійсні, але невідомі закономірності природи інших, сформульованих умоглядно, якщо отримані результати достатньо задовільно співпадали з реальними подіями – феноменологічний підхід. Однак по мірі розширення обсягу знань реальний стан речей відхилявся від передбачуваного теорією, і це вимагало ускладнення системи. Класичним прикладом стає геоцентрична система світу Птолемея. У своєму найпростішому вигляді вона дозволяла достатньо точно описати видимий рух Сонця, Місяця й зірок, але робила неприпустимі збої, коли справа стосувалася планет. Саме тому в межах первісно простої системи були придумані вельми складні закони руху планет (що включали так звані епіцикли й деференти).

Поступово, під впливом розширення загальних знань про світ, структура філософії змінювалася. Надалі ці зміни стали предметом усебічного аналізу вчених. Так, у першій половині XIX ст. представник німецької класичної філософії Фридрих Шеллінг звернув увагу на складність процесів, що відбувалися. Він уважав, що філософія знайшла «завершення у двох основних науках, що взаємно себе заповнювали й одна одну вимагали, попри свою протилежність у принципі та спрямованості», а саме: у трансцендентальній філософії й натурфілософії. Філософія у вигляді натурфілософії включала все провідне знання свого часу і в цій якості відігравала важливу роль в узагальненні знань про світ, сприяючи формуванню наукових методів.

Однак розвиток наукової парадигми носив суперечливий характер. У межах натурфілософії відкривалися нові явища реальності, створювалися нові методи дослідження, водночас у формуванні загальної картини світу, її окремих сфер, тривало користування уявленнями трансцендентальної філософії.

У середні віки найбільш рельєфно це проявлялося в алхімії. У зв'язку з тим, що використання хімічних процесів завжди відігравало важливу роль у житті суспільства, вважаємо доцільним виділити їх прикладний аспект. Людина вже на «первісному» етапі накопичує досвід застосування різних видів хімічних процесів, базований на тривалому практичному досвіді. Наприклад, використання вогню поступово ставало складовим елементом життєдіяльності. Його застосовували для приготування їжі, спікання, пізніше – сплавлення, відновлення металів, дублення шкір, бродіння, гниття тощо. В еллінську добу під численні знання в ці галузі, наприклад єгипетські жерці, підводили своєрідну теоретичну базу у вигляді вчення про чотири елементи – стихії, що поклало початок такої натурфілософської системи як алхімія. Ця теорія ґрунтувалася на уявленнях Аристотеля про те, що все навколо утворене з чотирьох первісних елементів (стихій), об'єднуваних попарно за принципом протилежності: вогонь – вода, земля – повітря [17].

Найвищого розвитку алхімія, як ми вже казали, отримала в середні віки. Практична діяльність алхіміків – спроби створити «еліксир безсмертя» і «філософський камінь», який перетворює метали в золото, – зробила великий внесок у розвиток науки. Саме алхімікам, уважав Д. І. Менделєєв [18], «наука зобов'язана першим точним зібранням алхімічних даних… Тільки завдяки запасу відомостей, зібраних алхіміками, можна було розпочати дійсні наукові вивчення хімічних явищ» [18, с. 357-358]. Водночас упродовж накопичення знань філософська система, всередині якої діяли алхіміки, ставала гальмом пізнання. У XVIII ст. теоретичні й практичні реалії призвели до «Рубікону» – занепаду і виродженню алхімії. Відповідно втратили значення й ідеї натурфілософії.

Це не означає, що зусиллями представників філософської думки можна нехтувати. Згідно з Ф. Шеллінгом, – його ідея нам видається заслуговує на увагу – залишалася друга частина філософії, на якій базувалися певні «всезагальні системи» знання, що об'єктивно сприяли створенню протягом століть нових систем. Кожна нова система, в певних часових проміжках, давала основу наступного просування вперед у пізнанні світу. Вирішувався

широкий спектр задач, сприятливих для наповнення «скарбниці знань», що закладало підґрунтя наукового пізнання світу. Представники філософської думки приводили до тимчасової відповідності загальнотеоретичні уявлення і наявний обсяг знань. Надалі все повторювалося, й чергова система вступала у протиріччя з накопиченим досвідом. Формат і глибина протиріч програмували створення нових «систем», які не відповідали об'єктивній меті й поступово перетворювались у своєрідну «гру розуму». У процесі збільшення суми знань і встановлення взаємозв'язку між ними зростала потреба в організації наукової системи знань про світ, яка й формувалася протягом тривалого часу.

Формування наукового ставлення до світу супроводжувалося появою окремих наук зі своїм предметом і, відповідно, – нової системи отримання й організації даних про навколишню дійсність. Створювалися базисні основи для формування науки як відкритої системи знань, яка не обмежувала рішення задач, що виникали, наперед заданими межами і принципово виходила з відносності й неповноти пізнаваних істин.

Історичні процеси свідчать, що наука не є цілісним і завершеним явищем, яке спирається на фундамент визначальних алгоритмів. Будь-яка наука в своєму розвитку прагне до цього, та наукова парадигма призводить до вихідних пунктів через множинність перехрещених і парадоксальних шляхів.

У такому контексті вважаємо доцільним акцентувати увагу на трьох стадіях отримання й організації знань, загальна характеристика яких вище презентована нами. Усі стадії об'єднує сукупність підходів: першого, практичного, – отримання знань із навколишнього світу, і другого, теоретичного, – конструювання на основі отриманих знань певної системи – узагальненої, ідеальної моделі світу, його елементів чи аспектів. Указані стадії мають суттєву відмінність стосовно зв'язку, теоретичного і практичного. Якщо на стадії міфології теоретична модель формується, перш за все, на основі знань, отриманих у процесі практичної діяльності, то філософська система, головним чином, складається на основі «абстрактних» спостережень. У науковій діяльності основним методом накопичення знань стає свідомий вплив із цією метою на об'єкти реального світу, або експеримент. У такий спосіб, наука об'єднує як експериментальне вивчення об'єктів дійсності, так і теоретичне їх дослідження, яке стосується вже не безпосередньо об'єкта, а його теоретичної моделі. У науці розподіл теоретичного і дослідного пізнання – двох сторін єдиного цілісного процесу, – доведено до свого логічного завершення.

Об'єктивна необхідність теоретичного (абстрактного) дослідження пояснюється, перед усім, складністю «охоплення» будь-якого об'єкта вивчення та його потенційних взаємозв'язків з іншими об'єктами. Американський математик, один з основоположників кібернетики й теорії штучного інтелекту, Н. Вінер підкреслював: «Абстракція – це заміна частини Всесвіту, яка розглядається, певною її моделлю, моделлю схожою, але більш простою структурою» [19, с. 171, 172]. Теоретичне дослідження будь-якого об'єкта передбачає його заміну, на основі отриманих відомостей, спрощеною моделлю об'єкта, створеною таким чином, щоб охопити основні елементи і зв'язки в конкретному випадку.

Неможливість повного ототожнення моделі з наявним об'єктом супроводжується виникненням невідповідності між теоретичними й експериментальними даними. Звідси, у результатах теоретичного дослідження присутні як істина, так і омана. Помилки і похибки, наявні в будь-якому дослідженні, можуть спровокувати принципові невідповідності. У цьому контексті звернемо увагу на те, що «закони, які формулюються в межах теорії, стосуються, по суті, не емпіричної реальності, а дійсності, як вона презентована ідеалізованим об'єктом», отже, забезпечити їх повну відповідність неможливо [9, с. 7]. У процесі подальшого пізнання з'являється новий цикл досліджень зі створенням моделі об'єкта, в якій наявні істини розвиваються, а омани виключаються. Нова модель проходить повторення циклів попередньої реальності, і такий процес осягнення істини в науці не має меж.

Забезпечити найбільшу відповідність моделі об'єкту стає можливим як на основі досвіду вивчення реальності, так і за допомогою аналізу, опрацювання отриманих відомостей. Результатом такої роботи стає, по-перше, система конкретних знань про навколишню

реальність; по-друге, методологічні уявлення, які є «зводом» уявлень про схожість чинних у ній законів. Перші достатньо повно формалізовані у вигляді системи наук, другі систематизовані частково як визначені закономірності кількісних змін (наприклад, математика), частково – у вигляді менш конкретних методологічних «законів» у логіці, діалектиці, загальній теорії систем, синергетиці й т. ін.

Реалії суспільного розвитку свідчать, що закономірності, які описують рух систем різної природи, мають значну формальну подібність. Математичне моделювання ґрунтоване на можливості вивчення різноманітних явищ на основі однакового математичного опису. Так, одними й тими самими рівняннями можливо описати електричний коливальний контур і пружинний маятник [20, с. 3]. Ці рівняння можуть використовуватися для визначення інших процесів у різноманітних системах.

Сучасні здобутки дозволяють припустити, що коли б науці були відомі основні закони руху матерії, то їхні математичні вираження дозволили б описати всі явища природи й суспільного життя. Однак нам відомі не всі основні закони, і «кожен крок у вивченні природи – це завжди тільки наближення до істини» [21, с. 136]. Необхідно враховувати й безкінечне число взаємозв'язків між об'єктами реального світу, які, можливо, ніколи не дозволять обмежити опис руху реального об'єкта самими математичними закономірностями. І все ж, узагальнення множинності окремих випадків виробило в науці здатність якісної оцінки явищ, зокрема постулатів, що приймаються як даність, без доведень (аксіоматичний метод). Крім того, наука має в арсеналі методологічні прийоми, спрямовані на узагальнене розуміння отриманих експериментальним шляхом відомостей, які використовуються в процесі побудови теоретичної моделі й планування експериментів. Усе це складає наукову парадигму, сформовану в результаті тривалого і складного шляху розвитку людського пізнання.

Висновки. Отримання й використання знань про об'єктивний світ здійснювалося суспільством у різноманітних, історично необхідних формах. Ці форми – міфологічна, філософська й наукова, зміщуючи одна одну, згідно з кількісними змінами в накопиченні знань, забезпечували як можливість практичної діяльності суспільства, так і формування узагальнених уявлень про світ. Основну роль у цьому контексті відіграє наука. Саме вона взяла на себе функцію забезпечення суспільства системою необхідних знань.

На сучасному етапі розвитку цивілізації наука не зникає, вона змінює своє якісне – парадигматичне значення. Відбувається зміна розуміння «природи» сучасної науки, що передбачає її переосмислення. Виникає необхідність охопити історію науки на рівні її базисних джерел у глобальному історичному контексті. Слід переосмислити і врахувати весь комплекс передумов її виникнення та співвіднести з попередніми щодо появи науки факторами: світоглядними, релігійними, міфологічними, філософськими.

Тому, з нашого погляду, міркування про зниження ролі науки, яка закономірно розвивається як особливий пізнавальний процес у результаті тривалих і глибоких історичних трансформацій, надто песимістичні. Природно, можна припустити, що наука, як і попередні форми отримання й організації знань, поступиться коли-небудь місцем іншим, поки не відомим формам. Однак сьогодні, попри низку серйозних проблем у його розвитку, наукове знання не втрачає фундаментальних позицій. Звільняючись від впливу рудиментів минулих систем, наука зберігає своє суспільне значення. Переконливим доказом цьому слугують не тільки нові наукові відкриття, що часом докорінним чином змінюють уявлення про світ, але і збільшувана роль науки у формуванні нового виробничого укладу, її активне перетворення в безпосередню виробничу силу суспільства.

ЛІТЕРАТУРА:

1. Дугин А. Эволюция парадигмальных оснований науки, Москва: Арктогея, 2002. 210 с.

2. Рузавин Г. И. Фундаментальные и прикладные исследования в структуре научно-технического знания. – Философские вопросы технического знания. Москва: Наука, 1984. С. 32-51.

3. Генон Р. Кризис современного мира. Пер. с франц. Москва: Эксмо, 2008. 784 с.

4. Хайдеггер М. Время и бытие. Пер. с нем. В.В. Бибихина. Харьков: «Фолио», 2003. 503 с.

5. Шпенглер О. Закат Европы. Москва: Мысль, 1993. 632 с.
6. Элиаде М. Священное и мирское. Москва: Издательство МГУ, 1994. 144 с.
7. Юнг К. Г. Архетип и символ. Москва: Ренессанс, 1991. 121 с.
8. Лосев А. Ф. История античной эстетики: Итоги тысячелетнего развития. Москва: Искусство, 1992. 243 с.
9. Онищенко Н. П. Становление и развитие теории в технической науке и практике. Минск, 1990. 128 с.
10. Бєсов Л. М. Історія науки і техніки // 3-є вид. переробл. і доп. Харків: НТУ «ХПІ», 2005. 376 с.
11. Конт Огюст. Курс положительной философии. – СПб.: "Книжный Магазин Т-ва "Посредник", 1899. 175 с.
12. Гайденко П. П. История греческой философии в ее связи с наукой. Москва: ЛИБРОКОМ, 2009. 264 с.
13. Башмакова И. Г. Лекции по истории математики в Древней Греции // Историко-математические исследования. Выпуск XI. Москва: ГИФМЛ, 1958. С. 225-438.
14. Миркина З., Померанц Г. Великие религии мира. Москва: Рипол, 1995. 220 с.
15. Рожанский И. Д. История естествознания в эпоху эллинизма и Римской империи. Москва: Наука, 1988. 486 с.
16. Ильенков Э. В. Философия и культура. Москва: Политиздат, 1991. 464 с.
17. Рабинович В. Л. Алхимия как феномен средневековой культуры. Москва: Наука, 1979. 427 с.
18. Менделеев Д. И. Сочинения: В 25- т. Ленинград–Москва: Изд-во АН СССР, 1949. т. 15. 646 с.
19. Неуймин Я. Г. Модели в науке и технике. Ленинград: Наука, 1984. 190 с.
20. Григорьев Л. Л. Моделирование и технические науки. Москва, 1967. 248 с.
21. Фейнман Р., Лейтон Р., Сэндс М. Фейнмановские лекции по физике. Т. 1. Современная наука о природе. Законы механики. Москва: АСТ, 1967. 259 с.

REFERENCES:

1. Dugin A. Evolution of the paradigm foundations of science, Moscow: Arctogea, 2002. 210 s. (rus).
2. Ruzavin G. I. Fundamental and applied research in the structure of scientific and technical knowledge. – Philosophical issues of technical knowledge. Moscow: Science, 1984. C. 32-51. (rus).
3. Genon R. Crisis of the modern world. Lane with franz. Moscow: Eksmo, 2008. 784 s. (rus).
4. Heidegger M. Time and being. Lane with German V.V. Bibikhin. Kharkov: Folio, 2003. 503 s. (rus).
5. Spengler O. Sunset of Europe. Moscow: Thought, 1993. 632 s. (rus).
6. Eliade M. Sacred and worldly. Moscow: Moscow State University Publishing House, 1994. 144 s.
7. Jung K. G. Archetype and symbol. Moscow: Renaissance, 1991. 121 s. (rus).
8. Losev A. F. History of ancient aesthetics: Results of millennium development. Moscow: Art, 1992. 243 s. (rus).
9. Onishchenko N. P. Formation and development of theory in technical science and practice. Minsk, 1990. 128 s. (rus).
10. Biesov L. M. Istoriia nauky i tekhniky // 3-ye vyd. pererobl. i dop. Kharkiv: NTU «KhPI», 2005. 376 s. (ukr).
11. Comte Auguste. Course in positive philosophy. – St. Petersburg: "Bookstore T-va" Intermediary, "1899. 175 s. (rus).
12. Gaidenko P. P. History of Greek philosophy in its connection with science. Moscow: LIBROCOM, 2009. 264 s. (rus).
13. Bashmakova I. G. Lectures on the history of mathematics in Ancient Greece // Historical and mathematical studies. Release XI. Moscow: GIFML, 1958. C. 225-438. (rus).
14. Mirkina Z., Pomeranz G. The great religions of the world. Moscow: Ripol, 1995. 220 s. (rus).
15. Rozhansky I. D. The history of natural science in the era of Hellenism and the Roman Empire. Moscow: Science, 1988. 486 s. (rus).
16. Ilyenkov E. V. Philosophy and culture. Moscow: Politizdat, 1991. 464 c. (rus).
17. Rabinovich V. L. Alchemy as a phenomenon of medieval culture. Moscow: Science, 1979. 427 s.
18. Mendeleev D. I. Essays: In 25- vols. Leningrad-Moscow: Publishing House of the USSR Academy of Sciences, 1949. vol. 15. 646 s. (rus).
19. Neuymin Y. G. Models in science and technology. Leningrad: Science, 1984. 190 s. (rus).
20. Grigoriev L. L. Modeling and technical sciences. Moscow, 1967. 248 s. (rus).
21. Feynman R., Leighton R., Sands M. Feynman lectures on physics. T. 1. Modern nature science. Laws of mechanics. Moscow: ACT, 1967. 259 s. (rus).

D.Sc. Mashtalir V.V., D.Sc. Griffen L.O., D.Sc. Ryzheva N.O.

LOOK AT THE HISTORICAL PROCESSES OF THE FORMATION OF SCIENTIFIC PARADIGMS

The article examines the historical development of the processes of knowledge accumulation, which eventually led to the formation of the current scientific paradigm, which is the information basis of modern human life. The article is based on the scientific-critical use of previous achievements in the field of history of science.

The scientific novelty of the article is a comprehensive presentation of the historical development of the scientific paradigm as a result of a natural dialectical change of its specific stages with appropriate systematization of knowledge (mythology, philosophy, science), caused by the growth of knowledge and development of research methods. contemplation, experiment with the subsequent formation of a theoretical model).

Materials, research in the article allow us to say that current trends in the role of science in modern society are forcing us to return to the processes of formation of the scientific paradigm. The latter were complex and nonlinear, and the formation of scientific principles of cognition was their natural result. Throughout human history, the acquisition and use of knowledge about the objective world has been carried out in various, historically necessary forms - both in the methodology of cognition and in the method of systematization, which was determined by the level of their accumulation.

The authors note that the accumulation of knowledge in society took place in the process of direct practical activity, on the basis of alleged "external" contemplation and as a result of conscious influence on the object of study (experiment) with their different "specific weight" at different historical stages. Thus, today the scientific paradigm is a natural result of the historical development of forms of knowledge and its highest achievement, and the reduction of its role objectively leads to a decrease in the effectiveness of social development.

Keywords: scientific paradigm, history of science, methodology, mythology, philosophy, science.

УДК 355/359.08

к.т.н., доц. **Черних Ю.О.** (ВІКНУ)
Черних О.Б. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2020/68-13

СИСТЕМА ПІДГОТОВКИ ОФІЦЕРСЬКИХ КАДРІВ У РЕСПУБЛІЦІ УГОРЩИНА

У статті проаналізовано досвід підготовки офіцерських кадрів для збройних сил республіки Угорщина. Проведено аналіз структури системи військової освіти та наведено основні нормативно-правові акти, на підставі яких організовано навчання військових фахівців. Розглянуто мережу військових навчальних закладів для підготовки офіцерів тактичної, оперативної та стратегічної ланок військового управління. Означено відомості щодо ролі та міста цивільної освіти і базової військової освіти у загальної системі підготовки військового фахівця.

Підготовка офіцерів для всіх рівнів військового управління проводиться на факультеті військових наук і підготовки офіцерів Національного університету державної служби. Приведено вимоги для вступників до військового навчального закладу різних ступенів підготовки. Зміст навчання офіцерів будується за трьома рівнями військової освіти. Кожний рівень військової освіти завершується отриманням певного рівня кваліфікації. Основними загальними тенденціями розвитку вищої угорської військової школи є: поліпшення якості відбору абітурієнтів, індивідуалізація навчання курсантів і слухачів, стабілізація їх числа на сучасному рівні; подальша інформатизація навчального процесу, впровадження мультимедійних засобів навчання тощо. Аналіз концепції, структури, цілей, змісту і технологій підготовки офіцерського складу в збройних силах республіки Угорщина показує, що система військової освіти відображає сучасний етап розвитку збройних сил, а також національну культурну специфіку країни. Головним напрямком підготовки офіцерів є їх фундаментальна військово-професійна підготовка як у військовій, так і в цивільній сферах.

Ключові слова: система військової освіти республіки Угорщина, підготовка офіцерів, рівень підготовки.

Постановка проблеми. Проводячи дослідження закордонного досвіду будівництва та реформування збройних сил інших країн, у тому числі їхньої складової - системи військової освіти (СВО), бачимо, що в кожній країні він має специфічне національне підґрунтя. Водночас у військовій педагогічній практиці різних країн світу існують загальні методичні підходи, які доцільно враховувати і використовувати. Творче використання міжнародного досвіду підготовки військових фахівців за кордоном набуває особливої актуальності в умовах подальшого реформування збройних сил (ЗС) України. На наш погляд, цікаво дослідити трансформацію та побудову СВО ЗС країн, що раніш входили до складу організації колишнього варшавського договору, зокрема у збройних силах республіки Угорщина (РУ). У статті наведено аналіз досвіду підготовки офіцерів у ЗС РУ, що виконаний під час проведення дослідження у рамках науково-дослідної роботи «Науково-організаційні засади проектування основних вимог до змісту підготовки офіцерських кадрів з вищою освітою для Збройних Сил України» (шифр - Підготовка-П).

Аналіз останніх досліджень і публікацій. Висвітленню досвіду підготовки військових фахівців для збройних сил інших країн присвячено низку публікацій вітчизняних та зарубіжних авторів, зокрема, Болгарії [1]; Великої Британії [2], країн Балтії [3, 4], Німеччини [5-7], Польщі [8], Сполучених Штатів Америки [9-11]; Франції [12, 13] та ін. Це пов'язано з тим, що підготовка військових фахівців у цих країнах відображає найхарактерніші риси сучасного підходу до створення освітніх структур та їх функціонування. Разом з тим, слід зазначити, що незважаючи на різноманітність публікацій щодо систем військової освіти в інших країнах, у першу чергу, провідних країн-членів НАТО, дослідження сучасного стану системи військової освіти у ЗС Республіки Угорщина, у тому числі підготовки офіцерських кадрів, наражаються на такі проблеми: неповнота та недостатня аналітичність джерельної

бази; нехтування необхідністю ґрунтовного вивчення досвіду підготовки військових фахівців у країнах, що мають невеликі за чисельністю ЗС тощо.

Метою статті є проведення аналізу сучасного стану підготовки офіцерських кадрів для ЗС республіки Угорщина для врахування її досвіду під час проведення подальшої реформи національної СВО.

Виклад основного матеріалу. Зміни в організації навчання військовослужбовців угорської армії вперше стали темою для обговорення в процесі деполітизації її організації, пізніше – в період підготовки до вступу в НАТО, а нині – як невід'ємна частина переходу до повністю добровільних, професійних збройних сил і діяльності у повної інтеграції в НАТО. Ці періоди супроводжувалися значними змінами в нормативно-правовому та структурному аспектах кадрової політики та підготовки офіцерських кадрів. Нова обстановка безпеки, членство в НАТО і нові соціокультурні реалії потребували, з одного боку, менших за чисельністю особового складу, а з іншого боку, більш професійних збройних сил. Разом з цим, обмеження ринкової економіки, у свою чергу, вимагали ефективних у фінансовому плані рішень щодо захисту національних і державних інтересів. Враховуючи все це, були вжити заходи стосовно вдосконалення системи підготовки офіцерських кадрів.

У новій кадрової політиці переважала так звана ідея «в гору або геть»: той, хто не зможе за певний проміжок часу піднятися в ієрархії офіцерського корпусу вище, залишає збройні сили. Така переважаюча, але не виняткова ідея, визначила нову систему підготовки кадрів. Сьогодні в угорських збройних силах існує певна група посад, на яких офіцер може залишатися обмежений час, а потім повинен або піднятися вище (якщо він відповідає наперед визначеним умовам), або піти у цивільний сектор. Існує також інша (менша) група посад , що вимагають певних знань, досвіду і тренування, на яких можна залишатися до досягнення загальної вікової межі або закінчення терміну контракту.

Для забезпечення функціонування такої системи кадрового менеджменту необхідна ефективна система військової освіти. На трансформацію системи підготовки офіцерських кадрів після виходу Угорщини з організації варшавського договору впливало декілька чинників, серед яких основними були: зміни у векторі розвитку країни та радикальні зміни, що відбулися в її збройних силах; жорсткі фінансові обмеження, оновлення законодавства у галузі освіти.

На законодавчому рівні на реформування системи освіти вплинули зміни, що були внесені в закон "Про вищу освіту" в редакціях 1993 року та 1999 року [14]. Так, закон у редакції 1993 року висунув більш жорсткі освітні стандарти для усіх угорських університетів. Цей закон встановив обов'язковий процес акредитації для кожного вищого навчального закладу, включаючи Національний університет оборони імені Міклоша Зріньі, у якому раніш відбувалася підготовка офіцерських кадрів. Питаннями надання сертифікату про акредитацію займалась акредитаційна рада за підтримки австрійських, німецьких та американських експертів. Згідно зі змінами до закону в редакції 1999 року загальна кількість угорських вищих навчальних закладів та коледжів повинна була скорочена приблизно до тридцяти. Це планувалося досягти через їх функціональну інтеграцію. Відповідно до нових редакцій цього закону суттєві зміни відбулися в системи підготовки офіцерів. З метою підвищення ефективності організації освітнього процесу для підготовки кадрів у сфері державного управління (у тому числі офіцерів) 1 січня 2012 року в м. Будапешт був створений новий вищий навчальний заклад - Національний університет державної служби шляхом інтеграції Національного університету оборони, Поліцейської академії та факультету державного управління Будапештського університету імені Корвіна.

На цей час до складу університету входять [15]: 5 факультетів (політичних наук та державного управління; міжнародних та європейських досліджень; військових наук та підготовки офіцерів; правоохоронних органів; водних наук), 3 інститути (досліджень та розвитку в галузі державного управління; національної безпеки; управління боротьбою зі стихійними лихами); 4 докторантури (державного управління; військової науки; військової техніки; правоохоронних органів).

Підготовка офіцерських кадрів відбувається на факультеті військових наук та підготовки офіцерів. Загальна структура факультету наведена на рис. 1.

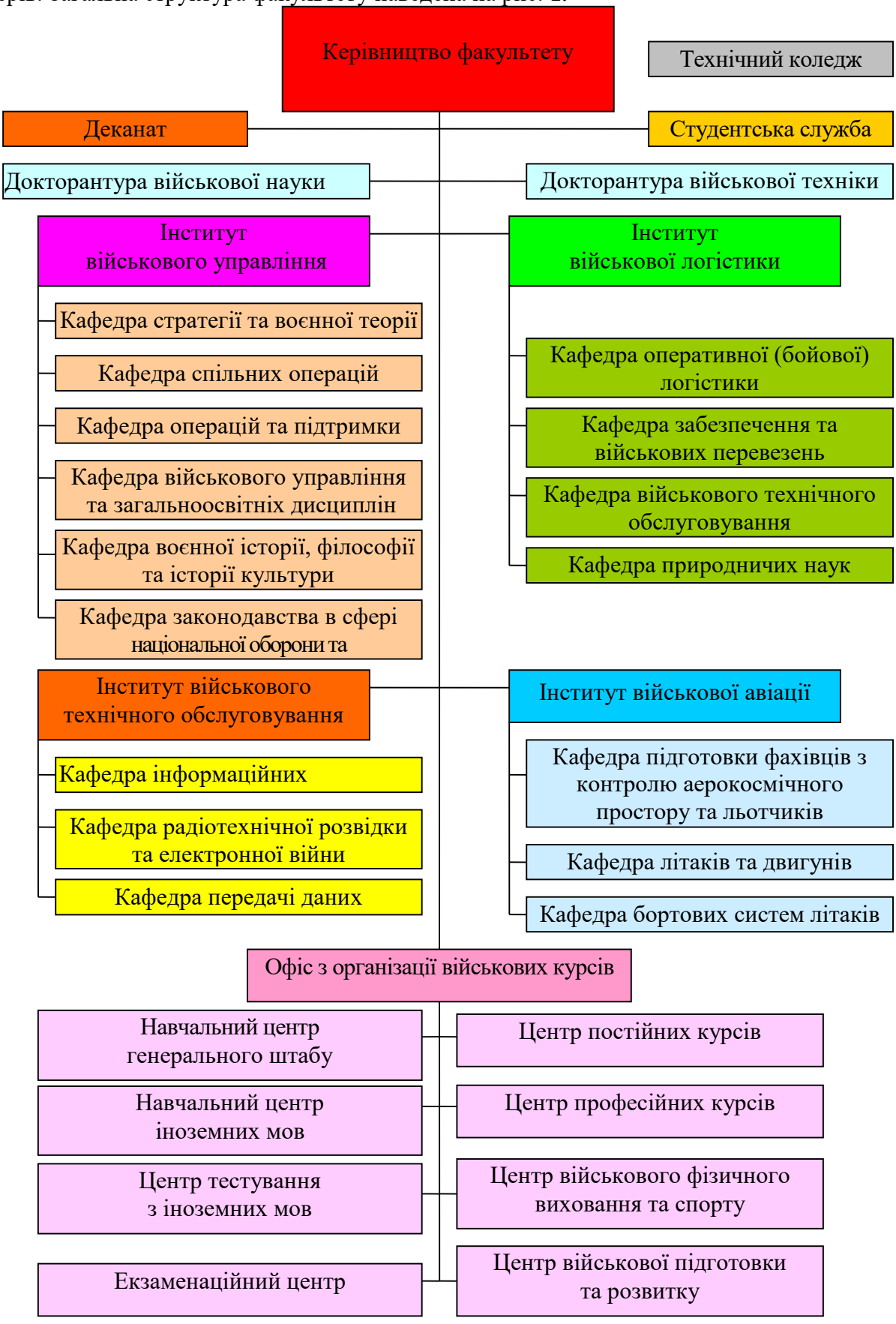


Рисунок 1 – Загальна структура військових наук та підготовки офіцерів

До складу факультету військових наук та підготовки офіцерів входять: **керівництво** (декан факультету; заступник декана з науки та міжнародних відносин; заступник декана з освіти; голова деканату (начальник навчального відділу); **докторантури** (військової техніки; військової науки), інститути (військового управління; військової логістики; військового технічного обслуговування; військової авіації); **навчальні центри** (генерального штабу; іноземних мов; тестування з іноземних мов; екзаменаційний; постійних курсів; професійних курсів; військової підготовки та розвитку; військової фізичної виховання та спорту) [16].

Завданням *інституту військового управління* є проведення підготовки офіцерів командного фаху для підрозділів сухопутних військ на освітніх рівнях бакалавра та магістра.

Інститут військової логістики проводить підготовку офіцерів до виконання завдань на командних (керівних) посадах в підрозділах логістики в якості начальників відділів логістики (заступників начальників з логістики) військових частин або в якості посадових осіб підрозділів логістики вищих ланок військового управління. Інститут має дві багатонаціональні програми підготовки (тренінги), що проводяться сумісно з партнерами з Австрії, Чехії та Великобританії: багатонаціональний об'єднаний тренінг з логістики MAGLITE (оперативний рівень); тренінг з логістики FOURLOG (тактичний рівень).

Інститут військового технічного обслуговування здійснює підготовку офіцерів до виконання завдань на командних (керівних) посадах у сфері передачі даних, ведення електронної війни, а також застосування інформаційних технологій у збройних силах.

Інститут військової авіації (розташований в м. Сольнок) забезпечує підготовку офіцерів льотного та інженерно-авіаційного профілю, а також офіцерів з контролю повітряного простору.

Навчальний центр генерального штабу проводить 11-ти місячний навчальний курс для підготовки офіцерів з метою отримання ними стратегічного рівня військового управління - найвищого рівня національної військової освіти.

Навчальний центр з іноземних мов має широкий спектр завдань, що включають до себе навчання курсантів за програмою бакалаврату та їх підготовки до мовного тестування відповідно до вимог навчальної програми. Центр також проводить навчальні мовні курси, де військовослужбовці та співробітники міністерства оборони отримують та вдосконалюють свої знання з мовної підготовки.

Центр тестування з іноземних мов проводить акредитовані мовні тестування в 3-х різних мовних тестових системах: ARMA – двомовний військовий мовний тест з 9-ти мов (англійська, французька, німецька, італійська, російська, хорватська, сербська, словацька, українська); НАТО STANAG 6001 – одномовний військовий мовний тест (англійська); спільний мовний тест на 5-ти мовах (англійська, французька, німецька, італійська, російська). Тестування проводиться на трьох рівнях: початковому; середньому; просунутому в рамках 9 екзаменаційних сесій. Середня кількість кандидатів на тестування - приблизно 1100 осіб на рік, більшість з яких проходить військовий мовний тест НАТО STANAG 6001. У разі успішного проходження мовного тесту кандидати отримують акредитовані сертифікати, які визнані в Угорщині без обмеження у часі.

Екзаменаційний центр має подвійну мету. По-перше, це проведення офіцерських і унтер-офіцерських (сержантського складу) сертифікаційних екзаменів для просування по службі. По-друге, проведення екзаменів на здобуття бакалаврського та магістерського ступенів освіти тими, хто навчається на факультеті.

Центр військової підготовки та розвитку сумісно з центрами постійних курсів та професійних курсів відповідає за організацію та проведення різноманітних курсів професійної перепідготовки та підвищення кваліфікації офіцерського складу перед призначенням на вищі посади.

Головним завданням *центру військового фізичного виховання та спорту* є розвиток та удосконалення сили, витривалості та спритності курсантів в різних умовах.

Загальна кількість викладачів факультету складає біля 270 осіб.

Початковий освітній рівень підготовки для офіцерів збройних сил Угорщини є «бакалавр». Підготовка офіцерів на первинні посади здійснюється за бакалаврськими програмами з числа громадян Угорщини, які на час вступу мають вік від 18 років до 25 років, отримали повну середню освіту, відповідають вимогам щодо стану здоров'я, розумової та фізичної придатності та які успішно пройшли відповідну співбесіду (інтерв'ю). Приймальна комісія оцінює загальну поінформованість кандидата, його схильність до військової кар'єри, навички спілкування і поведінкову культуру. Одною з основних вимог при вступі на бакалаврські програми факультету є наявність у кандидата визнаного державою сертифіката досягнення мовного рівня B2 (раніше Intermediate – середній) або еквівалентного документа щодо тестування з англійської мови [16].

Термін навчання - 4 роки. Щорічний набір становить близько 90 осіб. На навчання приймаються як чоловіки, так й жінки. За бакалаврськими програмами навчається переважно молодь у віці до 25 років, з якої близько 60 % від загальної чисельності курсантів – особи у віці від 18 років до 21 років, 30 % – особи, яким від 22 років до 25 років, та 10 % – ті, кому більше 25 років. При цьому, з кандидатів на навчання (з тих, хто вступили на 1 курс) близько 75 % від загальної чисельності вступників складають ті, хто закінчив середню школу, та 25 % ті, хто закінчив професійно-технічний навчальний заклад.

Ті, хто навчаються, мають статус курсанта (офіцера-кадета). Їхні права та обов'язки регулюються відповідними законодавчими та нормативно-правовими актами. Курсанти під час навчання в університеті забезпечуються встановленою формою одягу, їжею, гуртожитком, медичним обслуговуванням, регулярним місячним базовим грошовим утриманням, навчальними та навчально-методичними посібниками. Для курсантів мешкання в гуртожитках є обов'язковим.

При підготовці використовуються різні види навчальних занять (лекції, групові, практичні, лабораторні, семінарські заняття тощо), проводиться постійний обмін досвідом із закордонними військовими навчальними закладами. Для всіх спеціальностей передбачена професійна практика (стажування) терміном 8-16 тижнів поза університетом у військових частинах на майбутніх первинних офіцерських посадах. Велика увага приділяється мовній підготовці. Курсанти готуються до проміжних або просунутих спеціалізованих мовних екзаменів у відповідності до навчальних програм підготовки та освіти. Для отримання диплому бакалавра курсант повинний здати державний екзамен з іноземної мови (середнього рівня) та типовий військовий мовний тест з англійської мови STANAG 6001 НАТО рівня 2.2.2.2. [17].

Для забезпечення міждисциплінарної підготовки курсантів технічних спеціальностей на факультеті створений технічний коледж Tivadar Puskás. Навчальні заняття проводяться за темами, які не розглядаються в традиційній навчальній програмі, однак пов'язані з нею. Це надає курсантам додаткові знання до програм університетської освіти.

У навчальному процесі широко застосовується різного типу тренажери (імітатори), які є розробками угорських виробників. Так, угорська фірма Artifex спеціалізується на розробці та впровадженні систем моделювання та підготовки, які використовуються в навчальному процесі та у військах. Серед розробок фірми можна відмітити наступні програмні тренажерні комплекси: віртуальний тренажер KRONOS; конструктивний тактичний симулятор розташування Marcus. Усі тренажери, що використовуються, відповідають сертифікатам якості ISO 9001 та NATO AQAP 2110.

Віртуальний тренажер KRONOS - тактичний тренажер реального часу. Кожний користувач має автоматизоване робоче місце в залежності від його номеру розрахунку та функцій, а саме - управління транспортним засобом або системою озброєння. Під час тренування курсанти можуть спостерігати за тактичною обстановкою через призми та біноклі, як в реальному бою. Тренажер не є лише "стріляючою грою", він вимагає виконання усіх функцій відповідно до реальних зразків зброї. Персонал екіпажу для передачі команд використовує імітовану радіомережу. В тренажері реалізований реалістичний ландшафт, демонструються візуальні удари та вибухи, які супроводжуються реалістичними звуковими

ефектами. Він може симулювати бойове застосування, як наземних зразків техніки (наприклад, танк), так і повітряної техніки (наприклад, вертоліт).

Конструктивний тактичний симулятор розташування Marcus має наступні переваги: конструктивне моделювання корпоративного рівня; висока деталізація, реалістичний віртуальний бій; багаторазове моделювання; дозволяє поєднувати рівні для рішення великих завдань (вправ); швидка підготовка та зміна сценаріїв; підтримка вбудованої автоматичної маршрутизації з обхідними шляхами; високий рівень настроювання.

Підготовка льотчиків для військово-повітряних сил в інституті військової авіації розпочалася у 2018 році після двадцятирічної перерви на авіаційній базі м. Сольнок. Термін навчання складає також 4 роки. При цьому, загальна підготовка - 2 роки, льотна – 2 роки із загальним нальотом 220 годин. Основним критерій відбору кандидатів на навчання – ідеальне здоров'я. Триденне медичне обстеження проводиться у військовому шпиталі м. Кечкемет. Планується здійснювати підготовку льотчиків на літаки-винищувачі, літаки транспортної авіації та вертольоти, що знаходяться на озброєнні військово-повітряних сил. Серед тренувального парку: літаки Zlín Z42 (2 літаки), Zlín Z43 (2 літаки - замовлені) та Saab JAS 39 Gripen (2 літаки) є новими типами літаків, а літаки Як-52 (9 літаків) та Л-39 (7 літаків знаходяться на зберіганні) є застарілими та отримані Угорщиною ще у 1993 – 1994 роках з Німеччини.

Після здачі екзаменів та отримання дипломів бакалавра випускники університету направляються у війська та займають первинні офіцерські посади. Для подальшого просування по службі, як правило, у військовому званні «капітан» або «майор» офіцери продовжують навчання в магістратурі факультету військових наук та підготовки офіцерів. При цьому, кандидат на навчання повинен отримати попередній дозвіл на вступ від начальника генерального штабу, а також пройти базову експертизу з державної служби. В рамках процедури прийому в магістратуру проводиться співбесіда.

Магістерські програми засвоюються протягом 1 навчального року. В магістратурі факультету навчається біля 90 % офіцерів у віці понад 35 років. Як виняток передбачений вступ на навчання за магістерськими програмами безпосередньо після отримання випускником університету диплома бакалавра. Чисельність тих, хто вступає на навчання до магістратури безпосередньо після завершення бакалаврської програми, складає до 5 % від загальної чисельності вступників (у 2017/2018 навчальному році – 1 особа).

Програма підготовки зазначених офіцерських кадрів охоплює і забезпечує надання таких знань: поглиблене бачення щодо завдань і діяльності збройних сил, ґрунтовні знання про вид збройних сил; ґрунтовні бачення і навички, пов'язані з управлінням підрозділами різних видів збройних сил (родів військ), а також управління військовими підрозділами (частинами), підсиленими ротою, батальйоном (або рівнозначними); теоретичні основи і практичні навички оцінки ситуації та прийняття рішення; обов'язкові процедури, які здійснюються в штабах НАТО; бойові можливості та основи застосування роду військ в різних умовах бойової обстановки; загальні основи оперативного мистецтва і тактики різних родів військ відповідного виду збройних сил; основи організації і методика проведення підготовки (проведення навчань) частин і з'єднань [17].

Після успішного завершення навчання випускники отримують відповідні дипломи та призначаються на посади з штатно-посадовою категорією «підполковник».

Навчальний курс генерального штабу, як найвищий рівень національної військової освіти, пропонує 11-місячну програму [17]. Навчальна програма передбачає підготовку відібраних військових керівників до виконання обов'язків стратегічного керівництва з використання збройних сил. Протягом навчання слухачі отримують знання щодо проблем міжнародної і національної безпеки, функціонування органів системи національної безпеки, теорії та практики стратегічного управління обороною та збройними силами. Удосконалюються їх практичні навички прийняття стратегічних рішень, планування та управління операціями збройних сил у різних умовах навколишнього середовища. Навчання

розвиває здатність працювати в багатокультурному середовищі та багатонаціональних штабах, які відповідають вимогам НАТО.

Крім того, навчальна програма призначена для: сприяння розвитку стратегічного мислення тих, хто навчається; розвитку їх спроможності керувати на стратегічному рівні військового управління; підвищення здатності критично мислити на рівні військово-стратегічних концепцій в динамічному міжнародному середовищі; розширення розуміння офіцерами природи конфліктів та існуючих і майбутніх загроз для Угорщини та її союзників по НАТО. Ці знання та навички є ключовими для керування з'єднаннями та об'єднаннями збройних сил з врахуванням основних чинників, що формують стратегічне середовище національної безпеки та оборони, включаючи планування та керівництво збройними силами.

Курс складається з трьох модулів: *загальний базовий модуль* – містить курси, пов'язані з керівництвом, безпекою навколишнього середовища, воєнним мистецтвом, внутрішньою обороною та суспільством; *військовий модуль* – містить курси, пов'язані з теорією і практикою планування та проведення операцій і передбачає відвідуванням слухачами військових частин; *заключний модуль* – передбачає вивчення останніх наукових досліджень у галузі військових наук, відвідування військових і цивільних компаній та ознайомчі поїздки закордон. Випускники можуть бути призначені на керівні посади стратегічного рівня в міністерстві оборони, збройних силах Угорщини, багатонаціональних штабах НАТО та ЄС.

Висновки: Існуюча СВО Угорщини успішно пройшла період трансформації збройних сил до вимог НАТО, використовує досвід підготовки військових фахівців у розвинутих країнах-членах альянсу з урахуванням особливостей національної системи освіти. Вона забезпечує підготовку офіцерських кадрів за необхідними військовими спеціальностями.

ЛІТЕРАТУРА:

1. Черних, Ю.О. Система підготовки офіцерських кадрів у збройних силах республіки Болгарія /Ю.О. Черних, О.Б. Черних //Зб. наук. праць ВІКНУ ім. Т. Шевченка. – 2018. – Вип. № 59. – С. 204-215.

2. Богунов, С.О. Основи організації та функціонування системи військової освіти Великобританії – аналітичний огляд /С.О. Богунов, Ю.О. Черних, О.Б. Черних //*Військова освіта.* – 2017.- № 2 (36). – С. 234-245.

3. Богунов, С.О. Організація підготовки офіцерів для збройних сил республіки Литва /С.О. Богунов, Ю.О. Черних, О.Б. Черних //Військова освіта. – 2018. – № 1 (37). – С. 272-285.

5. Мітягін, О.О. Система підготовки військових фахівців у збройних силах країн Балтії: досвід для України» // О.О. Мітягін, О.Б. Черних, Ю.О. Черних //*Науковий вісник інноваційних технологій.* – 2018. – № 1(17). – С. 49-61.

5. Гацко М. Профессиональная подготовка унтер-офицеров и сержантов в зарубежных армиях / М. Гацко *// Зарубежное военное обозрение.* – 2009. – № 5. – С. 21-28.

6. Лазукин, В. Подготовка офицерских кадров в ВС ФРГ /В. Лазукин // *Зарубежное военное обозрение.* – 2008. – № 2. – С. 26-30.

7. Черних, Ю.О. Основи організації та функціонування системи військової освіти Німеччини – аналітичний огляд» /Ю.О. Черних, О.Б Черних//*Зб. наук. праць ВІКНУ ім. Т. Шевченка.* – 2017. – вип. № 57. – С. 238-248.

8. Черних, О.Б. Аналіз сучасного стану системи військової освіти республіки Польща: досвід для України /О.Б. Черних, О.О. Мітягін, Ю.О. Черних //*Військова освіта.*– 2017. – № 1 (35). – С. 200-208.

9. Владимирова, С. Исследования в области совершенствования профессионализма личного состава вооруженных сил США /С. Владимирова, А. Стрелецкий // *Зарубежное военное обозрение.* – 2006. – № 5. – С. 15-19.

10. Приходько, Ю.І. Підготовка військових фахівців у провідних країнах світу: основоположні засади та тенденції /Ю.І. Приходько //*Педагогічні науки: теорія, історія, інноваційні технології.* – 2017. – № 3 (67). – С. 285-299.

11. Толок, І.В. Особливості підготовки військових фахівців тактичного рівня у ВВНЗ США та окремих країн НАТО / І.В. Толок, Ю.М. Супрунов //*Військова освіта.* – 2018. – № 1 (37) – С. 259-271.

12. Колесов, П. Сен-Сирская специальная военная школа вооруженных сил Франции /П. Колесов, А. Стрелецкий //Зарубежное военное обозрение. –2006. – № 6. – С. 26-32.

13. Черних, Ю.О. Основи організації та функціонування системи військової освіти Франції – аналітичний огляд /Ю.О. Черних, О.Б. Черних //*Зб. наук. праць ВІКНУ ім. Т. Шевченка.* – 2017. – Вип. № 56. – С. 249-257.

14. Törvény a nemzeti felsőoktatásról [Електронний ресурс] /Режим доступу/ http://njt.hu/cgi_bin/njt_doc.cgi?docid=142941.357426.

15. Nemzeti Közszolgálati Egyetem [Електронний ресурс] /Режим доступу/ https://www.uni-nke.hu/.

16. Hadtudományi és honvédtisztképző kar. [Електронний ресурс] /Режим доступу/ https://nbi.uni-nke.hu/intezetunkrol/az-intezet-feladatai.

17. Haditechnika szakirány közös tárgyak [Електронний ресурс] /Режим доступу/ https://hhk.uni-nke.hu/oktatasi-egysegek/haditechnikai-tanszek/a-katonai-logisztikai-alapkepzesi-szak-haditechnikai-specializacio-tantargyai/haditechnika-szakirany-kozos-targyak.

REFERENCES:

1. Chernykh, Yu.O., Chernykh, O.B. (2018). Systema pidhotovky ofitserskykh kadriv u zbroynykh sylakh respubliky Bolhariya [Officer training system in the armed forces of the republic of Bulgaria]. Zb. nauk. prats VIKNU im. T. Shevchenka, 59, 204-215. (in Ukrainian).

2. Bohunov, S.O., Chernykh, Yu.O., Chernykh, O.B. (2017). Osnovy orhanizatsiyi ta funktsionuvannya systemy viyskovoyi osvity Velykobrytanyy - analitychnyy ohlyad [Basics of organization and functioning of the Great Britain military education system - analytical review]. Military education, 2 (36), 234-245. (in Ukrainian).

3. Bohunov, S.O., Chernykh, Yu.O., Chernykh, O.B. (2018). Orhanizatsiya podhotovky ofitseriv dlya zbroynykh syl respubliky Lytva [Organisation of officer training for the armed forces of the republic of Lithuania]. Military education, 1 (37), 272-285. (in Ukrainian).

4. Mityahin, O.O., Chernykh, O.B., Chernykh, Yu.O. (2018). Systema pidhotovky viyskovykh fakhivtsiv u zbroynykh sylakh krayin Baltiyi: dosvid dlya Ukrayiny [Educational system for military specialists in the armed forces of the Baltic countries: experience for Ukraine].Scientific Bulletin of innovative technologies, 1(17), 49-61. (in Ukrainian).

5. Gatsko, M. (2009). Professional'naya podgotovka unter-ofitserov i serzhantov v zarubezhnykh armiyakh [Professional training of non-commissioned officers and sergeants in foreign armies]. Foreign military review, 5, 21-28. (in Russian).

6. Lazukin, V. (2008). Podgotovka ofitserskikh kadrov v VS FRG [Training of officer cadres in the Armed Forces of the FRG]. Foreign military review, 2, 26-30. (in Russian).

7. Chernykh, Yu.O., Chernykh, O.B.,. (2017). Osnovy orhanizatsiyi ta funktsionuvannya systemy viyskovoyi osvity Nimechchyny – analitychnyy ohlyad [Basics of organization and functioning of the Germany military education system - analytical review] Zb. nauk. prats VIKNU im. T. Shevchenka, 57, 238-248. (in Ukrainian).

8. Chernykh, O.B.,. Mityahin, O.O,. Chernykh, Yu.O, (2017). Analiz suchasnoho stanu systemy viyskovoyi osvity respubliky Polshcha: dosvid dlya Ukrayiny [The current state analysis of the military education system of the republic of Poland: experience for Ukraine]. Military education, 1 (35), 200-208. (in Ukrainian).

9. Vladimirova, S., Streletskiy,A. (2006). Issledovaniya v oblasti sovershenstvovaniya professionalizma lichnogo sostava vooruzhennykh sil SSHA [Studies in the field of improving the professionalism of the personnel of the US armed forces]. Foreign military review, 5, 15-19. (in Russian).

10. Prykhodko, Yu.I., (2017). Pidhotovka viyskovykh fakhivtsiv u providnykh krayinakh svitu: osnovopolozhni zasady ta tendentsiyi [Training of military specialists in leading countries of the world: fundamental principles and trends]. Pedagogical sciences: theory, history, innovative technologies, 3 (67), 285-299. (in Ukrainian).

11. Tolok, I.V., Suprunov Yu.M. (2018). Osoblyvosti pidhotovky viyskovykh fakhivtsiv taktychnoho rivnya u VVNZ SSHA ta okremykh krayin NATO [Peculiarities of training of tactical-level military specialists]. Military education, 1 (37), 259-271. (in Ukrainian).

12. Kolesov, P., Streletskii, A. (2006). Sen-Sirskaya spetsial'naya voyennaya shkola vooruzhennykh sil Frantsii [Saint-Sire Special Military School of the French Armed Forces]. Foreign military review, 6, 26-32. (in Russian).

13. Chernykh, Yu.O., Chernykh, O.B.,. (2017). Osnovy orhanizatsiyi ta funktsionuvannya systemy viyskovoyi osvity Frantsiyi – analitychnyy ohlyad [Basics of organization and functioning of the French

military education system - analytical review]. Zb. nauk. prats VIKNU im. T. Shevchenka, 56, 249-257. (in Ukrainian).

14. Law on national higher education. Available at: http://njt.hu/cgi_bin/-njt_doc.cgi?docid=-142941.357426, (in Hungarian).

15. National university of public service. Available at: https://www.uni-nke.hu/,(in Hungarian).

16. Faculty of military sciences and military officers. Available at: https://nbi.uni-nke.hu/intezetunkrol/az-intezet-feladatai, (in Hungarian).

17. Military engineering major in common subjects. Available at: https://hhk.uni-nke.hu/oktatasi-egysegek/haditechnikai-tanszek/a-katonai-logisztikai-alapkepzesi-szak-haditechnikai-specializacio-tantargyai/haditechnika-szakirany-kozos-targyak, (in Hungarian).

Ph.D. Chernykh J, Chernykh O.

OFFICER TRAINING SYSTEM IN THE REPUBLIC OF HUNGARY

Analysis of the foreign experience of the organisation and reformation of the armed forces in other countries, with the respective systems of military education being an integral part, reveals the specific national aspect of such activities in each country. In the meantime, there are some general methodological approaches used in military pedagogic practice across different countries of the world to be practicably considered and applied. The article examines the experience of officers' training for the armed forces of the Republic of Hungary. The article provides information on the existing network of military educational institutions for the officer training of tactical, operational and strategic level of military command. Requirements for admission to military educational institutions for the officer training of different levels of training has been given. The terms of military specialists' training on tactical, operational and strategic level have been defined. The analysis of the content of officer training for different armed services of the armed forces and different levels of military administration has been conducted.

We used the system of the general scientific methods of theoretical and empirical research, in particular, the theoretical-methodological analysis of the problem and the relevant scholarly resources, systematization and generalization of the scientific information pertaining to the essence and content of the set objectives, monitoring of the existing system of military specialists training in the Armed Forces of the republic of Hungary, scientific generalisation, the general scientific methods of logical and comparative analysis, systems approach, peer review, analysis and interpretation of the obtained theoretical and empirical data.

The general structure of the National University of Public Administration, the Faculty of Military Sciences and the training of officers is shown, as well as the main tasks that are solved by the institutes and training centers that are part of it are identified. An analysis of the concept, structure, goals, content and technologies of officers' training in the armed forces of the Republic of Hungary shows that the military education system reflects the current stage of development of the armed forces, as well as the national cultural specificity of the country. Education and training of officers is carried out on the basis of national cultural and military tradition. The main direction of officers' training is their fundamental military and professional training in both the military and civilian fields.

The content of the officers' training is based on two military education levels. Each level of military education ends with a certain level of qualification. It is possible to distinguish the general tendencies of development of the higher Hungarian military school: improvement of the quality of applicants' selection, individualization of training of cadets and trainees, stabilization of their number at the present level; further informatization of the educational process, introduction of multimedia learning tools.

Certainly, the positive elements of the experience of the Hungarian army can be used in the training of officers in the Ukrainian Armed Forces under the conditions of gradual transition to the recruitment on a contract basis.

Keywords: military education system; the armed forces of Hungary; officer training experience.

ДАНІ ПРО АВТОРІВ

Атаманюк Алла Василівна, магістр кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету.

Ахмаметьєва Ганна Валеріївна, кандидат технічних наук, доцент Одеського національного політехнічного університету, https://orcid.org/0000-0002-0567-902X.

Банзак Геннадій В'ячеславович, кандидат технічних наук, доцент кафедри Метрології та метрологічного забезпечення Одеської державної академії техничного регулюівання та якості, http://orcid.org/0000-0003-1684-3785.

Банзак Оксана Вікторівна, доктор технічних наук, доцент, завідувач кафедри електрорніки та мікросистемної техніки Одеської державної академії технічного регулювання та якості, https://orcid.org/0000-0003-6649-5013.

Баранюк Ганна Андріївна, студентка Одеського національного політехнічного університету.

Баргилевич Анатолій Владиславович, Командувач територіальної оборони Командування Сухопутних військ Збройних Сил України, https://orcid.org/0000-0002-4799-0908.

Бичков Олексій Сергійович, доктор технічних наук, доцент, професор кафедри, завідувач кафедри програмних систем і технологій, факультет інформаційних технологій, Київський національний університет ім. Тараса Шевченка, https://orcid.org/0000-0002-9378-9535.

Вишняков Володимир Михайлович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, http://orcid.org/0000–0003-4668-712X.

Возікова Людмила Михайлівна, старший викладач кафедри Електроніки та мікросистемної техніки Одеської державної академії техничного регулюівання та якості, http://orcid.org/0000-0002-9983-5731.

Георгадзе Олександр Аміранович, кандидат військових наук, професор кафедри керівництва військами (силами) в мирний час, Національний університет оборони України імені Івана Черняховського, https://orcid.org/0000-0002-9306-6660.

Гріффен Леонід Олександрович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, провідний науковий співробітник Центру пам'яткознавства Національної академії наук України і Українського товариства охорони пам'яток історії та культури.

Джулій Володимир Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, http://orcid.org/0000-0003-1878-4301.

Дружинін Володимир Анатолійович, доктор технічних наук, професор, професор кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, http://orcid.org/0000-0002-5340-6237.

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.

Комаров Володимир Олександрович, Заслужений винахідник України, начальник науково-дослідного відділу Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, https://orcid.org/0000-0002-4929-4527.

Лещенко Олег Іванович, кандидат технічних наук, доцент, доцент кафедри електроніки та мікросистемні техніки Одеської державної академії техничного регулюівання та якості, https://orcid.org/0000-0001-8589-8596.

Лєнков Євген Сергійович, кандидат технічних наук, старший науковий співробітник наукового центру Центрального науково-дослідного інституту Збройних Сил України, http://orcid.org/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, https://orcid.org/0000-0001-7689-239X.

Лоза Віталій Миколайович, кандидат технічних наук, начальник відділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-8050-3614.

Маслов Олег Вікторович, доктор технічних наук, доцент, завідувач кафедри Фізики Одеського національного політехнічного університету, https://orcid.org/0000-0002-0288-0289.

Машталір Вадим Віталійович, доктор історичних наук, доцент, Заслужений винахідник України, начальник управління організації комплектування офіцерським складом Головного управління персоналу Генерального штабу Збройних Сил України, ORCID: http://orcid.org/0000-0002-8132-217X.

Міночкін Дмитро Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри телекомунікацій Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», http://orcid.org/0000-0003-4988-7098.

Мокрицький Вадим Анатолійович, доктор технічних наук, професор, професор кафедри Інформційних технологій проектування в електроніці та телекомунікаціях Одеського національного політехнічного університету, https://orcid.org/0000-0002-2514-4137.

Нікіфоров Микола Миколайович, кандидат військових наук, старший науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-2849-5688.

Орленко Вікторія Сергіївна, кандидат технічних наук, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету.

Пампуха Ігор Володимирович, кандидат технічних наук, доцент, начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-4807-3984.

Пархоменко Іван Іванович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та захисту інформації Київський національний університет імені Тараса Шевченка, http://orcid.org/0000-0002-1919-9174.

Петрівський Володимир Ярославович, аспірант кафедри програмних систем і технологій, факультет інформаційних технологій, Київський національний університет ім. Тараса Шевченка, https://orcid.org/0000-0001-9298-8244.

Плющ Олександр Григорович, кандидат технічних наук, доцент, професор кафедри Мобільних та відеоінформаційних технологій Державний університет телекомунікацій, http://orcid.org/0000-0001-5310-0660.

Рижева Надія Олександрівна, доктор історичних наук, професор, професор кафедри історії Миколаївського національного університету імені В.О. Сухомлинського, https://orcid.org/0000-0001-8379-4325.

Сєлюков Олександр Васильович, доктор технічних наук, старший науковий співробітник, заступник директора ТОВ «Укрспецконсалтинг», https://orcid.org/0000-0001-7979-3434.

Степанов Михайло Миколайович, доктор технічних наук, старший науковий співробітник, професор кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченко, http://orcid.org/0000-0001-6376-4268.

Сушин Ігор Олексійович, магістрант кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», http://orcid.org/0000-0003-4866-4351.

Толок Ігор Вікторович, кандидат педагогічних наук, доцент, Заслужений працівник освіти України, Лауреат Державної премії України в галузі освіти, начальник Військового інституту, Київський національний університет імені Тараса Шевченка, http://orcid.org/0000-0001-6309-9608.

Толюпа Сергій Васильович, доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київський національний університет імені Тараса Шевченка, http://orcid.org/0000-0002-1919-9174

Трофимчук Вікторія Миколаївна, викладач кафедри комп'ютерної інженерії Державного університету телекомунікацій.

Хлапонін Юрій Іванович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, http://orcid.org/0000–0002-9287-0817.

Черних Ольга Борисівна, старший науковий співробітник науково-дослідного відділу військової освіти і науки центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняхівського, https://orcid.org/0000-0001-9865-5598.

Черних Юрій Олексійович, кандидат технічних наук, доцент, Заслужений працівник освіти УКраїни, провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002- 0780-6627.

Чернишев Денис Олегович, доктор технічних наук, професор, перший проректор Київського національного університету будівництва і архітектури, http://orcid.org/0000-0002-1946-9242.

Шевченко Віктор Леонідович, доктор технічних наук, професор, кафедра програмних систем і технологій, факультет інформаційних технологій, Київський національний університет ім. Тараса Шевченка, https://orcid.org/0000-0002-9457-7454.

Шевчук Віталій Вікторович, кандидат військових наук, начальник науково-дослідної лабораторії проблем воєнної безпеки держави кафедри стратегії національної безпеки та оборони України імені Івана Черняховського, https://orcid.org/0000-0002-8532-739X.

Алфавітний покажчик

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

№ 68

Усі матеріали надруковані в авторській редакції.
Деякі статті не рецензуються, у зв'язку з пріоритетною кваліфікацією авторів або через сумніви редколегії у змісті.

Підписано до друку 18.12.20 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