ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ВІСНИК
ЧЕРКАСЬКОГО ДЕРЖАВНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ

Технічні науки

Заснований у грудні 1996 р. **3/2020**

ЗАСНОВНИК І ВИДАВЕЦЬ – Черкаський державний технологічний університет

Свідоцтво про державну реєстрацію друкованого засобу масової інформації КВ № 6061 від 16.04.2002 р.

Виходить 4 рази на рік

У ВИПУСКУ:

АДРЕСА РЕДАКЦІЇ:
ЧДТУ, к. 604/1, бульвар Шевченка, 460,
м. Черкаси, 18006,
тел. (0472) 51-15-89
vtn.chdtu.edu.ua (подання статей)

Сисоєнко С. В. *(технічний секретар)*
Мельник І. В. *(відповідальний секретар)*
тел. (0472) 51-36-39; e-mail: mal_04@ukr.net

3·2020

ВІСНИК
Черкаського державного технологічного університету

ТЕХНІЧНІ НАУКИ

VISNYK
Cherkaskogo derzhavnogo
tehnologichnogo universitetu

TECHNICAL SCIENCE
3 • 2020

Видання включене до Переліку наукових фахових видань України як фахове видання з технічних наук (спеціальності 101, 113, 121, 122, 123, 125, 126, 131, 132, 133, 151, 152, 161, 172) категорія «Б»
(накази МОНУ від 02.07.2020 №886, від 24.09.2020 №1188)

Видання зареєстровано у міжнародних наукометричних базах, каталогах і системах пошуку:
Index Copernicus Journals Master List, BASE, CiteFactor, Google Scholar, Crossref, Directory of Open Access Journals (DOAJ), Eurazian Scientific Journal Index (ESJI), ResearchBib – Academic Recource Index, Ulrich's Periodicals Directory, WorldCat, Наукова періодика України, Open Ukrainian Citation Index

Електронна версія:
visnyk.chdtu.edu.ua; vtn.chdtu.edu.ua
https://chdtu.edu.ua

ISSN 2306-4412 (Print),
ISSN 2306-4455 (CD-ROM),
ISSN 2708-6070 (Online)

Затверджено вченою радою Черкаського державного технологічного університету, протокол № 3 від 19.10.2020 р.

ЗМІСТ

АВТОМАТИЗАЦІЯ І ПРИЛАДОБУДУВАННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ХІМІЧНІ ТЕХНОЛОГІЇ ТА ІНЖЕНЕРІЯ, ЕКОЛОГІЧНА БЕЗПЕКА

CONTENTS

AUTOMATION AND CONSTRUCTION OF DEVICES

INFORMATION TECHNOLOGIES

CHEMICAL TECHNOLOGIES AND ENGINEERING, ECOLOGICAL SECURITY

УДК 621.3.047.42:004.942

[0000-0003-1329-635X] **V. B. Kyselov**
e-mail: vladkis.777@gmail.com
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

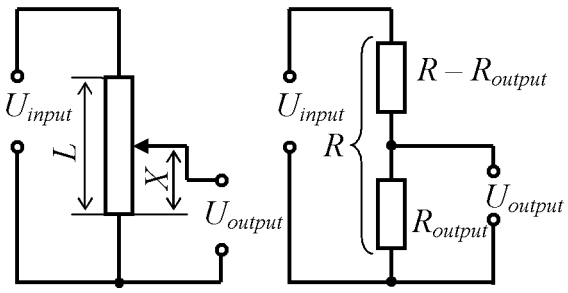
METHOD OF CONSTRUCTING A MATHEMATICAL MODEL OF WEAR-RESISTANCE IN POTENTIOMETER SENSORS

This article highlights the method of constructing a mathematical model of wear-resistance in potentiometer sensors. Depreciation process of working surfaces is so complex that by this time there are no reliable methods of its forecasting. Tribological processes taking place during potentiometer sensor performance are complicated by electric current influence that flows through the contact surface and accelerates the process of contact surfaces wear. As a result, the mathematical model is offered, that considers the simultaneous action of tribological elastic contact, plastic deformation, microcutting and electrical erosion with constant number of performance cycles. Wear-resistance is represented as the magnitude of change in volume of the worn material depending on the shape and material of contact surfaces, contact pressure and magnitude of electric current. The model is represented in the form of dependence, interpreted by the direct equation, greatly simplifies the forecasting of wear-resistance on the basis of experimental data. Mathematical model, obtained by adding bulk models of mechanical and current wear can be used to predict durability in the design and operation of potentiometer sensors, wire potentiometers and other devices that have a similar structure and work under the current.

Keywords: *sliding contact, wire potentiometer, tribological processes, capacious erosion, reliability of work.*

Introduction. Potentiometer sensors are designed to convert a mechanical movement into an electrical signal by changing the active resistance of electrical circuit. Signal of the engine position in the tension meter is being removed, as from the voltage divider, after the power supply to the sensor. Potentiometer sensors are used mainly as sensors of linear and angular displacements. Potentiometer sensor is designed for the following purposes: control and measurement of mechanism displacements, working bodies of machinery and other objects; feedback segment in robotics and automation systems; defining distances to objects; testing in laboratories, mechanism performance control. For example, these sensors enable to set control over the position of latches, valves, vane on the weather station, antennas, cutting tools and much more [1, 2, 3]. They can also be used to transmit the indicators of non-electrical metering devices, such as manometers, liquid level meters, to transmit the notification of aeroplane chassis, etc [1, 3].

Potentiometer sensor is a potentiometer of the changeable resistance itself, which can be switched on by following the scheme of circuit voltage divider (Figure 1) [1]. When moving a contact under the influence of controlled magnitude X, there occurs a change in sensor resistance. Power supply voltage is activated within the entire winding of the potentiometer through the fixed contact of this winding. Output voltage, removed from the fixed contact and rolling engine, is proportional to the displacement of the engine. In electric engineering such a scheme of inclusion is called potentiometric or circuit voltage divider.



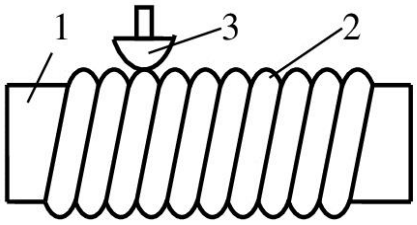
U_{input} – input voltage; U_{output} – output voltage; L – length of potentiometric sensor of potentiometer sensor winding; X – movement of the engine (brush) of potentiometric sensor; R – total resistance of potentiometric sensor; R_{output} – output resistance of potentiometric sensor

Figure 1 – Activation scheme of potentiometric sensor

DOI: 10.24025/2306-4412.3.2020. 199294

In automatic systems, the engine can be mechanically connected to any device (valve, steering wheel, receiver, cutting tool, etc.), location of the latter should be measured and passed in the form of an electric signal [3]. The effort, under the action of which the engine moves, is quite big in this case. Therefore, to ensure a reliable contact between engine and winding, you should have a pretty-strong force pressing the engine. The presence of a sliding contact reduces the reliability of potentiometer sensor and remains its basic disadvantage.

Structurally potentiometer sensor (Figure 2) consists of a frame 1, which is wrapped by one layer of the wiring 2 from the thin wire [2]. The engine (brush) slips 3 on the twisted coil, mechanically linked to the object and the displacement of which should be measured. The coil is made of isolated wire, and the path, on which the engine slips, is eliminated from isolation beforehand.



1 – frame; 2 – wiring; 3 – engine (brush)

Figure 2 – Line diagram of potentiometric sensor for measuring linear movement

Resolution defines the maximum possible accuracy of potentiometric sensor performance. It can be improved by increasing the number of turns *n*. It becomes possible via lengthening the wound part of the potentiometer *L* (at a given diameter of the wire), or reducing the cross section of the wire. Diameter reduction of the wire leads to technological difficulties in the manufacturing of windings, but, what is more important, reduces the reliability of the potentiometer, as mechanical strength of the winding is deteriorating and it is erased more quickly.

To ensure the reliability of the performance of sliding contacts in potentiometer sensors the requirements for their physical, mechanical and tribotechnical properties are set. Particular difficulty in solving tribotechnical problems in sliding contacts is an action of an electric current, which leads to a strengthening of friction and wear [4-7].

Classical wear theory considers the speed of material removal as a function of sliding speed, hardness of the material, applied load and the likelihood that the material will create a part of wear in a given contact situation [8-12].

The wear mode, typical for the end seals of the boundary friction, is most fully described by I. V. Kragelsky who worked out molecular-mechanical (adhesion-deformation) theory of friction and fatigue wear [11, 12]. According to this theory friction is caused, on the one hand, by the deformation of the material, which leads to a violation of the whole (elastic or plastic imprint), on the other hand, by overcoming the molecular (adhesion) connections in the contact area.

The process of working surface wear is so complex, that by this time there are no reliable methods of its forecasting [6, 9, 13, 14]. Even for the same materials, the intensity of wear may vary in several orders while the operating mode is changed: when changing the pressure of the sealing fluid, angular velocity, temperature, axial and angular vibrations. So far, the estimation of wear indicators is based on the operation experience and high degree of authenticity can't be demanded from them. The most reasonable and acceptable for engineering calculations formulae for wear intensity are given in the fundamental guide [1], but special physical and mechanical characteristics of these formulae (curve frictional fatigue setting; correction coefficient to the number of cycles corresponding to the separation of wear parts; coefficient characterizing the tense condition on the spot of contact, etc.) are partially systematized only for some of the most widespread constructional materials in dry friction conditions and do not take into account the influence of electric current.

In a number of works [7, 13] dependencies of wear rate from the contact pressure and the slip rate are experimentally defined. The Archard formula [8, 9, 15] contains parameters such as surface hardness, defined by the indentation method, the wear coefficient, which must be determined experimentally for each combination of material in the contacting pair and the seal liquid, and also for the certain operation conditions, including the friction mode, temperature, presence of vibrations, abrasive particles, etc.

It was Holm who proposed to take into account the impact of current on the value of mechanical wear in coal brushes of electric cars [6, 7, 9].

There are four dominant methodologies in this field – energy balance, mass balance, strain analysis, and contact mechanics approach [8, 9]. There is currently no direct connection or agreement between various models that can be found in

DOI: 10.24025/2306-4412.3.2020. 199294

the literature, and formal standardization as such in this area does not exist, which creates difficulties for both researchers and engineers who are trying to fight the effects of wear in its various forms [14, 15].

The aim of the study is to obtain wear mathematical model of contact pair of slip under current load by combining and improving the known mathematical approaches, taking into account the design features of wire potentiometers and potentiometer sensors.

Presentation of the main material in the research. Structurally potentiometer sensors are similar to wire potentiometers. Material of current-collection element of the slider, as well as the material of the resistive element, should be resistant against electrical erosion and corrosion, easily handled, possess properties that prevent the welding of contacts, have high heat and electrical conductivity, high durability together with the selected resistive wire, small and stable in time joint resistance.

The proposed estimation methodology of the contact pair of slipping under the current with constant development cycles N is to represent the total volume of wear as a sum of two components [16]:

$$V_{\Sigma} = V_m + V_I, \qquad (1)$$

where V_m is a mechanical wear under current, equal to zero; V_I is an additional wear, caused by the passage of current through the contact, i.e. current wear.

Taking into account that the wire, wound on a potentiometer frame, represents a cylinder with the radius R, and a sliding contact can be presented as a sphere of radius R, the result of the interaction is presented in Figure 3 as a wear scar in the pair of a cylinder-sphere with the unchanged spherical radius R.

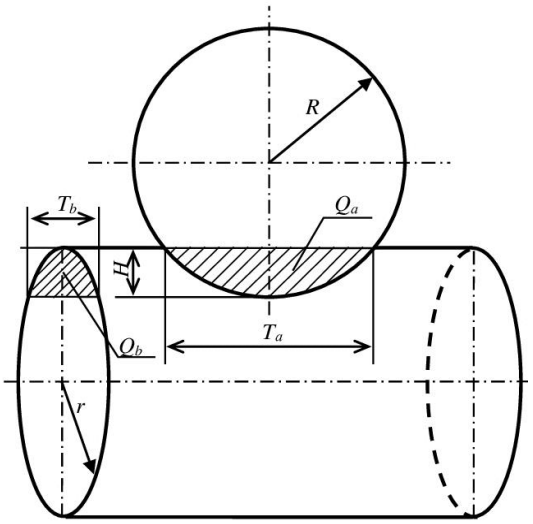
Mechanical processes that occur as a result of contact movement affect the dependence of the transition resistance on the value of contact pressures and stresses – the predominant type of deformation processes in the contact material. The values of shock and vibration loads associated with movement, the speed of movement of the current collector, the coefficient of friction, and other mechanical factors can be represented as an energy model.

Mechanical energy of a single junction expended during friction and wear depends on the value of the maximum tangential stresses τ or contact pressure P_k and the length of the junction path l, i.e. $W = f_1(\tau,\ l)$, or $W = f_2(P_{\kappa},\ l)$.

Depending on the magnitude of tangential stresses and the state of the surfaces of the mating bodies, all three types of deformation processes can occur at the point of contact: elastic displacement, removal and micro-cutting due to wear particles.

In elastic contact, wear occurs due to long-term friction fatigue, and in plastic deformation due to crumpling forces, so the amount of wear in both cases will be proportional to the friction energy W_f, but with different values of the proportionality coefficients [16].

The volume V_m of mechanically worn material at an elastic contact will be proportional to the friction power W_f, and at the microcutting of the material is proportional to the energy of the shear force W_s. To determine the wear patterns of contact pairs cylinder-sphere at W = const (for "dry" contact pairs"), the volume of worn material will be determined by the generalized pattern of wear to height H or to chord T_a.



R – radius sphere; r – radius cylinder; H – height wear; T_a – chord of wear along the length of the cylinder; T_b – chord wear; Q_a – wear area along the length of the cylinder; Q_b – the area of the cylinder wear

Figure 3 – Wear scar in the pair of a cylinder-sphere with unchanged spherical radius *R*

According to the notations taken in Figure 3, at constant geometric dimensions of contact ($4 \cdot H_{Bk} \to \infty$), the volume of worn material of cylindrical wire in the transverse movement of spherical contact will be:

DOI: 10.24025/2306-4412.3.2020. 199294

$$V \approx \frac{1}{3} \cdot Q_b \cdot T_a. \quad (2)$$

Let's indicate the magnitude of volume V through the controlled wear parameter T_b

$$Q_b = \frac{T_b^3}{16 \cdot r};$$

$$H = \frac{T_b^2}{8 \cdot r} = \frac{T_a^2}{8 \cdot R},$$

and here we get:

$$T_a = T_b \cdot \sqrt{\frac{R}{r}}. \quad (3)$$

After the value substitution Q_b and T_a into (2) we get:

$$V = \frac{T_b^4}{48 \cdot r} \cdot \sqrt{\frac{R}{r}} = C_V \cdot T_b^4 \quad (4)$$

and

$$dV = \frac{T_b^3}{12 \cdot r} \cdot \sqrt{\frac{R}{r}} dT_b = 4 \cdot C_V \cdot T_b^3 dT_b, \quad (5)$$

where $C_V = \frac{1}{48 \cdot r} \cdot \sqrt{\frac{R}{r}}$.

The power of friction forces W_f and cut W_s at a single transition in the dT_b path will be equal to [16]:

$$dW_f = K_f \cdot P_k dT_b, \quad (6)$$

$$dW_s = \tau dQ dT_b. \quad (7)$$

where τ is a yield limit per slice; K_f is a coefficient of friction; Q is a cross-section of the track at a single junction.

After integration within the wear boundaries T_b of one transition and considering the performance within N transitions, we get:

$$W_{f\Sigma} = K_f \cdot P_k \cdot T_b \cdot N, \quad (8)$$

$$W_{s\Sigma} = \frac{\tau \cdot P_k \cdot T_b^4 \cdot N}{64 \cdot r} \cdot \sqrt{\frac{R}{r}}. \quad (9)$$

Having considered $T \sim \tau \sim P_k^{\frac{1}{3}}$ and $W \sim V \sim T^4$, we obtain

$$W_{f\Sigma} \sim \tau^4 \cdot N \sim P_k^{\frac{4}{3}} \cdot N,$$

$$W_{s\Sigma} \sim \tau^5 \cdot N \sim P_k^{\frac{5}{3}} \cdot N$$

or

$$T_f \sim \tau \cdot N^{\frac{1}{4}} \sim P_k^{\frac{1}{3}} \cdot N^{\frac{1}{4}}, \quad (10)$$

$$T_s \sim \tau^{\frac{4}{5}} \cdot N^{\frac{1}{4}} \sim P_k^{\frac{5}{12}} \cdot N^{\frac{1}{4}}. \quad (11)$$

For the equally possible effect of the friction forces and shear we have:

$$V = K_V \cdot \tau^{\frac{9}{2}} \cdot N, \quad (12)$$

hence the wear pattern will be

$$T_b \sim \tau^{\frac{9}{8}} \cdot N^{\frac{1}{4}} \sim P_k^{\frac{9}{8}} \cdot N^{\frac{1}{4}}, \quad (13)$$

that corresponds to the accepted at present empirical engineering wear model [10, 18].

When moving the engine (brush) along the coils of potentiometric sensor winding, there is a sharp to contacts are opened under current. When the contacts are opened under current, there is a sharp increase in transient resistance and voltage drop on them, which leads to an increase in the temperature of contacted protrusions, up to melting point of contact material. At the first moment of contact opening is formed between them a bridge of molten coating metal contacts and metal contacts themselves, which in the further divergence of the contacts will not thin in the middle, but closer to positive electrode, where, at last, will be interrupted. This phenomenon is similar to electrolysis. This process causes the transfer of metal from one contact to another. This phenomenon is called bridging the erosion of the contacts. As a result of erosion, the microgeometry of the contact surfaces changes, which leads to increased mechanical wear of the contact surfaces. If the voltages and currents in the open circuit are lower than certain values for specific contact materials (for example, for silver $U < 12\ V$, $I < 0{,}4\ A$), bridge erosion will be the main type of electrical wear of the contacts. This is highly undesirable, since this mode of operation dramatically reduces the resource of normal operation of contacts [19].

Switching by contacts of low-power circuits with active load is accompanied by erosion phenomena caused by the formation of molten bridges in the contact zone at certain moments of contact movement. When switching current with breaking contacts, there are time intervals when such a small area contacts that the current density in it reaches values sufficient for melting and subse-

DOI: 10.24025/2306-4412.3.2020. 199294

quent evaporation of the contact material. The liquid metal switches the inter-contact gap, forming a molten conductive bridge.

Bridges can occur both when closing and opening contacts. It is generally accepted that bridges on closed contacts arise due to the pulling of softened contact material heated by electrostatic radiation currents with sufficiently small Inter-contact gaps by electrostatic field forces [7].

The maximum length of the bridge at the time of its explosion by current is from the ratio [7]

$$S_{ex} = \upsilon_{av} \cdot \tau_{ex},$$

where υ_{av} is an average speed of opening the contacts of polarized relays, determined for each relay at the specified supply and control voltages, and τ_{ex} is a time interval from the beginning of disconnection of the contacts to the moment of explosion of the bridge, determined by the voltage waveforms on the bridge.

We will define the value of current wear. Contacts, which dial currents, less than minimum current of the rod at volltages less than 300 V, are called low powerful. In this case, the erosion of the contacts occurs as a result of the formation of bridges and pulse low-voltage discharges. This transfer is called a thin transfer. For the bulk positive thin metal transfer of a single cycle we have a dependency of the type [7]:

$$V_I = a \cdot I^{\alpha}, \qquad (14)$$

where a is a coefficient of current impact on the wear that depends on the contact material; α is an indicator of impact level of the current onto the wear.

In the vast majority of cases, the direction of the transfer is positive, that is, a crater appears on the anode, and a peak is on the cathode.

Total wear volume formula can be expressed via the relative value of the lateral wear:

$$V_{\Sigma} = V_m \cdot \left(1 + \frac{V_I}{V_m}\right), \qquad (15)$$

or

$$V_{\Sigma} = V_m \cdot \left(1 + K_I \cdot I^{\alpha}\right), \qquad (16)$$

where $K_I = \frac{a}{V_m}$ is a relative coefficient of the current load.

Considering the wear pattern T of the contact pair of the cylinder-sphere with (12) and (13) in the general case, the volume of wear can be represented by the equation:

$$V = m \cdot T^4.$$

where m is proportion coefficient.

Then

$$\frac{V_{\Sigma}}{V_m} = \left(\frac{T_{\Sigma}}{T_m}\right)^4.$$

Considering $t = \frac{T_{\Sigma}}{T_m}$, and taking into account (16) we get:

$$t = \left(1 + K_I \cdot I^{\alpha}\right)^{\frac{1}{4}}. \qquad (17)$$

In the equation (17), regarding the wear of the contact pair cylinder-sphere coefficient K_I and degree indicator α must be determined according to the research data. It is convenient to use the equation

$$\lg\left(t^4 - 1\right) = \lg K_I + \alpha \cdot \lg I, \qquad (18)$$

obtained after taking the logarithm of the equation (17). The dependency (18) is expressed by the equation of the line, where $\lg K_I$ is the initial coordinate and the indicator of degree α is equal to the tangent of the straight line.

For approximate calculations, for $K_I \cdot I^{\alpha} < 0{,}1$ we can decompose equation (17) into a Maclaurin series, limiting it to two terms:

$$t \approx 1 + \frac{K_I}{4} I^{\alpha} \approx 1 + K_I \cdot I^{\alpha}. \qquad (19)$$

In turn, equation (19) can be represented as

$$t \approx e^{K_I \cdot I^{\alpha}}. \qquad (20)$$

In equation (20), the coefficients K_I and α can be determined graphically, for which, by performing double logarithm, we obtain the equation of the line

$$\ln^2 t = \ln K_I + \alpha \cdot \ln I. \qquad (21)$$

This approach simplifies the determination of coefficients and expands the scope of the model (17), but reduces the accuracy of forecasting.

Conclusions. As a result of the research, the mathematical model of potentiometer sensor wear-resistance has been developed considering

DOI: 10.24025/2306-4412.3.2020. 199294

current loads. Given that the model (17) obtained by adding classical models (6), (7) and (14) and simplified by combining similar parameters, the accuracy of calculations for the second use will remain the same as for classical models, but the number of calculations will be reduced. It also reduces the number of experiments needed to determine unknown constants. The use of a single controlled wear parameter *t* is more convenient for predicting the wear resistance of potentiometric sensors by identification method. Presentation of the model in the form of the dependence, which is expressed by the equation of the line, greatly simplifies the forecasting of wear-resistance on the basis of experimental data, which is the main advantage of the obtained model. Developed mathematical model can be used for the prediction of wear-resistance in the design and operation of potentiometer sensors, wire potentiometers and other devices, that have a similar structure and operate under the current.

To predict the wear resistance of potentiometric sensors, it is recommended to use an identification method that allows to get a model of changes in the chord of the wear trace of the wire *T* as the main parameter depending on the impact of the most significant operating factors: contact pressure P_k, the number of cycles of working life *N* and switching current *I* with other constant factors (constant value of the path and speed of movement of the contact under normal environmental conditions). The choice of these parameters can be carried out both based on the materials of existing studies and on the results of experiments.

References

[1] B. V. Shandrov, and A. D. Chudakov, *Technical means of automation:* textbook. Moscow, Russia: Izd. tsentr "Akademiya", 2007. [in Russian].

[2] S. A. Shahvorostov, *Technical means of automation:* tutorial. Moscow, Russia: MADI, 2011. [in Russian].

[3] Yu. I. Pyndus, R. R. Zaverukha, *Electronic and microprocessor equipment of cars:* tutorial. Ternopil, Ukraine: TNTU, 2016 [in Ukrainian].

[4] A. S. Ishkov, A. V. Svetlov, G. A. Solodimova, and S. I. Torgashin, "Monitoring the technical condition of resistive potentiometers using scanning electron microscopy", *Izmerenie. Monitoring. Upravlenie. Kontrol*, no.4 (22), pp. 77-83, 2017. [in Russian].

[5] A. M. Mrachkovskyi, "Investigation of electric erosion of surfaces of various contact pairs of low-flying switching devices", *Naukovyi visnyk Natsionalnoho universytetu bioresursiv i pryrodo-korystuvannia Ukrainy. Seriia: Tekhnika ta enerhetyka APK*, iss. 242, pp. 155-158, 2016. [in Ukrainian].

[6] R. Holm, *Electric contacts: theory and application* / by Ragnar Holm with Else Holm; preface by J.B.P. Williamson, 4th ed. Berlin/London: Springer, 2011.

[7] M. A. Razumihin, *Erosion resistance of low-power contacts.* Moscow, Russia: Energiya, 1964. [in Russian].

[8] I. I. Kudish, and M. J. Covitch, *Modeling and analytical methods in tribology*, CRC Press, 2010.

[9] S. Montgomery, D. Kennedy, and N. O'Dowd, "Analysis of wear models for advanced coated materials. Matrib", *International Conference on Materials, Tribology, Recycling*. Lipanj, Croatia, June 24-26, 2009.

[10] I. I. Vorovich, and V. M. Aleksandrov, *Mechanics of contact interactions*. Moscow, Russia: Fizmatlit, 2001. [in Russian].

[11] I. V. Kragelskiy, M. N. Dobyichin, and V. S. Kombalov, *Fundamentals of friction and wear calculations*. Moscow, Russia: Mashinostroenie, 1977. [in Russian].

[12] I. V. Kragelskiy, and N. M. Mihin, Friction units of machines: handbook. Moscow, Russia: Mashinostroenie, 1984. [in Russian].

[13] V. G. Nedorezov, and A. I. Tsyigankov, "The influence of wear products of the contact pair of the potentiometer on the reliability of its operation", *Nadezhnost i kachestvo:* Proc. of Int. Symposium. Penza, Russia: PGU, 2015, vol. 2, pp. 153-154. [in Russian].

[14] N. K. Myishkin, and V. V. Konchits, *Electrical contacts.* Dolgoprudnyiy, Russia: Intellekt, 2008. [in Russian].

[15] D. Kuhlmann-Wilsdorf, "Uses of theory in the design of sliding electrical contacts", in *Proc. of the Thirty-Seventh IEEE Holm Conf. on Electrical Contacts*, 1991, pp. 1-24.

[16] O. O. Sytnyk, V. B. Kyselov, and H. O. Kyselova, "On one of the methods of building a mathematical model of wear resistance of film potentiometers". *Molodyi*

DOI: 10.24025/2306-4412.3.2020. 199294

vchenyi: sci. journ., no. 2 (78), pp. 189-192, Febr. 2020. [in Ukrainian].

[17] A. G. Kuzmenko, *Development of contact tribomechanics methods*. Hmelnitskiy, Ukraine: HNU, 2010. [in Russian].

[18] I. G. Goryacheva, and M. N. Dobyichin, *Contact problems in tribology*. Moscow, Russia: Mashinostroenie, 1988. [in Russian].

[19] L. I. Safonov, and A. L. Safonov, "Rectangular electrical connectors. Analysis of physical processes occurring in contact", *Tekhnologii v elektronnoj promyshlennosti*, no. 6, pp. 54-58, 2007. [in Russian].

Список використаних джерел

[1] Б. В. Шандров, и А. Д. Чудаков, Технические средства автоматизации: учебник для студ. высш. учеб. заведений. Москва, Россия: Изд. центр "Академия", 2007.

[2] С. А. Шахворостов, *Технические средства автоматизации:* учеб. пособие. Москва, Россия: МАДИ, 2011.

[3] Ю. І. Пиндус, та Р. Р. Заверуха, *Електронне та мікропроцесорне обладнання автомобілів:* навч. посіб, Тернопіль, Україна: ТНТУ, 2016.

[4] А. С. Ишков, А. В. Светлов, Г. А. Солодимова, и С. И. Торгашин, "Контроль технического состояния резистивных потенциометров с применением растровой электронной микроскопии", *Измерение. Мониторинг. Управление. Контроль,* № 4 (22), с. 77-83, 2017.

[5] А. М. Мрачковський, "Дослідження електричної ерозії поверхонь різних контактних пар низьковольтних комутаційних апаратів", *Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Техніка та енергетика АПК,* вип. 242. с. 155-158, 2016.

[6] R. Holm, *Electric contacts: theory and application* / by Ragnar Holm with Else Holm; preface by J.B.P. Williamson, 4th ed. Berlin/London: Springer, 2011.

[7] М. А. Разумихин, Эрозионная устойчивость *маломощных* контактов, Москва, Россия: Энергия, 1964.

[8] I. I. Kudish, and M. J. Covitch, *Modeling and analytical methods in tribology*, CRC Press, 2010.

[9] S. Montgomery, D. Kennedy, and N. O'Dowd, "Analysis of wear models for advanced coated materials. Matrib", *International Conference on Materials, Tribology, Recycling*. Lipanj, Croatia, June 24-26, 2009.

[10] И. И. Ворович, и В. М. Александров, *Механика контактных взаимодействий*. Москва, Россия: Физматлит, 2001.

[11] И. В. Крагельский, М. Н. Добычин, и В. С. Комбалов, *Основы расчетов на трение и износ*. Москва, Россия: Машиностроение, 1977.

[12] И. В. Крагельский, и Н. М. Михин, *Узлы трения машин:* справочник. Москва, Россия: Машиностроение, 1984.

[13] В. Г. Недорезов, и А. И. Цыганков, "Влияние продуктов износа контактной пары потенциометра на надежность его работы", *Надежность и качество:* труды Междунар. симпозиума. Пенза, Россия: ПГУ, 2015, т. 2, с. 153-154,.

[14] Н. К. Мышкин, и В. В. Кончиц, *Электрические контакты*. Долгопрудный, Россия: Интеллект, 2008.

[15] D. Kuhlmann-Wilsdorf, "Uses of theory in the design of sliding electrical contacts", in *Proc. of the Thirty-Seventh IEEE Holm Conf. on Electrical Contacts*, 1991, pp. 1-24.

[16] О. О. Ситник, В. Б. Кисельов, та Г. О. Кисельова, "Про один з методів побудови математичної моделі зносостійкості плівкових потенціометрів", *Молодий вчений:* наук. журн., № 2 (78), с. 189-192, лют. 2020.

[17] А. Г. Кузьменко, *Развитие методов контактной трибомеханики*. Хмельницкий, Украина: ХНУ, 2010.

[18] И. Г. Горячева, и М. Н. Добычин, *Контактные задачи в трибологии*. Москва, Россия: Машиностроение, 1988.

[19] Л. И. Сафонов, и А. Л. Сафонов, "Прямоугольные электрические соединители. Анализ физических процессов, происходящих в контакте", *Технологии в электронной промышленности*, № 6, с. 54-58, 2007.

DOI: 10.24025/2306-4412.3.2020. 199294

В. Б. Кисельов
e-mail: vladkis.777@gmail.com
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

МЕТОД ПОБУДОВИ МАТЕМАТИЧНОЇ МОДЕЛІ ЗНОСОСТІЙКОСТІ ПОТЕНЦІОМЕТРИЧНИХ ДАТЧИКІВ

У статті розглядається метод побудови математичної моделі зносостійкості потенціометричних датчиків. Фізичні процеси, які відбуваються при роботі потенціометричних датчиків, мають дві основні складові – механічний рух контактуючих поверхонь ковзання одна відносно іншої та проходження струму через ці поверхні. Виходячи з цього, математична модель може бути представлена як сума моделей, які враховують ці властивості. В основу механічної складової моделі покладено вплив трибологічних процесів пружного контактування, пластичної деформації та мікрорізання. Вплив цих процесів подано через зміну об'єму зношеного матеріалу залежно від величини контактного тиску, виду деформаційних процесів у матеріалі контактів, пов'язаних з рухом, швидкістю переміщення струмознімача, коефіцієнта тертя та інших механічних факторів. Об'єм механічно зношеного матеріалу при пружному контактуванні буде пропорційним енергії тертя, а при мікрорізанні матеріалу – енергії сил зрізу. Таким чином, для оцінювання механічного зносу використано енергетичну модель, запропоновану Герцем. При проходженні струму через контактуючі поверхні виникають процеси нагрівання, розплавлення і перенесення металу з одного контакту на інший, що зумовлює прискорення процесу зносу контактуючих поверхонь. Комутація контактами малопотужних ланцюгів з активним навантаженням супроводжується ерозійними явищами, що викликаються утворенням розплавлених містків у зоні контактування в певні моменти руху контактів. Електрична ерозія контактів залежить від великої кількості різних електричних і термічних явищ, які відбуваються на поверхні контактів і в контактному проміжку, що визначають не тільки характер перенесення, але й його величину і напрямок. Незважаючи на складність залежності ерозії від параметрів електричного кола, матеріалу контактів і властивостей середовища, визначальний вплив на величину і знак ерозійного перенесення має величина комутуючого струму. Контакти, які комутують струми в потенціометричних датчиках, є малопотужними. В цьому випадку ерозія контактів відбувається в результаті утворення містків та імпульсних низьковольтних розрядів. Основним фактором впливу на об'єм зносу малопотужних ковзних контактів потенціометричних датчиків під струмом при постійній кількості циклів напрацювання є місткова ерозія. Об'єм зношеного матеріалу при містковій ерозії представлений через величину струму та коефіцієнти, які залежить від матеріалу контактів і показника ступеня впливу струму. Математична модель, отримана шляхом додавання об'ємних моделей механічного та струмового зносу та спрощена шляхом об'єднання подібних параметрів, може бути використана для прогнозування зносостійкості при проектуванні й експлуатації потенціометричних датчиків, дротяних потенціометрів та інших приладів, які мають схожу структуру та працюють під струмом.

Ключові слова: *ковзний контакт, дротяний потенціометр, трибологічні процеси, місткова ерозія, надійність роботи.*

DOI: 10.24025/2306-4412.3.2020. 199294

УДК 004:005.8:004.94

[0000-0002-6204-0708] **Т. О. Прокопенко,** *д.т.н., доцент,*
e-mail: t.prokopenko@chdtu.edu.ua
В. А. Прокопенко, *студент*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ГРАФОДИНАМІЧНЕ МОДЕЛЮВАННЯ УПРАВЛІННЯ СИТУАЦІЯМИ В ІННОВАЦІЙНИХ ПРОЄКТАХ НА ОСНОВІ МЕТОДОЛОГІЇ SCRUM

У статті розглядається питання побудови графодинамічної сценарної моделі управління ситуаціями в інноваційних проєктах на основі методології Scrum шляхом дослідження бінарної гри в умовах протиріччя між зацікавленими сторонами. Проаналізувавши учасників проєкту на основі гнучкої методології Scrum і розглянувши можливі протиріччя між різними зацікавленими сторонами проєкту, автори для розробки моделі застосували техніку бінарної гри на основі сценарних зв'язок.

Ключові слова: *управління ІТ проєктом, гнучка методологія Scrum, бінарна гра, сценарна зв'язка, ситуації.*

Вступ. Інноваційні проєкти, що розробляються, зокрема в галузі інформаційних технологій (ІТ), характеризуються складністю структур, наявністю багатьох цілей, активністю, недетермінованістю, тісним взаємозв'язком організаційних і технологічних процесів [1]. Динаміка реалізації ІТ проєкту вимагає чіткої постановки завдань, чіткого розподілу задач між виконавцями, чіткої координації дій і рішень, адаптації до стилю командної роботи. Водночас першочерговою вимогою в управлінні ІТ проєктом є забезпечення якості процесів, якості кінцевого продукту, гнучкості, мобільності, самоорганізації, продуктивності, мінімізації ризиків [2]. Тому застосування таких гнучких методологій, як Agile і Scrum [3, 4] надає можливості підвищення ефективності як безпосередньо управління, так і проєкту в цілому. Однак у ході реалізації ІТ проєкту на основі застосування методології Scrum можливе виникнення різних ситуацій, що можуть мати негативні наслідки, особливо в умовах кризи, конфліктів та протиріччя між зацікавленими сторонами. Щоб уникнути негативних наслідків, необхідно розглянути моделі розвитку ситуацій, в ході якого досліджуються можливі альтернативні варіанти вирішення проблем. Моделювання управління ІТ проєктом в умовах методології Scrum доцільно реалізувати на основі бінарних ігор [5], що забезпечить можливості інтеграції наочності з високим ступенем інформативності, сприятиме прийняттю ефективних управлінських рішень та унеможливить подальший розвиток негативної ситуації.

Аналіз останніх досліджень та публікацій. Для підвищення продуктивності розробників, а також отримання якісного продукту в управлінні ІТ проєктами широко застосовуються гнучкі методології Agile, Scrum, Kanban, які досліджуються на сьогоднішній день вітчизняними та зарубіжними вченими [3, 4, 6–11]. Більшість авторів акцентує увагу безпосередньо на описі основних ідей, принципів, особливостей або критиці цих методологій, порівняльній характеристиці. Однак зовсім не досліджується питання прийняття управлінських рішень у кризових, конфліктних ситуаціях, що матимуть негативні наслідки та вплинуть на ефективність ІТ проєкту. В такій постановці задача ставиться вперше.

Метою статті є розробка графодинамічної сценарної моделі управління ситуаціями в ІТ проектах на основі методології Scrum шляхом дослідження бінарної гри в умовах протиріччя між зацікавленими сторонами, що забезпечить можливості уникнення негативних ситуацій та підвищить ефективність управління ІТ проєктом.

Викладення основного матеріалу дослідження. В ІТ проєкті, що реалізується із застосуванням гнучкої методології Scrum, всі зацікавлені сторони діляться на дві групи. До першої групи входять регулярно і повністю задіяні команда розробників (Scrum Team) і керівник (Scrum master), а також власник продукту (Product owner PO), тоді як до другої – ті,

DOI: 10.24025/2306-4412.3.2020.211393

хто зацікавлені (і задіяні) у проекті, але не мають прямого відношення до безпосередніх процесів розробки, кому не завжди дозволяється безпосередньо впливати, змінювати або включатися в хід Scrum проекту, проте потреби, бажання, ідеї і вплив яких враховуються. До них відносяться користувачі (Users), клієнти і продавці (Stakeholders), експерти-консультанти (Consulting Experts) [11]. Тому можливість появи протиріч різного роду і характеру між різними сторонами і виконавцями може призвести до виникнення конфліктних ситуацій, а це, в свою чергу, – до втрат часу реалізації і відіб'ється на ефективності проєкту.

Для побудови моделі управління ситуаціями IT проекту застосуємо техніку графодинаміки згідно з [12] та уведемо наступні формалізми:

- граф цілей та дій;
- лінійний сценарій поведінки зацікавлених сторін IT проєкту відповідно до графу цілей та дій;
- бінарна сценарна зв'язка, що моделює взаємодії учасників проєкту.

До особливих факторів, які необхідно враховувати в ході досліджень, відносяться такі, як характер взаємодії зацікавлених сторін IT проєкту. оцінка часу, необхідного для виконання завдань, відповідність завдання поставленій цілі. Тому в основі дослідження розглянемо конфліктну ситуацію між зацікавленими сторонами на простому академічному прикладі IT проєкту розробки чат-бота для платформи Facebook Messenger, що реалізується в умовах гнучкої методології Scrum. Users та Stakeholders висувають нові вимоги, що суперечать архітектурі вже створеного і поставленого продукту, які не погоджують Scrum Team і Scrum master. У цій ситуації суб'єктами бінарної гри є, з одного боку, Users та Stakeholders, а з другого – Scrum Team і Scrum master. Домінантний фактор для Scrum Team і Scrum master – відповідність якості вимогам, Users та Stakeholders – висунуті ними нові вимоги.

Представимо структуру бінарної гри, що є в основі моделі, відповідно до введених формалізмів (рисунок 1).

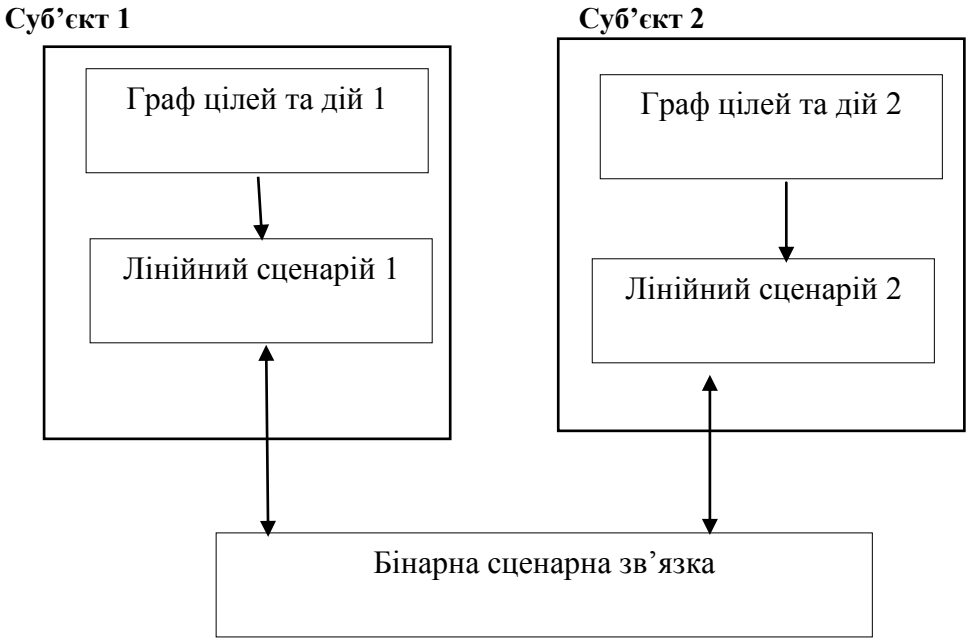


Рисунок 1 – Структура бінарної гри

Граф цілей та дій представимо у вигляді мережі Петрі [13, 14], тобто двочастковий орієнтований граф (що має складові) з двома компонентами зв'язності, що моделюють відповідно послідовні та паралельні процеси виконання дій суб'єктами гри, які спрямовані на досягнення цілей. Позиція в графі цілей та дій (зображується кружком) відповідає або дії, або цілі. Наявність маркера в позиції інтерпретується як виконання дії і досягнення цілі. Перехід в графі (зображується прямокутником) моделює стрибкоподібну зміну стану

DOI: 10.24025/2306-4412.3.2020.211393

мережі: видалення маркерів з вхідних позицій переходу і внесення маркерів у його вихідні позиції. Взаємодія складових графу цілей та дій зображується пунктирними стрілками.

На рисунку 2 зображено граф цілей та дій Scrum Team і Scrum master в Sprint інвестиційної фази проєкту розробки чат-бота для платформи Facebook Messenger.

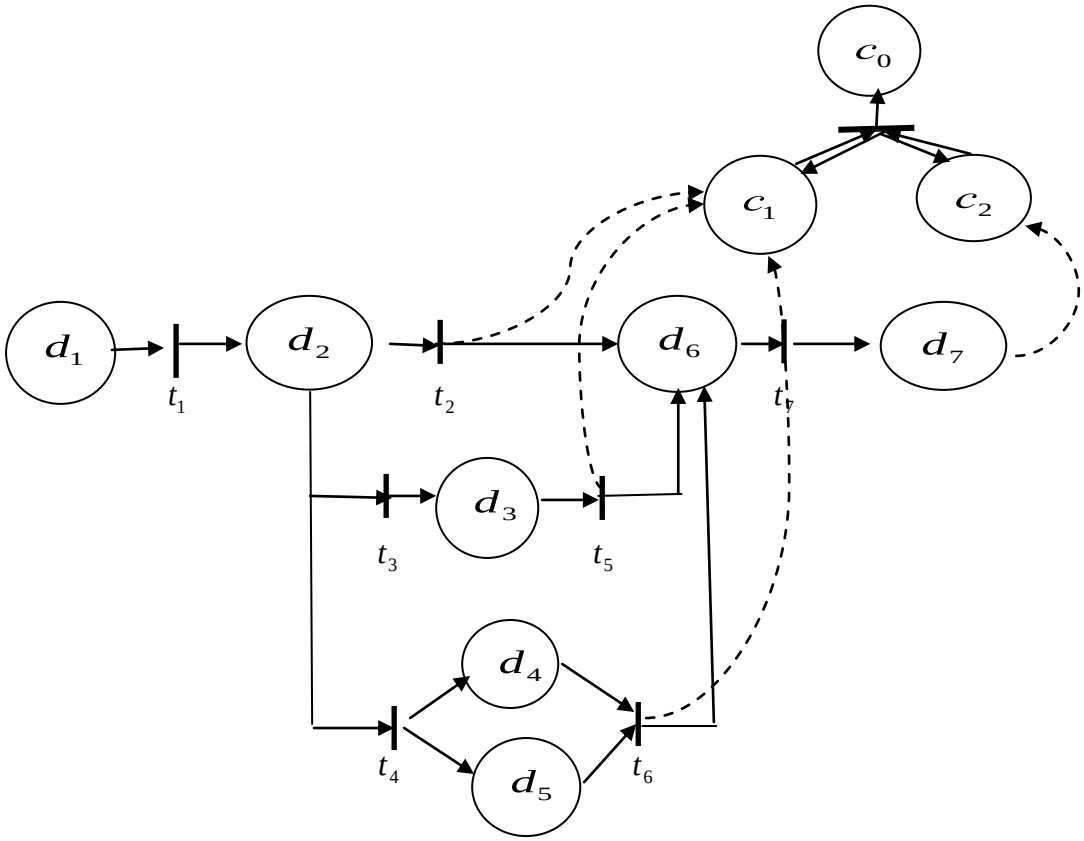


Рисунок 2 – Граф цілей та дій Scrum Team і Scrum master в Sprint

Дамо деякі пояснення до графу цілей та дій на рисунку 2.

Цілі Scrum Team і Scrum master в Sprint:

c_0 – отримання готового якісного продукту;

c_1 – збереження вже розробленого продукту;

c_2 – внесення змін до сформованих вимог.

Дії Scrum Team і Scrum master в Sprint:

d_1 – підготовка видачі мінімального приросту продукту за функціональністю;

d_2 – обговорення проблеми з Users та Stakeholders;

d_3 – знаходження компромісного рішення Scrum Team і Scrum master з Users та Stakeholders;

d_4 – реалізація внесених змін;

d_5 – рефакторинг та переробка на кожній черговій ітерації;

d_6 – Sprint Review Meeting;

d_7 – Sprint Retrospective.

Дії Scrum Team і Scrum master починаються з підготовки до видачі мінімального приросту продукту за функціональністю згідно з попередніми вимогами незалежно від результату обговорення та пошуку компромісного рішення (маркер в позиції d_1). Початок обговорення відмічається переміщенням маркера в позицію d_2 при спрацьовуванні переходу t_1. Позитивний результат обговорення моделюється переходом t_2, який передає маркер в позицію d_3 і далі, при спрацьовуванні d_4, маркери вносяться в позицію дії d_5 і цільову позицію c_1. Перехід t_6 передає мар-

DOI: 10.24025/2306-4412.3.2020.211393

кер в позицію d_6, а перехід t_7 – в позицію d_7, що означає, що компромісне рішення знайдено. Невдача обговорення проблеми Scrum Team і Scrum master з Users та Stakeholders моделюється спрацьовуванням t_3, внесенням маркера в d_4 та d_5, що реалізуються паралельно, і далі в d_6, d_7, c_2. Граф цілей та дій на рисунку 3 подібним чином моделює можливі варіанти поведінки Users та Stakeholders.

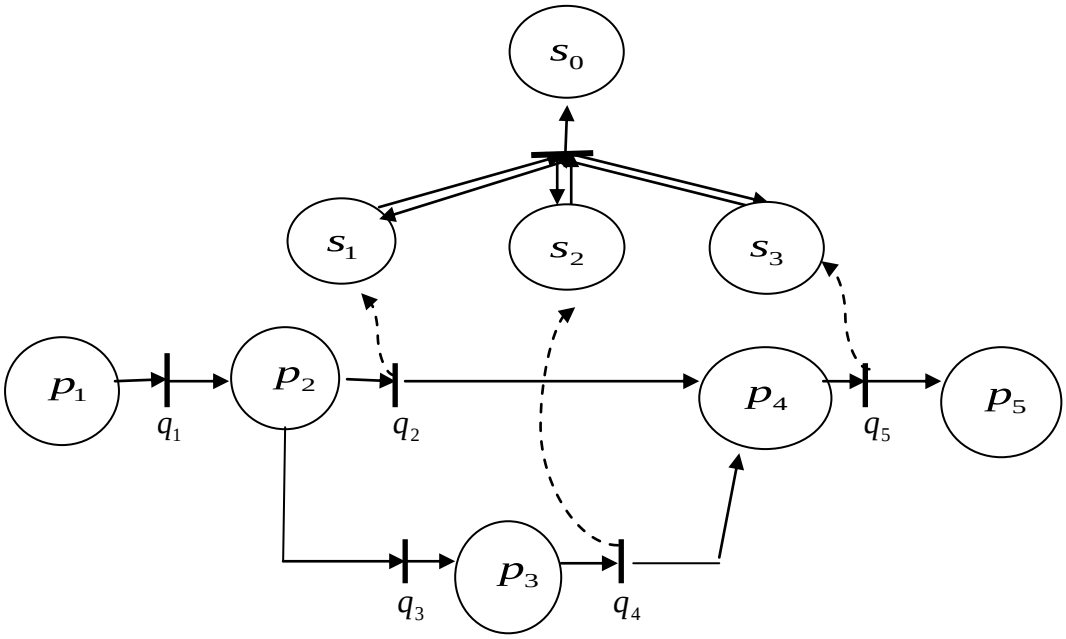


Рисунок 3 – Граф цілей та дій Users та Stakeholders

Цілі Users та Stakeholders в Sprint:

s_0 – отримання готового продукту з максимальними перевагами;

s_1 – залучення підтримки міжнародних організацій та фондів;

s_2 – розробка інноваційного продукту;

s_3 – збільшення цільової аудиторії користувачів.

Дії Users та Stakeholders в Sprint:

p_1 – висунуті нові вимоги до готового продукту;

p_2 – знаходження компромісного рішення Scrum Team і Scrum master з Users та Stakeholders;

p_3 – Users та Stakeholders наполягають на переробці згідно з новими вимогами;

p_4 – Sprint Review Meeting;

p_5 – Sprint Retrospective.

Сценарій суб'єкта моделюється лінійним графом, що формується на основі графу цілей та дій. Вершини графу сценарію відповідають діям, дуги – переходам мережі Петрі. Кожній дії відповідає структура, що виражається графом відношення: суб'єкта 1 до суб'єкта 2, а також суб'єктів 1 і 2 до домінантного зовнішнього фактора (ЗФ).

Суб'єктам гри можуть відповідати як однакові, так і різні фактори. Відношення може бути нейтральним (відсутність на графі відносин відповідної дуги), позитивним (суцільна дуга) і негативним (пунктирна дуга). Вершини графу сценарію зображено у вигляді квадратів, всередину яких розміщено графи відношення, а стрілки, що зображено над верхньою стороною квадрата, вказують на цілі, що досягнуті при виконанні дії. Визначений у такий спосіб лінійний сценарій поведінки суб'єкта гри відображає реалізовану ним послідовність дій, динаміку відносин і динаміку досягнення цілей у процесі реалізації цієї послідовності.

DOI: 10.24025/2306-4412.3.2020.211393

У розглянутому прикладі (рисунки 2, 3) можливі два лінійні сценарії поведінки обох суб'єктів гри – жорсткий і м'який. Жорсткі сценарії для Scrum Team і Scrum master (позначимо TM), а також для Users та Stakeholders (позначимо US) зображено на рисунку 4 (*а*, *б*).

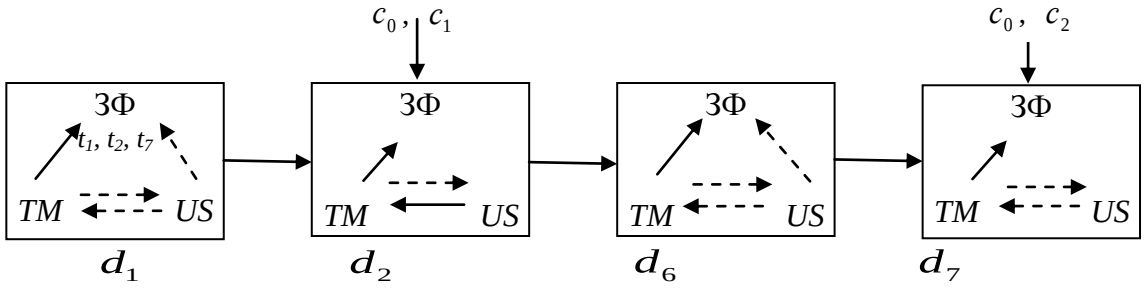


Рисунок 4, *а* – Лінійний сценарій поведінки Scrum Team і Scrum master

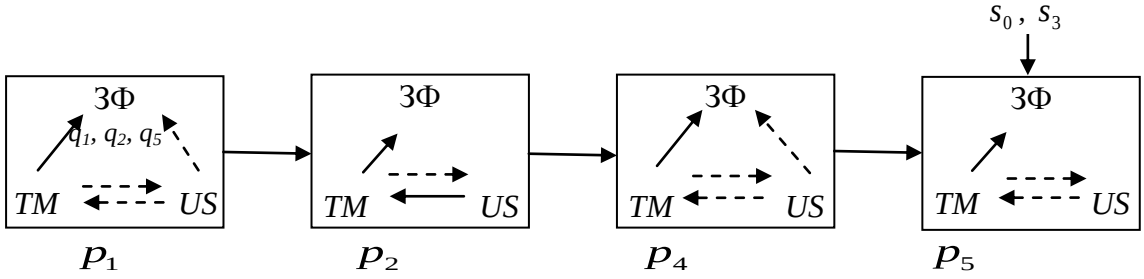


Рисунок 4, *б* – Лінійний сценарій поведінки Users та Stakeholders

Всередині кожного квадрата зображено структури, що відображають бачення відносин між відповідними суб'єктами. При підготовці видачі мінімального приросту продукту за функціональністю (дія d_1) Scrum Team і Scrum master виходять з домінанти реалізації готового продукту і мають упереджене ставлення до Users та Stakeholders. Вони враховують також негативне ставлення Users та Stakeholders відносно них. На стадії обговорення проблеми (дія d_2) як Scrum Team і Scrum master, так і Users та Stakeholders змушені ставитися один до одного як до партнерів, для Scrum Team і Scrum master домінує отримання якісного результату згідно з попередньо висунутими вимогами, Users та Stakeholders відносяться до цього нейтрально.

Бінарна сценарна зв'язка дає можливість спільно розглянути вибрані сценарії суб'єктів гри і встановити між ними обмежувальні відносини шляхом регламентації тривалості дій.

Висновки і перспективи подальшого розвитку. На основі дослідження простого академічного прикладу ІТ проєкту розробки чат-бота для платформи Facebook Messenger, що реалізується в умовах застосування гнучкої методології Scrum, розроблено графодинамічну модель управління ситуаціями шляхом аналізу бінарної гри в умовах протиріччя між зацікавленими сторонами, що забезпечить можливості уникнення негативних ситуацій та підвищить ефективність управління ІТ проєктом.

Реалізацію побудови графодинамічної моделі ситуаційного управління ІТ проєктом в умовах протиріччя між зацікавленими сторонами здійснено на основі дослідження бінарної гри шляхом застосування сценарного підходу. Це забезпечило можливості управління ситуацією та координацію дій між зацікавленими сторонами ІТ проєкту, поведінка яких впливає на реалізацію гнучкої методології Scrum. Водночас зацікавлені сторони ІТ проєкту розглядається як суб'єкти, що в цьому ІТ проєкті мають кожен свою мету, відрізняються своєю поведінкою, що може змінюватись, а характеризуються відношенням протиріччя між собою. Суб'єкти процесу можуть приймати компромісні рішення, що забезпечить вихід з кризової ситуації, які будуть узгоджуватися з факторами зовнішнього оточення, а також змінюватися. Лінійні сценарії поведінки Scrum Team і Scrum master, а також Users та Stakeholders при цьому базуються на моделюванні поведінки окремих суб'єктів, що узгоджує їх цілі, координує дії та рішення конфліктів між ними. Таким чином, цей підхід

DOI: 10.24025/2306-4412.3.2020.211393

дає змогу дослідити різні варіанти ситуацій, сформувати сценарій виходу з кризи та знайти компромісне рішення, що забезпечить задоволення всіх зацікавлених сторін. Водночас для кожної бінарної зв'язки аналізується розвиток ситуації. Ця модель застосовується для підтримки прийняття оптимальних рішень в управлінні ІТ проєктом на основі методології Scrum у кризових обставинах, що дає можливість підвищити ефективність проєкту за рахунок зменшення втрат часу, та може застосовуватись також для методологій Agile та Kanban.

Список використаних джерел

[1] Т. О. Прокопенко, та А. П. Ладанюк, *Інформаційні технології управління організаційно-технологічними системами*. Черкаси: Вертикаль, видавець Кандич С. Г., 2015.

[2] Т. А. Прокопенко, и А. П. Ладанюк, "Информационная модель управления технологическими комплексами непрерывного типа в классе организационно-технических систем", *Проблемы управления и інформатики*: междунар. науч.-техн. журн., № 5, с. 64-70, 2014.

[3] М. Кон, *Scrum: гибкая разработка ПО*. Москва: Вильямс, 2011, с. 576. ISBN 978-5-8459-1731-7.

[4] Дж. Сазерленд, *SCRUM. Революционный метод управления проектами*. Манн, Иванов и Фербер, 2016. ISBN 978-5-00057-722-6.

[5] N. Howard, "Drama Theory and its relation to Game Theory", *Group Decision and Negotiation*, vol. 32, pp. 187-206, 207-253, 1994.

[6] K. Schwaber, *Agile project management with Scrum*. Microsoft Press, 2004. ISBN 073561993X.

[7] Д. А. Новиков, и А. А. Иващенко, *Модели и методы организационного управления инновационным развитием фирмы*. Москва: КомКнига, 2006.

[8] Р. С. Мартин, Дж. В. Ньюкирк, и Р. С. Косс, *Быстрая разработка программ. Принципы, примеры, практика*. Москва: Вильямс, 2004. ISBN 0-13-597444-5.

[9] S. Orenga-Roglá, and R. Chalmeta, "Methodology for the implementation of knowledge management systems 2.0", *Business & Information Systems*, Springer, vol. 61, iss. 2, pp. 195-213, April 2019.

[10] К. Рубин, *Основы Scrum: Практическое руководство по гибкой разработке ПО*. Москва: Вильямс, 2016, с. 544. ISBN 978-5-8459-2052-2.

[11] D. Maximini, *The Scrum culture: Introduc - ng Agile methods in organizations. Management for professionals.* Cham: Springer, January 8, 2015. Retrieved August 25, 2016. P. 26. ISSN 978331911827.

[12] С. А. Юдицкий, *Моделирование динамики многоагентных триадных сетей*. Москва: СИНТЕГ, 2012.

[13] Дж. Питерсон, *Теория сетей Петри и моделирование систем*. Москва: Мир, 1984.

[14] В. Б. Мараховский, Л. Я. Розенблюм, и А. В. Яковлев, *Моделирование параллельных процессов. Сети Петри. Курс для системных архитекторов, программистов, системных аналитиков, проектировщиков сложных систем управления.* Санкт-Петербург: Проф. лит., АйТи-Подготовка, 2014.

References

[1] T. O. Prokopenko, and A. P. Ladanyuk, *Information technologies of management by organizational and technological systems.* Cherkasy: Vertical, publisher Kandych S. G., 2015. [in Ukrainian].

[2] T. A. Prokopenko, and A. P. Ladanyuk, "Information model of management by technological complexes of continuous type in the class of organizational and technical systems", *Problemy upravleniya i informatiki*: Int. sci.-tech. journal, no. 5, pp. 64-70, 2014. [in Russian].

[3] M. Con. *Succeeding with Agile: Software development using Scrum*. Moscow: Williams, 2011, p. 576. ISBN 978-5-8459-1731-7. [in Russian].

[4] J. Sutherland, *SCRUM. The art of doing twice the work in half the time*. Mann, Ivanov and Ferber, 2016. ISBN 978-5-00057-722-6. [in Russian].

[5] N. Howard, "Drama Theory and its relation to Game Theory", *Group Decision and Negotiation*, vol. 32, pp. 187-206, 207-253, 1994.

[6] K. Schwaber, *Agile project management with Scrum.* Microsoft Press, 2004. ISBN 073561993X.

DOI: 10.24025/2306-4412.3.2020.211393

[7] D. A. Novikov, and A. A. Ivaschenko, *Models and methods of organizational management of innovative development of the company*. Moscow: KomKniga, 2006. [in Russian].
[8] R. S. Martin, J. W. Newkirk, and R. S. Koss, *Agile software development. Principles, patterns, and practices*. Moscow: Williams, 2004. ISBN 0-13-597444-5. [in Russian].
[9] S. Orenga-Roglá, and R. Chalmeta, "Methodology for the implementation of knowledge management systems 2.0", *Business & Information Systems*, Springer, vol. 61, iss. 2, pp. 195-213, April 2019.
[10] K. Rubin. *Essential Scrum: A practical guide to the most popular Agile process*. Moscow: Williams, 2016. ISBN 978-5-8459-2052-2. [in Russian].
[11] D. Maximini, *The Scrum culture: Introducing Agile methods in organizations. Management for professionals*. Cham: Springer, January 8, 2015. Retrieved August 25, 2016. P. 26. ISSN 978331911827.
[12] S. A. Yuditsky, *Modeling the dynamics of multi-agent triad networks*. Moscow: SINTEG, 2012. [in Russian].
[13] J. Peterson, *Petri net theory and system modeling*. Moscow: Mir, 1984. [in Russian].
[14] V. B. Marakhovsky, L. Ya. Rosenblum, and A. V. Yakovlev, *Modeling of parallel processes. Petri nets. A course for system architects, programmers, system analysts, designers of complex control systems*. St. Petersburg: Prof.lit., IT-Podgotovka, 2014. [in Russian].

T. O. Prokopenko, *Dr.Tech.Sc, accociate professor,*
e-mail: t.prokopenko@chdtu.edu.ua
V. A. Prokopenko, *student*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

GRAPH-DYNAMIC SIMULATION OF SITUATION MANAGEMENT IN INNOVATIVE PROJECTS BASED ON SCRUM METHODOLOGY

Ambiguous situations affect the progress of the project in any area. They are unpredictable in nature and require consideration of fairly new and complex factors that to varying degrees determine the effectiveness of the project. The article considers the issue of building a model of graph-dynamic simulation of situation management in innovative projects based on Scrum methodology by studying the binary game in the conditions of conflict between stakeholders. After analyzing the project participants based on a flexible Scrum methodology and considering possible contradictions between different stakeholders of the project, the authors have used the technique of binary game based on scenario communications to develop the model. Knowledge and skills application of the situational approach in the conditions of flexible Scrum methodology will provide opportunities to the project manager to radically change a situation in the project and to achieve the motivated performance of each task. The authors offer a formalized presentation of the procedure for selecting the optimal solution in project management in the implementation of a flexible Scrum methodology. This takes into account all the features of flexible Scrum methodology. The procedure of making the optimal decision on the basis of research of binary game between the interested parties in the conditions of contradiction is offered. A set of scenarios is developed to help overcome the crisis situation, and possible alternatives are explored. The use of these approaches in the implementation of flexible Scrum methodology provides support for decision-making in crisis situations of possible conflicts with existing constraints on financial and time resources. The result of applying the developed model is to increase the efficiency of the project by reducing the loss of time in the project and overspending of financial resources.

Keywords: *IT project management, flexible Scrum methodology, binary game, scenario communication, situations.*

DOI: 10.24025/2306-4412.3.2020.211393

ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 621.395

[0000-0002-8683-3286] **О. І. Романов,** *д.т.н., професор,*
[0000-0003-0716-3788] **М. М. Нестеренко,** *к.т.н., доцент,*
[0000-0002-4291-0438] **В. Б. Маньківський,** *к.т.н., асистент,*
[0000-0002-6691-2438] **І. О. Сайченко,** *асистент*
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
пров. Індустріальний, 2, м. Київ, 03056, Україна

МОДЕЛЬ ОПТИМАЛЬНОГО РОЗПОДІЛУ НАВАНТАЖЕННЯ В МЕРЕЖІ ДОСТУПУ МОБІЛЬНОГО ОПЕРАТОРА

Основна увага при плануванні мережі мобільного оператора приділяється частотному розподілу та електромагнітній сумісності. Основний аргумент полягає в тому, що рішення цієї задачі забезпечить виконання умов оптимального розподілу частотного ресурсу і, як наслідок, дасть можливість оптимізувати рівень завад у сусідніх зонах. Водночас не розглядається питання рівномірності розподілу трафіку по елементах мережі. Як результат, такий підхід негативно впливає на показники пропускної здатності та якості обслуговування QoS. В роботі для підвищення ефективності розподілу навантаження при плануванні зон обслуговування базових станцій пропонується додатково враховувати результати аналізу потоків подій обслуговування в стільниках та дані системи білінгу.

Ключові слова: *QoS, пропускна спроможність, розподіл навантаження, сектор базової станції.*

Вступ. Нині в Україні йде активне впровадження технологій 4G і 5G на мережах операторів мобільного зв'язку. Однак внаслідок помилок у прогнозуванні тенденцій розвитку такого типу мереж склалася ситуація, при якій для обслуговування всього голосового трафіку ще довгий час будуть використовуватися мережі технологій 2G і 3G. Крім того, оператори отримують дохід – як фінансовий, так і іміджевий – від використання наявного сегмента мережі. Тому, при плануванні шляхів розвитку існуючих та перспективних мереж необхідно приділяти увагу підвищенню їх продуктивності.

Планування мережі оператора мобільного зв'язку починається з визначення розподілу частот, що в подальшому забезпечує електромагнітну сумісність мережевих елементів і якість послуг, що надаються.

Зміни кількості абонентів у стільниках, зростання обсягів вхідного навантаження вимагають проведення оптимізації структури мережі. Оператори мережі мобільного зв'язку використовують два основні підходи в процесі вирішення задач корекції існуючої мережі – аналіз частотно-територіального покриття і прогноз зон обслуговування базових станцій (BS, Base Station).

У сучасних мобільних мережах, особливо в зв'язку з появою технологій стека UMTS, кількість дзвінків у процентному співвідношенні скоротилася за рахунок зростання трафіку даних. Абонентське голосове навантаження не зростає, і оператори мобільних мереж концентруються на оптимізації радіопокриття для мережі передачі даних шляхом емпіричного підходу до визначення оптимальних параметрів базових станцій. При такому підході кожний оператор має свій алгоритм оптимального налаштування. Стандарти 3GPP виступають, з одного боку, лише як рекомендації для налаштування (нижня межа якості), а з другого – як рівень задоволеності абонентів якістю зв'язку (верхня межа).

Кількість скарг на радіопокриття при такому підході зросла, більша частина з них припадає на надання послуг з передачі голосу. Причинами зростання помилок і погіршення якості зв'язку при передачі мови є неефективне радіопланування з точки зору кінцевого абонента. Водночас, з точки зору рівня інтерференції і гістерезису, радіопланування виконано ідеально.

У GSM мережах основною стратегією побудови мереж було забезпечення задовільної якості радіочастотного покриття – забезпечення достатнього рівня сигналу. У мережах UMTS перевага надається пропускній здатності радіоресурсу, який може бути нада-

DOI: 10.24025/2306-4412.3.2020.200346

ний кінцевому абоненту у вигляді віртуального каналу.

Мета дослідження. В ході експлуатації мережі відбувається коригування спроектованої мережі на підставі даних про використання канального ресурсу.

В роботі пропонується для аналізу оптимальності розподілу навантаження використовувати дані, які описують характер самих даних. Такі дані мають й інше формулювання – метадані. Ці дані агрегуються в білінговій системі і використовуються при складанні прогнозу по наданню послуг відділами прогнозування.

Для підвищення ефективності функціонування мережі і якості послуг, що надаються, пропонується доповнити існуючі підходи до планування, враховуючи дані з білінгової системи для розрахунку виконаного навантаження з прив'язкою до секторів БС.

У роботі розглянуто стратегію доступу без резервування, коли в секторі радіоканали призначені для обслуговування як дзвінків усередині стільника, так і хендоверних викликів. Це спрощення зроблено для першого оцінювання ефективності підходу до оцінювання розподілу навантаження. Водночас запропоновано підхід без урахування радіоканалів резервування для обслуговування хендовера та основних викликів при перевантаженні (модель з втратами).

Аналіз останніх досліджень. У цій сфері більшість досліджень характеризуються однією спільною рисою – критерієм оптимального розподілу виступають показники радіотракту, наприклад потужність сигналу в точках прийому. Відповідно, при такому підході оптимізацію проводять без урахування самого характеру даних.

В роботах [1, 2] при аналізі не беруть до уваги ряд даних про характер дзвінка, таких як дзвінок прямий або хендоверний. Автори цих робіт не враховують особливості профілю абонента і не визначають взаємозв'язок із секторами обслуговування. Водночас ці дані агрегуються в білінгові системи і використовуються при складанні прогнозу по наданню послуг відділами прогнозування, але не використовуються при плануванні мережі.

Також у роботі [2] враховується розподіл навантаження з точки зору взаємного електромагнітного впливу. Запропонований підхід є одним з найбільш часто використовуваних – це модель розрахунку потужності сигналу Окамура–Хата.

В роботі [3] ефективність функціонування мережі розглядається з точки зору завантаженості каналу. Водночас інформативно вимірюється завантаженість каналів передачі даних (TCH – Traffic Channel) з точки зору співвідношення завантаженості та доступного ресурсу. Автори поглиблюються в ступінь завантаженості каналів даних, доходячи висновку, що завантаженість даних каналів наближається до 100 % (у ЧНН), що є критерієм оптимального розподілу навантаження.

Як показано в роботі [4], оптимальне покриття можна охарактеризувати візуально, на основі завантаженості мережі. Автори не беруть до уваги канали загального призначення (CCCH – Common Control Channel), які здатні значно уточнити дані по завантаженості в мережі, з розбивкою на транзитні виклики (handover, хендовер) та пошукові запити самих кінцевих пристроїв. При цьому завантаженість каналів прив'язується не до конкретної БС, а до центру комутації (MSC), хоча саме TCH має безпосереднє відношення до БС.

Проблематика. Зазначається, що на етапі планування мережі оператори мобільного зв'язку використовують різні математичні моделі розрахунку і прогнозування як покриття, так і абонентського навантаження. Однією з найбільш часто використовуваних є модель розрахунку потужності сигналу Окамура–Хата. Пропонований підхід у статті пропонує враховувати причину виникнення трафіку хендовер як результат неоптимального планування секторів БС.

Оператори в країнах СНД використовують мережі, які поєднують в собі технології стека UMTS і GSM. Вони не вважають рентабельним перехід до мереж LTE найближчим часом, концентруючи увагу на спільному використанні двох мереж одночасно (рисунок 1).

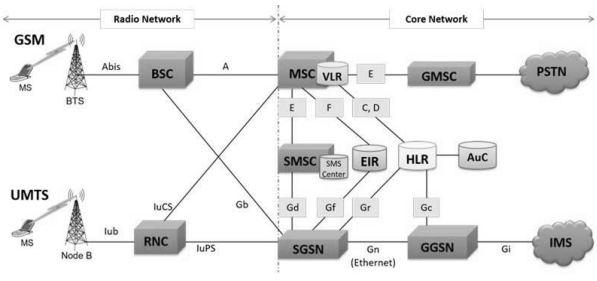


Рисунок 1 – Типова структура мобільної мережі GSM і UMTS операторів в Україні

В таких умовах оператори стикаються з низкою проблем, які були попередньо вирішені операторами розвинених країн, що

DOI: 10.24025/2306-4412.3.2020.200346

перейшли до «чистого» UMTS і зрештою до LTE.

У статті акцент зроблено на взаємному розташуванні секторів БС стільників UMTS і GSM з урахуванням їх взаємного впливу на розподіл навантаження. Цей сценарій характерний для територій із середньою щільністю мобільних пристроїв. Водночас поліпшення в зонах UMTS приведе й до поліпшення якості зв'язку в гібридних мережах. Критерієм підвищення якості зв'язку є зменшення кількості відмов у наданні з'єднань. Один із шляхів досягнення цього – домогтися оптимального розподілу навантаження в стільниках. У статті пропонується оцінити оптимальне покриття, ґрунтуючись на показниках білінгової системи, яка є невід'ємною частиною мережі оператора. Дані з білінгової системи допоможуть оцінити точність моделі оцінювання розподілу навантаження в мережі.

Аналіз узагальненої моделі показує, що на процес функціонування обслуговування навантаження впливає безліч різнорідних чинників. Урахування цих факторів, зниження їх негативного впливу, використання можливостей адаптації до змін у секторі обслуговування навантаження не за допомогою зміни порогів спрацьовування процедур хендовера, а при проектуванні зони покриття, виходячи з прогнозування рівня хендовера, дасть можливість підвищити ефективність функціонування обслуговування навантаження в секторах БС.

Модель оптимального розподілу навантаження в мережі. Аналіз процесу функціонування процесу обслуговування навантаження в системах мобільного зв'язку дає змогу виділити чотири компоненти моделі аналізу оптимальності розподілу трафіку в мережі (рисунок 2):

1. Сектор БС обслуговування мобільного терміналу.

2. Система зміни секторів БС.

3. Система забезпечення керуванням навантаження в секторі БС.

4. Фактори, що впливають на них.

Об'єктом управління є навантаження в секторах обслуговування БС, що являє собою сукупність функціонально пов'язаних і взаємодіючих між собою та абонентами елементів.

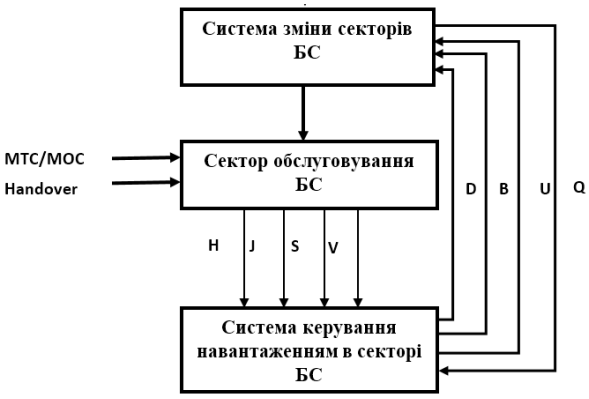


Рисунок 2 – Модель оптимального розподілу навантаження в мережі

У процесі функціонування системи між її елементами, які є об'єктами управління, й тими, що містять органи управління, здійснюється інформаційний обмін, який характеризується наявністю різного типу даних.

Від об'єктів управління в органи управління можуть передаватися такі дані:

• для контролю розподілу навантаження – показники швидкості зміни стільників, які передаються по каналу BCCH в кожному стільнику ($h1$, ... hi, ... ε H);

• параметр C1 для обслуговуючого стільника, менший нуля (C1 <0) протягом 5 с, коли втрати на радіоінтерфейсі занадто великі і для MS потрібно змінити стільник ($j1$, $j2$, ... ji, ... ε J);

• значення параметра C2 для сусідніх стільників, яке перевищує це ж значення для обслуговуючого стільника протягом 5 с ($q1$, $q2$, ..., qi, ... ε Q).

Від органів управління на об'єкти управління можуть передаватися такі команди:

• зміна стільника всередині LA (Location Area) ($u1$, $u2$, ..., ui, ... ε U) – інформація про те, що новий стільник належить тій же LA, по каналу BCCH сусідніх стільників;

• зміна стільника всередині одного MSC ($s1$, $s2$, ..., si, ... ε S) – MS при зміні стільника виявляє зміну LA на основі аналізу інформації, що передається по каналу BCCH;

• оновлення місцеположення при вході в зону обслуговування нового MSC / VLR ($b1$, $b2$, ..., bi, ... ε B) – оновлення місцеположення LU (Location Update) здійснюється тоді, коли MS переміщується в нову LA;

• використання необхідних резервних каналів для хендовера ($v1$, $v2$, ..., vi, ... ε V) – утримання розмови при транзитному використанні сектора ділянок мережі;

DOI: 10.24025/2306-4412.3.2020.200346

• система управління системою вимірів показника радіоінтерфейсу при доставці повідомлень (*d*1, *d2*, ..., *di*, ... ε *D*) – вимірювання рівнів сигналів BCCH на частотах, яка обслуговує і сусідні стільники.

Математична інтерпретація моделі. Для розгляду моделі секторного аналізу введемо такі параметри інтенсивностей викликів у секторах БС: вхідні – λ_{MOC}, вихідні – λ_{MTC} і хендовер – λ_{hand}.

Джерелами навантаження БС можуть бути наступні види викликів:

• ініційовано і завершено в одному й тому ж стільнику мережі GSM або UMTS;

• ініційовано в стільнику GSM і завершено в стільнику мережі UMTS, і навпаки;

• ініційовано в одному і завершено в іншому стільнику мережі UMTS;

• хендовера, що надійшов у стільник мережі GSM із сусідніх стільників цієї ж мережі і завершився в розглянутому стільнику;

• хендовера, що надійшов у стільник мережі GSM із сусідніх стільників мережі UMTS і завершився в розглянутому стільнику.

Для створення математичної моделі введемо обмеження і допущення:

1. Потоки ініційованих і завершених викликів (Mobile Originated Calls і Mobile Terminated Calls) і хендовера (Handover Calls) є пуассоновим потоком з інтенсивностями λ_{MOC}, λ_{MTC}, λ_{hand}. Сумарний потік викликів, що створюють навантаження на базову станцію, так само є пуассоновим як у каналах TCH (GSM), так і в каналах DTCH (UMTS):

$$\lambda=\lambda_{hand}+\lambda_{MOC}+\lambda_{MTC}+\lambda_{hand\_DTCH}+\lambda_{DLCH}+\lambda_{ULCH}. \quad (1)$$

Будь-який виклик з інтенсивністю μ_1 завершує обслуговування всередині стільника і з інтенсивністю μ_2 переходить на обслуговування в стільник інших мереж (Handover Calls). Закон розподілу тривалості обслуговування викликів як в стільнику, так і при хендовері, має експоненційний характер з параметрами μ_1 і μ_2 відповідно. Тривалість зайняття радіоканалу визначається сумою величин $\mu_1+\mu_2$.

2. Тривалість обслуговування будь-якого виклику описується експоненційним розподілом χ (t)

$$(X(t) \quad n). \quad (2)$$

3. Вхідне навантаження, що буде визначатися через інтенсивність вхідних потоків (1), позначимо через *Z*. Водночас виконане навантаження – інтенсивність обслужених заявок (2) – позначимо через *Y*.

Проаналізуємо приклад реалізації сценарію: виклик ініційовано і завершено в одному стільнику GSM, наявний вхідний хендовер від стільників UMTS, без обмеження на резервування радіоканалів для вхідного хендовера. Для цього сценарію використовуємо модель системи з відмовами – Ерланг B [4]. Ймовірність відмови (P_R) в такій системі може бути описана виразом

$$\frac{\frac{(\lambda\ \tau)^n}{}}{\sum_{n\ 0}^{N}(\frac{(\lambda\ \tau)^n}{})} \quad \frac{—}{\sum_{n\ 0}^{V}(—)}, \quad (3)$$

де τ – одиничний інтервал;

λ – кількість подій за τ.

Ймовірність відмови визначається як для МТС стандарту GSM цього стільника, так і для вхідного хендовера від стільників стандарту UMTS.

В процесі обслуговування з подіями в стільнику базової станції можуть відбуватися різні етапи життєвого циклу. Одним із показників, яким нехтують при обліку завантаженості стільника, є ймовірність того, що за час *t* всі канали вільні:

$$\overline{\left[\Sigma\ \ _0\left(—\right)\right]} \quad (4)$$

Саме цей показник доцільно використовувати при аналізі завантаженості БС, враховуючи, що БС може бути застосована як транзитна при хендовері. З огляду на те, що стандартним показником стільника БС є його завантаження в ЧНН (час найбільшого навантаження), вираз для оцінювання ймовірності зайнятості *V* каналів набуде вигляду

$$\left[—\right]. \quad (5)$$

Використовуючи рівняння (3)–(5), визначимо середню кількість зайнятих каналів:

$$\langle k\rangle \quad \sum \quad \left[\frac{}{(n\ 1)!}\right]. \quad (6)$$

Цей підхід до моделі дає можливість визначити перевантажені і недовантажені ділянки мережі, перейшовши від зайняття каналів до функціонуючого навантаження в стільнику БС, а далі, в процесі управління обслуговування заявок, використовувати отримані дані для забезпечення рівномірності завантаження елементів мережі, виявляючи трафік хендовера на сусідню БС, який не враховується при стандартному плануванні [8].

DOI: 10.24025/2306-4412.3.2020.200346

У запропонованому сценарії навантаження формуються в секторі GSM. У цій моделі процесом обслуговування викликів у стільнику виступає N-канальна (кількість радіоканалів у стільнику) повнодоступна система масового обслуговування (СМО), на яку надходять два пуассонові потоки заявок: 1 – потік викликів (λ_{MTC}), 2 – потік хендовера з UMTS в GSM-інтенсивність (λ_{hand}).

***Можливі два варіанти роботи*:**

• в момент надходження заявки (Z_0) виклик надходить на обслуговування і займає один канал, якщо є вільний (Y);

• якщо в момент надходження заявки в СМО немає вільних каналів, то виклик втрачається (R_0).

Тривалості обслуговування заявок – незалежні випадкові величини, що мають експоненційний розподіл з параметром інтенсивності μ (рисунок 3).

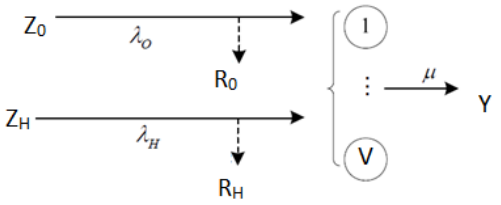


Рисунок 3 – Вхідне навантаження при сценарії хендовера меж секторами GSM та UMTS

Основними характеристиками для аналізу є ймовірність p_{lost_1} втрати викликів (блокування нового виклику) і ймовірність p_{lost_h} (ймовірність блокування хендовера). Для створення математичної моделі стільника необхідно використовувати наведене вище твердження для опису життєвого циклу системи – зміни стану системи (стільника). Подібний підхід було використано в роботі [5] при аналізі життєвого циклу GSM. У цій роботі акцент зроблено на специфіку комбінованих мереж GSM і UMTS, розглядаючи тільки хендовер між БС, що обслуговуються одним контролером BSC.

Стан стільника (який є СМО) може змінитися або за рахунок надходження викликів, або за рахунок завершення обслуговування викликів. Згідно з (1) сумарний потік викликів, що надходять на базову станцію стільника, є пуассоновим, тобто має одну з властивостей – відсутність післядії, отже, процес надходження заявок у стільник після моменту t не залежить від функціонування системи до моменту t [6].

Згідно з (2) тривалість обслуговування заявок, які надійдуть у стільник після t, не залежить від стану системи до моменту t. За властивістю стаціонарності пуассонового потоку ймовірність надходження дзвінка в момент від t до $t+\Delta t$ (малий інтервал, в межі – нескінченно малий) дорівнює Δt / T ($\Delta t << T$). З другого боку, якщо інтервал можна порівняти з T, формула працювати не буде, тому що вона диференціальна – для нескінченно малого інтервалу.

За властивістю стаціонарності пуассонового потоку тривалість обслуговування викликів залежить тільки від довжини інтервалу Δt. Ця властивість пуассонового потоку дає можливість представити його як потік, який має властивість потоку Маркова – властивість відсутності післядії.

Марковський процес задається графом переходів зі стану в стан. Цими станами є варіанти життя викликів у стільнику, а зміни цих станів визначаються ймовірністю переходу. Для розв'язання задачі використовуємо ланцюг Маркова з n станами обслуговування викликів у стільнику з дискретним часом, що викликано властивістю пуассонового потоку – стаціонарність, а також тим, що аналіз зміни системи проводиться в ЧНН з інтервалами в одну годину. Особливістю ланцюгів Маркова є те, що кількість таких станів є кінцевою. Ця властивість виконується, враховуючи, що канальний ресурс стільника є обмеженим, відповідно умови зайняття і звільнення цих каналів описуються кінцевою кількістю умов переходу. Ланцюг Маркова буде однорідним через властивості ординарності пуассонового потоку. Відповідно, матриця перехідних ймовірностей системи не буде залежати від поточного стану ланцюга.

Також цей марковський однорідний процес з дискретним станом – процес однорідної загибелі і розмноження, і він має вигляд, зображений на рисунку 4. Граф станів витягнуто в ланцюжок, в якому перескок через два стани можливий тільки через проміжний.

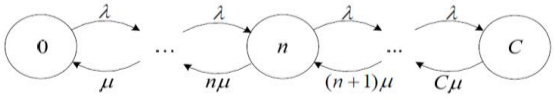


Рисунок 4 – Марковський процес зміни статусів при обслуговуванні заявки в мережі оператора

Для створення математичної моделі попередньо визначимо ймовірності деяких подій.

DOI: 10.24025/2306-4412.3.2020.200346

Після цього представимо у вигляді ланцюга Маркова умови зміни станів і уявімо розв'язувальну модель у вигляді матриці переходів, яка в майбутньому може бути розв'язана через рівняння Колмогорова або з використанням розв'язку задачі Коші.

Кількість подій пуассонового потоку (1) на інтервалі довжини Δt має розподіл з інтенсивністю $\lambda * \Delta t$. Отже, ймовірність того, що за час Δt в стільник вступить певна кількість викликів, дорівнює

$$P(t) = e^{\frac{-\tau}{T}} = e^{-\lambda * \tau}. \quad (7)$$

Визначимо тепер середній час очікування першого дзвінка. Ймовірність, що до моменту t дзвінка не було, а в інтервалі $(t + \Delta t)$ надійшов, дорівнює

$$P(t) = e^{\frac{-\tau}{T}} * \frac{\Delta t}{T}. \quad (8)$$

Помноживши (8) на Δt і беручи інтеграл, одержимо середній час очікування події:

$$\int_0^{\infty} t * e^{\frac{-\tau}{T}} * \frac{\Delta t}{T} = T. \quad (9)$$

Параметр T – це середній час очікування події: вхідного дзвінка (МТС) або події по хендоверу. Можна як параметр використовувати не T, а обернену величину λ, і тоді ймовірність настання події дорівнює $\lambda * \Delta t$ [7].

Параметр розподілу Пуассона – це середня кількість дзвінків в одиничному інтервалі. Абстрагуємося від одиничного інтервалу τ: якщо за інтервал відбувається λ подій, то ймовірність, що за цей інтервал відбувається k-подій, дорівнює

$$P(k, \lambda) = \frac{(\lambda)^k}{k!} \cdot e^{-\lambda}. \quad (10)$$

Використовуючи (10), отримаємо, що ймовірність того, що за час Δt в стільник не надходить виклик, дорівнює

$$P(0, \lambda) = \frac{(\lambda)^0}{0!} \cdot e^{-\lambda} = \frac{1}{1} \cdot e^{-\lambda} = e^{-\lambda}. \quad (11)$$

Ймовірність того, що за час Δt в стільник надійде одна заявка, дорівнює

$$P(1, \lambda) = \frac{(\lambda)^1}{1!} \cdot e^{-\lambda} = \frac{\lambda}{1} \cdot e^{-\lambda} = \lambda \cdot e^{-\lambda}. \quad (12)$$

Ймовірність того, що за час Δt в стільник надійде два і більше дзвінків або хендовер [9], можна описати з властивості ординарності простішого потоку, який характеризується тим, що за досить малий проміжок часу ймовірність появи двох або більшої кількості викликів є величиною малого порядку τ.

Властивість експоненційного розподілу є ймовірністю того, що за час Δt не закінчиться обслуговування виклику:

$$P(0, \mu) = \frac{(\mu)^0}{0!} \cdot e^{-\mu} = \frac{1}{1} \cdot e^{-\mu} = e^{-\mu}. \quad (13)$$

Тоді ймовірність того, що за час Δt в стільнику не закінчиться обслуговування n викликів, дорівнює

$$P(0, \mu) = \left[\frac{(\mu)^0}{0!} \cdot e^{-\mu}\right]^n = \left[\frac{1}{1} \cdot e^{-\mu}\right]^n = e^{-n \cdot \mu}. \quad (14)$$

Ймовірність, що за Δt завершений один виклик, дорівнює

$$P(1, \mu) = \left[\frac{(\mu)^1}{1!} \cdot e^{-\mu}\right]^n = \left[\frac{\mu}{1} \cdot e^{-\mu}\right]^n = \mu \cdot e^{-n \cdot \mu}. \quad (15)$$

Описані вище ймовірності є частиною життєвого циклу подій у стільнику мобільного оператора. Припустимо, що в момент t в стільнику обслуговувалося n викликів: $n = \{1, C\}$, де C – максимальна кількість можливих каналів у стільнику. Це можна записати як X $(t + \Delta t) = n$. В наступний момент часу $t + \Delta t = \tau$ стан стільника може:

1) не змінитися, тобто за час τ в стільник не надійде жодного нового виклику (11), і жоден виклик не закінчить обслуговування (14):

$$P_{n+0}(0, \lambda, \mu) = P(0, \lambda) \cdot P(0, \mu) = e^{-(n \cdot \mu + \lambda)}; \quad (16)$$

2) перейти в стан +1, якщо за час $t + \Delta t$ один виклик надійде в стільник (12), а жоден інший виклик із тих, що перебувають в обслуговуванні, не закінчить його (13):

$$P_{n+1}(0, \lambda, \mu) = P(1, \lambda) \cdot P(0, \mu) = \lambda \cdot e^{-(\mu + \lambda)}; \quad (17)$$

3) перейти в стан -1, якщо за час $t + \Delta t$ один виклик буде завершений у стільнику (15), і не надійде жодного нового виклику (11):

$$P_{n-1}(1, \lambda, \mu) = P(0, \lambda) \cdot P(1, \mu) = \mu \cdot e^{-(n \cdot \mu + \lambda)}; \quad (18)$$

4) ймовірність того, що за час Δt в стільник надійде два і більше дзвінків або хендовер (за досить малий проміжок часу) є величиною малого порядку τ.

У підсумку, за час τ в стільнику навантаження може збільшитися за рахунок надходження нового виклику, зменшитися за рахунок обслуговування виклику або залишитися на тому ж рівні. Одночасне надходження двох типів викликів будемо розглядати як послідовні події на ділянці $t + \Delta t$ при $\Delta t \to 0$, виражене властивістю ординарності потоку подій [10]. Таким чином, вирази (16)–(18) описують життєвий цикл перебування викликів у стільнику

DOI: 10.24025/2306-4412.3.2020.200346

як процес розмноження і загибелі з наступними перехідними ймовірностями зі стану n в стан $n + 1$ (або $n – 1$):

$$\begin{cases} P_{n+0}(0,\lambda,\mu) = e^{-(n\cdot\mu+\lambda)}, \\ P_{n+1}(0,\lambda,\mu) = \lambda \cdot e^{-(\mu+\lambda)}, \\ P_{n-1}(1,\lambda,\mu) = \mu \cdot e^{-(n\cdot\mu+\lambda)}, \\ P_{n+2}(2,\lambda,\mu) = o(\tau) \end{cases} \quad (19)$$

Результати математичної моделі. Основною особливістю марковських процесів є те, що їх умовні функції щільності ймовірностей задовольняють диференціальним рівнянням часткових похідних типу. Такий підхід для розв'язання лінійних рівнянь прийнятий у телекомунікаціях як достатній [11]. Ця система рівнянь (19) розв'язується методом задачі Коші або рівняннями Колмогорова.

Для однорідного процесу загибелі і розмноження згідно з графом станів (див. рисунок 4) система рівнянь (19) може бути представлена в діагональній матриці порядку n, котрий відповідає однорідній системі лінійних алгебраїчних рівнянь щодо вектора граничних ймовірностей станів [7]. Для розв'язання такої системи рівнянь можна скористатися підходом локального балансу і умовою нормування:

$$P(1,\lambda) = 1 - P(0,\lambda) = 1 - e^{-\lambda}. \quad (20)$$

Відповідно, для будь-якого n

$$P_n = \frac{P_{k-1}}{k!} P_k \cdot \frac{P_k}{(k+1)!} P_{k+1} \cdots \frac{P_{k-n}}{(k+n)!} P_{k+n} = \frac{P^n}{n!} \cdot P_0 . \quad (21)$$

Враховуючи умови нормування (20), отримаємо P_0:

$$P_0 = \sum_{n=0}^{V} \frac{Z^n}{n!} , n \in \{0, V\}. \quad (22)$$

Визначимо ймовірність втрати заявки в стільнику, виходячи з умов, що в момент τ (надходження заявки) в стільнику відсутні вільні канали (V), тобто розподіл χ (τ) = V. Використовуючи вирази (21)–(22), отримаємо

$$P_R = \frac{Z_0^V}{V!} \cdot \left[\sum_{n=0}^{V} \frac{Z^n}{n!}\right]^{-1}. \quad (23)$$

Вираз (23) можна застосувати при допущенні, що величина надходження двох і більше заявок є величиною малого порядку τ.

На наступному етапі визначимо ймовірність втрати заявки в стільнику під час хендовера з сусідніх стільників (GSM, UMTS):

$$P_{R\_handover} = \frac{Z_h^V}{V!} \cdot \left[\sum_{n=0}^{V} \frac{Z^n}{n!}\right]^{-1}. \quad (24)$$

У статті використано локальну частину мережі одного з операторів мобільного зв'язку міста Київ з досліджуваною топологією мережі, як показано на рисунку 1. В мережі аналіз проведено на трьох ділянках БС GSM-1800, які підключені до одного контролера BSC і мають найбільший відсоток завантаженості в мережі – умовно ці зони зобразимо на рисунку 5. Середній діаметр кожної зони – до 1 км.

а) *б*) *в*)

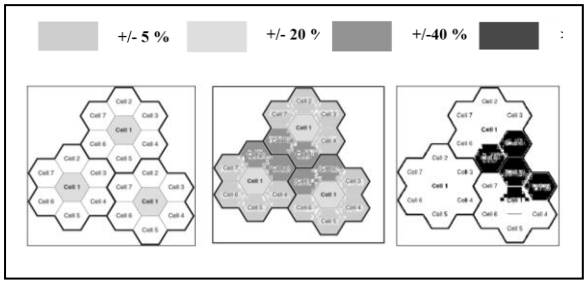


Рисунок 5 – Навантаження в стільниках: плановане (*а*), прогнозоване (*б*), реальне (*в*)

Спочатку ділянка (рисунок 5, *а*) Cell1 – Cell7) мала тільки одну групу секторів, але в ході експлуатації було збільшено ще на групи БС (дві групи секторів Cell1 – Cell7). Проте питання ефективності такого підходу полягає в зменшенні кількості скарг від абонентів. Тому на цьому прикладі пропонується оцінити доцільність збільшення зони покриття.

Оцінювання результатів здійснено шляхом порівняння запланованої частини (вона закладена в плануванні) з прогнозованим розподілом навантаження на мережу. На рисунку 5, *б* показано ступінь відхилення прогнозованого навантаження: колір відповідає проценту відхилення від прогнозу.

Темні ділянки на рисунку 5, *в* показують область із недостатньою кількістю вільних каналів для обслуговування навантаження. Водночас ця модель передбачала збільшення +20 % порівняно із запланованою (рисунок 5, *а*, *б*) в зоні приграничних секторів. У той же час похибка моделі становила 9 %, не передбачаючи відсутності вільних каналів для обслуговування навантаження на граничній ділянці (рисунок 5, *в*). Цю помилку можна пояснити тим, що дані сусідніх секторів БС не були враховані. Ці сусідні сектори належали іншому BSC, і передача, яка була зроблена із сусідньої БС, призвела до збільшення навантаження, яке не було включено в модель.

Необхідні дані формуються в ході обслуговування, центром накопичення таких даних є білінгова система оператора. Ця система

DOI: 10.24025/2306-4412.3.2020.200346

виступає не тільки як система взаєморозрахунку з абонентом, а як система агрегації та аналізу даних. Для розв'язання цієї задачі було проаналізовано дані CDR (Call Data Records – формат збереження подій). Ці дані було згруповано по секторах БС, також було виділено в окрему групу хендоверні дані. При такому групуванні було враховано ряд специфічних характеристик, притаманних білінговій системі. Одна з них – CDR відноситься до того сектора БС, в якому було завершено виклик, навіть якщо більшу частину часу виклик обслуговувався в іншому секторі БС.

Висновки. В цьому варіанті розглянуто стратегію доступу без резервування, коли в секторі радіоканали призначені для обслуговування як дзвінків усередині стільника, так і хендоверних викликів, без радіоканалів резервування для обслуговування хендовера. Тому, ймовірності відмови в обслуговуванні для надходження викликів і хендоверів рівні.

Коли мережа вже в експлуатації, аналіз її роботи здійснюється за допомогою оцінювання статистичних даних щодо подій у системі, використовуючи різні аналітичні програмні комплекси. До останніх відносяться: хендоверні характеристики, скинуті з'єднання, невдалі спроби встановлення з'єднань, інтерференція та ін. Для оптимального оцінювання роботи системи недостатньо знати кількість подій у системі, необхідно оперувати характеристиками навантаження при обслуговуванні цієї ділянки мережі: тривалість подій, час початку, показники якості події.

Було змодельовано і показано, що використана модель прогнозування виконаного навантаження вхідного трафіка ефективніша, ніж традиційні підходи до радіопланування, за рахунок виявлення трафіку, «перекинутого» на сусідній стільник БС, який не враховується при радіоплануванні. Продуктивність мережі значно підвищується при використанні цього методу.

Перспективи подальшого дослідження. В цьому варіанті розглянуто стратегію доступу без резервування, це упущення є досить суттєвим для більш точного прогнозування. В першу чергу, необхідно продумати математичну величину, яка опише це значення. Крім того, такий показник має бути внесений у формування загальної ймовірності.

У статті розглянуто лише один сценарій: виклик ініційовано і завершено в одному стільнику GSM, наявний вхідний хендовер від стільників UMTS. У самій роботі цей сценарій обраний як найбільш характерний для мобільної мережі. В подальших дослідженнях планується розглянути й інші сценарії, які доповнять запропоновану модель. Так, найістотнішим доповненням до моделі буде розгляд такого сценарію – передачу даних ініційовано і завершено в іншому стільнику UMTS.

У подальших висвітленнях необхідно звернути увагу на підходи до віртуалізації обладнання [12]. Такий підхід буде спрямований на віртуалізацію обладнання в центрі мережі, що дасть можливість збільшити швидкість аналізу даних CDR та перенести цей процес в режим реального часу. Це є перспективним напрямом, з урахуванням того, що трафік можна буде перенаправляти від одного сектора до іншого, не чекаючи перевантаження в секторі.

Подальші дослідження мають бути зміщені в бік LTE, як найбільш поширеної в місцях підвищеної концентрації мобільних пристроїв. Виділяючи при цьому окрему нішу для мобільних пристроїв IoT. Для цих пристроїв виділяють окрему зону в спектрі спеціально виділеного діапазону частот (NB-IoT).

Список використаних джерел

[1] Syahfrizal Tahcfulloh, and Eka Riskayadi, "Optimized suitable propagation model for GSM 900 path loss prediction", *Telkomnika Indonesian Journal of Electrical Engineering*, vol. 14, p. 162, 2015.

[2] A. Degollado-Rea, S. Vidal-Beltrán, J. López-Bonilla, and G. Bahadur Thapa, "Okumura-Hata, Walfish-Ikegami and 3GPP propagation models in urban environments for UMTS networks", *The SciTech, Journal of Science & Technology*, pp. 70-78, 2015.

[3] Segun I. Popoola, and Olasunkanmi Fatai Oseni, "Empirical path loss models for GSM network deployment in Makurdi, Nigeria", *International Refereed Journal of Engineering and Science (IRJES)*, vol. 3, pp. 85-94, 2014.

[4] Ю. В. Гайдамака, Э. Р. Зарипова, и К. Е. Самуйлов, *Модели обслуживания вызовов в сети сотовой подвижной связи*: учеб.-метод. пособие. Москва: РУДН, 2008.

[5] О. І. Романов, О. В. Чмиренко, та В. Б. Маньківський, "Оцінка ємності мережі мобільного зв'язку WCDMA", *Сис-*

DOI: 10.24025/2306-4412.3.2020.200346

теми озброєння і військова техніка, № 1 (21), с. 184-188, Київ, 2010.

[6] М. А. Скулиш, О. І. Романов, та Л. С. Глоба, "Принцип обслуговування потоків у гетерогенному телекомунікаційному середовищі", *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки*, № 2, с. 92-98, 2018.

[7] Т. Л. Саати, *Математические методы исследования операций*. Москва: Воениздат, 1963.

[8] В. Ю. Бабков, М. А. Вознюк, и П. А. Михайлов, *Сети мобильной связи. Частотно-территориальное планирование*: учеб. пособие для вузов. Москва: Горячая линия-Телеком, 2007.

[9] C. Fuchs, N. Aschenbruck, P. Martini, and M. Wieneke, "Indoor tracking for mission critical scenarios: A survey", *Pervasive and Mobile Computing*, vol. 7, no. 1, pp. 1-15, 2011.

[10] A. Bhuvaneshwari, R. Hemalatha, and T. Satyasavithri, "Statistical tuning of the best suited prediction model for measurements made in Hyderabad City of Southern India", in *Proc. World Congress on Engineering and Computer Science*, San Francisco, 2013, vol. II.

[11] Dusit Niyato, and Dong In Kim, "Relay-centric radio resource management and network planning", *IEEE Transactions on Wireless Comunication*, vol. XX, pp. 76-89, 2009.

[12] O. Romanov, M. Nesterenko, N. Fesokha, and V. Mankivskyi, "Evaluation of productivity virtualization technologies of switching equipment telecommunications networks", *Information and Telecommunication Sciences*, vol. 1, pp. 53-58, 2020.

References

[1] Syahfrizal Tahcfulloh, and Eka Riskayadi, "Optimized suitable propagation model for GSM 900 path loss prediction", *Telkomnika Indonesian Journal of Electrical Engineering*, vol. 14, p. 162, 2015.

[2] A. Degollado-Rea, S. Vidal-Beltrán, J. López-Bonilla, and G. Bahadur Thapa, "Okumura-Hata, Walfish-Ikegami and 3GPP propagation models in urban environments for UMTS networks", *The SciTech, Journal of Science & Technology*, pp. 70-78, 2015.

[3] Segun I. Popoola, and Olasunkanmi Fatai Oseni, "Empirical path loss models for GSM network deployment in Makurdi, Nigeria", *International Refereed Journal of Engineering and Science (IRJES)*, vol. 3, pp. 85-94, 2014.

[4] Yu. V. Gaydamaka, E. R. Zaripova, and K. Ye. Samuylov, *Cellular mobile call service models*. Moscow, Russia: RUDN, 2008. [in Russian].

[5] A. I. Romanov, A. V. Chmyrenko, and V. B. Mankivskyi, "Estimation of WCDMA mobile network capacity", *Systemy ozbroiennia i viiskova tekhnika*, no. 1 (21), pp. 184-188, Kyiv, 2010. [in Ukrainian].

[6] M. A. Skulysh, O. I. Romanov, and L. S. Globa, "The principle of flow maintenance in a heterogeneous telec-?mmunications environment", *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky*, no. 2, pp. 92-98, 2018. [in Ukrainian].

[7] T. L. Saati, *Mathematical methods of operations research*. Moscow, Russia: Voenizdat, 1963. [in Russian].

[8] V. Yu. Babkov, M. A. Voznyuk, and P. A. Mikhaylov, *Mobile networks. Frequency spatial planning*. Moscow, Russia: Goryachaya liniya-Telekom, 2007. [in Russian].

[9] C. Fuchs, N. Aschenbruck, P. Martini, and M. Wieneke, "Indoor tracking for mission critical scenarios: A survey", *Pervasive and Mobile Computing*, vol. 7, no. 1, pp. 1-15, 2011.

[10] A. Bhuvaneshwari, R. Hemalatha, and T. Satyasavithri, "Statistical tuning of the best suited prediction model for measurements made in Hyderabad City of Southern India", in *Proc. World Congress on Engineering and Computer Science*, San Francisco, 2013, vol. II.

[11] Dusit Niyato, and Dong In Kim, "Relay-centric radio resource management and network planning", *IEEE Transactions on Wireless Comunication*, vol. XX, pp. 76-89, 2009.

[12] O. Romanov, M. Nesterenko, N. Fesokha, and V. Mankivskyi, "Evaluation of productivity virtualization technologies of switching equipment telecommunications networks", *Information and Telecommunication Sciences*, vol. 1, pp. 53-58, 2020.

DOI: 10.24025/2306-4412.3.2020.200346

A. I. Romanov, *Dr.Tech.Sc., professor,*
M. M. Nesterenko, *Ph.D., accociate professor,*
V. B. Mankivskyi, *Ph.D., assistant,*
I. O. Saichenko, *assistant*
Igor Sikorsky Kyiv Polytechnic Institute,
Industrial lane, 2, Kyiv, 03056, Ukraine

MODEL OF OPTIMAL LOAD DISTRIBUTION IN MOBILE OPERATOR ACCESS NETWORK

The main attention when planning the network of a mobile operator is paid to frequency distribution and electromagnetic compatibility. The main argument is that the solution of this problem will ensure the fulfillment of the conditions of optimal frequency resource allocation and, as a consequence, will allow to optimize the level of interference in neighboring zones. At the same time, the issue of uniformity of traffic distribution among network elements is not considered. As a result, this approach negatively affects the performance and quality of service. In order to increase the efficiency of load distribution in the planning of base station service areas, it is proposed to additionally take into account the results of the analysis of service event flows in cells and the data of the billing system.

Initially, radio planning determines the further quality of services on mobile network. At the same time there is no adaptation to changing external conditions. In large cities with a developed infrastructure, the constantly changing situation forces mobile operator to constantly adjust the conditions of signal propagation. The constant increase in volume of transmitted information requires the optimization of load distribution on cellular structure, the search for optimal methods of ensuring electromagnetic compatibility (EMC), the territorial distribution of the frequency resource of the operator. High efficiency of network quality in such conditions is provided by the operator at close interaction of the services of planning, optimization and operation of network by use of expensive software. This paper offers a look at the problem in terms of subscriber traffic.

In the paper, the strategy of access without redundancy is considered, when in the sector radio channels are designed to service both calls within the cell and hand-made calls, without radio redundancy channels to service handover. Therefore, the probabilities of denial of service for incoming calls and handovers are equal.

Keywords: *quality of service (QoS), bandwidth, load distribution, base station sector.*

DOI: 10.24025/2306-4412.3.2020.200346

ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 007:004.56:616-036.21.2019

[0000-0002-8555-5712] **М. Д. Василенко,** *д.ф.-м.н., д.ю.н., професор, в.о. завідувача кафедри кібербезпеки*,
e-mail: nvas08@ukr.net
[0000-0003-2059-0581] **В. П. Новіков,** *к.т.н., доцент, доцент кафедри кібербезпеки*,
e-mail: novikovodessa0@gmail.com
[0000-0003-1793-016X] **В. О. Рачук,** *асистент кафедри кібербезпеки*,
e-mail: rachuk960@gmail.com
[0000-0002-6082-981X] **В. М. Слатвінська,** *аспірантка кафедри господарського права та процесу,*
e-mail: slatvinskaya_valeriya@ukr.net
Національний університет «Одеська юридична академія»
Фонтанська дорога, 23, м. Одеса, 65009, Україна

КІБЕРБЕЗПЕКА В ПРОЯВАХ РИЗИКІВ У ПЕРІОД ПАНДЕМІЇ: СТАН ТА ГЕНЕЗА

Стаття покликана стимулювати інтерес до проявів ризиків у кібербезпеці в умовах COVID-19 (коронавірусу). Зокрема, проаналізовано та надано оцінку проявам кіберризиків у контексті кібербезпеки як нової проблеми, пов'язаної з появою COVID-19, а також з'ясовано її стан та генезу. Запропоновано вирішити проблему управління різними видами ризиків шляхом інституційного розуміння забезпечення юридичного підґрунтя та багатофакторного проєктування або прогнозування, а також запропоновано основний метод посилення захисту – технічний, що використовує, перш за все, алгоритмічні методи, а в окремих випадках – можливість використання сил «Червоної команди» захисної структури. Показано, що в умовах принципового збільшення телеконференцій (у період пандемії) суттєво збільшується кількість кіберризиків. Зазначено основні заходи безпеки, потрібні для захисту інформаційно-комунікативної інфраструктури в умовах дії пандемії по COVID-19 (коронавірусу). Авторами доведено, що, оскільки ризики все більше стають послідовними та взаємопов'язаними процесами як невід'ємні складники системи управління, то в цьому випадку більш доречними стають періодичні перевірки офісних приміщень на виявлення використання технічних засобів скритого зняття інформації та періодичне проведення онлайн семінарів зі співробітниками з питань безпеки.

Ключові слова: *кібербезпека, ризик, оцінювання ризику, невизначеність, пандемія, COVID-19.*

Вступ. Епідемія коронавірусу (COVID-19), що створила безпрецедентну глобальну надзвичайну ситуацію, стала серйозним тестом для урядів, громадян та економік більшості країн світу, які підпали під серйозні ризики. Так, за даними Центру скарг на інтернет-злочини (ЦСІЗ) ФБР (США), наведеними у звіті про злочинність в Інтернеті за 2019 рік, злочини та шахрайства з використанням всесвітньої мережі не мають жодних ознак щодо їх припинення, а мають тенденцію до стрімкого збільшення. ЦСІЗ зафіксував за останній рік збитки у розмірі майже чотири мільярди доларів для приватних осіб і постраждалого бізнесу [1]. Аналіз інформації, яка надходить з країн-членів ЄС, також підтверджує той факт, що в результаті пандемії з великим відсотком ймовірності очікуються ризикові економічні й політичні негаразди. З появою коронавірусу додаткові проблеми з'явилися майже в усіх країнах і в усіх владних структурах, а урядові рекомендації, що стосувалися COVID-19, привели до безпрецедентного переходу на онлайн-роботу. За цих виняткових обставин невирішеною важливою проблемою залишається забезпечення зниження ризиків загалом і кіберризиків зокрема. Через те, що під час пандемії безперервна діяльність в основному відбувається завдяки використанню віддалених операцій, у світі з'явилася величезна кількість «фішингових» кампаній. Загальновідомо, що фішинг являє собою різновид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів. Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень усередині різних сервісів, наприклад від імені банків, або усередині соціальних мереж. У листі часто

DOI: 10.24025/2306-4412.3.2020.214774

міститься пряме посилання на сайт, який зовні важко відрізнити від реального, або на сайт з редиректом. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленій сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дає шахраям можливість отримати доступ до облікових записів та банківських рахунків. У той час як сьогодні в багатьох країнах запроваджують заходи, щоб допомогти жертвам COVID-19 і обмежити зараження, хакери використовують кризу та продовжують свої дії для здійснення цілеспрямованих кібератак на підприємства, зокрема на робочі місця. У період кризи хакери намагаються використовувати увагу, яку приділяють вірусам, і пов'язаний з ними панічний ефект для проведення фішингових кампаній, видаючи себе за сповіщення, пов'язані з COVID-19 (див. [2]). Отже, майже всі випадки можливих загроз базуються на розумінні та використанні ризиків і ризикових ситуацій.

Аналіз публікацій та джерел досліджень/дослідження. З багатьох публікацій щодо дослідження ризиків у вітчизняних та іноземних виданнях відомо безліч визначень «ризику», що допускає досить широке його тлумачення. Так, тільки в Інтернет-словниках містяться сотні тлумачень ризику у багатьох сферах, допомагаючи розкривати сутність самого ризику та пов'язаних з ним понять [3]. Праць, присвячених суто кібербезпеці, також досить багато, включаючи ті, в яких досліджуються питання кіберризиків. Однак праць, в яких йдеться про вирішення цих проблем у кіберсередовищі в період пандемії, дуже мало. Насамперед, відзначимо працю співавторів цієї статті, де досліджувалися проблеми кіберризиків в умовах комунального буття в господарствах міст у період пандемії [2]. На основі зазначеного першоджерела необхідно дослідити, як вплинула ситуація з пандемією на стан кібербезпеки та кіберризиків. Також відзначимо наукові праці (див. [4], [5], [6], [7]), в яких йдеться, зокрема, про онлайн-роботу вдома під час COVID-19, заходи в галузі кібербезпеки під час пандемії та кібератаки на так звані «смарт-будинки». Проте наразі ми не можемо використати наведені актуальні дослідження з огляду на те, що нас цікавить, яким чином пандемія вплинула на наявний рівень кібербезпеки.

Новизна означеної статті полягає в аналізі розширення «поверхні атаки», яке відбулося через пандемію, коли користувачі Інтернету масово заполонили інтернет-ресурси, що дало: (а) з технічного боку – більше сервісів, схильних до вразливостей, при розширенні сервісів, щоб відповісти на запити ринку, безпеці приділялося недостатньо уваги, що спричинило збільшення атак; (б) з соціального боку – більше приводів для фішингу. А це, в свою чергу, привело до того, що в умовах нових проблем сучасності під час пандемії необхідно запропонувати їх практичне вирішення.

Метою дослідження є аналіз і оцінювання генези та проявів кіберризиків як нової проблеми функціонування кіберпростору, пов'язаної з появою COVID-19 (коронавірусу).

Виклад основного матеріалу. Поняття «ризик» має досить широке трактування. Водночас його соціальна сутність полягає, перш за все, в тому, що суб'єкт, свідомо відступаючи від встановлених у суспільстві правил поведінки, створює конфліктну ситуацію, загострює проблему до межі і, використовуючи переваги екстремальної ситуації, прагне вирішити поставлене завдання, яке найчастіше має негативний сенс. Тому зрозумілими стають ймовірні ризики від дій непрофесійних керівників, які вважають себе «ефективними менеджерами».

Відповідно, такий стан характерний також і для сфери інформаційної безпеки та елементів і засобів кібернетики, яка наразі впроваджена в будь-яку систему управління. У зв'язку з цим аналіз і розкриття поняття «ризику» для його подальшої інтерпретації розширить можливості з підвищення ефективності ще й інформаційної безпеки. Враховуючи, що ризики стосуються різних предметних галузей, це поняття слід розглянути з точки зору безпеки, психології, економіки, медицини тощо. Воно показано як у безлічі публікацій, так і в різних нормативних документах (див., наприклад, [8]). Втім, виникає проблема управління різними видами ризиків, що потребує, на нашу думку, інституційного розуміння. Крім того, для розв'язання, наприклад, управлінських завдань слід визначитися з використанням прогнозування (оцінювання) ризиків. Нерідко для цього автори виходять із позицій кібернетичного бачення явища та кібернетики в цілому, яка, за визначенням академіка В. М. Глушкова, являє собою «науку

DOI: 10.24025/2306-4412.3.2020.214774

про загальні закони одержання, зберігання, передавання й перетворення інформації у складних системах управління» [9].

Визначення ризику містяться в багатьох нормах різних галузей господарства і техніки. Однак існує Міжнародний стандарт ISO 31000 [10], який використовується для загального оцінювання ризику. Щоб реалізовувати процес керування ризиком, він має бути інтегрованим зі складовими керування ризиками, що включає обмін інформацією та консультування; встановлення контексту (оточення); загальне оцінювання ризику (його ідентифікація, аналіз та оцінювання); оброблення та узагальнення отриманих результатів обраного типу ризику; моніторинг і критичне аналізування.

Міжнародний стандарт ISO 31000 враховує, в цілому, більшу частину можливих ризиків та пов'язаних із ними складових, у тому числі й епідемічних ризиків. З позиції загальної теорії ризиків слід звернути увагу на принципову особливість, а саме на те, що «прогнозуванням» часто замінюють «оцінювання» ризиків. Якісне прогнозування, як, наприклад, метод експертних оцінок, використовують у нетехнічній сфері, і тут воно, схоже, функціонує аналогічно оцінюванню. Однак між ними існує різка відмінність у стандартній моделі статистичного оцінювання. Так, у гуманітарних науках частіше говорять про обґрунтований ризик, що не викликає зауважень з нашого боку. Обґрунтований ризик слід відмежовувати від спричинення шкоди в стані крайньої необхідності, коли для деяких категорій осіб дія в стані крайньої потреби поставлена в обов'язок, а ризик виступає як виключно суб'єктивне право будь-якого суб'єкта. У разі крайньої необхідності спонукальним мотивом дій суб'єкта є загрозлива небезпека суспільно значущим інтересам, а при ризику – досягнення соціально значущої мети. За умов крайньої необхідності, наприклад пандемії, критеріями порівняння є: тяжкість шкоди, заподіяної зловмисниками, та запобігання їй з урахуванням витрат, а при підвищеному ризику акцент робиться на порівнянні ступеня вірогідності спричинення шкоди (наприклад гранично допустимий ризик тяжких наслідків, але з мінімальним ступенем вірогідності).

В інформаційних технологіях, які забезпечують нормальну (безперешкодну) роботу інформаційно-комунікаційної інфраструктури, ризики мають більш суттєве значення, визначаючи реально виражену конкретику. За даними Інтернет-спільноти, в період пандемії з COVID-19 зросла кількість атак на інформаційні ресурси таких інфраструктур. Точних цифр авторам віднайти не довелося, але приблизна оцінка зростання кількості атак, найімовірніше, перебуває в діапазоні (15–25) % [2].

Зростання у суспільстві паніки, яка пов'язана з розповсюдженням COVID-19, стало приводом як для появи нових кіберризиків, так і посилення старих шахрайських дій та інших негативних проявів. Задля цього шахраї вставляють шкідливі програми, які ставлять під загрозу пристрої користувачів та їхню особисту інформацію. Коли співробітники органів самоврядування, державних та господарських структур працюють вдома (онлайн), а їх пристрої підключені до віддалених серверів, під загрозу підпадають як зазначені прилади, так і вся інформаційна структура і сама мережа в цілому. Досить широко розповсюджені вже зазначені вище «фішингові» повідомлення (листи) з профілактики і лікування COVID-19, які, начебто, направлені від державних установ або органів охорони здоров'я. Одним із найпростіших і популярних методів фішинг-атак став спосіб, коли зловмисники вказують у темі листа назву вірусу COVID-19, і людина відкриває його, інфікуючи свій пристрій. В цілому, відзначимо, що таке кібершахрайство набуло стрімкого та стійкого зростання майже в усіх країнах.

В умовах необхідності створення безпеки в інформаційно-комунікаційних системах оцінювання та якісний аналіз інформаційних ризиків дають можливість визначити необхідний рівень захисту інформації, здійснити його підтримку і розробити стратегію розвитку інформаційної структури системи. Мається на увазі, що це стосується самої компанії або підприємства. Оцінювання та аналіз інформаційних ризиків виступають необхідною умовою при створенні системи керування ризиками і формуванні плану забезпечення стабільної роботи підприємства, а також при забезпеченні безперервності роботи та відновлення бізнесу. В широкому сенсі, у разі дослідження інформаційної безпеки, ризик часто відображається імовірністю функціонально (стохастично) пов'язаних з нею понять. У цьому випадку можливий вимір результату визначається ймовірністю матеріальних та інших втрат через вірогідність появи несприятливого результату

DOI: 10.24025/2306-4412.3.2020.214774

або події. Трапляється також визначення ризику як дії або діяльності, реалізація якої ставить під загрозу задоволення будь-якої досить важливої потреби. В окремих джерелах ризик трактується як міра небезпеки, що характеризує ймовірність її появи й розміри пов'язаної з нею шкоди. Трапляються і визначення ризику, які зображують його як небезпеку вибору з двох або більше альтернативних варіантів дій і передбачають хоча б мінімальне збереження вже досягнутого раніше.

При дослідженні технічних ризиків виділяють їх базові витоки: ризик розглядають як вимірювану або розраховану в деяких межах ймовірність отримання можливих результатів; ризик пов'язують з настанням певної події (як правило, несприятливої); поняття ризику розкривається через практичну діяльність суб'єкта; ризик розкривається через не залежну від суб'єкта діяльності подію, настання якої кількісно можливо оцінити; водночас часто акцент робиться на кількісному та якісному оцінюванні ризику – «мірі ризику»; поняття «ризику» розкривається через невизначеність; ризик відображається ситуацією можливості вибору з двох або з певної визначеної множини варіантів дії; ризик сприймається як небезпека, частота витрати і втрати, всебічна характеристика ситуації, а також комплексний аналіз деякого функціоналу, заданого на множині вірогідних значень (деякої сумарної величини). В цьому разі при обговоренні поняття «ризику» можна виділити одну характеристику, яка є в усіх визначеннях, наведених вище, та об'єднує їх. Це є ніякий функціонал події, яка має відбутися і яка пов'язана з імовірністю, дією або діяльністю, мірою, частотою, вибором певних рішень, невизначеністю, з втратами, небезпекою і т. д. Водночас саме управління ризиками розглядають як процес ідентифікації, управління, усунення або зменшення ймовірності подій, здатних негативно впливати на ресурси інформаційної системи, зменшення ризиків безпеки, що потенційно мають можливість впливати також на інформаційну безпеку, за умови прийнятної вартості засобів захисту. Управління ризиками містить всі операції, які можна проводити над ризиком інформаційної безпеки: мінімізація, нейтралізація, прийняття очікуваної частки ризику, передача ризику або страхування.

Аналіз та оцінювання ризику визначають послідовними взаємопов'язаними процедурами, які входять у процес управління. Оцінювання ризику розглядається як процес ідентифікації визначальних параметрів інформаційних ресурсів системи і загроз цим ресурсам, а також можливих втрат, що ґрунтуються на оцінюванні частоти виникнення подій і розміру збитку. Аналіз ризику розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що вимагають захисту. Отже, прийняття раціональніших рішень у цих випадках вимагає використання специфічного математичного апарату теорії статистичних рішень, нейронних мереж, генетичних алгоритмів, теорії ігор. Цільова невизначеність виникає у багатоцільових завданнях, які потребують багатокритеріального вибору та оптимальних рішень, а оцінювання ризику передбачає дослідження стану, ситуації (сценаріїв) з наявними ознаками небезпеки, невизначеності та/або випадковості. Найефективнішим методом його здійснення є забезпечення юридичного підґрунтя та багатофакторне проєктування або прогнозування. На етапі оцінювання ризиків формується стратегія управління ризиками, а оскільки повністю уникнути ризиків у більшості випадків неможливо, то вагоме значення має вирішення питання допустимості (прийнятності, виправданості) ризику, яке потребує подальшого дослідження та обґрунтування. Оцінювання ризику, що використовують у технічних системах, розглядається як процес ідентифікації інформаційних ресурсів системи і загроз цим ресурсам, а також можливих втрат, що базується на оцінюванні частоти виникнення подій і розміру збитку. Аналіз ризику розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що потребують захисту. На прикладі впливу обмежувально-карантинних заходів на навчальний процес, а саме введення в дію дистанційного навчання засобами телеконференцій через Інтернет-мережі, з'явився ще один напрям ризику, що спричинений самим реальним фактом значного підвищення активності користувачів безпосередньо в мережі Інтернет.

Популярність та капіталізація сервісу відеоконференцій в десятки разів зросла з початком пандемії коронавірусу. При спілкуванні автоматично активізуються інтернет-

DOI: 10.24025/2306-4412.3.2020.214774

злочинці, інтернет-шахраї, закономірно, що зростає загроза в кіберпросторі.

Пов'язані з коронавірусною пандемією карантинні заходи та режими самоізоляції привели до різкого зростання різних онлайн-сервісів – до них входять, у тому числі, онлайн-магазини, онлайн-послуги різного роду і сервіси онлайн-зв'язку (зокрема онлайн-конференції). Багато сервісів запускалися і масштабувалися без урахування заходів безпеки – в спробі довести пропозицію до рівня стрімко висхідного попиту. Це призвело до розширення «поверхні атаки» – можливостей для широкого спектра атак, а масштабування і запуск нових сервісів призвели до проявів нових вразливостей. Результатом цього було різке зростання кіберзлочинів, що корелює зі зростанням попиту на онлайн-сервіси.

Найбільш гучні атаки відбулися на систему онлайн-конференцій Zoom, коли під час пандемії кількість таких конференцій збільшилася в десятки разів. В [11] описується вразливість у Zoom, в якій був залучений помилковий анімований GIF-файл. 18 травня 2020 року стався масштабний вихід з ладу безлічі серверів Zoom на кілька годин. Як з'ясувало розслідування інциденту по гарячих слідах, зловмисники зареєстрували безліч помилкових адрес, афілійованих з Zoom, і скористалися ними для фішингу, що спричинило масштабний витік особистих даних користувачів системи (зокрема логінів і паролів). Надалі ці дані були використані в безлічі інших атак – зокрема 12 травня було зламано трансляцію церемонії випускників Оклахомського університету. Ще до інциденту було виявлено безліч неприємних подробиць стосовно організації захисту Zoom, точніше того, які ключові ланки в ній відсутні. Зокрема представники Zoom у березні визнали, що система не використовує "end-to-end" шифрування, відповідно, у зловмисників буде доступ до персональних даних користувачів, якщо вони будь-яким чином отримають доступ до серверів компанії.

З'явився новий тип фішингових розсилок, який використовує коронавірусні теми – зокрема маскується під центри контролю захворювань [12], сервіси та додатки, що дають змогу відстежувати епідемічну картину, і навіть пропозиції про спільне виробництво ізоляційних масок [13]. При цьому як «носій» у рамках kill-chain можуть використовуватися як нові, так і «перевірені» представники шкідливого програмного забезпечення. Наприклад, за звітами центру реагування на інциденти інформаційної безпеки (CERT-GIB) [12], більшу частину фішингових листів становлять програми-шпигуни і бекдори – сумарно 96 %, залишок припадає на шифрувальники. Найчастіше використовуються трояни AgentTesla (45 %), Netware (30 %) і LokiBot (8 %).

Навіть якщо взяти тільки програми відеоконференцій, які в інтернет-просторі зарекомендували себе з найкращої сторони: Zoom, Skype, Discord, Google Hangouts, TrueConf, MyOwnConference, Mind, GoToMeeting, VideoMost, Proficonf, то в будь-якому разі, провівши аналіз інформації стосовно реалізації та впливу кіберзагроз на вищезазначені програми телеконференцій, ще до введення в дію карантинно-обмежувальних заходів, пов'язаних з пандемією, ми побачимо реально наявні та дієві кіберзагрози в «мирний» час.

Фактично стрімко зростаюча інформатизація всіх видів діяльності конкурентоспроможних фахівців приводить до необхідності тісної взаємодії, з одного боку, у галузі інформаційних процесів і технологій, з другого боку, реалізації процесів, які мають бути підтримані засобами інформатизації. Саме на це спрямовані дії інтернет-злочинців. Протидія кіберзагрозам під час реалізації відеоконференцій нині є надзвичайно важливою проблемою. Адже під загрозу підпадає не тільки навчальний процес, одержання знань слухачами, але й практично вся господарська діяльність усієї країни.

З позиції моделювання ризиків у нашому випадку реалізується модель «небезпека – ризик», яка базується на концепції ризику як прояву (наслідку) дії небезпек різного походження. В рамках цієї моделі вважається, що результатом реалізації небезпек або породжених ними загроз є сукупність можливих негативних подій, кожна з яких характеризується парою параметрів: ймовірністю реалізації і величиною збитку, який буде отриманий у разі реалізації цієї події. Обов'язковою умовою появи ризику є наявність кількох варіантів можливого розвитку негативних подій (ризик отримання того чи іншого збитку), тобто невизначеність на рівні наслідків реалізації небезпек. Модель добре співвідноситься з механізмом утворення

DOI: 10.24025/2306-4412.3.2020.214774

ризиків для завдань захисту інформації. Відповідно до [14] було введено певну формалізацію об'єктів, безпосередньо пов'язану з існуванням ризиків, і визначено дві категорії об'єктів, з яких перша – об'єкти ризику, а друга – джерела небезпеки, тобто конкретизовано у вигляді загрози в нашому випадку. Всі загрози характеризуються своїми імовірнісними показниками, а при розгляді окремих конкретних ситуацій – відповідними збитками або втратами, гіпотетичними або реальними. Фактично наш випадок підпадає під один із базових принципів безпеки життєдіяльності – аксіоми потенційної небезпеки [14]. Суть цієї аксіоми полягає в тому, що будь-яка діяльність приховує потенційну небезпеку, тому об'єкти, які беруть участь у цій діяльності, – це об'єкти ризику, які за певних умов можуть зазнати витрат або втрат. Введені вище категорії об'єкта ризику і джерела небезпеки дають можливість описати виникнення ризиків як таких, коли у разі існування небезпеки і проявів обумовлених загроз, можливі два сценарії розвитку подій. Відповідно до першого, коли реалізація загрози (загроз) призводить до наслідків катастрофічного характеру, функціонування об'єкта ризику фактично припиняється. За другим сценарієм у результаті реалізації загроз відбувається погіршення умов функціонування об'єкта ризику. Однак в обох випадках кінцевою і принципово істотною ланкою в ряду негативних змін, викликаних впливом існуючої небезпеки, будуть втрати (витрати), яких зазнав об'єкт ризику через погіршення якості свого функціонування. За умови точного визначення властивостей небезпек (їх детермінування) існує принципова можливість обчислення фактичних характеристик вектора стану параметрів X (стан об'єкта ризику), розрахунку складових вектора Y, що являє собою цільовий комплексний показник якості об'єкта та відповідного значення скалярного показника функціонала якості (F). Якщо відхилення значень двох останніх показників від їх номінальних значень досить істотні, вживаються певні заходи щодо нейтралізації або зменшення рівня небезпек. Для цього визначаються ступінь і характер впливу кожної з небезпек на якість функціонування об'єкта ризику і згідно з результатами аналізу моделі реалізуються необхідні коригувальні дії, виконання яких нормалізує умови функціонування цього об'єкта. Тобто для цієї ситуації, коли відома вся інформація про характер небезпек, їх зв'язок зі станом об'єкта ризику і якістю його функціонування, притаманні цілком свідомі й однозначно детерміновані рішення щодо усунення небезпек або зменшення їх рівня, які гарантовано забезпечують необхідну якість функціонування об'єкта. Зауважимо, що для отримання цього кінцевого результату попередньо треба вирішити ряд завдань:

1) отримати вихідну інформацію про характер і рівень наявних небезпек;

2) визначити параметри стану об'єкта ризику (вектор X);

3) розрахувати значення комплексного цільового показника Y (або скалярного показника (F) якості роботи об'єкта ризику;

4) прийняти рішення про доцільність і, якщо це виявилося необхідним, визначити спосіб нейтралізації небезпек для нормалізації умов функціонування об'єкта ризику.

Випадок, для якого в повному обсязі досягається вирішення всіх перелічених вище завдань, насправді є ідеалізованою ситуацією, яка на практиці фактично не трапляється.

Характерною особливістю реального функціонування об'єкта ризику є наявність невизначеності при вирішенні будь-якого з перелічених вище завдань. Джерела цієї невизначеності різні. Виходячи з цього, при аналізі і вирішенні практичних завдань рівень невизначеності варіюється в досить широких межах і, як це вже було відзначено нами раніше, існують різні джерела подібної невизначеності. Зокрема, один із них – недостатня інформація про сам об'єкт ризику, його структуру, закономірності функціонування, характеристики і параметри. Тому не можна однозначно пов'язати сукупність значень складових вектора X зі значеннями елементів вектора Y, тобто відсутні точні відомості про те, як впливає стан об'єкта ризику на ефективність його роботи (на якість продукції або послуг на виході об'єкта ризику). Ця невизначеність, в першу чергу, ускладнює ефективність процедури нормалізації стану об'єкта ризику за допомогою нейтралізації небезпек, в умовах яких він функціонує.

Отже, слід підкреслити, що принциповим при аналізі та інтерпретації цієї концептуальної моделі ризиків є можливість виявлення невизначеності, породженої існуванням небезпек, яка якраз і створює ситуацію

DOI: 10.24025/2306-4412.3.2020.214774

ризиків, обумовлюючи назву моделі: «небезпека – ризик», що і проявляється в нашому випадку.

Наостанок доречно нагадати основні заходи безпеки, потрібні для захисту інформаційно-комунікативної інфраструктури в умовах дії пандемії по COVID-19 (коронавірусу):

- не клікати на лінки та не завантажувати програми, в яких ви не впевнені, щоб уникнути ризику зараження свого ПК або гаджету;

- ігнорувати онлайн-акції по вакцинації від коронавірусу і будь-яких інших, пов'язаних з вірусом пропозицій, зі значним дисконтом;

- не реагувати на листи від незнайомих адресатів з пропозицією допомогти в лікуванні вірусу і в цілому не реагувати на пропозиції, які не піддаються здоровій логіці;

- не відповідати на незнайомі номери телефону чи критично ставитися до отриманої інформації, особливо щодо вас чи ваших родичів;

- не відправляти гроші наперед при купівлі товарів в Інтернеті;

- не відчиняти двері незнайомим особам, навіть якщо вони одягнуті у спецодяг;

- перевіряти отриману інформацію в офіційних, державних і правоохоронних органах;

- проводити ретельні перевірки та background-checks по потенційних компаніях-контрагентах, постачальниках та кандидатах, у тому числі ретельно вивчаючи ціни та умови співпраці;

- в обов'язковому порядку проводити наступний (систематичний) моніторинг діючих контрагентів і постачальників з метою оперативного реагування на будь-які зміни;

- вивчати інформаційне поле навколо бізнесу, в регіонах його ведення та ситуацію в державі загалом;

- посилити фізичний і технічний захист об'єктів компанії, ключових співробітників, власників бізнесу та членів їх сімей;

- проводити періодичну перевірку ключових приміщень на технічні засоби прихованого зняття інформації;

- організувати безпечні умови праці для співробітників, клієнтів та відвідувачів під час пандемії COVID-19 (транспортування на роботу та додому, встановлення плакатів, які заохочують гігієну рук, дезінфікуючі засоби для рук, маски, рукавички, серветки, технічні засоби виявлення ознак захворювання, систематичне прибирання та провітрювання приміщень тощо);

- організувати проведення аудиту безпеки бізнесу у зв'язку зі зміною бізнес-моделі ведення фінансово-господарської діяльності, з метою оцінювання ризиків;

- розробити плани екстрених дій у випадках: масових заворушень; рейдерської атаки; нападу на об'єкти, транспорт і співробітників компанії; інформаційної атаки; неправомірних дій контролюючих та правоохоронних органів; кібератак та ін.;

- проводити періодичні онлайн-семінари зі співробітниками з питань безпеки;

- створити «Кризову групу» з метою оперативного реагування на інциденти, в яку залучити експертів з корпоративної безпеки.

Висновки. В умовах різкого розширення спектра загроз у період дії COVID-19 з'явилися нові вразливості й виникла нагальна необхідність в активізації інтересу кібергромадськості до нової проблеми, через масовий перехід населення на роботу в мережах і, отже, збільшений внаслідок цього прояв кількості та якості кібератак, а отже і збільшення кількості кіберризиків.

Аналіз літератури і джерел дослідження свідчить про недостатню увагу вчених до практичних наслідків пандемії на стан кібербезпеки і кіберризиків, які є послідовними взаємопов'язаними процедурами в процесі управління при прийнятті рішень. Генеза кіберризиків під час пандемії пов'язана з низкою технічних, психологічних, соціальних, політичних чинників, серед яких, насамперед, відзначаємо технічне навантаження на мережу та створення сприятливих умов для кіберзлочинів; збільшення використання кіберпростору пересічними користувачами, які не мають кібербезпекових навиків, психологічні аспекти пандемії сприяють неадекватному прийняттю рішень в кризовому режимі на політичному, побутовому рівнях внаслідок низького/високого рівня довіри до учасників мережі.

Оцінювання ризику передбачає дослідження стану, ситуації (сценаріїв) з наявними ознаками небезпеки, невизначеності та/або випадковості.

Найефективнішим методом уникнення цього є забезпечення юридичного підґрунтя

DOI: 10.24025/2306-4412.3.2020.214774

протидії ризикам і багатофакторне проектування або прогнозування.

На етапі оцінювання ризиків формується стратегія управління ризиками, а оскільки повністю уникнути ризиків у більшості випадків неможливо, то вагоме значення має вирішення питання допустимості (прийнятності, виправданості) ризику, яке потребує подальшого дослідження та обґрунтування.

Оцінювання ризику, що використовують у технічних системах, розглядається як процес ідентифікації інформаційних ресурсів системи та загроз цим ресурсам, а також можливих втрат, що ґрунтується на оцінюванні частоти виникнення подій і розміру збитку. Аналіз ризику розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що потребують захисту.

Перспективи подальших досліджень. Зазначені вище ризики мають принципову робочу «онлайн» складову, що дає можливість віднести їх до ризиків з великим людським фактором ризику, внаслідок якого в умовах коронавірусу користувачами робляться «вирішальні» помилки, породжені страхом і невпевненістю через багаточасове онлайн-спілкування. Саме воно, на нашу думку, сприяє появі втоми у людей і формує «швидкісні помилки» через обмеження у часі. При цьому активізується і проблема захисту персональних даних та стрімке збільшення їх крадіжок. Отже, необхідно на майбутнє проводити подальше удосконалення кібербезпеки в проявах відповідних екстремальних ризиків із урахуванням таких феноменів, як поточний стан і «конкретна» ґенеза ризику.

Список використаних джерел

[1] 2019 Internet Crime Report. FBI’s Internet Crime Complaint Center, 2020. [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf. Accessed on: Oct. 18, 2020.

[2] М. Д. Василенко, О. Б. Козін, М. О. Козіна, та В. О. Рачук, "Кіберризики в муніципальному господарстві в період пандемії: збитки та боротьба за кібербезпеку", *Комунальне господарство міст. Серія: технічні науки та архітектура*: наук.-техн. зб., вип. 3 (156), с. 80-87, Харків, 2020.

[3] В. В. Индеева, "К вопросу об определении понятия "риск". *Сборник заочных электронных конференций.* Москва: Рос. акад. естествознания, 2009. [Электронный ресурс]. Режим доступа: http:www.rae.ru/arj/ 2007/02/Indeeva.pdf

[4] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic", *Journal of Medical Internet Research*, vol. 22, no. 9, 2020. [Online]. Available: https://www.jmir.org/2020/9/e23692/pdf

[5] T. Weil, and S. Murugesan, "IT risk and resilience – cybersecurity response to COVID-19," in *IT Professional*, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330.

[6] R. O. Andrade, I. Ortiz-Garcés, and M. Cazares, "Cybersecurity attacks on Smart Home during Covid-19 pandemic," in *2020 Fourth World Conf. on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, United Kingdom, 2020, pp. 398-404, doi: 10.1109/WorldS450073.2020.9210363.

[7] Tabrez Ahmad, Corona Virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity, April 5, 2020. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3568830

[8] М. Д Василенко, "Право в теорії ризиків: ґенеза ризиків від правової до інформаційної складових (інституційний підхід)", *Юридичний вісник*, № 4, с. 43-51. Одеса: ВД «Гельветика», 2019.

[9] Б. Н. Малиновский, *Академик Виктор Глушков. Золотые вехи истории и техники Украины*. Киев, Украина: ВМУРоЛ, 2003.

[10] Международный стандарт ИСО 31000. Менеджмент риска: руководство. 2-е изд. Пер. АНО ДПО "ИСАР", 2018.

[11] P. Wagenseil, "Zoom security issues: Here's everything that's gone wrong (so far) ", *Toms Guide*, 1-3. [Online]. Available: https://www.tomsguide.com/news/zoom-security-privacy-woes. Accessed on: May 19, 2014.

[12] K. Okereafor, and O. Adebola, "Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety",

DOI: 10.24025/2306-4412.3.2020.214774

Journal Homepage, vol. 8, no. 2, 2020. [Online]. Available: http://ijmr. net. in

[13] Group-IB: шпионские программы лидируют в почтовых рассылках, паразитирующих на теме коронавируса – Group-IB Медиа-центр. [Электронный ресурс]. Режим доступа: https://www.group-ib.ru/media/covid-phishing-campaings/. Дата обращения: Окт. 18, 2020.

[14] Я. Д. Вишняков, и Н. Н. Радаев, *Общая теория рисков*: учеб. пособие. Москва, Россия: Академия, 2008.

References

[1] 2019 Internet Crime Report. FBI's Internet Crime Complaint Center, 2020. [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf. Accessed on: Oct. 18, 2020.

[2] M. D. Vasilenko, O. B. Kozin, M. A. Kozina, and V. A. Rachuk, "Cyber-risks in the municipal economy during the pandemic: losses and the fight for cybersecurity", *Komunalne hospodarstvo mist. Seriia: tekhnichni nauky ta arkhitektura*: sci.-tech. coll., iss. 3 (156), pp. 80-87, Kharkiv, 2020. [in Ukrainian].

[3] V. V. Indeeva, "To the question of the definition of the "risk" notion". *Sbornik zaochnykh elektronnykh konferentsiy*. Moscow: Ros. akad. estestvoznaniya, 2009. [Online]. Available: http:www.rae.ru/arj/2007/02/Indeeva.pdf

[4] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic", *Journal of Medical Internet Research*, vol. 22, no. 9, 2020. [Online]. Available: https://www.jmir.org/2020/9/e23692/pdf

[5] T. Weil, and S. Murugesan, "IT risk and resilience – cybersecurity response to COVID-19," in *IT Professional*, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330.

[6] R. O. Andrade, I. Ortiz-Garcés, and M. Cazares, "Cybersecurity attacks on Smart Home during Covid-19 pandemic," in *2020 Fourth World Conf. on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, United Kingdom, 2020, pp. 398-404, doi: 10.1109/WorldS450073.2020.9210363.

[7] Tabrez Ahmad, Corona Virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity, April 5, 2020. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3568830

[8] M. D. Vasilenko, "Law in the theory of risks: the genesis of risks from legal to informational components (institutional approach)", *Yurydychnyi visnyk*, no. 4, pp. 43-51. Odessa: VD "Helvetika", 2019. [in Ukrainian].

[9] B. N. Malinovsky, *Academician Viktor Glushkov. Golden milestones of history and technology of Ukraine.* Kyiv, Ukraine: VMURoL, 2003. [in Russian].

[10] International standard ISO 31000. Risk management: manual. 2nd ed. Transl. ANO DPO "ISAR", 2018. [in Russian].

[11] P. Wagenseil, "Zoom security issues: Here's everything that's gone wrong (so far)", *Toms Guide*, 1-3. [Online]. Available: https://www.tomsguide.com/news/zoom-security-privacy-woes. Accessed on: May 19, 2014.

[12] K. Okereafor, and O. Adebola, "Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety", *Journal Homepage*, vol. 8, no. 2, 2020. [Online]. Available: http://ijmr. net. in

[13] Group-IB: spyware prigrams lead the way in mailings that parasitize on the topic of coronavirus – Group-IB Media center. [Online] Available: https://www.group-ib.ru/media/covid-phishing-campaings/. Accessed on: Oct. 18, 2020.

[14] Ya. D. Vishnyakov, and N. N. Radaev, *General theory of risks*: textbook. Moscow, Russia: Academy, 2008. [in Russian].

DOI: 10.24025/2306-4412.3.2020.214774

M. D. Vasilenko, *Dr.Phys.-Math.Sc., Doctor of Law, professor,*
acting head of the Department of cybersecurity,
e-mail: nvas08@ukr.net
V. P. Novikov, *Ph.D., associate professor,*
associate professor of the Department of cybersecurity,
e-mail: novikovodessa0@gmail.com
V. O. Rachuk, *assistant of the Department of cybersecurity,*
e-mail: rachuk960@gmail.com
V. M. Slatvinska, *postgraduate student of the Department of economic law and process,*
e-mail: slatvinskaya_valeriya@ukr.net
National university «Odessa Law Academy»
Fontanskaya doroga, 23, Odessa, 65009, Ukraine

CYBERSECURITY IN THE MANIFESTATIONS OF RISKS DURING THE PANDEMIC PERIOD: CONDITION AND GENESIS

The coronavirus pandemic has created an unprecedented global emergency related to risks, including cyber-risks, which threaten cybersecurity at both local and global levels. An analysis of the information carried out by the US and EU special institutions confirms that with the appearance of COVID-19 (coronavirus) as a result of a pandemic serious risky economic and political problems are expected with a high percentage of probability. Additional problems are created by the unprecedented transition to online work, when continuous activity during a pandemic occurs mainly using remote operations.

Definitions of specific risks are contained in many standards of various sectors of the economy and equipment. However, there is an international standard ISO 31000, which is used for general risk assessment. To implement the risk management process in the current conditions in cybersecurity, it must be integrated with the components of risk management in particular and in general, including the exchange of information and consulting; establishing the context (environment); general risk assessment (its identification, analysis and evaluation); processing and summarizing the results of the selected type of risk; monitoring and critical analysis, as well as dealing with unforeseen threats.

It is shown that in the context of a fundamental increase in teleconferences (during the pandemic), the number of cyber risks significantly increases. It is noted that risks are consistent interrelated procedures that are included in the management process and require a more planned systematic approach, given that risk assessment involves studying the state, situation (scenarios) with existing signs of danger, uncertainty and/or randomness. An effective method of its implementation is to provide a legal basis and multi-factor design or forecasting. However, in the first part, the legislative decision almost always comes late. Previously, at the stage of technical risk assessment, a risk management strategy is formed, and since it is impossible to completely avoid risks in most cases, it is important to solve the issue of admissibility (acceptability, justification) of risk, which requires further research and justification. Risk assessment used in technical systems is considered as a process of identifying information resources of the system and threats to these resources, as well as possible losses, based on an assessment of the frequency of events and the amount of damage. Risk analysis is revealed as the process of identifying risks, determining their magnitude, and identifying areas that require protection.

Consequently, the COVID-19 pandemic has created and continues to create social and technical problems that are expressed in the emergence of new risks, new cyber risks. Risks become even more consistent and interconnected processes, inherently entering the management system. In this case it becomes more appropriate to make periodical checks of key premises to identify the use of technical means of hidden information retrieval and periodically conduct online seminars with security officers.

Keywords: *cybersecurity, risk, risk assessment, uncertainty, pandemic, COVID-19.*

DOI: 10.24025/2306-4412.3.2020.214774

ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

УДК 004.052.2

[0000-0002-2046-481X] **Е. В. Фауре,** *д.т.н., професор*,
e-mail: e.faure@chdtu.edu.ua
[0000-0003-1791-6755] **О. О. Харін,**
[0000-0002-1596-4123] **А. О. Лавданський,** *к.т.н.*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ОЦІНКА ВЛАСТИВОСТЕЙ СИНТЕЗОВАНИХ НА ОСНОВІ ТЕОРІЇ РЕШІТОК СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ ДЛЯ НЕРОЗДІЛЬНИХ ФАКТОРІАЛЬНИХ КОДІВ

У роботі досліджено основні параметри систем передавання даних з нероздільним факторіальним кодуванням, що використовують сигнально-кодові конструкції, синтезовані на основі теорії решіток. Цей метод формування сигнально-кодових конструкцій дає можливість максимізувати швидкість коду для заданого рівня достовірності, що визначається мінімальною відстанню Хеммінга між перестановками. Виконано оцінювання таких параметрів, як відносна швидкість передавання і ймовірність невиявленої помилки. Побудовано експериментально-розрахункову модель, що дало змогу визначити, яким чином змінюються ймовірнісні характеристики коду залежно від імовірності бітової помилки в каналах зв'язку з незалежними бітовими помилками. На основі отриманих експериментальних даних виконано аналіз здатності досліджуваних сигнально-кодових конструкцій до виправлення помилок. Визначено переваги та недоліки методу формування сигнально-кодових конструкцій на основі теорії решіток.

Ключові слова: *факторіальний код, відносна швидкість передавання, ймовірність бітової помилки, завадостійке кодування, криптографічний захист.*

Вступ. Однією з головних функцій комп'ютерних систем і мереж є забезпечення безпеки інформації, що в них циркулює. Водночас не менш важливою функцією є захист інформації від впливу завад, що виникають у каналі зв'язку.

Використання факторіальних кодів є одним із підходів до поєднання завадостійкого кодування та криптографічного захисту, ефективність якого підтверджується результатами, отриманими в роботах [1]–[7]. Разом з тим, факторіальні коди з відновленням даних за перестановкою (ФКВД) [1], [3], [4] вразливі до помилок парної кратності, таких, що призводять до трансформації однієї перестановки з дозволеної множини в іншу перестановку, що належить цій же множині. Описаний у [8] метод дає змогу підвищити стійкість факторіального коду до таких помилок, виявляючи всі двократні помилки, але має низьку швидкість.

Мета дослідження полягає в оцінюванні основних характеристик методу формування сигнально-кодової конструкції (СКК) [9], [10] для ФКВД, що забезпечує досягнення необхідного значення достовірності передавання і дає можливість максимізувати швидкість коду за рахунок формування підмножини перестановок на основі теорії решіток. Оцінюванню підлягають відносна швидкість передавання та ймовірність невиявленої помилки в результаті застосування синтезованих СКК у системах з нероздільним факторіальним кодуванням.

Виклад основного матеріалу. Для оцінювання сутності методу формування СКК на основі теорії решіток спочатку визначимо деякі поняття та терміни.

Визначення 1. Питомою помилкою $f_{per}(t)$ називається математичне сподівання кількості невиявлених помилок кратності t для кожного з вузлів решітки.

Визначення 2. Сигнальним вектором називається перестановка π з дозволеної множини перестановок, представлена в двійковому вигляді.

Визначення 3. Сигнально-кодовою конструкцією називається множина сигнальних векторів, що використовується для кодування інформації.

Визначення 4. Решіткою називається СКК, в якій відстань Хеммінга $d_{i,j}$ між будь-якими двома сигнальними векторами (π_i, π_j) не менша деякого, наперед заданого значення $d_{\min}$. Водночас така СКК повинна бути не-

DOI: 10.24025/2306-4412.3.2020.214937

критичною (інваріантною) до розміщення вузлів усередині решітки.

Основними параметрами решітки є:

– мінімальна відстань $d_{\min}$;

– кількість вузлів решітки N_{sv}, відстань між якими не менша за $d_{\min}$;

– потужність множини символів перестановки (довжина перестановки) M.

Зазначимо, що збільшення мінімальної відстані $d_{\min}$ дає можливість підвищити достовірність передавання даних, але призводить до зменшення кількості вузлів решітки N_{sv} і, як наслідок, до зменшення швидкості коду. Відповідно до [10] метод формування СКК на основі теорії решіток передбачає наступні дії:

– обирається деяке початкове значення M, для якого будується підмножина не менше ніж з двох перестановок з попарними відстанями Хеммінга $d_{i,j} \geq 2t+1$. У результаті (після $M! \cdot M!$ перевірок) отримаємо не менше двох перестановок (π_i, π_j), де i і j – номери цих перестановок в упорядкованій множині всіх $M!$ перестановок з попарними відстанями $d_{i,j} \geq 2t+1$;

– потужність множини символів (довжина перестановки) M збільшується на одну одиницю, до значення $M+1$. Для цього по черзі над усіма вузлами сформованої решітки, що містять M символів, одночасно виконують одну з можливих підстановок і вставляють $(M+1)$-й символ між символами перестановки, після чого відбирають тільки такі перестановки, в яких між будь-якою парою перестановок (π_i, π_j) мінімальна відстань задовольняє умові $d_{i,j} \geq 2t+1$. За такої процедури потужність сформованої СКК збільшується в $(M+1)$ разів. Цю операцію повторюють доти, поки кількість перестановок у підмножині перестановок не досягне або не перевищить наперед заданого значення, що забезпечує необхідну швидкість коду. На цьому процедура формування підмножини перестановок, інваріантних до обертання осей СКК, завершена;

– після завершення процедури формування інваріантних перестановок (інваріантної підмножини перестановок) уточняється кількість біт k, що переносяться кожною перестановкою цієї підмножини;

– уточнивши склад інваріантної підмножини, формується СКК у вигляді таблиці відображення $\{A(x)\} \to \{\pi\}$ множини слів джерела $A(x)$ у множину перестановок π для кодера і таблиці відображення $\{\pi\} \to \{A(x)\}$ для декодера.

Для оцінювання ефективності запропонованого методу формування СКК використаємо методи факторіального кодування з відновленням даних за перестановкою (ФКВД) [1] та факторіального кодування з відновленням даних за перестановкою з виправленням помилок (ФКВДвп) для СКК в метриці Хеммінга (ФКВДвп-2) [11]–[14], де також представлено теоретичну оцінку ймовірності невиявленої помилки.

З метою визначення ймовірності невиявленої помилки розроблено експериментально-розрахункову модель, що імітує середовище передавання даних з незалежними бітовими помилками. Модель дає змогу для заданої якості каналу (ймовірності бітової помилки) оцінити наступні ймовірнісні характеристики:

– ймовірність виявлення помилки P_{det};

– ймовірність невиявлення помилки P_{ud};

– ймовірність прийому кодового слова без помилок Q.

Водночас сума всіх ймовірностей дорівнює одиниці: $P_{det} + P_{ud} + Q = 1$.

Відносна швидкість передавання визначається відповідно до формули

$$v_0 = v_1 v_2,$$

де $v_1 = k / n$ – швидкість коду;

v_2 – динамічна складова втрати швидкості внаслідок повторних запитів [15].

Для систем з ФКВД з виявленням помилок і їх виправленням шляхом перезапиту

$$v_2 = Q + P_{ud}.$$

Відзначимо, що для систем з ФКВДвп-2, де передбачено виправлення помилок, динамічна складова v_2 відсутня, тому відносна швидкість передавання в таких системах фактично дорівнює швидкості коду.

Результати досліджень. Першим етапом роботи розробленої експериментально-розрахункової моделі є формування СКК для заданої потужності множини символів перестановки M та мінімальної відстані між вузлами решітки $d_{\min}$. Після цього для отриманої множини перестановок визначається зна-

DOI: 10.24025/2306-4412.3.2020.214937

чення питомої помилки $f_{per}(t)$ для подальшого застосування в обчисленні ймовірнісних характеристик.

Наступним етапом роботи моделі є використання синтезованих решіток як таблиць замін у програмних моделях для систем з ФКВД та ФКВДвп-2 за різних значень імовірності бітової помилки p_0. Отримані на цьому етапі роботи моделі ймовірнісні характеристики дали змогу виконати оцінювання основних параметрів синтезованих решіток у системах з вирішальним зворотним зв'язком та з детермінованим виправленням помилок.

У таблицях 1 і 2 наведено значення питомої помилки на вузол решітки $f_{per}(t)$ для решіток на 10 та 60 вузлів. Зазначимо, що для сформованих за допомогою запропонованого методу СКК значення $f_{per}(t)$ не залежать від того, які саме перестановки входять в решітку, тобто вони інваріантні відносно складу сигнальних векторів СКК і залежать тільки від кількості вузлів у ній.

На рисунку 1 зображено графіки залежності ймовірностей невиявленої помилки ФКВД від імовірності бітової помилки p_0 за незалежних бітових помилок для $k=3$, $M=5$ та $k=5$, $M=6$ при $d_{\min}=5$.

На рисунку 2 зображено графік залежності ймовірності невиявленої помилки ФКВДвп-2 від ймовірності бітової помилки p_0 для розміру інформаційної частини $k=5$, $M=6$, $N_{sv}=60$, $d_{\min}=5$.

Таблиця 1 – **Значення $f_{per}(t)$ для решітки** $k=3$, $M=5$, $N_{sv}=10$, $d_{\min}=5$

Кратність помилки t	$f_{per}(t)$
1-5	0
6	4,5
7	0
8	1
9	0
10	1,5
11-15	0

Таблиця 2 – **Значення $f_{per}(t)$ для решітки** $k=5$, $M=6$, $N_{sv}=60$, $d_{\min}=5$

Кратність помилки t	$f_{per}(t)$
1-5	0
6	9,375
7	0
8	12,063
9	0
10	6,063
11	0
12	2,875
13	0
14	0,625
15-18	0

На рисунку 3 представлено результати порівняння ймовірностей невиявленої помилки ФКВД та ФКВДвп-2 для $k=5$, $M=6$, $N_{sv}=60$, $d_{\min}=5$.

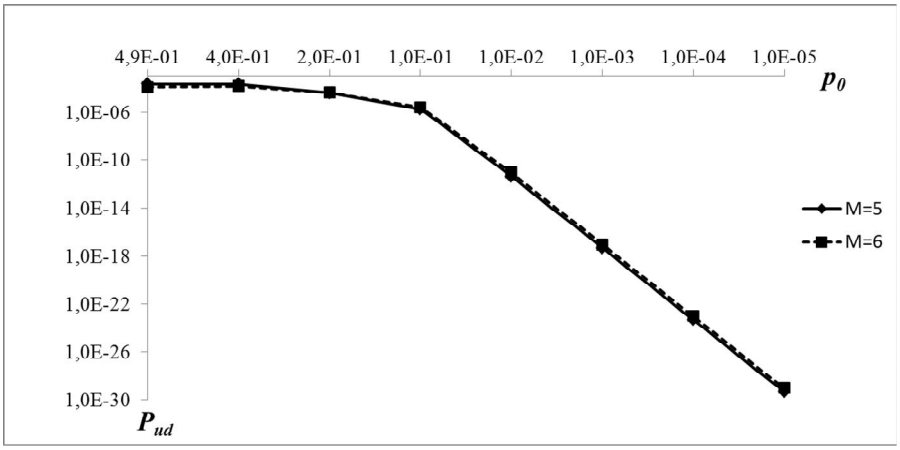


Рисунок 1 – Графіки залежностей імовірностей невиявленої помилки ФКВД від ймовірності бітової помилки для $k=3$, $M=5$, $N_{sv}=10$ та $k=5$, $M=6$, $N_{sv}=60$ та $d_{\min}=5$

DOI: 10.24025/2306-4412.3.2020.214937

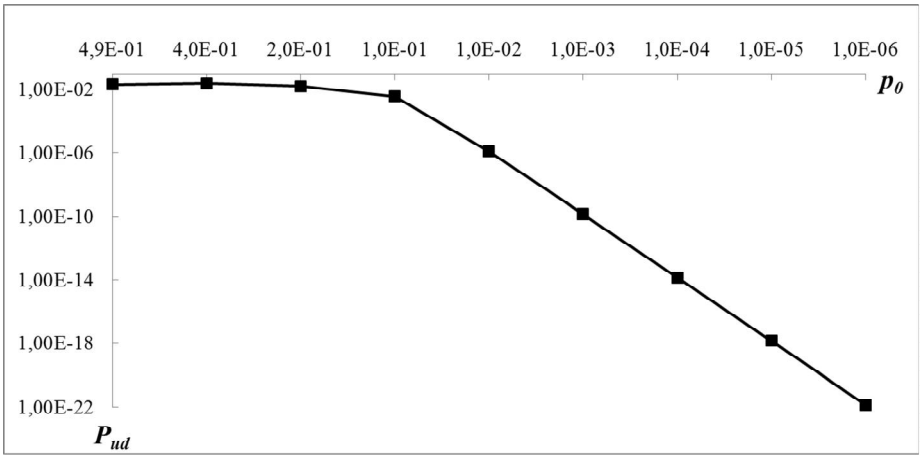


Рисунок 2 – Графік залежності ймовірностей невиявленої помилки ФКВДвп-2 від ймовірності бітової помилки p_0 для $k = 5$, $M = 6$, $N_{sv} = 60$, $d_{\min} = 5$

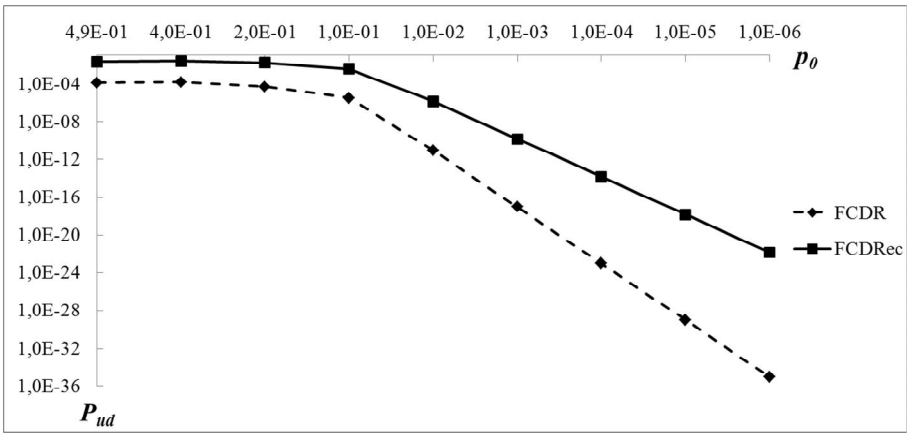


Рисунок 3 – Графіки залежностей імовірностей невиявленої помилки ФКВД та ФКВДвп-2 для $k = 5$, $M = 6$, $N_{sv} = 60$, $d_{\min} = 5$

На рисунку 4 зображено залежність швидкості коду ФКВДвп-2, СКК якого сформовано за допомогою запропонованого методу для різних довжин інформаційного вектора k.

Характер зображеної залежності подібний до характеру залежності швидкості ФКВД, зображеної на рисунку 1 в [1]. Такий вигляд обумовлений тим, що зі збільшенням довжини інформаційного вектора k виникає необхідність збільшення потужності множини символів перестановки M, щоб виконувалась умова $M! \geq 2^k$. У випадках, коли для деякого k справедливо $2^k \leq M! < 2^{k+1}$, збільшення значення M на одиницю призводить до різкого падіння швидкості коду внаслідок збільшення надлишковості через неоптимальну довжину інформаційного вектора.

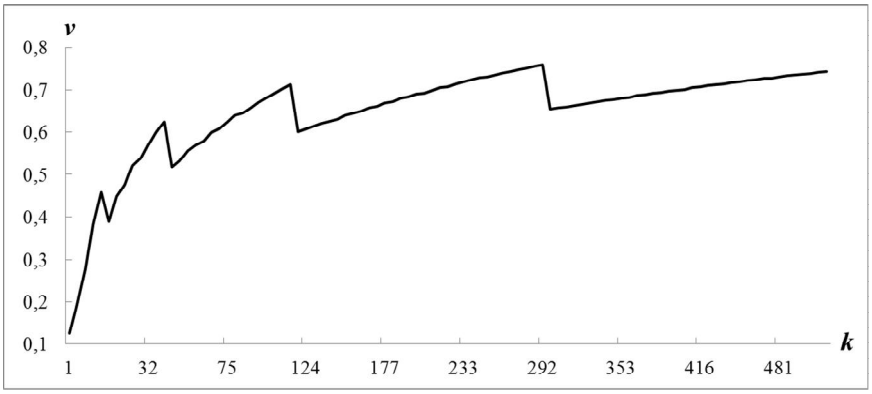


Рисунок 4 – Графік залежності швидкості коду ФКВДвп-2 від довжини блока даних на вході кодера для $d_{\min} = 5$

DOI: 10.24025/2306-4412.3.2020.214937

На рисунку 5 зображено залежність відносної швидкості передавання ФКВД і ФКВДвп-2 від імовірності бітової помилки p_0 для $k = 5$, $M = 6$.

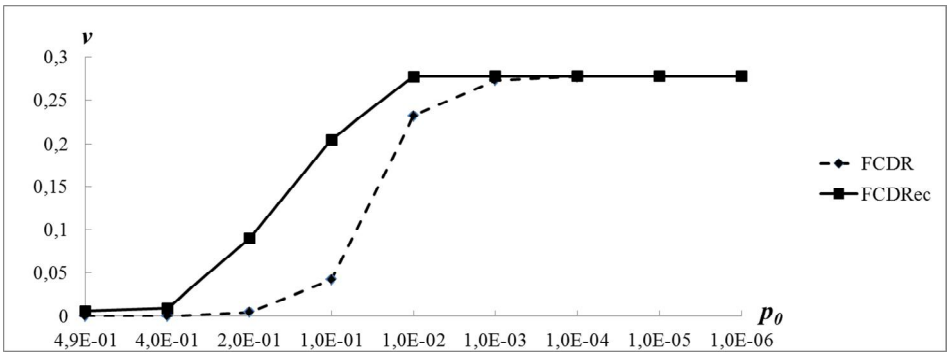


Рисунок 5 – Графіки залежностей відносної швидкості передавання ФКВД та ФКВДвп-2 для $k = 5$, $M = 6$

Обговорення результатів. Дані, наведені в таблицях 1 і 2, показують, що сформовані решітки забезпечують виявлення всіх помилок непарної кратності, а також усіх помилок з кратністю $t \le 5$.

Рисунок 1 показує, що сформована СКК забезпечує ймовірність невиявленої помилки, що не перевищує значення 10^{-4} для $p_0 = 0,49$, тобто в умовах, близьких до стану обриву каналу зв'язку, за якого на вхід приймача надходить лише шум. За такої ймовірності бітової помилки загальновідомі системи передавання даних не зможуть працювати через втрату циклової синхронізації, в той час, коли ФКВД має властивість до самосинхронізації. Це дає можливість використовувати цей метод формування СКК для кодування даних в умовах активної радіоелектронної боротьби або в умовах, коли достовірність передавання даних важливіша швидкості коду. Також з графіка видно, що синтезовані СКК забезпечують майже однакові значення ймовірності невиявленої помилки. Це обумовлено тим, що рівень достовірності визначається мінімальною відстанню між вузлами решітки $d_{\min}$ і майже не змінюється при зміні потужності множини символів M.

З рисунків 2 і 3 випливає, що ФКВДвп-2 має більшу ймовірність невиявленої помилки порівняно з ФКВД для заданої СКК, оскільки мінімальна відстань між вузлами решітки $d_{\min} = 5$, що забезпечує виправлення помилок кратності $t \le 2$. Усі помилки, кратність яких $t > 2$, призводять до помилки декодування, в той час, коли ФКВД виправляє такі помилки шляхом повторного запиту блока.

З рисунка 4 випливає, що запропонований метод формування СКК забезпечує відносно малу швидкість коду, яка зростає зі збільшенням кількості вузлів у решітці.

У свою чергу, рисунок 5 свідчить про те, що ФКВДвп-2 має значно вищу відносну швидкість передавання для каналів низької якості $(0,1 \le p_0 \le 0,49)$, але водночас забезпечує нижчу достовірність передавання даних через велику кількість помилок кратності $t > 2$, що призводять до помилкового декодування.

Разом з тим, зі зменшенням імовірності бітової помилки відносна швидкість передавання для обох методів вирівнюється внаслідок зменшення кількості помилок і, як результат, зменшення втрат часу на повторні запити спотворених блоків у системах з ФКВД.

Висновки. Виконаний у роботі аналіз методу формування СКК на основі теорії решіток для систем з нероздільним факторіальним кодуванням дав змогу визначити наступні параметри:

- питому помилку $f_{per}(t)$;
- імовірність невиявленої помилки P_{ud};
- відносну швидкість передавання v_0.

DOI: 10.24025/2306-4412.3.2020.214937

Показано, що метод формування СКК на основі теорії решіток дає змогу підвищити достовірність передавання даних за рахунок використання для перенесення інформації лише тих перестановок, що знаходяться на відстані Хеммінга, не меншій за $d_{\min}$, яке визначається на етапі проектування системи. Чим більше значення $d_{\min}$, тим вища достовірність передавання даних і тим менша швидкість коду, оскільки зменшується кількість перестановок-носіїв інформації.

Виконане порівняння зазначених характеристик для систем з ФКВД та ФКВДвп-2 показало, що ФКВДвп-2 має більшу відносну швидкість передавання в каналах низької якості, але водночас забезпечує гіршу достовірність передавання порівняно з ФКВД в результаті помилкового виправлення помилок.

Недоліком методу формування СКК є те, що він вимагає значних обчислювальних ресурсів для побудови решіток зі збільшенням потужності множини символів перестановки M. Крім того, зазначимо, що ФКВДвп передбачає детермінований процес виправлення помилок, що призводить до помилкового виправлення і, як наслідок, не виявленої кодом помилки у випадках, коли кратність помилки перевищує задане значення t.

Список використаних джерел

[1] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету*, № 2, с. 33-39, 2016.

[2] Е. В. Фауре, та О. О. Харін, "Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних", на *Всеукр. наук.-практ. конф. Актуальні задачі та досягнення у галузі кібербезпеки*: тези доп., Кропивницький, 2016, с. 178-179.

[3] Е. В. Фауре, О. О. Харін, В. В. Швидкий, та А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", *Укр. пат. 117004*, Черв. 12, 2017.

[4] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с восстановлением данных", *Вісник Черкаського державного технологічного університету*, № 4, с. 57-61, 2016.

[5] О. О. Харін, "Порівняльна оцінка факторіальних кодів", *Вісник Черкаського державного технологічного університету*, № 4, с. 88-93, 2017.

[6] Е. В. Фауре, О. О. Харін, В. В. Швидкий, та А. О. Лавданський, "Ефективність виявлення помилок факторіальними кодами", на *V Міжнар. наук.-практ. конф. Інформаційні технології в освіті, науці і техніці (ІТОНТ-2020)*: тези доп. Черкаси: ЧДТУ, 2020, с. 94-95.

[7] О. О. Харін, "Оцінка властивостей каскадного коду, що поєднує факторіальний та рівноважний код", *Вісник Черкаського державного технологічного університету*, № 2, с. 86-90, 2017.

[8] E. V. Faure, A. I. Shcherba, and A. A. Kharin, "Factorial code with a given number of inversions", *Radio Electronics, Computer Science, Control*, vol. 2, pp. 143-153, 2018.

[9] О. О. Харін, та А. І. Щерба, "Спосіб факторіального кодування в метриці Хеммінга", *Укр. пат. 130458*, Груд. 10, 2018.

[10] О. О. Харін, "Формування сигнально-кодової конструкції на основі теорії решіток", на *ІІ Всеукр. наук.-практ. конф. з міжнар. участю. Наука України – погляд молодих вчених крізь призму сучасності:* тези доп., Черкаси: ЧДТУ, 2019, с. 42-44.

[11] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в *Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба*: монографія В. М. Безрука, В. В. Баранника, Харьков, Украина: Лидер, 2017, с. 291-323.

[12] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок", *Радіоелектроніка, інформатика, управління*, № 3, с. 130-138, 2017.

[13] Е. В. Фауре, та О. О. Харін, "Факторіальне кодування з відновленням даних і виправленням помилок", на *Всеукр. наук.-*

DOI: 10.24025/2306-4412.3.2020.214937

практ. Internet-конф. Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: тези доп., Черкаси: ЧДТУ, 2017, с. 74-76.

[14] Е. В. Фауре, О. О. Харін, В. В. Швидкий, та А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", *Укр. пат. 121361*, Груд. 11, 2017.

[15] Л. М. Финк, *Теория передачи дискретных сообщений*. Москва, Россия: Сов. радио, 1970.

References

[1] E. V. Faure, "Factorial coding with data recovery", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 2, pp. 33-39, 2016 [in Russian].

[2] E. V. Faure, and O. O. Kharin, "Investigation of the probability of decoding error when using factorial code with data recovery", in *Proc. All-Ukr. Conf. Current Challenges and Achievements in the Field of Cybersecurity,* Kropyvnytskyi, 2016, pp. 178-179 [in Ukrainian].

[3] E. V. Faure, O. O. Kharin, V. V. Shvydkyi, and A. I. Shcherba, "Method of factorial coding with data recovery", *Ukr. Patent 117004*, June 12, 2017 [in Ukrainian].

[4] E. V. Faure, "A method of increasing the efficiency of factorial coding with data recovery", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 4, pp. 57-61, 2016 [in Ukrainian].

[5] O. O. Kharin, "Comparative evaluation of factorial codes", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 4, pp. 88-93, 2017 [in Ukrainian].

[6] E. V. Faure, O. O. Kharin, V. V. Shvydkyi, and A. O. Lavdanskyi, "Efficiency of error detection by factorial codes", in *Proc. Vth Int. Conf. Information technologies in education, science and technology (ITONT-2020),* Cherkasy, 2020, pp. 94-95 [in Ukrainian].

[7] O. O. Kharin, "Estimation of properties of the cascade code, which combines the factorial and equilibrium codes", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu*, no. 2, pp. 86-90, 2017 [in Ukrainian].

[8] A. A. Kharin, "Factorial code with a given number of inversions", *Radio Electronics, Computer Science, Control*, vol. 2, pp. 143-153, 2018.

[9] O. O. Kharin, and A. I. Shcherba, "The method of factorial coding in the Hamming metric", *Ukr. Patent 130458*, Dec. 10, 2018 [in Ukrainian].

[10] O. O. Kharin, "Formation of signal-code construction based on lattice theory", in *Proc. II Int. Conf. Science of Ukraine – the view of young scientists through the prism of modernity,* Cherkasy, 2019, pp. 42-44 [in Ukrainian].

[11] E. V. Faure, "Factorial coding with error correction. Theoretical substantiation and examples of implementation", in *Science-intensive technologies in infocommunications: information processing, cybersecurity, information warfare*: monograph by V. M. Bezruk, V. V. Barannik. Kharkiv, Ukraine: Lider, 2017, pp. 291-323 [in Russian].

[12] E. V. Faure, "Factorial coding with error correction", *Radio Electronics, Computer Science, Control*, no. 3, pp. 130-138, 2017 [in Russian].

[13] E. V. Faure, and O. O. Kharin, "Factorial coding with data recovery and error correction", in *Proc. All-Ukr. Internet-Conf. Automation and computer-integrated technologies in production and education: state, achievements, development prospects*, Cherkasy, 2017, pp. 74-76 [in Ukrainian].

[14] E. V. Faure, O. O. Kharin, V. V. Shvydkyi, and A. I. Shcherba, "Method of factorial coding with error detection and correction", *Ukr. Patent 121361*, Dec. 11, 2017 [in Ukrainian].

[15] L. M. Fink, *Discrete message transmission theory*. Moscow, Russia: Sov. radio, 1970 [in Russian].

DOI: 10.24025/2306-4412.3.2020.214937

E. V. Faure, *Dr.Sc., professor*,
e-mail: e.faure@chdtu.edu.ua
O. O. Kharin,
A. O. Lavdanskyi, *Ph.D.*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

EVALUATION OF PROPERTIES OF SIGNAL-CODE STRUCTURES SYNTHESIZED ON THE BASIS OF LATTICE THEORY FOR INSEPARABLE FACTORIAL CODES

One of the main functions of computer systems and networks is to ensure the security of information circulating in the system. At the same time, an equally important function is to protect information from the effects of interference in the communication channel.

The use of factorial codes is one approach to combining noise-tolerant encryption and cryptographic protection. But these codes are vulnerable to even errors, which lead to the transformation of one permutation from the allowed set to another permutation belonging to the same set. Therefore, the issue of improving the reliability of data transmission in systems with factorial coding is relevant.

The purpose of the study is to evaluate the method of forming a signal-code structure, which ensures the achievement of the required value of transmission reliability and allows to maximize the code speed by forming a subset of permutations based on lattice theory. The relative transmission rate and the probability of undetected error as a result of the use of synthesized signal-code constructs in systems with integral factorial coding are subject to evaluation.

To evaluate the efficiency of the synthesized signal-code constructions, the methods of factorial coding with data recovery by permutation and factorial coding with data recovery by permutation with error correction have been used. In order to determine the probability of undetected error, a software model has been developed that simulates a data transmission environment with independent bit errors.

The results of the software model have made it possible to establish the dependence of the probability of undetected error in systems with integral factorial coding on the probability of bit error in channels with independent bit errors. A comparative analysis of the relative transmission rate and the probability of undetected error in systems with factorial coding with data recovery by permutation and factorial coding with data recovery by permutation with error correction is also performed.

The results obtained in this paper have made it possible to determine the main advantages and disadvantages of the method of forming signal-code structures based on the lattice theory, as well as to determine the scope of this method.

Keywords: *factorial code, relative transmission rate, bit error probability, noise-tolerant encoding, cryptographic protection.*

DOI: 10.24025/2306-4412.3.2020.214937

УДК 005.8:35.075.5:378.09

[0000-0003-2784-883X] **Д. О. Тимченко,**
e-mail: dariatymchenko1@gmail.com
[0000-0002-0242-5497] **Н. П. Корогод,** *к.пед.н., доцент,*
[0000-0002-4654-843X] **Т. С. Новородовська,** *к.б.н., доцент*
Національна металургійна академія України
пр. Гагаріна, 4, м. Дніпро, 49000, Україна

УПРАВЛІННЯ ПРОДУКТОМ ПРОЕКТУ СТВОРЕННЯ ОФІСУ ТРАНСФЕРУ ТЕХНОЛОГІЙ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ

У результаті проведення досліджень у галузі управління проектом створення офісу трансферу технологій у закладі вищої освіти встановлено, що між представниками закладів вищої освіти та бізнесу відсутні сучасні комунікаційні канали, насамперед у мережі Інтернет. Водночас у результаті проведення науково-дослідних робіт співробітниками закладів вищої освіти створюються технології, розробки, реєструються об'єкти права інтелектуальної власності. Наявність сучасних комунікаційних каналів, а саме сайту, в рамках якого будуть висвітлені пропозиції закладу вищої освіти стосовно новостворених технологій та розробок, дасть можливість налагодити комунікаційний зв'язок з потенційними споживачами, що в цілому підвищить рівень впровадження науково-технічних розробок у реальний сектор економіки. Авторами у рамках реалізації проекту створення офісу трансферу технологій у закладі вищої освіти запропоновано створити додатковий продукт проекту – розділ сайту, присвячений технологіям та розробкам. Через те, що важливу роль відіграє зручність та простота у користуванні сайту, авторами також запропоновано методи перевірки відповідності прототипу розділу сайту потребам стейкхолдерів. На основі проведених досліджень пропонується запатентований шаблон розділу сайту, присвячений технологіям та розробкам, який може бути адаптований для будь-якого закладу вищої освіти.

Ключові слова: *проектний підхід, прототип сайту, стейкхолдери проекту, науково-технічні розробки, продукт проекту, офіс трансферу технологій.*

Вступ. На сьогоднішній день існує об'єктивна необхідність налагодження діалогу між наукою та бізнесом. Сучасний вектор політики держави спрямований на розбудову інноваційної екосистеми в Україні, одним із головних елементів якої виступають саме заклади вищої освіти (надалі – ЗВО). Створення офісу трансферу технологій (надалі – ОТТ), який, по суті, є проектним офісом, у ЗВО передбачає реалізацію відповідного організаційного проекту [1]. Однак аналіз останніх досліджень і публікацій показав, що питання створення проектних офісів у ЗВО є недостатньо висвітленими [2].

Аналіз останніх досліджень та публікацій. У PMBOK визначено поняття, типи офісів управління проектами [3]. В іншому міжнародному стандарті з управління проектами визначено функції проектного офісу [4]. ДСТУ 54870-2011 визначає роль офісу управління проектами [5]. Стандарт ISO 21500:2012 визначає ролі та зони відповідальності стейкхолдерів проекту [6]. С. Д. Бушуєв представив класифікацію та визначив функції проектних офісів [7]. І. Кендалл і С. Роллінз розглянули питання створення офісів управління проектами, однак без урахування специфіки ЗВО [8]. У багатьох наукових працях аргументовано створення ОТТ у ЗВО, однак дослідження проводилися без урахування проектного підходу [9].

Авторами проведено дослідження управління проектом створення ОТТ у ЗВО, в ході яких сформульовано нові моделі та методи управління проектами: концептуальна модель управління проектом створення ОТТ у ЗВО [10], метод створення ОТТ у ЗВО з елементами дизайн-мислення, модель ОТТ, інформаційна модель процесу управління проектом створення ОТТ у ЗВО [1]. У результаті практичного впровадження запропонованих моделей і методів реалізовано проект створення ОТТ у ЗВО, основним продуктом якого є ОТТ, додатковим продуктом проекту став розділ сайту ЗВО, присвячений технологіям та розробкам. У цій роботі роз-

DOI: 10.24025/2306-4412.3.2020.214879

глядається питання створення саме розділу сайту ЗВО.

Постановка проблеми в загальному вигляді. Під час проведення дослідження питання управління проектом створення проектного офісу (ОТТ) у ЗВО було визначено проблеми, одна з яких – відсутність сучасних комунікаційних каналів між представниками науки та бізнесу. З метою вирішення цієї проблеми в ході реалізації проекту створення ОТТ у ЗВО було прийнято рішення створити розділ сайту, присвячений технологіям і розробкам ЗВО. Адже, зважаючи на глобальні тренди дигіталізації, налагодження співпраці між представниками науки та бізнесу неможливо реалізувати без застосування сучасних інформаційних технологій [11].

Так, у кожного ЗВО є власний веб-сайт, на якому розміщена інформація щодо керівництва ЗВО, структури, умов вступу тощо. У загальному розумінні сайт – це свого роду точка контакту потенційних клієнтів з бізнесом [12]. Сайти ЗВО здебільшого спрямовані на цільову аудиторію – студентів [13]. Водночас далеко не кожний сайт ЗВО містить інформацію про створені в ньому технології та об'єкти права інтелектуальної власності (надалі – ОПІВ). І навіть якщо такий розділ на сайті є, його досить складно знайти [11]. Проте наявність такої інформації і такого розділу на сайті допоможе залучити іншу цільову аудиторію, не менш важливу для ЗВО, – представників реального сектору економіки, які можуть бути зацікавлені у придбанні технологій ЗВО або ж співпраці з ним.

Метою дослідження є опис результату практичної реалізації створення прототипу розділу сайту ЗВО, присвяченого технологіям і розробкам, та опис методів визначення відповідності створеного прототипу потребам стейкхолдерів проекту.

Виклад основного матеріалу. Під час проведення дослідження у ході визначення відповідності створеного прототипу розділу сайту ЗВО, присвяченого технологіям і розробкам, потребам стейкхолдерів було застосовано такі методи: A/B тестування та юзабіліті-тестування.

Сутність A/B тестування полягає в тому, що різні варіанти виконання розділу сайту демонструють однаковій кількості користувачів, а потім отримана таким чином інформація аналізується [14]. Цей метод було застосовано під час порівняння існуючої версії розділу сайту та створеного прототипу.

Сутність юзабіліті-тестування полягає в тому, що до потенційних користувачів звертаються з проханням скористатися розділом сайту та виконати набір завдань і, спостерігаючи за їх поведінкою, роблять висновок щодо юзабіліті запропонованого прототипу [14]. Під юзабіліті слід розуміти властивість продукту бути придатним для використання та зручність продукту під час його використання [15]. Юзабіліті сайту – зручність і простота його використання; юзабіліті вважається високою за умови, якщо, вперше потрапивши на сайт, відвідувач може відразу зрозуміти, яким чином ним користуватися, а також він легко орієнтується на сайті, потрапивши на нього вдруге [16].

Отримана в результаті тестувань інформація щодо прототипу розділу сайту допоможе прийняти рішення щодо необхідності його доопрацювання або початку повноцінного функціонування.

З метою підтвердження практичних результатів проведеного дослідження під час управління проектом створення ОТТ у Національній металургійній академії України (надалі – НметАУ) на етапі генерування та відбору ідей було прийнято рішення про створення розділу сайту НМетАУ, присвяченого технологіям, максимально "user friendly".

Під час проведення A/B тестування респондентами було однозначно встановлено, що створений прототип розділу сайту НМетАУ, присвячений технологіям та розробкам, значно більше відповідає потребам стейкхолдерів, ніж існуючі окремі розділи сайту, які мають відношення до технологій. Нижче наведено опис і порівняння існуючих розділів сайту та створеного у результаті реалізації проекту прототипу розділу сайту.

Поточна версія головної сторінки сайту НМетАУ [17] перенасичена інформацією, яка не структурована, а тому користувачу досить важко відшукати потрібну. І хоча сайт містить розділ «ГКР технологія», він розташований у лівому сайдбарі серед розділів про новини, керівництво, факультети тощо, а тому «губиться». Водночас у розділі «Наука», розташованому нижче розділу «ГКР технологія», міститься підрозділ «Наукові розробки», який можна обрати у правому сайдбарі. У розділі «ГКР технологія» і підрозділі «Наукові розробки» дублюється інформація про технології

DOI: 10.24025/2306-4412.3.2020.214879

та розробки НМетАУ. Також у розділі «Наука» виокремлений підрозділ «Винахідницька діяльність», який містить перелік патентів НМетАУ.

Таким чином, сайт НМетАУ в цілому не спрямований на цільову аудиторію – представників бізнесу. Адже інформація, яка може зацікавити представників бізнесу і принести дохід ЗВО, має виділятися на сайті та привертати увагу. Важливо, щоб така інформація була зібрана в одному розділі сайту і її не довелося довгий час шукати. Тобто, якщо на сайт ЗВО потрапить представник бізнесу, який потенційно може бути зацікавлений у технологіях або розробках цього ЗВО, цей сайт має бути налаштований максимально “user friendly” (інтуїтивно зрозумілий, зручний у користуванні) [11].

Сайт НМетАУ в цілому потребує змін для того, аби стати юзабіліті, адже він був створений ще у 2006 р. та наразі не відповідає сучасним трендам і вимогам. Однак з огляду на обмеженість ресурсів під час відбору ідей було прийнято рішення обмежитися створенням розділу сайту, присвяченого технологіям та розробкам НМетАУ.

Проте деякі зміни до головної сторінки сайту необхідно внести. У хедері замість логотипу з правої сторони слід розмістити кнопку, при натисканні на яку можна перейти до розділу, присвяченого технологіям, розробкам та ОПІВ НМетАУ. Пропонуємо назвати цю кнопку «Технології НметАУ» (рисунок 1), при наведенні курсора на яку буде спливати підказка: «Технології, розробки та винаходи НметАУ». Завдяки цій кнопці буде відбуватися перехід до розділу, присвяченого технологіям, розробкам та винаходам НМетАУ, який фактично об’єднає розділ «ГКР технологія», підрозділи «Наукові розробки» та «Винахідницька діяльність», які відповідно пропонуємо видалити з сайдбарів задля уникнення дублювання елементів сайту і зменшення інформаційного перевантаження головної сторінки. Також пропонуємо або змінити повністю фон хедера, або скоротити кількість фотографій, які розконцентровують увагу користувачів.

Рисунок 1 – Фрагмент головної сторінки сайту НМетАУ

Таким чином, інформація щодо створених технологій та ОПІВ ЗВО завдяки кнопці, розташованій у хедері сайту, буде виділятися та привертати увагу і водночас завдяки тому, що хедер наразі є фіксованим елементом, користувач зможе швидко перейти до відповідного розділу у будь-який момент.

При натисканні на таку кнопку технології та/або ОПІВ мають бути структурованими за галузями або іншими критеріями; на цій сторінці веб-сайту має бути лише перелік назв у вигляді посилань на наступну сторінку, де буде розміщена вже повна інформація про технологію та/або ОПІВ; назва технології та ОПІВ має однозначно вказувати, на вирішення якої саме проблеми спрямована ця технологія або ОПІВ [11]. Для зручного та швидкого пошуку технологій пропонуємо також розташувати пошуковий рядок у цьому розділі.

Опис технології повинен бути лаконічним, написаним доступною та зрозумілою для стейкхолдерів мовою (українською, англійською і російською) з уникненням суто технічної інформації, включати інформацію щодо орієнтовної кількості необхідних грошових, трудових та часових витрат для реалізації проекту трансферу технології та в чому саме полягає економічна вигода від впровадження.

Також доцільним буде розміщення інформації про успішні кейси впровадження технологій та ОПІВ у реальний сектор економіки з конкретними показниками ефективності, що, вочевидь, буде свідчити про наявність зворотного зв’язку від представників бізнесу і заохочуватиме до співпраці.

Наразі на сайті НМетАУ існує водночас декілька розділів, присвячених технологіям та ОПІВ. У розділі «ГКР технологія» стейкхол-

DOI: 10.24025/2306-4412.3.2020.214879

дерам буде важко відшукати інформацію про необхідну технологію з огляду на наступне:

- вся інформація подається виключно англійською мовою, можливість перейти на українську або російську відсутня;

- технології розміщені хаотично – не структуровані за певними критеріями або категоріями;

- перелік технологій чергується з технічним описом однієї з них, відео та фотографіями, які створюють надлишкове інформаційне навантаження на користувача і водночас не містять необхідну для стейкхолдерів інформацію про технологію;

- необхідність завантажувати на комп'ютер користувача описи технологій для ознайомлення з ними створює додаткові незручності;

- контактна особа на основній сторінці розділу та контактна особа, наведена у завантажуваних описах, – різні, а тому постає питання, до кого звертатись у разі зацікавленості у придбанні технологій.

Підрозділ «Наукові розробки» розділу «Наука» викладений трьома мовами, проте наповнення української, російської та англійської версій відрізняється і змістовно, і графічно. Технології структуровані за роками створення, що навряд чи є зручним для користувача.

Водночас під назвами технологій 2017–2018 рр. наведено їх опис. У 2017 р. цей опис навіть чітко структурований з виокремленими елементами: призначення та сфера застосування; важливі показники, які характеризують рівень отриманого наукового результату; стан захисту інтелектуальної власності; основні технічні характеристики; затребуваність на ринку; стан розробки. У 2018 р. такі структурні елементи вже не виділяються, описи технологій не регламентовані. У 2016 р. зазначається лише перелік технологій з можливістю завантажити їх описи.

У деяких описах технологій зазначено інформацію, що отримано патенти на винахід або корисну модель, проте номери патентів відсутні, як і інформація щодо того, чи діють ці патенти. Адже, якщо чинність патентів не підтримувалася і вони не діють, фактично такий ОПІВ перейшов у суспільне надбання і кожен може вільно використовувати його. А тому пропонувати такі ОПІВ є недоречним.

У більшості випадків назва технології або є занадто складною, або не вказує на призначення цієї технології. А в деяких випадках, навіть виходячи з опису, досить важко зрозуміти призначення технології та яку проблему вона вирішує.

У нижній частині розділу наведено додатки-файли для завантаження описів деяких технологій, водночас назви файлів не дають уявлення про зміст завантажуваного файлу. Також недоліком є відсутність контактів у цьому підрозділі сайту, їх можна знайти лише у завантажуваних файлах.

У підрозділі «Винахідницька діяльність» розділу «Наука» відображено перелік патентів, згрупований за роками одержання: 2016–2019 рр. Наведено наступну інформацію про патенти: порядковий номер отриманого патенту; номер патенту; назва; автори. Таким чином, залишаються невисвітленими такі важливі питання: це патент на винахід або корисну модель; які переваги надає використання даного ОПІВ; галузі застосування; чинний патент або ні.

Проаналізувавши наявні розділ та два підрозділи сайту НМетАУ, присвячені технологіям, розробкам та ОПІВ, можна дійти висновку, що наведена в них інформація структурована незручно для стейкхолдерів.

З огляду на виявлену проблему, пропонуємо об'єднати проаналізовані розділи в один. Зупинимося детальніше на внесенні змін до єдиного розділу сайту НМетАУ «Технології». Так, при натисканні на кнопку «Технології НметАУ» на головній сторінці сайту та переході на відповідну сторінку (розділ) сайту пропонуємо структурувати контент наступним чином:

1. Хедер (шапка) складається з наступних елементів (рисунок 2): логотип з лівої сторони, під яким розташовуються кнопки переходу на українську, англійську або російську мови; кнопки «Контакти», «Пошук» та «Замовити технологію» (рисунок 3) з правої сторони; назва розділу «Технології, розробки та винаходи НметАУ» в центральній частині, під якою розміщене меню, що складається з п'яти розділів (виробництво, модифікації, ресурсо-зберігаючі технології, системи автоматизації, пристрої).

DOI: 10.24025/2306-4412.3.2020.214879

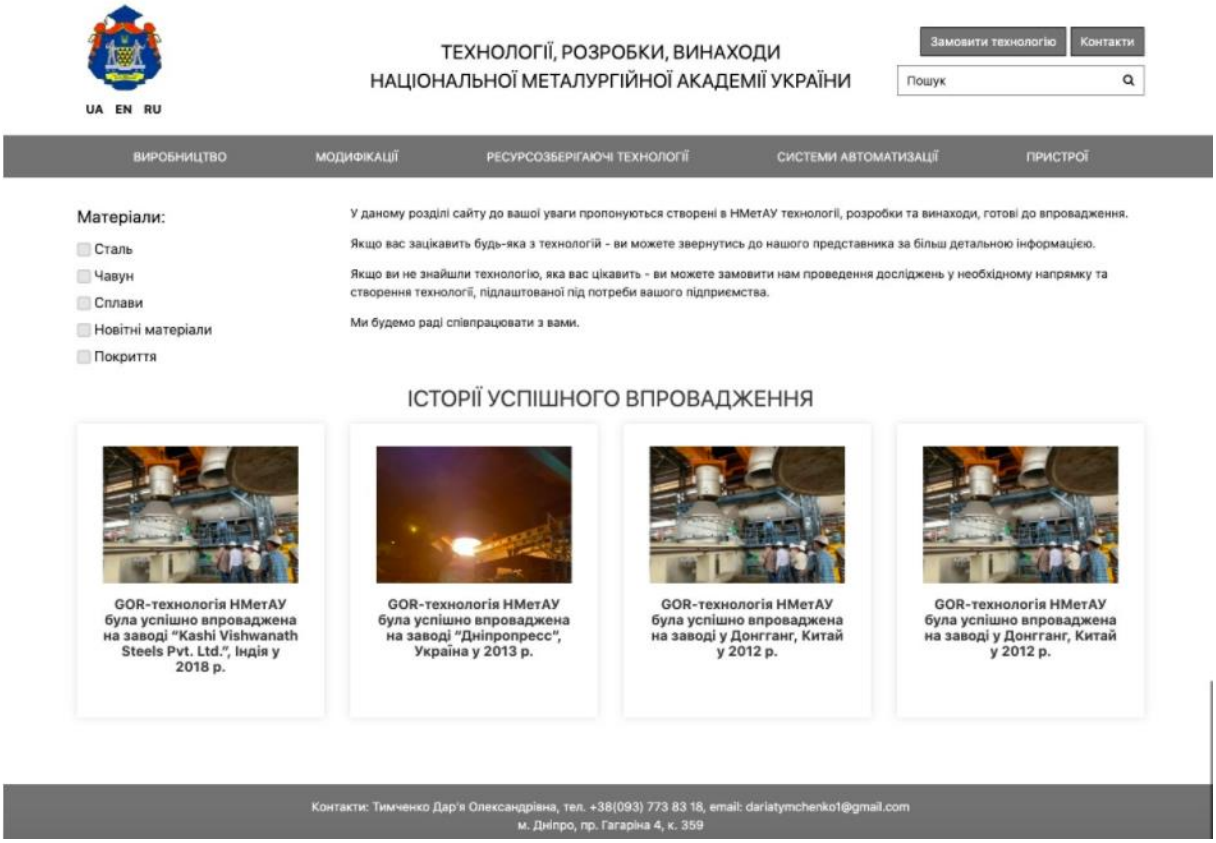


Рисунок 2 – Перша сторінка прототипу розділу сайту НметАУ

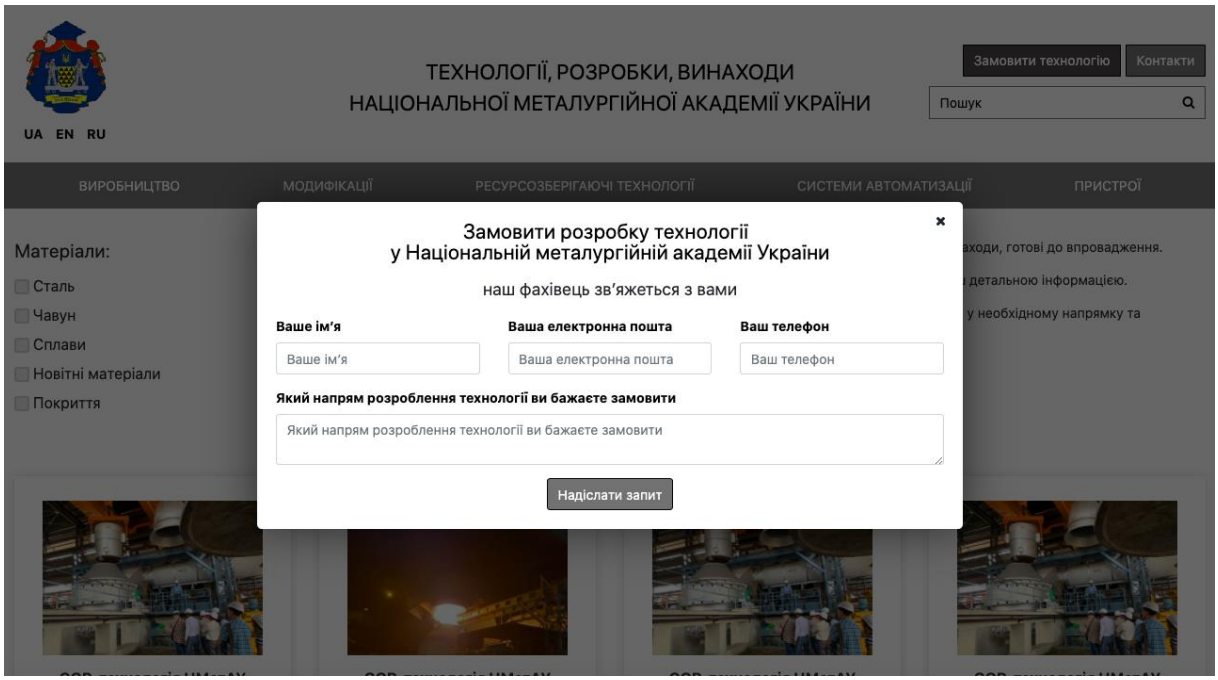


Рисунок 3 – Форма замовлення технології у прототипі розділу сайту НМетАУ

2. Сайдбар (sidebar – бічні колонки) розташовується з лівої сторони та являє собою чекбокс (checkbox) «Матеріали», який дає змогу обрати одну або більше опцій – стосовно НМетАУ пропонуємо можливість обрати за матеріалами: сталь, чавун, сплави, новітні матеріали, покриття.

DOI: 10.24025/2306-4412.3.2020.214879

3. Контент сайту розташовується в центральній частині. При переході на розділ про технології на першій сторінці розміщується загальна інформація про цей розділ сайту в цілому (стисло про напрями створення технологій, розробок та ОПІВ, варіанти співпрацювання НМетАУ з представниками бізнесу), нижче – історії успішного впровадження технологій НМетАУ. При виборі будь-якої вкладки меню та/або матеріалів загальна інформація зміниться на перелік відфільтрованих технологій, розробок та/або ОПІВ (рисунок 4), при натисканні на які відбувається перехід на наступну сторінку сайту з повною інформацією (описом) про обрану технологію.

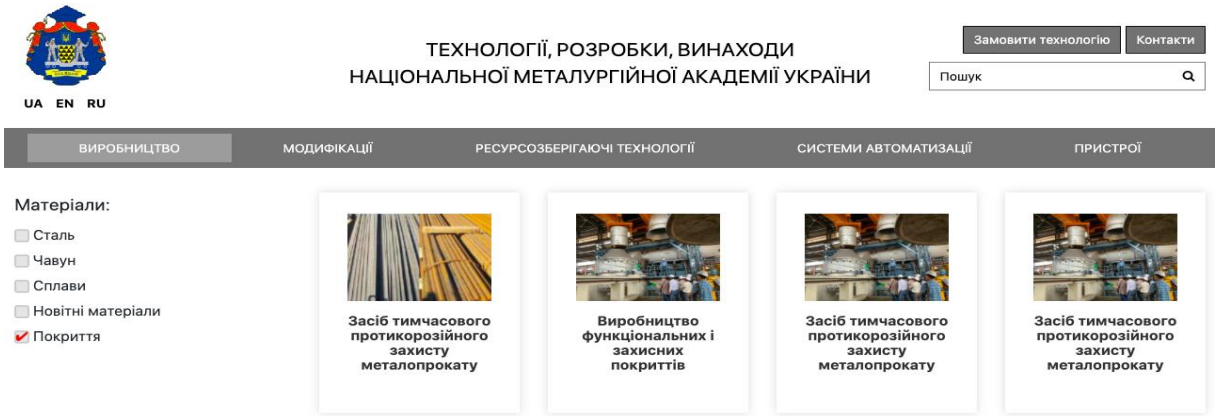


Рисунок 4 – Друга сторінка прототипу розділу сайту НМетАУ

Водночас назва технології має однозначно вказувати, на вирішення якої саме проблеми спрямована ця технологія або ОПІВ.

Опис технології обов'язково має бути структурованим і включати такі елементи:

- назва технології;
- сфера застосування;
- функції технології та проблеми, які вона вирішує;
- переваги порівняно з аналогами, насамперед – економічна вигода від впровадження;
- грошові, трудові та часові витрати на впровадження;
- інформація виключно про чинні патенти;
- вартість технології (не обов'язково зазначати на сайті, проте в особи, відповідальної за трансфер технологій у НметАУ, має бути інформація про таку вартість, для того щоб у разі зацікавленості з боку представників бізнесу можна було оперативно відповісти на це питання).

4. Футер містить прізвище, ім'я, по батькові та контакти особи, відповідальної за трансфер технологій в НМетАУ. Контактні дані обов'язково мають бути актуальними.

Вся інформація на сайті має бути написана максимально доступною, зрозумілою мовою. Слід уникати формул, таблиць, термінів, а також наступних висловів: «Розробка відповідає кращим світовим аналогам», якою кафедрою розроблено, інших абстрактних неінформативних фраз. Опис має бути дуже стислим та водночас інформативним, адже користувач не буде переглядати велику кількість інформації. Головне завдання ЗВО – зацікавити представника бізнесу та сфокусувати його увагу на необхідності й вигоді від співпраці.

Налаштування сайту ЗВО подібним чином допоможе збільшити його відвідуваність (трафік), що є запорукою успішного розвитку ЗВО, налагодження співпраці з представниками бізнесу та підвищення конкурентоспроможності ЗВО.

Під час проведення юзабілітітестування респондентами було встановлено, що прототип розділу сайту є зручним у використанні та інтуїтивно-зрозумілим.

Результати досліджень являють собою експериментальні дані, отримані в роботі. Розроблений прототип розділу сайту захищений патентом України на промисловий зразок [18], свідоцтвом України про реєстрацію авторського права на комп'ютерну програму

DOI: 10.24025/2306-4412.3.2020.214879

[19], свідоцтвом України про реєстрацію авторського права на складений твір [20]. Зазначені ОПІВ можуть бути адаптовані під потреби будь-якого ЗВО або наукової установи.

Висновки. У статті наведено опис результату практичної реалізації створення прототипу розділу сайту ЗВО, присвяченого технологіям та розробкам, та опис методів визначення відповідності створеного прототипу потребам стейкхолдерів проекту. За результатами проведеного дослідження можна дійти висновку, що ефективне налагодження комунікаційних зв'язків між представниками науки та бізнесу неможливо здійснити без використання сучасних інформаційних технологій. Наукова новизна полягає у розробці моделей та методів управління проектами створення ОТТ у ЗВО, а в цій роботі розглядається їх практичне застосування. Практична значущість наукових результатів полягає у створенні прототипу розділу сайту ЗВО, присвяченого технологіям та розробкам, як додаткового продукту проекту створення ОТТ у ЗВО. Водночас описаний у статті прототип може бути адаптований під потреби кожного ЗВО. Проведені A/B тестування та юзабілітітестування показали відповідність прототипу потребам стейкхолдерів проекту.

Перспективи подальших досліджень. Проблема налагодження комунікаційних каналів між представниками ЗВО та бізнесу, які дадуть змогу підвищити рівень впровадження науково-технічних розробок у реальний сектор економіки, є перспективним та актуальним напрямом подальших досліджень.

Список використаних джерел

[1] D. Tymchenko, N. Korogod, and T. Novorodovska, "Information model of project management process of creating a technology transfer office", *Science and Education a New Dimension. Natural and Technical Sciences*, VIII (29), iss. 238, Sept., pp. 63-66, 2020.

[2] Д. О. Тимченко, "Сучасні підходи до управління проектами створення проектних офісів у закладах вищої освіти", *Управління розвитком складних систем*, № 42, с. 29-36, 2020.

[3] A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Sixth ed., USA, PMI, 2017.

[4] Individual Competence Baseline for Project, Programme & Portfolio Management / International Project Management Association (IPMA) Global Standart, Version 4.0, 2015.

[5] ГОСТ Р 54869-2011 Проектный менеджмент. Требования к управлению проектом (Переиздание). [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/ 1200089604. Дата обращения: Май 03, 2020.

[6] ISO 21500:2012. Guidance on project management. [Online]. Available: http://www.isopm.ru/download/iso_21500.pdf. Accessed on: May 03, 2020.

[7] С. Д. Бушуєв, Н. С. Бушуєва, та Д. І. Шороп, "Проектний офіс як методологія мультипроектного управління", *Управління проектами та розвиток виробництва*: зб. наук. пр. Луганськ: видво СНУ ім. В. Даля, 2004. [Електронний ресурс]. Режим доступу: https://cyberleninka.ru/article/n/proektniy-ofis-yak-metodologiya-multiproektnogo-upravlinnya/viewer. Дата звернення: Трав. 03, 2020.

[8] И. Кендалл, и К. Роллинз, *Современные методы управления портфелями проектов и офис управления проектами: Максимизация ROI*. Москва, Россия: ПМСОФТ, 2004.

[9] С. О. Єгоров, Д. І. Дятчик, та Т. В. Покшевницька, "Офіс трансферу технологій в університеті", на *VIII Міжнар. бізнес-форумі Проблеми та перспективи розвитку інноваційної діяльності в Україні* (Київ, 19 берез. 2015 р.); відп. ред. А. А. Мазаракі, Київ: Київ. нац. торг.-екон. ун-т, 2015, с. 89-90.

[10] Д. О. Тимченко, "Концептуальна модель управління проектом створення офісу трансферу технологій у закладі вищої освіти", на *XVI Міжнар. наук.-практ. конф. Управління проектами: стан та перспективи* (8-11 верес. 2020 р.), Миколаїв: НУК, с. 110-113.

[11] Д. О. Тимченко, та Т. С. Новородовська, "Управління трансфером технологій у закладах вищої освіти в умовах дигіталізації суспільства", на *XVII Міжнар. наук.-практ. конф. Управління проектами в умовах дигіталізації суспільст-*

DOI: 10.24025/2306-4412.3.2020.214879

ва (15-16 трав. 2020), Київ, 2020, с. 329-333.

[12] В. Федоричак, "Типи трафіку в Інтернеті: 5 основних каналів залучення відвідувачів на сайт" [Електронний ресурс]. Режим доступу: https://lemarbet.com/ua/razvitie-internet-magazina/tipy-trafika-v-internete/. Дата звернення: Трав. 03, 2020.

[13] Л. А. Мартинюк, "Персональний сайт викладача як засіб упровадження новітніх інформаційних технологій", *Інформаційні технології і засоби навчання*, т. 41, № 3, с. 299-310, 2014.

[14] Полное руководство новичка по UX исследованию, 05.07.2018, Команда Medium. [Электронный ресурс]. Режим доступа: https://medium.com/@grifer163/%D0%BF%D0%BE%D0%BB%D0%BD%D0%BE%D0%B5-%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE-%D0%BD%D0%BE%D0%B2%D0%B8%D1%87%D0%BA%D0%B0-%D0%BF%D0%BE-ux-%D0%B8%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8E-319d69c928cb. Дата обращения: Май 03, 2020.

[15] Юзабіліті, SEO словник. [Електронний ресурс]. Режим доступу: https://igroup.com.ua/seo-articles/yuzabiliti/. Дата звернення: Трав. 03, 2020.

[16] Юзабіліті, IT словник, 20.04.2016. [Електронний ресурс], Режим доступу: https://igroup.com.ua/seo-articles/yuzabiliti/. Дата звернення: Трав. 03, 2020.

[17] Сайт Національної металургійної академії України. [Електронний ресурс]. Режим доступу: https://nmetau.edu.ua/ua. Дата звернення: Трав. 03, 2020.

[18] Д. О. Тимченко, "Графічний інтерфейс розділу сайту "Технології, розробки, винаходи" для закладів вищої освіти", *патент України на промисловий зразок № 41896,* Лип. 10, 2020.

[19] Д. О. Тимченко, "Комп'ютерна програма "Розділ сайту "Технології, розробки, винаходи" Національної металургійної академії України", *свідоцтво України про реєстрацію авторського права № 97737*, Черв. 03, 2020.

[20] Д. О. Тимченко, "Дизайн розділу сайту "Технології, розробки, винаходи" Національної металургійної академії України", *свідоцтво України про реєстрацію авторського права № 97738*, Черв. 03, 2020.

References

[1] D. Tymchenko, N. Korogod, and T. Novorodovska, "Information model of project management process of creating a technology transfer office", *Science and Education a New Dimension. Natural and Technical Sciences*, VIII (29), iss. 238, Sept., pp. 63-66, 2020.

[2] D. O. Tymchenko, "Modern approaches to project management of project offices creation in higher education institutions", *Upravlinnia rozvytkom skladnykh system*, iss. 42, pp. 29-36, 2020. [in Ukrainian].

[3] A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Sixth ed., USA, PMI, 2017.

[4] Individual Competence Baseline for Project, Programme & Portfolio Management / International Project Management Association (IPMA) Global Standart, Version 4.0, 2015.

[5] GOST R 54869-2011 Project Manageme.-t. Project management requirements (Reprint). [Online]: Available: http://docs.cntd.ru/document/ 1200089604. Accessed on: May 03, 2020].

[6] ISO 21500:2012. Guidance on project management. [Online]. Available: http://www.isopm.ru/download/ iso_21500.pdf. Accessed on: May 03, 2020.

[7] S. D. Bushuyev, N. S. Bushuyeva, and D. I. Shorop, "Project office as a methodology of multi-project manag-?ment", *Upravlinnia proektamy ta rozvytok vyrobnytstva*: col. of sci. works. Luhansk: vyd-vo SNU im. V. Dalya, 2004. [Online]. Available: https://cyberleninka.ru/article/n/ proektniy-ofis-yak-metodologiya-multiproektnogo-upravlinnya/viewer. Accessed on: May 03, 2020.

[8] I. Kendall, and K. Rollins, *Modern methods for project portfolio management*

DOI: 10.24025/2306-4412.3.2020.214879

and project management office: Maximizing ROI. Trans. from Engl. Moscow, Russia: PMSOFT, 2004. [in Russian].

[9] S. O. Yehorov, D. I. Diatchyk, and T. V. Pokshevnytska, "Technology transfer office at the university", in *VIII Int. Business Forum Problems and prospects for the development of innovation in Ukraine* (Kyiv, March 19, 2015); resp. ed. A. A. Mazaraki. Kyiv: Kyiv. nat. trade-econ. un-t, 2015, pp. 89-90. [in Ukrainian].

[10] D. O. Tymchenko, "Conceptual model of project management for the creation of a technology transfer office in a higher education institution", in *XVI Int. sci.-pract. conf. Project management: status and prospects* (Sept. 8-11, 2020), Mykolayiv: NUK, pp. 110-113. [in Ukrainian].

[11] D. O. Tymchenko, abd T. S. Novorodovska, "Management by technology transfer in higher education institutions in the context of digitalization of society", in *XVII Int. sci.-pract. conf. Project management in the context of digitalization of society* (May 15-16, 2020), Kyiv, 2020, pp. 329-333. [in Ukrainian].

[12] V. Fedorychak, "Types of traffic on the Internet: 5 main channels to attract visitors to the site" [Online]. Available: https://lemarbet.com/ua/razvitie-internet-magazina/tipy-trafika-v-internete/. Accessed on: May 03, 2020.

[13] L. A. Martynuik, "Personal teacher's site as a means of new information technologies", *Informatsiini tekhnolohii i zasoby navchannia*, vol. 41, no. 3, pp. 299-310, 2014. [in Ukrainian].

[14] The Complete Beginner's Guide to UX Research, 05.07.2018, Medium team. [Online]. Available: https://medium.com/@grifer163/%D0%BF%D0%BE%D0%BB%D0%BD%D0%BE%D0%B5-%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE-%D0%BD%D0%BE%D0%B2%D0%B8%D1%87%D0%BA%D0%B0-%D0%BF%D0%BE-ux-%D0%B8%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8E-319d69c928cb. Accessed on: May 03, 2020.

[15] Usability, SEO dictionary. [Online]. Available: https://igroup.com.ua/seo-articles/yuzabiliti/. Accessed on: May 03, 2020.

[16] Usability, IT dictionary, 20.04.2016. [Online]. Available: https://igroup.com.ua/seo-articles/yuzabiliti/. Accessed on: May 03, 2020.

[17] Site of National Metallurgical Academy of Ukraine. [Online]. Available: https://nmetau.edu.ua/ua. Accessed on: May 03, 2020.

[18] D. O. Tymchenko, "Graphical interface of the section of the site "Technologies, developments, inventions" for higher education institutions", *patent of Ukraine for industrial design № 41896*, July 10, 2020. [in Ukrainian].

[19] D. O. Tymchenko, "Computer program "Site section "Technologies, developments, inventions" of the National Metallurgical Academy of Ukraine", *certificate of copyright registration of Ukraine № 97737*, June 03, 2020. [in Ukrainian].

[20] D. O. Tymchenko, "Design of the section of the site "Technologies, developments, inventions" of the National Metallurgical Academy of Ukraine", *certificate of copyright registration of Ukraine № 97738*, June 03, .2020. [in Ukrainian].

DOI: 10.24025/2306-4412.3.2020.214879

D. O. Tymchenko,
e-mail: dariatymchenko1@gmail.com
N. P. Korogod, *Ph.D., associate professor,*
T. S. Novorodovska, *Ph.D., associate professor,*
National Metallurgical Academy of Ukraine
Gagarin Ave., 4, Dnipro, 49000, Ukraine

PROJECT PRODUCT MANAGEMENT OF A TECHNOLOGY TRANSFER OFFICE ESTABLISHMENT IN A HIGHER EDUCATION INSTITUTION

As a result of research in the field of project management of a technology transfer office establishment in a higher education institution, it has been found that there are no modern communication channels between representatives of higher education institutions and business, primarily on the Internet. This is confirmed, in particular, by the results of observations and surveys. At the same time, as a result of research, employees of higher education institutions create technologies, develop and register intellectual property. The availability of modern communication channels, namely a website, which will cover the proposals of the higher education institution on newly created technologies and developments based on it, as well as give to the business representatives the opportunity to file a request for technology development in a convenient form, will establish a communication link to potential consumers. This, in turn, will increase the level of implementation of scientific and technical developments in the real sector of the economy. Based on observations and surveys conducted as a part of the project of a technology transfer office establishment in a higher education institution, the authors propose to create an additional product of the project – a section of the site devoted to technologies and developments. Due to the fact that the convenience and ease of the use of the site play an important role, the authors also propose methods to verify the compliance of the prototype section of the site to the needs of stakeholders. Based on the research, the authors propose a patented template section of the site, devoted to technologies and developments, which can be adapted by any institution of higher education. This template includes a graphical interface of the site section, which displays the main elements and their location, as well as program code. Usability testing has found that such a prototype section of the site, devoted to technologies, developments and intellectual property rights of higher education institutions, is easy to use and intuitively understandable for business representatives.

Keywords: *project approach, site prototype, project stakeholders, scientific and technical developments, project product, technology transfer office.*

DOI: 10.24025/2306-4412.3.2020.214879

УДК 004:316.4:005.334

[0000-0001-5657-9144] **О. Б. Данченко,** *д.т.н., професор,*
e-mail: elen_danchenko@rambler.ru
[0000-0003-3389-5720] **Є. В. Ланських,** *к.т.н., доцент,*
e-mail: yevhenlanskykh@gmail.com
[0000-0002-4309-3556] **О. В. Семко,** *магістр*
e-mail: semkoinga77@gmail.com
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ІНФОРМАЦІЙНІ РИЗИКИ ЦИФРОВОГО ФОРМАТУ

Стаття присвячена питанню надійності та захисту інформаційних ресурсів, аналізу можливих негативних наслідків при настанні ризикових ситуацій. Автори визначили сутність та зміст поняття «інформаційний ризик» в умовах цифрової революції і нових технологій, відзначили необхідність комплексного підходу до ідентифікації, аналізу інформаційних ризиків та розробки плану управління інформаційними ризиками. Особливу увагу приділено інформаційним ризикам як окремій групі ризиків, що виникають при застосуванні інформаційних технологій.

Важко уявити, з якими ще ризиками на шляху діджиталізації зіткнеться організація та суспільство в найближчому майбутньому. У цьому сенсі цілком перспективною виглядає спроба пошуку шляхів та можливостей для безпечного подолання потенційних загроз, спираючись на тенденції та пріоритети, які диктує ринок і суспільство.

Ключові слова: *інформаційний ризик, цифрова трансформація, управління ризиками, класифікація, інформаційні технології.*

Вступ. Розвиток інформаційних технологій нині розглядається через призму створення глобальних промислових мереж з використанням штучного інтелекту (AI), поширенням Інтернету речей (Internet of things), впровадженням кіберфізічних систем та нейротехнологій з принципово новим механізмом взаємодії (пристроєм) «людина–машина», поширенням сервісів автоматичної ідентифікації, збору та обробки глобальних баз даних (big data), хмарних сервісів (cloud computing), розумних пристроїв та промислових об'єктів (smart everything), розвитком соціальних мереж, різноманітних платформ, сервісів цифрового середовища Інтернету [1].

Цифровий формат сучасного життя змінює традиційні уявлення про способи і механізми зберігання, обігу та захисту інформації, відкриває дорогу до інноваційного розвитку підприємств, що дає можливість поєднати всі виробничі процеси в єдину цифрову систему та максимально автоматизувати управління цією системою:

– використовуючи стратегію Mobile First, компанії отримують і монетизують мобільний трафік, який за своїми показниками вже наздогнав трафік зі стаціонарних пристроїв;

– готові рішення дають змогу економити час на вирішення завдань. Різні програми, розширення та конектори оптимізують роботу компанії і вимагають мінімальних витрат часу на їх впровадження та адаптацію;

– масове впровадження інтелектуальних датчиків в обладнання та виробничі лінії (технології індустріального Інтернету речей);

– перехід на безлюдне виробництво і масове впровадження роботизованих технологій;

– перехід на зберігання інформації та проведення обчислювань із власних потужностей на розподілені ресурси («хмарні» технології);

– наскрізна автоматизація та інтеграція виробничих і управлінських процесів у єдину інформаційну систему («від обладнання до міністерства»);

– використання всієї маси збираних даних (структурованої та неструктурованої інформації) для формування аналітики (технології «великих» даних);

– перехід на обов'язкову оцифровану технічну документацію та електронний документообіг («безпаперові» технології»);

– цифрове проектування та моделювання технологічних процесів, об'єктів, виро-

DOI: 10.24025/2306-4412.3.2020.200792

бів протягом усього життєвого циклу від ідеї до експлуатації (застосування інженерного програмного забезпечення);

– застосування технологій нарощування матеріалів взамін зрізання («адитивні» технології, 3D прінтинг);

– застосування сервісів із автоматичного замовлення витратних матеріалів і сировини для виробництва продукції й автоматичного постачання готової продукції споживачу, оминаючи посередницькі ланцюжки;

– застосування безпілотних технологій у транспортних системах, у т. ч. для постачання промислових товарів;

– застосування мобільних технологій для моніторингу, контролю процесів та управління ними у житті та на виробництві;

– перехід на реалізацію промислових товарів через Інтернет [2].

Цифрова революція, яка охопила світову економіку, вражає масштабом, темпами і географією. З кожним роком зростає інтенсивність впровадження нових технологій у виробництво й обслуговування людських потреб [3].

Однак інший бік масштабної цифровізації сфер життя веде до того, що громадяни України та бізнес усе більше потерпатимуть від зростання кіберзлочинності. Найнебезпечнішими для економіки та громадян є кібератаки на критичну інфраструктуру (енергозабезпечення, транспортне управління, банківський і телекомунікаційний сектори, медичне обслуговування, водопостачання тощо) України [4].

Мета дослідження – ідентифікувати та класифікувати інформаційні ризики; проаналізувати сучасні методи та засоби управління інформаційними ризиками в процесі цифрової трансформації.

Виклад основного матеріалу. В дослідженнях провідних фахівців у галузі контролю та управління ризиками О. Окишева та Г. Городової зазначено, що функція управління ризиками допомагає організаціям домогтися успіхів при впровадженні цифрових ініціатив. Сьогодні організації стрімко освоюють цифрові технології в умовах, коли обсяг даних збільшується, рівень автоматизації збільшується, кібератаки стають більш витонченими. На теперішній час ідентифіковано й описано більшість ризиків, але впровадження цифрових технологій «створює» передумови появи нових, ще не відомих ризиків.

«Готовність функції управління ризиками до цифрової трансформації» має дві складові:

– наявність навичок і компетенцій для надання стратегічних консультацій стейкхолдерам, проведення аудиту ініціатив, які пов’язані з цифровою трансформацією організації;

– зміни процесу та інструментарію управління ризиками повинні відбутися таким чином, щоб робота функції управління ризиками максимально базувалася на використанні даних і цифрових технологій для прогнозування ризиків та реагування на них з тим об’ємом і швидкістю, які необхідні при цифровій трансформації організації [5].

Фахівець відділу безпеки компанії Infopulse О. Дячук наголошує, що потреби клієнтів, які постійно змінюються, посилюють тиск на компанії, що мають застарілі системи і процеси; організації, що зволікають із впровадженням цифрових трансформацій, змушені поступатися своєю сферою впливу іншим конкурентним компаніям, які вже «народжені цифровими». Крім того, організаціям потрібно враховувати можливі ризики внаслідок використання технологій і ресурсів, які їм не належать або які вони не контролюють повністю.

Основна мета програмного забезпечення з управління ризиками та дотримання нормативних актів (GRC) (або будь-якого з його модулів) – автоматизувати більшість робочих процесів, пов’язаних зі звітуванням, моніторингом та документообігом [6].

В роботі І. А. Кораблінової зазначено, що вітчизняні компанії, які ще не мають достатньої захищеності від загроз зовнішнього середовища, можуть, скориставшись наполегливою рекомендацією здійснити «цифрову трансформацію», зробити такі кроки, які нанесуть збитки не тільки їм, а й вітчизняній економіці взагалі. Тобто, якщо організація прагне долучитися до всебічної цифровізації, то слід розуміти, чи може ця організація гідно прийняти нові загрози, які за своєю природою будуть залежати від інформації з нових цифрових систем, до яких вона інтегрується.

Оскільки цифрові перетворення пов’язують із розробкою та впровадженням інформаційно-комунікаційних технологій, під якими розуміють сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збору, обробки, збереження, поширення, відображення та викорис-

DOI: 10.24025/2306-4412.3.2020.200792

тання інформації в інтересах її користувачів, ризики, що виникають у процесі цих перетворень, отримали назву «інформаційні» [7].

У дослідженні [8] автори розкривають суть «інформаційних ризиків», які виникають на різних ієрархічних рівнях (держави, економіки в цілому, корпорацій, окремих підприємств тощо), і свій склад ризиків, що утворюють обсяг поняття «інформаційний ризик», який відбиває особливості його прояву на цьому рівні та враховує певні умови його функціонування. Так, наприклад, незважаючи на те, що проблема ризиків, пов'язаних з використанням інформації та інформаційних технологій, є відносно новою у загальній теорії ризиків, деякі з них вже включено до переліку глобальних ризиків, які загрожують людству та з якими воно поки що не в змозі впоратися [9].

У роботі Г. Мельника розроблено економіко-математичну модель, яка дає змогу точніше оцінювати ступінь інформаційних ризиків на підприємстві [10]. Також автор відзначає, що аналіз інформаційних ризиків є основою для побудови підсистеми управління інформаційною безпекою підприємства, і підкреслює необхідність виконувати такі кроки:

– ідентифікація інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику, можливих загроз активу, та визначення рівня загроз безпеці КІС підприємства;

– оцінювання рівня дієвості засобів контролю безпеки корпоративної системи; оцінювання вразливості корпоративної системи, що розглядається як результат впливу факторів вірогідного рівня сили загрози та рівня дієвості засобів контролю;

– оцінювання частоти подій втрат від інформаційних ризиків як результату впливу факторів частоти виникнення загрози та вразливості корпоративної системи; оцінювання величини можливих збитків від інформаційних ризиків у корпоративній системі;

– оцінювання рівня інформаційних ризиків у корпоративній системі як результуючої двох факторів: частоти подій втрат та величини можливих втрат від інформаційних ризиків.

Діджиталізація – неоднозначна модель розвитку суспільства, економіки і виробництва, при всіх її позитивних ефектах необхідно прогнозувати, ідентифікувати та управляти негативними загрозами, викликами.

Результати досліджень. Ризик – невизначена подія або умова, настання якої негативно або позитивно позначається на цілях проекту [11].

На сьогодні ще немає однозначного поняття «інформаційний ризик». Деякі фахівці розглядають інформаційний ризик як подію, яка безпосередньо впливає на інформацію: її видалення, спотворення, порушення її конфіденційності або доступності. Інші розглядають це поняття, обмежуючи зону інформаційного ризику лише комп'ютерними системами [12].

Можливість настання випадкової події в інформаційній сфері (інформаційній системі) підприємства, в результаті якої підприємству буде завдано збитку, називають інформаційним ризиком [13].

Інформаційна система організації охоплює всі сфери її діяльності (адміністративну, виробничу, фінансову), є сполучною ланкою при розробці стратегії бізнесу та якості управління організацією і персоналом. Вона містить відомості, що стосуються планів, стану матеріальних та фінансових потоків, договірної діяльності, дані фінансового і управлінського обліку.

Така інформація має цілісний, конфіденційний характер, а її втрата може виявитися критичною для роботи всієї організації. Тому передбачається, що побудова роботи користувачів з інформацією, яка міститься в системі, вимагає спеціальних заходів захисту, які забезпечують конфіденційність, цілісність і доступність даних [14].

За останній час почав активно розвиватися науковий напрям з ефективного управління IT-ризиками. Сучасний рівень інформатизації в організаціях дає змогу використовувати визначення рівня ризику з метою ефективного управління інформаційними технологіями та забезпечення економічної безпеки організації за допомогою підвищення надійності бізнес-процесів. Тобто, ідентифікацію ризиків з їх подальшим аналізом та оцінкою необхідно розглядати як основу сталого функціонування організації. Управлінські рішення по створенню і модернізації інформаційних технологій мають ґрунтуватися на регулярному оцінюванні інформаційних ризиків [11, 13].

Обговорення результатів. Для проведення цілісного аналізу інформаційних ризиків необхідно створити класифікаційну базу ризиків. Якщо інформаційні ризики згрупува-

DOI: 10.24025/2306-4412.3.2020.200792

ти відповідно за окремими критеріями, то можна застосувати індексовану схему класифікації. Пропонуємо цю схему у вигляді схеми Ісікави (рисунок 1).

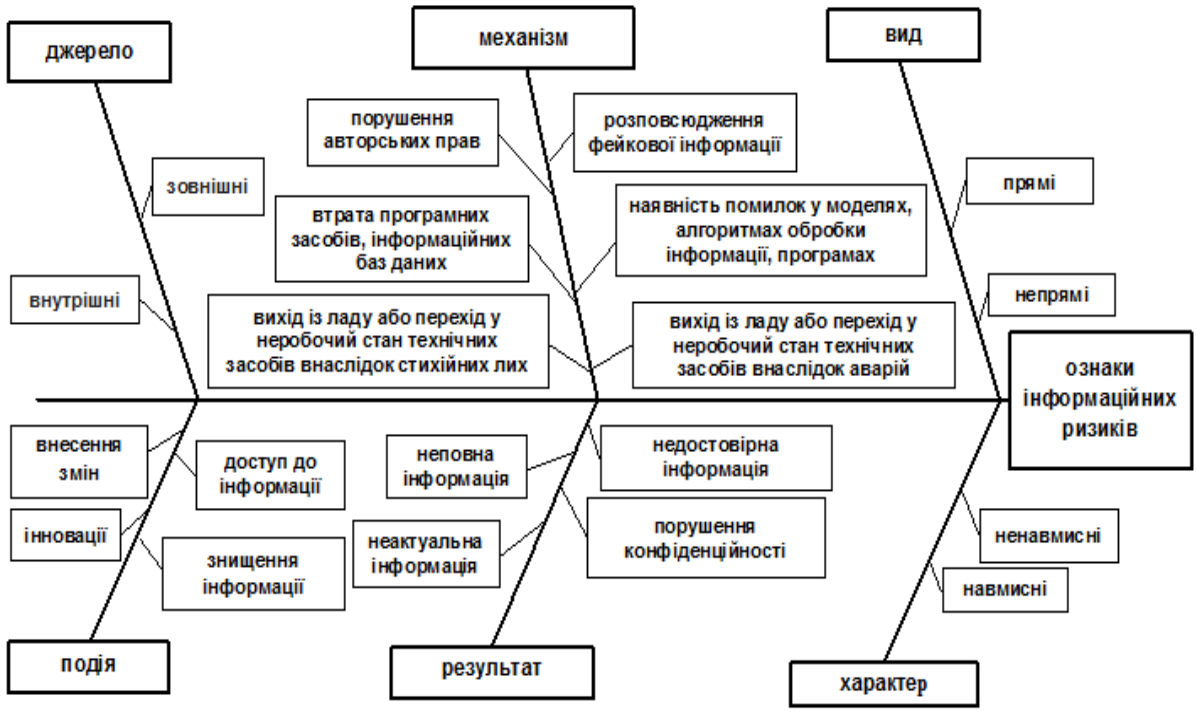


Рисунок 1 – Індексована схема класифікації інформаційних ризиків

Складено за: [13]

Методологія управління ризиками базується на якісному та кількісному оцінюванні ідентифікованих ризиків, не винятком є й інформаційні ризики. Завданням якісного оцінювання є визначення можливих видів ризиків, оцінювання принципового рівня пріоритетності загроз, а також виділення чинників, які впливають на рівень обґрунтування різних можливих контрзаходів [15]. Якісне оцінювання часто супроводжується кількісним, яке визначає імовірність виникнення ризиків та наслідків, що несуть ризикові події. Автор роботи [15] відзначає, що на початкових етапах аналізу інформаційних ризиків, як правило, використовується якісне, а на кінцевому – кількісне оцінювання.

Однозначної загальної методики, за якою можна було б визначити кількісну величину ризику, на сьогоднішній день не існує, що обумовлено відсутністю достатнього обсягу статистичної інформації про можливість виникнення будь-якої конкретної загрози. Крім того, визначити величину вартості конкретного інформаційного активу досить важко (рисунок 2).

Рисунок 2 – Фактори оцінювання інформаційних ризиків

Складено за: [10, 16]

Виділяють наступні етапи аналізу інформаційних ризиків (таблиця 1).

DOI: 10.24025/2306-4412.3.2020.200792

Таблиця 1 – **Етапи аналізу інформаційних ризиків**

№	Етап	Складові етапу
1	Ідентифікація	інформаційні ресурси (активи) організації як об'єкт ризику
		можливі загрози (комбінації загроз) активу та ідентифікація можливих небезпек, які загрожують
2	Оцінювання частоти виникнення загрози можливих втрат від настання ризикової ситуації	експертне оцінювання рівня загроз за набором показників, які характеризують можливість доступу порушника відповідного класу до інформаційних ресурсів
		очікуване реагування засобів контролю впродовж відведеного часового інтервалу
		вразливість як результат впливу факторів можливого рівня сили загрози та реагування засобів контролю на загрозу
		частота виникнення загрози як можлива частота реалізації чинників ризику (агентів загрози) в межах певного часового інтервалу
		частота виникнення подій втрат – можлива частота протягом визначеного часового інтервалу, з якою агент загрози завдає шкоди активу, розглядається як результат впливу факторів частоти виникнення загрози та вразливості
3	Оцінювання величини можливих втрат від настання ризикової ситуації	ввизначення можливої дії кожного з агентів загрози інформаційному активу
		оцінювання величини кожної з можливих форм втрат, що пов'язані з дією певного агента загрози
		оцінювання величини всіх можливих форм втрат
4	Результат аналізу та контрзаходи	оцінювання загального рівня інформаційних ризиків у корпоративній системі; план реагування на ризики із зазначенням пріоритетів рішень по ризиках
5	Моніторинг та контроль	контроль поточного стану захищеності інформаційних систем та планування заходів із захисту
		моніторинг дій та результатів проведення заходів, спрямованих на підвищення ефективності захисту інформації

Складено за: [10, 16]

Результати якісного оцінювання використовуються для формування зв'язку між імовірністю та наслідками події для ключових ризиків. З його допомогою можна вимірювати та описувати профіль ризику організації. Приклад наведено в таблиці 2, яка містить інформацію на основі даних рисунка 1.

Оцінювання важливості ризиків, тобто пріоритетності для обробки, здійснюється за допомогою матриці імовірності та впливу настання ризикових подій (таблиця 3).

В дослідженні [5] автори відзначають, що чим більше функція управління ризиками відповідає планам діджиталізації, тим вища імовірність досягнення мети організації, передбаченої цифровими ініціативами, і пропонують наступні характеристики управління ризиками, які допомагають у прийнятті обґрунтованих рішень, що, в свою чергу, збільшують шанси на успіх у цифровізації:

– повна залученість у план цифрової трансформації організації;

– підвищення кваліфікації спеціалістів задля відповідності темпам розвитку організації;

– визначення балансу компетенцій для роботи з новими технологіями;

– активна взаємодія з особами, що приймають рішення з питань основних цифрових ініціатив;

– комунікація та синхронізація з метою створення єдиної думки про ризик.

DOI: 10.24025/2306-4412.3.2020.200792

Таблиця 2 – **Якісне оцінювання груп інформаційних ризиків**

№ п/п	Найменування групи ризиків	Усереднена імовірність виникнення ризиків (0 ÷ 1)	Усереднений вплив на інформаційні активи від настання ризиків (0 ÷ 1)
1.	Ризики за механізмом виникнення	0,8	0,9
2.	Ризики за характером виникнення	0,7	0,7
3.	Ризики за видами виникнення	0,5	0,6
4.	Ризики за джерелом виникнення	0,5	0,6
5.	Ризики за характером події	0,8	0,8
6.	Ризики за результатом	0,6	0,5

Складено з урахуванням [13]

Таблиця 3 – **Матриця імовірності та впливу настання ризикових подій**

Вплив	Імовірність				
	0,1	0,3	0,5	0,7	0,9
0,8 ÷ 1,0				5	1
0,6 ÷ 0,8			7	2	
0,4 ÷ 0,6			3, 4		
0,2 ÷ 0,4					
0,0 ÷ 0,2					

– зона помірних ризиків;
– зона високих ризиків;
– зона низьких ризиків.

За результатами ідентифікації та оцінювання інформаційних ризиків приймають рішення щодо можливості уникнення або зниження рівня наслідків інформаційних ризиків. Реагування на настання ризикових подій базується на розробці методів і технологій зниження негативного впливу ризиків. Тому готують кілька варіантів стратегій (сценаріїв) реагування, головна мета яких спрямована, в першу чергу, на виключення умов виникнення ризиків.

На ринку інформаційних технологій існує велика кількість програмних засобів, впровадження яких забезпечує ефективне управління інформаційними потоками та виявлення інформаційно-технологічних ризиків, що пов'язані з діяльністю організації, для якої застосовуються ті чи інші методи управління.

До якісних методик управління ризиками на основі вимог ISO 17999 відносяться методики Risk Advisor, COBRA, КОНДОР+, Proteus Enterprise, OCTAVE, а також Digital Security Office, РискМенеджер, Oracle Crystal Ball, @Risk, Risk Watch [17].

До основних результатів автори статті відносять узагальнення аналізу інструментальних засобів оцінювання ризиків.

Висновки. На основі проведеного в статті аналізу можна зробити наступні висновки. По-перше, цифрова трансформація виробництва, суспільного життя неминуча. Її здійснення веде як до розширення можливостей організацій у мережі, так і до небезпек. По-друге, інформаційні ризики, які часто супроводжують процес цифровізації, підпорядковуються стандартам управління ризиками, головним інструментарієм для «боротьби» з ними є ідентифікація та оцінювання ризиків інформаційних активів компанії. По-третє, формулювання та здійснення політики без-

DOI: 10.24025/2306-4412.3.2020.200792

пеки усунення ризиків не буде ефективним, якщо існуючі стандарти використовуються не за правилами. Саме тому роботи із забезпечення інформаційної безпеки повинні бути комплексними.

Управління інформаційними ризиками – досить суб'єктивний та складний процес у діяльності організацій, особливо, якщо діяльність пов'язана з конфіденційною інформацією або прихованою інформацією, або просто з великими обсягами інформації, коли імовірність її непередбаченого витоку є досить великою.

Тому ця проблематика на сьогодні є досить актуальною, а задачі захисту інформації від можливих ризиків – перспективними, які потребують вдосконалення вже існуючих методів протидії чи розробки нових, що дає необхідність продовжити роботу в цьому напрямі.

Подальші дослідження полягають в ідентифікації й якісному та кількісному оцінюванні окремих ризиків серед запропонованих груп інформаційних ризиків з подальшою розробкою протидій у процесі ризик-менеджменту. Також у сучасних умовах цифрової трансформації суспільства актуальною є розробка нових методів управління саме інформаційними ризиками, які б інтегрували в собі процеси інформаційного менеджменту та управління ризиками в компанії в цілому, елементи ризик-менеджменту в проектах, а також засоби інформаційної безпеки.

Список використаних джерел

[1] А. А. Карцхия, "Цифровая революция: новые технологии и новая реальность", *Правовая информатика,* № 1, 2017.

[2] І. Г. Яненкова, "Цифрова трансформація промисловості України: ключові акценти", *Економіка та управління національним господарством. Проблеми економіки,* № 4, с. 179-184, 2017.

[3] И. Н. Макаров, О. В. Широкова, В. А. Арутюнян, и Е. Э. Путинцева, "Цифровая трансформация разномасштабных предприятий, вовлеченных в реальный сектор российской экономики", *Экономические отношения*, т. 9, № 1, с. 313-326, 2019. doi: 10.18334.

[4] Валерій Фіщук, Володимир Матюшко, Єгор Чернєв, Олександр Юрчак, Яна Лаврик, та Анатолій Амелін, "2030 Е – країна з розвинутою цифровою економікою". [Електронний ресурс]. Режим доступу: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2-10. Дата звернення: Берез. 2020.

[5] А. Окишев, и А. Городова, "Разумное управление рисками в ходе цифровой трансформации", *Исследование из серии "Взгляд на риски" за 2019 год*. [Электронный ресурс]. Режим доступа: http://pwc.com/us/RiskStudy. Дата обращения: Март 2020.

[6] О. Дячук, "Як вирішити проблеми в системі безпеки під час цифрової трансформації бізнесу". [Електронний ресурс]. Режим доступу: https://ain.ua/2020/02/08/yak-virishiti-problemi-v-sistemi-bezpeki-pid-chas-cifrovoï-transformacii-biznesu/. Дата звернення: Берез. 2020.

[7] І. А. Кораблінова, "Цифрова трансформація" як джерело ризику компаній у сучасних умовах", *Інноваційна економіка*, № 1-2, с. 217-223, 2018.

[8] В. М. Гранатуров, та І. А. Кораблінова, "Інформаційний ризик підприємства: щодо вирішення проблеми qui pro quo у визначенні поняття", *Інноваційна економіка,* № 5-6 (69), с. 199-206, 2017.

[9] The Global Risks Report 2017. Available: http://www3.weforum.org/docs/GRR17_Report_web.pdf.

[10] Г. Мельник, "Модель оцінювання рівня інформаційних ризиків в корпоративних системах", *Вісник Київського національного університету ім. Тараса Шевченка. Економіка*, № 6 (171), с. 48-54, 2015.

[11] "A guide to the project management body of knowledge (PMBOK guide)", *BISAC: Business & Economics / Project Management*, 6 th. edition, Newtown Square, PA, USA: Project Management Institute, pp. 395-458, 2017.

[12] И. А. Киселева, и С. О. Искаджян, "Информационные риски: методы оценки и анализа", *ИТпортал*, № 2, 2017 [Электронный ресурс]. Режим доступа: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/. Дата обращения: Март 2020.

[13] М. И. Левина, и В. Ю. Петров, "Управление информационными рисками при

DOI: 10.24025/2306-4412.3.2020.200792

внедрении информационных систем", *Международный студенческий научный вестник*, № 2, с. 1-5, 2014.

[14] О. Б. Кузнецова, "Оценка информационных рисков в обеспечении экономической безопасности предприятия", *Труды ИСА РАН*, т. 31, с. 77-98, 2007.

[15] О. Архипов, та А. Скиба, "Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації", *Захист інформації*, т. 15, № 4, с. 366-375, жовтень-грудень, 2013.

[16] J. A. Jones, "An introduction to FAIR", *Trustees of Norwich University,* p. 67, 2005.

[17] Б. Я. Корнієнко, Ю. О. Максімов, та Н. М. Марутовська, "Прикладні програми управління інформаційними ризиками", *Захист інформації*, № 4, с. 60-64, 2012.

References

[1] A. A. Kartshia, "The digital revolution: new technologies and the new reality", *Pravovaya informatika,* no. 1, 2017. [in Russian].

[2] I. G. Yanenkova, "Digital transformation of the Ukrainian industry: key highlights", *Ekonomika ta upravlinnia natsionalnym hospodarstvom. Problemy ekonomiky,* no. 4, pp. 179-184, 2017. [in Ukrainian].

[3] I. N. Makarov, O. V. Shirokova, V. A. Arutyunyan, and E. E. Putintseva, "Digital transformation of large-scale enterprises involved in the real sector of Russian economy", *E`konomicheskie otnosheniya,* vol. 9, no. 1, pp. 313-326, 2019. doi: 10.18334. [in Russian].

[4] Valeriy Fishchuk, Volodymyr Matyushko, Yehor Chernev, Oleksandr Yurchak, Yana Lavryk, and Anatolii Amelin, "2030 E is a country with developed digital economy". [Online]. Available: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2-10. Accessed on: Mar. 2020.

[5] A. Okishev, and A. Gorodova, "Reasonable risk management in the course of digital transformation. Risk Sight Survey. 2019 [Online]. Available: http://pwc.com/us/RiskStudy. Accessed on: Mar. 2020

[6] O. Dyachuk, "How to solve security problems during digital business transformation". [Online]. Available: https://ain.ua/2020/02/08/yak-virishiti-problemi-v-sistemi-bezpeki-pid-chas-cifrovoï-transformacii-biznesu/. Accessed on: Mar. 2020.

[7] I. A. Korablinova, "Digital transformation as a source of risk for companies in today's environment", *Innovatsiina ekonomika,* no. 1-2, pp. 217-223, 2018. [in Ukrainian].

[8] V. M. Granaturov, and I. A. Korablinova, "Enterprise information risk: to solve the qui pro quo problem in defining a concept", *Innovatsiina ekonomika,* no. 5-6 (69), pp. 199-206, 2017. [in Ukrainian].

[9] The Global Risks Report 2017. [Online]. Available: http://www3.weforum.org/docs/GRR17_Report_web.pdf. Accessed on: Mar. 2020.

[10] G. Melnyk, "A model for assessing the level of information risks in corporate systems", *Visnyk Kyivskoho natsionalnoho universytetu im. Tarasa Shevchenka. Ekonomika,* no. 6 (171), pp. 48-54, 2015. [in Ukrainian].

[11] "A guide to the project management body of knowledge (PMBOK guide)", *BISAC: Business & Economics / Project Management*, 6 th. edition, Newtown Square, PA, USA: Project Management Institute, pp. 395-458, 2017.

[12] I. A. Kiseleva, and S. O. Iskadzhian, "Information risks: methods of assessment and analysis". *ITPortal,* no. 2, 2017 [Online]. Available: http://itportal.ru/ science/economy/informatsionnye-riski-metody-otsenk/. Accessed on: Mar. 2020.

[13] M. I. Levina, and V. Yu. Petrov, "Information risk management in the implementation of information systems", *Mezhdunarodnyiy studencheskiy nauchnyiy vestnik,* no. 2, pp. 1-5, 2014. [in Russian].

[14] O. B. Kuznetsova, "Assessment of information risks in ensuring the economic security of the enterprise", *Trudyi ISA RAN,* vol. 31, pp. 77-98, 2007. [in Russian].

[15] O. Arkhipov, and A. Skiba, "Information risks: methods and ways of research, risk models and methods for their identification". *Zakhyst informatsii,*

DOI: 10.24025/2306-4412.3.2020.200792

vol. 15, no. 4, pp. 366-375, Oct.-Dec., 2013. [in Ukrainian].

[16] J. A. Jones, "An introduction to FAIR", *Trustees of Norwich University*, pp. 67, 2005.

[17] B. Ya. Kornienko, Yu. O. Maksimov, and N. M. Marutovska, "Information risk management applications", *Zakhyst informatsii,* no. 4, pp. 60-64, 2012. [in Ukrainian].

O. B. Danchenko, *D.Sc., professor,*
e-mail: elen danchenko@rambler.ru
E. V. Lanskykh, *Ph.D., associate professor,*
e-mail: yevhenlanskykh@gmail.com
O. V. Semko, *M.Sc.*
e-mail: semkoinga77@gmail.com
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

INFORMATION RISKS OF THE DIGITAL FORMAT

The article is devoted to the issue of reliability and protection of information resources, possible negative consequences when risk situations arise. The authors have made an attempt to define the essence and content of the concept of information risk in the conditions of the digital revolution and new technologies, noted the need for a comprehensive approach to the identification and analysis of information risks, reducing negative consequences in case of risk events. Particular attention is paid to information risks as a component of risks arising from the use of different information technologies.

Losses from information risks can be material (in the form of damages, lawsuits, etc.), and can be viewed through the prism of intangible losses (in the form of loss of trust or, in general, reputation). The main task of information security professionals is to apply timely and complete assessment of IT risks using methodological bases of risk management. Organizations must determine their strategy in information security in order to further manage their risks effectively.

In the article the authors give an example of analysis, estimation, probability matrix and possible influence of risk events in the process of digitization. To help combat IT risks in the information technology market, software has been developed to provide adequate management by information flows and IT risks, including Risk Advisor, COBRA, KONDOR +, Proteus Enterprise, OCTAVE, as well as Digital Security Office, RiskManager, Oracle Crystal Ball, @Risk, Risk Watch.

It is difficult to imagine what other risks an organization and society will face in the near future in the way of digitization. In this sense, an attempt to find ways and opportunities to safely overcome potential threats, based on trends and priorities which are dictated by the market and society, is quite promising.

Keywords: *information risk, digital transformation, risk management, classification, information technologies.*

DOI: 10.24025/2306-4412.3.2020.200792

УДК 519.87

[0000-0003-4043-5300] **А. В. Гончаров,** *к.т.н., доцент,*
[0000-0002-9296-6827] **С. О. Могілей,** *аспірант*
Черкаський державний технологічний університет
б-р Шевченка, 460, Черкаси, 18006, Україна

РЕАЛІЗАЦІЯ МУЛЬТИМОДАЛЬНИХ ТРАНСПОРТНИХ ЗАДАЧ В РІЗНИХ ПРОГРАМНИХ СЕРЕДОВИЩАХ

У статті виконано постановку та реалізацію мультимодальної транспортної задачі за допомогою таких програмних засобів, як MS Excel, Mathcad та Matlab. Проаналізовано відмінності та особливості алгоритмів реалізації мультимодальної та класичної транспортних задач в цих середовищах програмування. На основі модельних даних продемонстровано ідентичність результатів, отриманих з використанням різних програмних пакетів.

Ключові слова: *мультимодальна транспортна задача, опорний план, критерій оптимізації, цільова функція.*

Вступ. Класична транспортна задача полягає у відшуканні оптимального плану транспортних перевезень з пунктів відправки до пунктів доставки вантажів за критерієм мінімальної собівартості. Якщо в постановці такої задачі врахувати наявність кількох видів транспорту (що функціонують «паралельно»), то таку задачу називають мультимодальною.

Класичні задачі оптимізації, в тому числі транспортні, так само, як і задачі інтермодальних, мультимодальних та змішаних перевезень, є предметом вивчення багатьох вітчизняних та зарубіжних науковців [1-11]. В їхніх дослідженнях такі задачі розглядаються, насамперед, з точки зору розробки спеціалізованого та вузькопрофільного програмного забезпечення (програмних додатків), які дають змогу автоматизувати процес реалізації відповідної задачі та прийняти оптимальне управлінське рішення.

Розв'язувати класичну транспортну задачу можна за допомогою різних програмних засобів. Так, зокрема, реалізації цієї задачі в програмному середовищі MS Excel присвячено доволі велику кількість сучасних досліджень [12-14]. Основним механізмом реалізації в цьому випадку виступає спеціальна надбудова «Пошук рішення» (англ. Solver), яка дає можливість одразу отримати оптимальний план транспортних перевезень при заданих початкових обмеженнях задачі.

Схожий підхід застосовується і при реалізації класичної транспортної задачі за допомогою Mathcad [15]. В цьому випадку буде використовуватися вбудована функція Minimize (за аналогією з цільовою функцією собівартості, що мінімізується).

Крім того, ще одним доволі поширеним програмним засобом реалізації задач подібного типу є середовище Matlab. В дослідженні [16] подано лістинги програм, що реалізують класичну транспортну задачу за допомогою найбільш відомих методів. У цій роботі буде використано зведення транспортної задачі до задачі лінійного програмування, а її реалізація проведена за допомогою функції Linprog.

Метою цієї роботи є дослідження можливостей різних програмних середовищ (на прикладі MS Excel, Mathcad та Matlab) реалізовувати саме мультимодальну транспортну задачу за допомогою наявних вбудованих механізмів.

Постановка мультимодальної транспортної задачі. Мультимодальна транспортна задача полягає у відшуканні оптимального плану транспортних перевезень за наявності кількох видів транспорту: наприклад, автомобільного, залізничного та водного. Критерієм оптимізації в рамках цієї транспортної задачі є найменша сумарна собівартість перевезень вантажів [17].

Математична формалізація цієї задачі є наступною:

$$S = \sum_{i,j=1}^{m,n} a_{ij} x_{ij} + \sum_{i,j=1}^{m,n} b_{ij} y_{ij} + \sum_{i,j=1}^{m,n} c_{ij} z_{ij} \to \min, \quad (1)$$

де $i = \overline{1,n}$, $j = \overline{1,m}$ – n пунктів відправки та m пунктів доставки відповідно;

x_{ij}, y_{ij}, z_{ij} – кількість одиниць товару, що перевозиться з i-го пункту відправки до j-го

DOI: 10.24025/2306-4412.3.2020.215516

пункту доставки відповідно автомобільним, залізничним та водним транспортом (шукані величини);

a_{ij}, b_{ij}, c_{ij} – вартість перевезення одиниці товару з *i*-го пункту відправки до *j*-го пункту доставки відповідно автомобільним, залізничним та водним транспортом;

S – функція собівартості.

В загальному випадку ця задача є закритою, оскільки до неї можна звести відкриту задачу, що суттєво не вплине на алгоритм її розв'язання. Інакше кажучи, сума потреб пунктів доставки дорівнює сумі запасів у пунктах відправки. Так само можна обмежитися розглядом задачі мінімізації, зважаючи на те, що вона є двоїстою до задачі максимізації.

Таким чином, множина обмежень *D* задачі складається з таких рівнянь та нерівностей:

$$D: \begin{cases} \sum\limits_{i,j=1}^{m,n} x_{ij} \le x; \sum\limits_{i,j=1}^{m,n} y_{ij} \le y; \sum\limits_{i,j=1}^{m,n} z_{ij} \le z; \\ \sum\limits_{j=1}^{m} N_j = \sum\limits_{i,j=1}^{m,n} (x_{ij} + y_{ij} + z_{ij}) = \sum\limits_{i=1}^{n} M_i, \end{cases} \quad (2)$$

де x, y, z – сумарна вантажопідйомність парків автомобільного, залізничного та водного видів транспорту відповідно;

M_i, N_j – величини запасів в *i*-му пункті відправки та потреб *j*-го пункту доставки відповідно.

Розглянемо реалізацію цієї задачі за допомогою MS Excel, Mathcad та Matlab.

Реалізація поставленої задачі за допомогою MS Excel. Заповнимо таблиці вартостей перевезень (в умовних грошових одиницях) з пунктів відправки до пунктів доставки по кожному виду транспорту (таблиці 1-3).

Таблиця 1 – **Вартість перевезень автомобільним транспортом (ум. гр. од.)**

23	45	11
43	12	3
7	9	65

Таблиця 2 – **Вартість перевезень залізничним транспортом (ум. гр. од.)**

21	42	8
48	10	1
19	8	37

Таблиця 3 – **Вартість перевезень річковим транспортом (ум. гр. од.)**

27	39	9
40	14	2
13	6	46

Початкові опорні плани по кожному з видів транспорту залишаємо порожніми. Встановимо наступні обмеження за кількістю запасів і потреб пунктів відправки та доставки: (4200; 5300; 3700) та (3100; 4600; 5500).

За допомогою надбудови «Пошук рішення», врахувавши обмеження за величинами запасів та потреб, а також умову невід'ємності елементів планів перевезень, отримаємо наступні плани (в умовних одиницях) по кожному виду транспорту (таблиці 4-6).

Таблиця 4 – **План перевезень автомобільним транспортом (ум. од.)**

0	0	0
0	0	0
3100	0	0

Таблиця 5 – **План перевезень залізничним транспортом (ум. од.)**

0	0	4200
0	4000	1300
0	0	0

DOI: 10.24025/2306-4412.3.2020.215516

Таблиця 6 – **План перевезень річковим транспортом (ум. од.)**

0	0	0
0	0	0
0	600	0

Водночас загальна собівартість перевезень становитиме 100 200 ум. од. Зазначимо, що сумарний план транспортних перевезень буде наступним (таблиця 7):

Таблиця 7 – **Сумарний план перевезень (ум. од.)**

0	0	4200
0	4000	1300
3100	600	0

Отже, за допомогою відповідної надбудови функціонал MS Excel дає можливість знайти оптимальні плани транспортних перевезень при реалізації поставленої задачі. Сам алгоритм реалізації мультимодальної транспортної задачі доволі незначно відрізняється від аналогічного алгоритму, що застосовується при розв'язанні відповідної класичної задачі.

Реалізація мультимодальної транспортної задачі в середовищі Mathcad. Матриці вартостей перевезень на автомобільному, залізничному та річковому видах транспорту виглядатимуть наступним чином (рисунок 1):

$$Ca := \begin{pmatrix} 23 & 45 & 11 \\ 43 & 12 & 3 \\ 7 & 9 & 65 \end{pmatrix} \qquad Cr := \begin{pmatrix} 21 & 42 & 8 \\ 48 & 10 & 1 \\ 19 & 8 & 37 \end{pmatrix} \qquad Cw := \begin{pmatrix} 27 & 39 & 9 \\ 40 & 14 & 2 \\ 13 & 6 & 46 \end{pmatrix}$$

Рисунок 1 – Матриці вартостей перевезень по кожному виду транспорту

Далі введемо матриці обмежень за величинами запасів та потреб у пунктах відправки і доставки (рисунок 2):

$$A := \begin{pmatrix} 4200 \\ 5300 \\ 3700 \end{pmatrix} \qquad B := \begin{pmatrix} 3100 \\ 4600 \\ 5500 \end{pmatrix}$$

Рисунок 2 – Матриці обмежень запасів та потреб

Будуємо цільову функцію оптимізації та вводимо початкові (нульові) значення для елементів опорних планів по кожному виду транспорту (рисунок 3):

$$f(x,y,z) := \sum_{i=0}^{2} \sum_{j=0}^{2} \left[\left(Ca_{i,j} \cdot x_{i,j} \right) + \left(Cr_{i,j} \cdot y_{i,j} \right) + \left(Cw_{i,j} \cdot z_{i,j} \right) \right]$$

$$x_{2,2} := 0 \qquad y_{2,2} := 0 \qquad z_{2,2} := 0$$

Рисунок 3 – Цільова функція задачі

DOI: 10.24025/2306-4412.3.2020.215516

Описуємо блок Given, в якому враховуємо обмеження, наведені в матрицях A та B, а також умову невід'ємності елементів опорних планів (рисунок 4):

$$\sum_{j=0}^{2}\left(x_{0,j}+y_{0,j}+z_{0,j}\right)=A_0 \qquad \sum_{j=0}^{2}\left(x_{1,j}+y_{1,j}+z_{1,j}\right)=A_1 \qquad \sum_{j=0}^{2}\left(x_{2,j}+y_{2,j}+z_{2,j}\right)=A_2$$

$$\sum_{i=0}^{2}\left(x_{i,0}+y_{i,0}+z_{i,0}\right)=B_0 \qquad \sum_{i=0}^{2}\left(x_{i,1}+y_{i,1}+z_{i,1}\right)=B_1 \qquad \sum_{i=0}^{2}\left(x_{i,2}+y_{i,2}+z_{i,2}\right)=B_2$$

$$x \geq 0 \qquad y \geq 0 \qquad z \geq 0$$

Рисунок 4 – Опис обмежень поставленої задачі

За допомогою функції Minimize отримаємо плани перевезень на автомобільному, залізничному та річковому видах транспорту окремо (рисунок 5).

$$V := \text{Minimize}(f, x, y, z)$$

$$V = \begin{pmatrix} \{3,3\} \\ \{3,3\} \\ \{3,3\} \end{pmatrix}$$

$$V_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 3.1 \times 10^3 & 0 & 0 \end{pmatrix} \qquad V_1 = \begin{pmatrix} 0 & 0 & 4.2 \times 10^3 \\ 0 & 4 \times 10^3 & 1.3 \times 10^3 \\ 0 & 0 & 0 \end{pmatrix} \qquad V_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 600 & 0 \end{pmatrix}$$

Рисунок 5 – Плани перевезень по кожному виду транспорту

Сумарний план перевезень та їх загальна вартість відображені на рисунку 6.

$$V_0 + V_1 + V_2 = \begin{pmatrix} 0 & 0 & 4.2 \times 10^3 \\ 0 & 4 \times 10^3 & 1.3 \times 10^3 \\ 3.1 \times 10^3 & 600 & 0 \end{pmatrix} \qquad f\left(V_0, V_1, V_2\right) = 1.002 \times 10^5$$

Рисунок 6 – Сумарний план перевезень та мінімальне значення цільової функції

Таким чином, функціональних можливостей програмного середовища Mathcad виявляється достатньо для повноцінного розв'язання мультимодальної транспортної задачі. З другого боку, отримати результат її реалізації в явному вигляді не видається можливим через його «багатомірність». Втім, особливої потреби в цьому немає, оскільки значення мають лише розв'язки в розрізі кожного з видів транспорту окремо.

Реалізація мультимодальної транспортної задачі в середовищі Matlab. Розв'язання досліджуваної задачі в цьому середовищі програмування виглядатиме наступним чином (лістинги 1 і 2):

DOI: 10.24025/2306-4412.3.2020.215516

Лістинг 1

Мультимодальна транспортна задача (М-файл)

```
% Розв'язання транспортної задачі
% за допомогою зведення її до задачі лінійного програмування
clc
clear all
% Вектор коефіцієнтів
    % автомобільний
f = [23; 45; 11; 43; 12; 3; 7; 9; 65;
    % залізничний
     21; 42; 8; 48; 10; 1; 19; 8; 37;
    % річковий
     27; 39; 9; 40; 14; 2; 13; 6; 46];
% Бінарні коефіцієнти в обмеженнях
Aeq = [1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0
       0 0 0 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0
       0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 1 1 1

       1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0
       0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0
       0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1];
% "Праві" частини обмежень
Beq = [4200; 5300; 3700; 3100; 4600; 5500];
% Нульовий вектор для задання умови невід'ємності
% обсягів перевезень
lb = zeros(27, 1);
% Функція обчислення шуканих обсягів перевезень
[x,fval] = linprog(f, [], [], Aeq, Beq, lb);
Xopt = reshape(x,3,9)'
Fopt = fval
```

Лістинг 2

Мультимодальна транспортна задача (командне вікно)

```
Optimal solution found.


Xopt =

           0           0           0
           0           0           0
        3100           0           0
           0           0        4200
           0        4000        1300
           0           0           0
           0           0           0
           0           0           0
           0         600           0


Fopt =

      100200
```


DOI: 10.24025/2306-4412.3.2020.215516

Основна особливість такого способу реалізації полягає в тому, що матриці розцінок перевезень мають бути подані у вигляді векторів коефіцієнтів, що, в свою чергу, передбачає досить громіздку форму введення початкових даних задачі. На противагу цьому сам процес розв'язання реалізується за допомогою лише однієї вбудованої функції.

Висновки. Досліджено основні підходи до реалізації класичних транспортних задач у таких програмних продуктах, як MS Excel, Mathcad та Matlab. Виконано постановку та реалізацію мультимодальної транспортної задачі в межах функціоналу відповідного програмного забезпечення.

В ході реалізації поставленої задачі в наведених програмних середовищах на основі модельних даних було продемонстровано ідентичність отриманих результатів. Ці результати вказують на можливість розширення постановки задачі, а саме: врахування більшої кількості засобів доставки вантажу, збільшення розмірності задачі – тобто кількості пунктів відправки та доставки, переходу до аналогічних задач з багатьма критеріями оптимізації тощо.

Що стосується проблеми вибору найбільш оптимального програмного забезпечення для розв'язання мультимодальних транспортних задач, то на поточному етапі дослідження важко знайти вагомі аргументи на користь тієї чи іншої програми (з розглянутих вище). Очевидно, що при реалізації подібних задач з великими масивами даних вкрай важливим буде критерій швидкодії алгоритму цієї реалізації. Таким чином, варто буде використати програмне забезпечення з «відкритим» кодом – на відміну від вбудованих функцій, це дасть можливість провести більш глибинний аналіз ефективності різних (чисельних) методів розв'язання мультимодальних транспортних задач.

Список використаних джерел

[1] В. І. Пасічник, Ю. С. Грисюк, та О. В. Пацьора, "Ефективність інтермодальних перевезень як елемент забезпечення високої якості транспортних послуг", *Управління проектами, системний аналіз і логістика. Технічна серія*, вип. 12, с. 125-131, 2013.

[2] Р. С. Щербина, "Методологічний аспект основних елементів змішаних перевезень експортних вантажів", *Збірник наукових праць ДЕТУТ. Серія: Транспортні системи та технології*, вип. 26-27, с. 242-249, 2015.

[3] C. C. Lin, and S. W. Lin, "Two-stage approach to the intermodal terminal location problem", *Computers and Operations Research*, vol. 67, pp. 113-119, 2016. doi: https://doi.org/10.1016/j.cor.2015.09.009.

[4] M. Slavova-Nocheva, "Competitiveness of the transport market in Bulgaria", *Ikonomicheski Izsledvania*, vol. 21 (3), 2012.

[5] В. В. Сторожев, "Оптимізація параметрів транспортних засобів в мультимодальних системах доставки вантажів", автореф. дис. канд. техн. наук, Одес. нац. морський ун-т, Одеса, 2008.

[6] H. Ayed, C. Galvez-Fernandez, Z. Habbas, and D. Khadraoui, "Solving time-dependent multimodal transport problems using a transfer graph model", *Computers and Industrial Engineering*, vol. 61, pp. 391-401, 2011. doi: 10.1016/j.cie.2010.05.018.

[7] H. Ayed, Z. Habbas, D. Khadraoui, and C. Galvez-Fernandez, "A parallel algorithm for solving time dependent multimodal transport problem", in *Proc. IEEE Conf. on Intelligent Transportation Systems (ITSC)*, 2011, pp. 722-727. doi: 10.1109/ITSC.2011.6082973.

[8] J. E. Flórez, Á. Torralba, J. García, C. Linares López, Á. García-Olaya, and D. Borrajo, "TIMIPLAN: An application to solve multimodal transportation problems", in *Scheduling and Planning Applications Workshop (SPARK)*, 2010.

[9] R. Zelenika, D. Sever, S. Zebec, and B. Pirš, "Logistic operator – fundamental factor in rational production of services in multimodal transport", *Promet – Traffic – Traffico*, 2005.

[10] D. Elias, B. Nadler, F. Nadler, and G. Hauger, "OPTIHUBS – multimodal hub process optimization by means of micro simulation", *Transportation Research Procedia*, 2016. doi: 10.1016/j.trpro.2016.05.098.

[11] J. García, J. E. Florez, Á. Torralba, D. Borrajo, C. L. López, Á. García-Olaya, and J. Sáenz, "Combining linear programming and automated planning to solve intermodal transportation problems", *European Journal of Operational Research*, vol. 227, pp. 216-226, 2013.

DOI: 10.24025/2306-4412.3.2020.215516

[12] L. Chandrakantha, "Using excel solver in optimization problems", *John Jay College of Criminal Justice of CUNY*, 2014, pp. 42-49.
[13] O. Ezeokwelume, "Solving linear programming problems and transportation problems using excel solver", *International Journal of Scientific & Engineering Research*, vol. 7, iss. 9, pp. 134-142, 2016.
[14] B. Vats, and A. KumarSingh, "Solving transportation problem using excel solver for an optimal solution", *MIT International Journal of Mechanical Engineering*, vol. 6, no. 1, pp. 18-20, 2016.
[15] V. Ovcharuk, N. Vovkodav, T. Kryvets, and I. Ovcharuk, "Linear programming in Mathcad on the example of solving the transportation problem", *Scientific Works of NUFT*, vol. 21, iss. 4, pp. 110-117, 2015.
[16] J. Sengamalaselvi, "Solving transportation problem by using Matlab", *International Journal of Engineering Sciences & Research Technology*, no. 6 (1), pp. 374-381, 2017. doi: 10.5281/zenodo.259588.
[17] С. В. Заболотній, та С. О. Могілей, "Оптимізація методу побудови опорних планів мультимодальної транспортної задачі", *Технологічний аудит та резерви виробництва*, № 2 (45), с. 15-20, 2019. doi: https://doi.org/10.15587/2312-8372.2019.154561

References

[1] V. I. Pasichnyk, Yu. S. Grysyuk, and O. V. Patsyora, "Efficiency of intermodal transport as an element of ensuring high quality of transport services", *Upravlinnja proektamy, systemnyj analiz i logistyka. Tehnichna serija,* iss. 12, pp. 125-131, 2013. [in Ukrainian].
[2] R. S. Shherbyna, "Methodological aspect of the main elements of mixed transportation of export cargo", *Zbirnyk naukovyh prac' DETUT. Serija: Transportni systemy ta tehnologii'*, iss. 26-27, pp. 242-249, 2015. [in Ukrainian].
[3] C. C. Lin, and S. W. Lin, "Two-stage approach to the intermodal terminal location problem", *Computers and Operations Research*, vol. 67, pp. 113-119, 2016. doi: https://doi.org/10.1016/j.cor.2015.09.009.
[4] M. Slavova-Nocheva, "Competitiveness of the transport market in Bulgaria", *Ikonomicheski Izsledvania*, vol. 21 (3), 2012.
[5] V. V. Storozhev, "Optimization of vehicle parameters in multimodal cargo delivery systems", Ph.D. thesis, Odessa Nat. Marine Univ., Odessa, 2008. [in Ukrainian].
[6] H. Ayed, C. Galvez-Fernandez, Z. Habbas, and D. Khadraoui, "Solving time-dependent multimodal transport problems using a transfer graph model", *Computers and Industrial Engineering*, vol. 61, pp. 391-401, 2011. doi: 10.1016/j.cie.2010.05.018.
[7] H. Ayed, Z. Habbas, D. Khadraoui, and C. Galvez-Fernandez, "A parallel algorithm for solving time dependent multimodal transport problem", in *Proc. IEEE Conf. on Intelligent Transportation Systems (ITSC)*, 2011, pp. 722-727. doi: 10.1109/ ITSC.2011.6082973.
[8] J. E. Flórez, Á. Torralba, J. García, C. Linares López, Á. García-Olaya, and D. Borrajo, "TIMIPLAN: An application to solve multimodal transportation problems", in *Scheduling and Planning Applications Workshop (SPARK)*, 2010.
[9] R. Zelenika, D. Sever, S. Zebec, and B. Pirš, "Logistic operator – fundamental factor in rational production of services in multimodal transport", *Promet – Traffic – Traffico*, 2005.
[10] D. Elias, B. Nadler, F. Nadler, and G. Hauger, "OPTIHUBS – multimodal hub process optimization by means of micro simulation", *Transportation Research Procedia*, 2016. doi: 10.1016/ j.trpro.2016.05.098.
[11] J. García, J. E. Florez, Á. Torralba, D. Borrajo, C. L. López, Á. García-Olaya, and J. Sáenz, "Combining linear programming and automated planning to solve intermodal transportation problems", *European Journal of Operational Research*, vol. 227, pp. 216-226, 2013.
[12] L. Chandrakantha, "Using excel solver in optimization problems", *John Jay College of Criminal Justice of CUNY*, 2014, pp. 42-49.
[13] O. Ezeokwelume, "Solving linear programming problems and transportation problems using excel solver", *International Journal of Scientific & Engineering Research*, vol. 7, iss. 9, pp. 134-142, 2016.
[14] B. Vats, and A. KumarSingh, "Solving transportation problem using excel solver for an optimal solution", *MIT International Journal of Mechanical Engineering*, vol. 6, no. 1, pp. 18-20, 2016.
[15] V. Ovcharuk, N. Vovkodav, T. Kryvets, and I. Ovcharuk, "Linear programming in

DOI: 10.24025/2306-4412.3.2020.215516

Mathcad on the example of solving the transportation problem", *Scientific Works of NUFT*, vol. 21, iss. 4, pp. 110-117, 2015.

[16] J. Sengamalaselvi, "Solving transportation problem by using Matlab", *International Journal of Engineering Sciences & Research Technology*, no. 6 (1), pp. 374-381, 2017. doi: 10.5281/zenodo.259588.

[17] S. V. Zabolotnii, and S. O. Mogilei, "Optimization of the method of constructing reference plans of multimodal transport problem", *Tekhnolohichnyi audyt ta rezervy vyrobnytstva*, no. 2 (45), pp. 15-20, 2019. doi: https://doi.org/10.15587/2312-8372.2019.154561. [in Ukrainian].

A. V. Honcharov, *Ph.D., associate professor,*
S. O. Mogilei, *Ph.D. student*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

IMPLEMENTATION OF MULTIMODAL TRANSPORT TASKS IN DIFFERENT SOFTWARE ENVIRONMENTS

Multimodal problem is the classic transport problem that assumes simultaneous (parallel) application of several means of cargo delivery. It means, the criterion for optimizing a multimodal transportation problem is, as compared with the classic one, the minimal ultimate transportation cost, whereas there are more than one accessible means of cargo delivery. Today's scientific description, both in the Ukrainian and foreign investigations, considers the problems of this type insufficiently, therefore the issue of testing their models and methodologies is quite significant. Apparently, the calculations of these problems appear to be as well complicated, so it is rather correct to employ for it special programming methods.

The article regards the multimodal transport problem presented and realized through different programming means, among them MS Excel, Mathcad and Matlab. The transportation means are presented as equal to three, since we regard the automobile, the railroad and the river deliveries. The problem requires, for various programming performances, the standard (built-in) functions and methods like Solver for MS Excel, Minimize for Mathcad (as well as Given block) and Linprog for Matlab (using a multimodal transport problem modified into a linear programming problem).

The research has resulted in the analysis of peculiar algorithms for multimodal and classic transport problems, the above mentioned programming methods. Also, the model data has demonstrated identical results obtained through the application of various programming means. The obtained algorithms for solving the multimodal transport problem can be expanded for a larger, than three, number of means for transport delivery.

In perspective, the research holds to solve the multicriteria, at least, two-criteria, multimodal transport problem that would assume more than one criterion of optimization. One of these would be minimizing the level of risks in transportation logistics.

Keywords: *multimodal transport problem, reference plan, optimization criterion, objective function.*

DOI: 10.24025/2306-4412.3.2020.215516

УДК 004.4 / С88

[0000-0001-5657-9144] **О. Б. Данченко[1],** *д.т.н., доцент,*
[0000-0002-7435-3533] **О. Є. Іларіонов[2],** *к.т.н., доцент,*
oleg.ilarionov@knu.ua
[0000-0003-1986-6130] **Г. В. Красовська[2],** *к.т.н., доцент,*
Т. С. Короткова[2], *магістрант*
[1] Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2] Київський національний університет імені Тараса Шевченка
вул. Б. Гаврилишина, 24, м. Київ, 04118, Україна

РОЗРОБКА СИСТЕМИ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЛЮДИНИ У ВІДЕОПОТОЦІ З ДОПОВНЕНОЮ РЕАЛЬНІСТЮ

Розглянуто проблему розпізнавання обличчя людини у відеопотоці з доповненою реальністю, досліджено сучасний стан питання. Вивчено загальний процес розпізнавання обличчя та основні поняття доповненої реальності. Проведено аналіз сучасних підходів до розв'язання задачі розпізнавання обличчя, виявлено сильні та слабкі сторони використовуваних методів. Проведено пошук методу, інваріантного до масштабування, зміни сцени, поворотів голови, зміни освітленості, аксесуарів та зміни емоцій. Розроблено алгоритм, архітектуру та саму програмну систему, що розв'язує задачу розпізнавання обличчя людини у відеопотоці з доповненою реальністю. Методом для виявлення облич обрано гістограму направлених градієнтів (від англ. "Histogram of Oriented Gradients", HOG), розпізнавання облич розроблено на основі згорткової нейронної мережі архітектури ResNet34. Проведено експериментальні дослідження, систему протестовано як на одному, так і на кількох обличчях одночасно. Визначено оцінки якості розпізнавання розробленої програмної системи – побудова ROC-кривих, які показують залежність кількості помилкових спрацьовувань алгоритму розпізнавання (false positive) від точності розпізнавання (true positive rate), та обчислення AUC (від англ. "Area Under the Curve"). При розпізнаванні одного обличчя досягнуто значення AUC 0,95, при розпізнаванні кількох облич (максимум чотирьох) – 0,83.

Ключові слова: *розпізнавання обличчя, доповнена реальність, попередня обробка зображення, виявлення обличчя, виявлення ключових ознак.*

Вступ. Технологія розпізнавання облич використовується у багатьох галузях: безпека, медицина, розважальна індустрія і т. д. Багато з нас щодня користуються цією технологією (наприклад, щоб розблокувати свій смартфон). Проте розпізнавання обличчя, поєднане з технологіями доповненої реальності, може встановити нову планку, наприклад, використовувати Augmented Reality (AR) (з англ. – «доповнена реальність») і Artificial Intelligence (AI) (з англ. – «штучний інтелект»), щоб поєднати зображення людського обличчя з камери та інформацію про реальну людину. Можливості AR-технологій дуже великі – вони можуть знайти застосування чи не в усіх сферах нашого життя. Доповнена реальність збагатить та покращить якість комунікації, отримання інформації та обміну нею, ведення підприємницької діяльності. Віртуальний екскурсовод проведе нас по руїнах замку, та ще й покаже сценку, як саме цей замок розвалили, і яким він був до того. Мобільний додаток з AR допоможе позбутися паперових інструкцій, провівши інтерактивне заняття з користування щойно придбаним предметом. Віртуальна примірочна одягу, аксесуарів та макіяжу дасть можливість легше створити новий образ. Щоб алгоритм візуального відстеження був корисним у реальних сценаріях, він повинен бути в змозі обробляти та долати випадки, коли зовнішній вигляд об'єкта змінюється від кадру до кадру. Значна і швидка зміна зовнішнього вигляду внаслідок шуму, оклюзії, фонової перешкоди, пози, масштабу та змін освітленості є основними проблемами, які потрібно подолати детектору [1]. Саме тому важливо розуміти, який із методів розпізнавання буде найбільш ефективним для тієї чи іншої задачі

DOI: 10.24025/2306-4412.3.2020.200277

Мета дослідження. Сьогодні існує багато методів розпізнавання облич. При їх розробці бралися до уваги вимоги щодо розміру сформованих біологічних шаблонів облич, швидкості їх формування й порівняння та якості розпізнавання як основного критерію. Є кілька основних підходів. Наразі метрика Хеммінга для порівняння бінарних шаблонів є найшвидшою [2-3]. Проте, у свою чергу, кращі показники якості в розпізнаванні облич демонструють глибокі згорткові нейронні мережі, що використовують небінарні біометричні шаблони [4-5].

Раніше було запропоновано ряд підходів до формування біометричних шаблонів зображень облич, які можуть використовуватися для біометричної верифікації або ідентифікації осіб [6-7]. Однак практично всі останні результати в розпізнаванні осіб було отримано за допомогою використання глибинних згорткових нейронних мереж [8]. Існує багато підходів до навчання мереж для розпізнавання людей – мережі можуть бути навчені як за класифікацією, коли кожній особі відповідає свій клас, так і за принципом сіамських мереж на основі попарного порівняння для найкращої верифікації. Також є реалізації, що об'єднують обидва підходи. Найкращі сучасні результати на базі облич Labeled Faces in the Wild (LFW) отримано композицією глибоких мереж, навчених на різних фрагментах (патчах) осіб [9]. Проте використання об'єднання кількох архітектур нейронних мереж вимагає значно більших обчислювальних ресурсів, у той час як деякі однопатчеві мережі можуть бути досить ефективними. Як біометричний шаблон зазвичай використовується вихідний сигнал одного з шарів, найчастіше це останній прихований шар у мережі. Для зниження розмірності отриманих шаблонів зазвичай використовується метод головних компонент, а порівняння шаблонів здійснюється за допомогою косинусної або L2-відстані [9].

У роботі Ю. В. Візільтера, В. С. Горбацевича, А. В. Воротнікова, Н. А. Костромова [8] на основі згорткової мережі з хешуючим шаром було отримано згорткову нейронну мережу з хешуючим лісом (ЗНМХЛ). Ця модифікація дає можливість змінювати розмір шаблона, що використовується, від надкомпактних (десятки байтів) до великих (сотні байтів) шаблонів. Відмінність у них буде в якості розпізнавання. Це дало змогу будувати компактні біометричні шаблони (250 байт) з одночасно покращеними (порівняно з базовою мережею) показниками верифікації (98,14 %) та ідентифікації (91 % rank-1) на базі осіб LFW, а також ультракомпактні (25 байт) шаблони. З другого боку, описаний підхід дає можливість будувати великі біометричні шаблони, що дають змогу досягати високої якості розпізнавання – ЗНМХЛ з 2000 кодуючими 7-бітними деревами досягає 98,59 % точності верифікації 93 % rank-1 на LFW (надбавка більш ніж у 3 % в rank-1 щодо вихідної базової архітектури мережі).

У роботі J. Betty, I. Bülthoff, B. J. Mohlera, I. M. Thorntonb [10] було досліджено, як впливають на якість розпізнавання різні фактори. У результаті досліджень було отримано три основні висновки:

- ефективність розпізнавання є найкращою, коли спостерігач безпосередньо взаємодіє з цільовим об'єктом, досліджуючи його з різних сторін;

- якість розпізнавання покращується, коли спостерігається зміна кута погляду по вертикалі на об'єкт дослідження. Ця маніпуляція не так добре досліджена, як типові повороти по горизонталі, але в цьому випадку спостерігається, що витрати ресурсів збільшуються при взаємодії з людьми у сидячому положенні або стоячи на якомусь підвищенні;

- віртуальний сценарій можна використовувати для вивчення систем розпізнавання обличчя.

Метою статті є аналіз підходів до побудови технології розпізнавання облич у відеопотоці в системах з доповненою реальністю шляхом вивчення моделей, методів та алгоритмів розпізнавання обличчя людини, виявлення сильних та слабких сторін існуючих рішень, вибору найкращого сполучення методів виявлення та розпізнавання облич та доведення ефективності запропонованого підходу на основі гістограми направлених градієнтів та згорткової нейронної мережі архітектури ResNet34 для задачі розпізнавання облич у відеопотоці в системах з доповненою реальністю.

Виклад основного матеріалу

Основні поняття доповненої реальності. Доповнена реальність – це технологія, що розміщує в навколишньому світі графічні або текстові об'єкти у режимі реального часу за допомогою комп'ютерних пристроїв [11].

DOI: 10.24025/2306-4412.3.2020.200277

Необхідно розрізняти доповнену, віртуальну та змішану реальності. У доповненій реальності віртуальні об'єкти переносяться в реальний світ, доповнюють дійсне середовище. У віртуальній реальності світ не є справжнім, хоча й може бути схожим на нього. Він створюється за допомогою комп'ютерних систем, сприйняття якого наразі забезпечує сенсорна система людини (зорові, тактильні й інші відчуття). Змішана, або гібридна реальність поєднує ці поняття. Так, світ, у який занурюється людина, створюється за допомогою VR (з англ. "Virtual Reality" – віртуальна реальність), а додання віртуальних елементів забезпечується AR. Отже, віртуальна реальність взаємодіє лише з користувачами, а доповнена реальність – з усім зовнішнім світом [12].

Створення доповненої реальності у загальному випадку відбувається наступним чином: пристрій, оснащений доповненою реальністю (спеціальні окуляри, смартфон тощо), використовуючи камеру, захоплює об'єкт фізичного світу; за допомогою програмного забезпечення пристрою у режимі реального часу проводиться розпізнавання об'єкта, накладання відповідної цифрової інформації та виведення кінцевого зображення на пристрій візуалізації.

Основні поняття процесу розпізнавання обличчя. Загальний процес розпізнавання облич складається з виявлення облич, відстеження, вилучення ознак, зменшення розмірів та відповідного розпізнавання (рисунок 1).

Більш детальний опис цього процесу викладено нижче зі специфікою застосування до розробленої системи.

Опис програмного застосування. Для поставленої задачі було розроблено наступну цільову функцію (1):

$$\sum_{i=0}^{k} BestMatch_i\left(Descr\left(Detec\left(T_{features}\right)\right), Descr\left(Detec\left(E_{features}\right)\right)\right) \rightarrow max,$$

$$BestMatch_i = \left\{ \overrightarrow{Match_{t,e}} \mid t.dist < 0{,}7 \cdot e.dist, t = \overline{0, n-1}, e = \overline{0, n-1} \right\} \quad (1)$$

де T – тестове зображення, E – еталонне зображення, $T_{features}$ і $E_{features}$ – особливості T і E відповідно, *Detec*() – детектор, *Descr*() – дескриптор, $\overrightarrow{Match_{t,e}}$ – вектор відповідностей між дескрипторами зображень T та E, $BestMatch_i$ – кількість відповідностей між дескрипторами, що задовольняють обмеженню, *dist* – відстань між дескрипторами.

Вхідними даними розробленої програми є база даних облич людей та інформації про них. У результаті виконання програми знаходиться найкращий збіг обличчя, що відображається у відеопотоці, з обличчям із бази даних та відтворення інформації про цю людину на відео шляхом використання доповненої реальності.

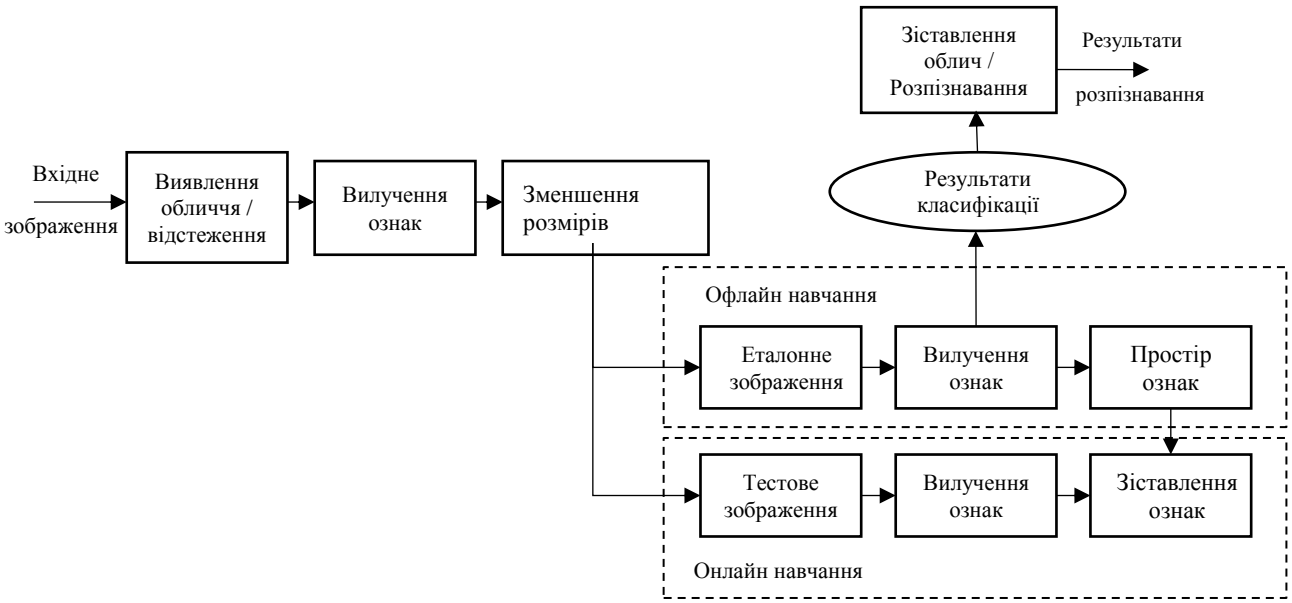


Рисунок 1 – Загальний процес розпізнавання обличчя людини

DOI: 10.24025/2306-4412.3.2020.200277

Для розпізнавання обличчя у програмі використовується наступний алгоритм:

1. Знайти всі обличчя на зображенні з відеопотоку.
2. Розпізнати кожне обличчя, навіть якщо воно знаходиться під кутом або під поганим освітленням.
3. Визначити унікальні риси обличчя, що відрізняють одну людину від іншої, наприклад форма обличчя, розмір очей тощо.
4. Порівняти знайдені особливості цього обличчя з усіма людьми, обличчя яких система вже знає, щоб зрозуміти, хто зараз зображений на відео.

З'єднавши цей ланцюг дій, ми отримаємо розв'язок поставленої задачі (рисунок 2).

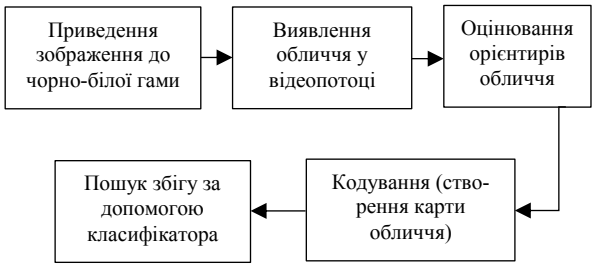


Рисунок 2 – Загальний алгоритм розробленої програми

Розглянемо кожний крок детальніше.

Крок 1. Пошук усіх облич

На першому етапі алгоритму потрібно знайти всі обличчя. Для цього було використано гістограму направлених градієнтів (від англ. "Histogram of Oriented Gradients", HOG).

Спочатку зображення приводиться до чорно-білої гами, тому що для пошуку обличчя дані про колір є надлишковими. Потім кожний піксель розглядається окремо і порівнюється з сусідніми. Мета цих дій – виявити, наскільки темним є поточний піксель порівняно з сусідніми. Потім малюється стрілка, що вказує, в якому напрямку зображення стає темнішим (градієнт). Таким чином, алгоритм отримує градієнтне зображення обличчя. Для кожної людини напрямок зміни кольору на обличчі від темного до світлого буде однаковим при будь-якому освітленні.

Крок 2. Оцінювання орієнтирів обличчя

Після знаходження обличчя необхідно розібратися з проблемою, коли обличчя, повернуті у різні сторони, здаються комп'ютеру різними людьми.

Для розв'язання цієї задачі кожне зображення перетворюється так, щоб очі і губи завжди знаходилися в якомусь визначеному місці. Це спрощує задачу порівняння облич на наступних кроках. Для цього використовується алгоритм оцінювання орієнтирів обличчя (від англ. – "face landmarks estimation").

Основна ідея полягає в тому, що ми відмічаємо 68 особливих точок (які називаються орієнтирами), що існують на кожному обличчі, – верхня частина підборіддя, зовнішня точка кожного ока, внутрішня точка кожної брові тощо. Після цього алгоритм машинного навчання знаходить ці 68 точок на кожному обличчі.

Коли відомо, де очі, а де рот, ми можемо повертати, масштабувати і зсувати зображення так, щоб очі та рот були якомога краще відцентровані. Для цього було використано афінні перетворення.

Крок 3. Кодування обличчя

Потрібно знайти спосіб зняти кілька основних вимірів з кожного обличчя, які можна було б порівняти з найближчими відомими вимірами та знайти найбільш схоже обличчя. Наприклад, можна змінити розмір кожного вуха, відстань між очима, довжину носа тощо.

Проблема в тому, що виміри, які здаються людям очевидними (наприклад колір очей), насправді не мають сенсу для комп'ютера, що роздивляється окремі пікселі зображення. Один із підходів – дозволити комп'ютеру самому зробити виміри того, що йому потрібно. Алгоритми глибинного навчання самостійно визначають, які частини обличчя потрібно вимірювати, а які – ні.

Розв'язок полягає у створенні згорткової нейронної мережі, яка може створювати 128 вимірів для кожного обличчя. 128 вимірів кожного обличчя називають картою. Ідея перетворення масиву необроблених даних, наприклад зображення, в список генерованих комп'ютером чисел вкрай важлива для машинного навчання.

Процес навчання згорткової нейронної мережі для отримання мапи облич (кодування обличчя) потребує великої кількості даних і великих обчислювальних потужностей. Саме тому було використано модель, навчену на кількох наборах даних упродовж кількох тижнів. Таким чином, залишається тільки пропустити зображення облич через готову навчену нейронну мережу, щоб отримати 128 вимірювань для кожного обличчя.

Крок 4. Пошук інформації людини за кодуванням

DOI: 10.24025/2306-4412.3.2020.200277

На останньому етапі потрібно знайти людину в базі відомих для розробленої програми людей, виміри обличчя якої найближчі до отриманих даних у реальному часі. Це робиться за допомогою класифікатора, що вимірює відстань між значеннями і визначає, наскільки вони схожі.

Для розпізнавання обличчя було обрано згорткову нейронну мережу архітектури ResNet34 [Residual Network (дослівно — «залишкова мережа»)]. ResNet має наступні переваги над базовими нейронними мережами, цим самим усуваючи їх основні недоліки [13]:

1. ResNet – глибинна нейронна мережа.

Згідно з загальною теоремою апроксимації ми знаємо, що мережа прямого поширення з одним шаром може відтворити будь-яку функцію. Проте шар має бути великим, через що нейронна мережа може бути схильною до перенавчання, що дасть погані результати. Для розв'язання цієї проблеми мережева архітектура має бути більш глибинною. ResNet може бути побудована як зі 100, так і з 1000 шарів.

2. ResNet долає проблему зникнення градієнта.

Глибинні мережі важко тренувати через проблему зникнення градієнта – оскільки градієнт повертається назад до більш ранніх шарів, повторне множення може зробити градієнт нескінченно малим. У результаті, оскільки мережа стає глибшою, її продуктивність стає насиченою або швидко починає знижуватись.

Завдяки наявності залишкових блоків (рисунок 3, [13]) ResNet мережа може ігнорувати градієнт деяких підмереж і просто пересувати градієнт від вищих шарів до нижніх шарів без будь-якої модифікації. Це означає, що ResNet може просто передати градієнт з останнього шару, наприклад шару 151, безпосередньо до першого шару.

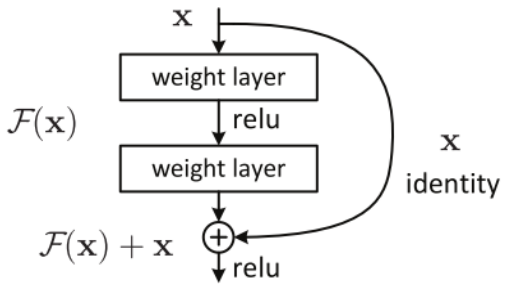


Рисунок 3 – Залишковий блок нейромережі ResNet

Для реалізації алгоритму обрано високорівневу мову програмування загального призначення Python. Для розпізнавання облич людей було використано бібліотеку face_recognition. Вона надає зручний API, який, у свою чергу, використовує бібліотеки OpenFace, dlib, OpenCV. Також ця бібліотека представляє методи роботи з якісно навченими моделями для визначення face landmarks і нейронною мережею ResNet34.

Спроектовану архітектуру системи розпізнавання обличчя у відеопотоці з доповненою реальністю зображено на рисунку 4.

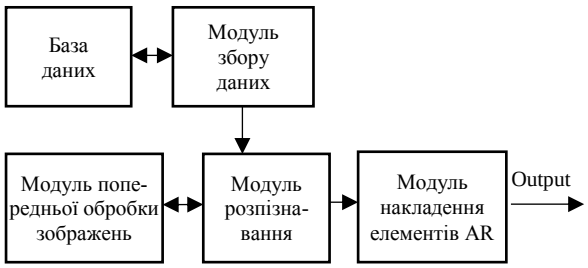


Рисунок 4 – Архітектура системи розпізнавання обличчя у відеопотоці з доповненою реальністю

Розглянемо мережу ResNet34 (нейромережа на архітектурі ResNet з 34 шарами) на рисунку 5 [13].

У першому шарі ResNet використовує згортку 7x7 з кроком 2 для зменшення вхідного сигналу у два рази (від англ. "downs-?mpling"), подібно шару агрегування (від англ. "pooling"). Потім йдуть три блоки ідентичності (або залишкові шари), після чого кількість пікселів вхідного зображення знову зменшується у два рази. Шар семплінгу (зменшення зображення) також є згортковим шаром, але не з'єднується з блоком ідентичності. Ці блоки архітектури повторюються аналогічним чином кілька разів.

Останній шар – це шар усередненого агрегування (від англ. "average pooling"), який створює 1000 карт властивостей (для даних ImageNet) і середнє значення для кожної карти об'єктів. Результатом буде 1000-мірний вектор, який потім подається безпосередньо в шар Softmax, тому він повнозв'язний (від англ. "fully connected") [13]. Основне призначення функції softmax полягає в перетворенні (ненормалізованого) виводу одиниць K (який, наприклад, представлений у вигляді вектора

DOI: 10.24025/2306-4412.3.2020.200277

K елементів) повнозв'язного шару у розподіл ймовірностей (нормалізований вихід), який часто представлений як вектор K елементів, кожен з яких знаходиться між 0 та 1 (ймовірність), а сума усіх цих елементів дорівнює 1 (розподіл ймовірності).

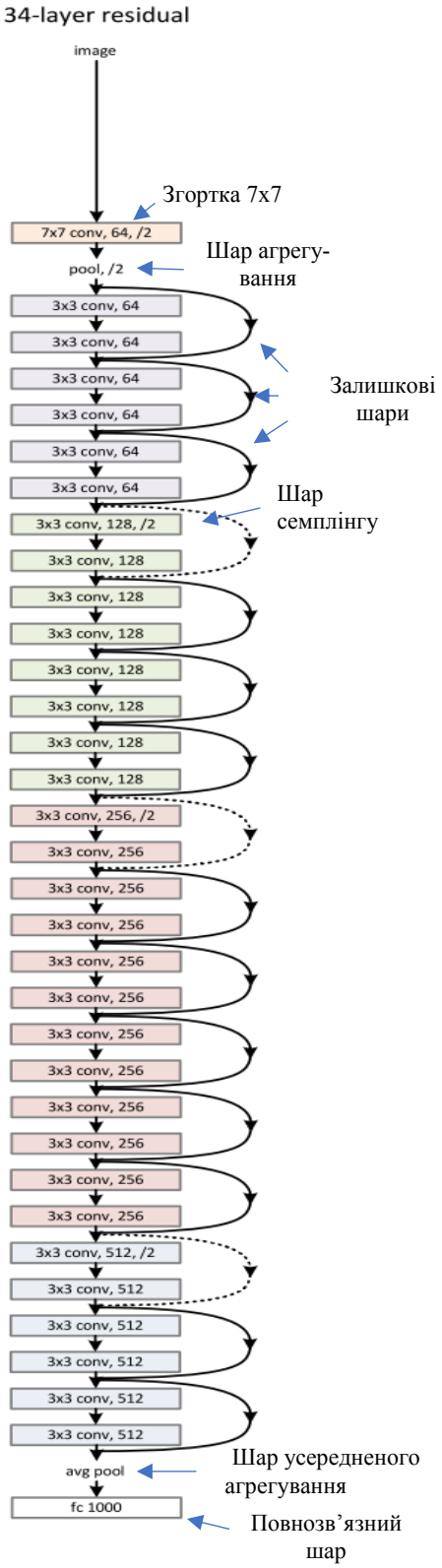


Рисунок 5 – Архітектура ResNet з 34 шарами

У випадку задачі класифікацією *i*-й елемент вектора, що створюється функцією softmax, відповідає ймовірності входу мережі, що належить до *i*-го класу.

DOI: 10.24025/2306-4412.3.2020.200277

Результати досліджень і їх обговорення. Розроблена програмна система, призначена для розпізнавання обличчя людини у відеопотоці з доповненою реальністю, показала прийнятні результати.

Додаток правильно розпізнає обличчя, наявне у базі даних, в умовах різного освітлення, повороту голови, за наявності аксесуарів, закриття деяких частин обличчя, зміни емоцій тощо, аналогічно – для розпізнання кількох облич одночасно. Система тестувалася на 520 прикладах: чотири людини окремо та разом у різних комбінаціях за різних умов освітлення, шумів, перешкод, аксесуарів, емоцій.

Для оцінювання якості детектування за допомогою розробленої програмної реалізації використовується показник, що дорівнює відношенню площі перетину прямокутника, отриманого в результаті детектування, і прямокутника з розмітки до площі їх об'єднання (від англ. "Intersection over Union", IoU). Таким чином, вважається, що обличчя виявлено правильно, якщо цей показник перевищує певний поріг. В іншому випадку приймається, що обличчя не виявлено. Спрацьовування алгоритму детектування на області, де обличчя відсутнє, вважається помилковим спрацьовуванням.

На підставі наведеного показника здійснюється побудова ROC-кривої (рисунки 6, 7), яка показує залежність кількості помилкових спрацьовувань алгоритму детектування (false positive) від точності детектування (true positive rate).

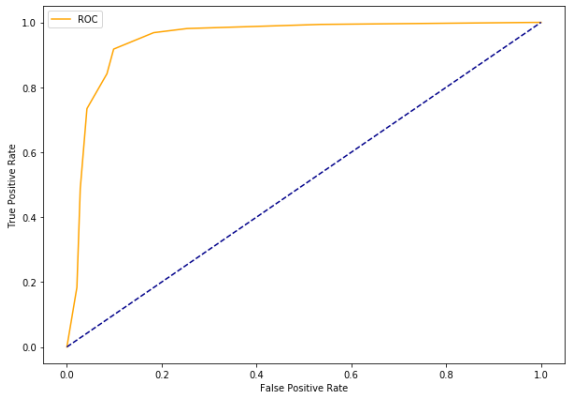


Рисунок 6 – ROC-крива при розпізнаванні одного обличчя, AUC=0,95

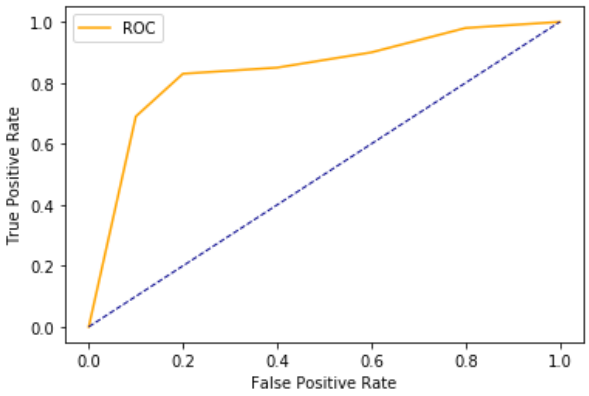


Рисунок 7 – ROC-крива при розпізнаванні кількох облич (максимум чотирьох), AUC=0,83

Висновки. Застосування нейромережі на архітектурі ResNet з відповідними налаштуваннями для детектування та розпізнавання обличчя людини у відеопотоці з доповненою реальністю є хорошим вибором – цей метод інваріантний до масштабування, зміни сцени, поворотів голови, зміни освітленості, аксесуарів та зміни емоцій.

Експерименти показують стабільні результати. За перешкод, а саме, коли закривається частина обличчя, яка є визначальною для розпізнавання, програма не може визначити, кого зображено, тому що не може порівняти особливі ознаки наявного зображення обличчя та обличчя з бази даних. Система є платформою для подальших розробок. Зокрема, планується проведення експериментальних досліджень з використанням інших методів розпізнавання обличчя у відеопотоці та виконання порівняльного аналізу отриманих результатів, а також створення більш зручного графічного інтерфейсу програми та адаптація для мобільної версії.

Список використаних джерел

[1] P. Sharma, R. N. Yadav, and K. V. Arya, "Pose-invariant face recognition using curvelet neural network", *IET Biometrics*, vol. 3, no. 3, pp. 128-138, 2014.

[2] Y. Gong, S. Lazebnik, A. Gordo, and F. Perronnin, "Iterative quantization: A procrustean approach to learning binary codes for large-scale image retrieval", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, iss. 12, pp. 2916-2929, 2012.

[3] K. Grauman, and R. Fergus, "Learning binary hash codes for large-scale image

DOI: 10.24025/2306-4412.3.2020.200277

search", in *Machine Learning for Computer Vision*, R. Cipolla, S. Battiato, and G. M. Farinella, Eds. Berlin, Heidelberg: Springer, 2013, pp. 49-87.

[4] W. Wang, J. Yang, J. Xiao, S. Li, and D. Zhou, *Face recognition based on deep learning*, Q. Zu, B. Hu, N. Gu, S. Seng, Eds. Human Centered Computing. Springer, 2015.

[5] X. Wu, "Learning robust deep face representation", arXiv preprint, 2015. [Online]. Available: https://arxiv.org/pdf/1507.04844.pdf. Accessed on: April 8, 2020.

[6] D. Chen, X. Cao, F. Wen, and J. Sun, "Blessing of dimensionality: High-dimensional feature and its efficient compression for face verification", *Proc CVPR*, pp. 3025-3032, 2013, doi: 10.1109/CVPR.2013.389.

[7] H.-V. Nguyen, and L. Bai, "Cosine similarity metric learning for face verif-?cation", *10th Asian Conf. on Computer Vision*, Queenstown, New Zealand, Nov. 8-12, 2010, Revised Selected Papers, Part II. [Online]. Available: https://www.researchgate.net/publication/220745463_Cosine_Similarity_Metric_Learning_for_Face_Verification/link/54dcd4880cf25b09b912d2ed/download. Accessed on: April 8, 2020.

[8] Ю. В. Визильтер, В. С. Горбацевич, А. В. Воротников, и Н. А. Костромов, "Идентификация лиц в реальном времени с использованием свёрточной нейронной сети и хэширующего леса", *Компьютерная оптика*, № 2, 2017. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/identifikatsiya-lits-v-realnom-vremeni-s-ispolzovaniem-svyortochnyy-neyronnoy-seti-i-heshiruyuschego-lesa. Дата обращения: Апр. 8, 2020.

[9] Y. Sun, X. Wang, and X. Tang, "Deep learning face representation by joint identification-verification", *Proc. 27th Int. Conf. on Neural Information Processing Systems*, 2014, pp. 1988-1996.

[10] J. Betty, I. Bülthoff, B. J. Mohlera, and I. M. Thornton, "Face recognition of full-bodied avatars by active observers in a virtual environment", *Vision Research*, vol. 157, pp. 242-251, 2019.

[11] P. Milgram, and F. Kishino, "A taxonomy of mixed reality visual displays", *IEICE Transactions on Information and Systems*, vol. 77, no. 12, pp. 1321-1329, 1994. [Online]. Available: https://www.researchgate.net/publication/231514051_A_Taxonomy_of_Mixed_Reality_Visual_Displays. Accessed on: Apr. 8, 2020.

[12] A. Nayyar, B. Mahapatra, D. Le, and G. Suseendran, "Virtual Reality (VR) & Augmented Reality (AR) technologies", *Int. Journal of Engineering & Technology*, vol. 7, pp.156-160 2018. [Online]. Available: https://www.researchgate.net/publication/324745910_Virtual_Reality_VR_Augmented_Reality_AR_technologies_for_tourism_and_hospitality_industry. Accessed on: Apr. 8, 2020.

[13] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition". [Online]. Available: https://arxiv.org/pdf/1512.03385.pdf. Accessed on: Apr. 8, 2020.

References

[1] P. Sharma, R. N. Yadav, and K. V. Arya, "Pose-invariant face recognition using curvelet neural network", *IET Biometrics*, vol. 3, no. 3, pp. 128-138, Sept. 2014.

[2] Y. Gong, S. Lazebnik, A. Gordo, and F. Perronnin, "Iterative quantization: A procrustean approach to learning binary codes for large-scale image retrieval", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, iss. 12, pp. 2916-2929, 2012, doi: 10.1109/TPAMI.2012.193.

[3] K. Grauman, and R. Fergus, "Learning binary hash codes for large-scale image search", in *Machine Learning for Computer Vision*, R. Cipolla, S. Battiato, and G. M. Farinella, Eds. Berlin, Heidelberg: Springer, 2013, pp. 49-87, doi: 10.1007/978-3-642-28661-2_3.

[4] W. Wang, J. Yang, J. Xiao, S. Li, and D. Zhou, "Face recognition based on deep learning", in *Human Centered Computing*, Q. Zu, B. Hu, N. Gu, S. Seng, Eds. Springer, 2015, doi: 10.1007/978-3319-15554-8_73.

[5] X. Wu, "Learning robust deep face representation", arXiv preprint, 2015. [Online]. Available: https://arxiv.org/pdf/1507.04844.pdf. Accessed on: April 8, 2020.

DOI: 10.24025/2306-4412.3.2020.200277

[6] D. Chen, X. Cao, F. Wen, and J. Sun, "Blessing of dimensionality: High-dimensional feature and its efficient compression for face verification", *Proc CVPR*, pp. 3025-3032, 2013, doi: 10.1109/CVPR.2013.389.

[7] H.-V. Nguyen, and L. Bai, "Cosine similarity metric learning for face verif-?cation", *Proc ACCV,* pp.709-720, 2010, doi: 10.1007/978-3-642-19309-5_55.

[8] Yu. V. Vizilter, V. S. Gorbatsevich, A. V. Vorotnikov, and N. A. Kostromov, "Real time face identification using convolutional neural network and hash for-est", *Kompyuternaya optika*, no. 2, 2017. [Online]. Available: https://cyberleninka.ru/article/n/identifikatsiya-lits-v-realnom-vremeni-s-ispolzovaniem-svyortochnyy-neyronnoy-seti-i-heshiruyuschego-lesa. Accessed: April 8, 2020.

[9] Y. Sun, X. Wang, and X. Tang, "Deep learning face representation by joint identification-verification", *Proc. 27th Int. Conf. on Neural Information Processing Systems*, 2014, pp. 1988-1996.

[10] J. Betty, I. Bülthoff, B. J. Mohlera, and I. M. Thornton, "Face recognition of full-bodied avatars by active observers in a virtual environment", *Vision Research*, vol. 157, pp. 242-251, 2019.

[11] P. Milgram, and F. Kishino, "A taxonomy of mixed reality visual displays", *IEICE Transactions on Information and Systems*, vol. 77, no. 12, pp. 1321-1329, 1994. [Online]. Available: https://www.researchgate.net/publication/231514051_A_Taxonomy_of_Mixed_Reality_Visual_Displays. Accessed on: Apr. 8, 2020.

[12]A. Nayyar, B. Mahapatra, D. Le, and G. Suseendran, "Virtual Reality (VR) & Augmented Reality (AR) technologies", *Int. Journal of Engineering & Technology*, vol. 7, pp.156-160 2018. [Online]. Available: https://www.researchgate.net/publication/324745910_Virtual_Reality_VR_Augmented_Reality_AR_technologies_for_tourism_and_hospitality_industry. Accessed on: Apr. 8, 2020.

[13] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition". [Online]. Available: https://arxiv.org/pdf/1512.03385.pdf. Accessed on: Apr. 8, 2020.

O. B. Danchenko[1], *D.Sc., professor,*
O. E. Ilarionov[2], *Ph.D., associate professor,*
oleg.ilarionov@knu.ua
H. V. Krasovska[2], *Ph.D., associate professor,*
T. S. Korotkova[2], *M.Sc.*
[1] Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
[2] Taras Shevchenko National University of Kyiv,
B. Gavrylyshyn st., 24, Kyiv, 04118, Ukraine

DEVELOPMENT OF FACE RECOGNITION SYSTEM IN A VIDEO STREAM WITH AUGMENTED REALITY

In the paper, the problem of face recognition in a video stream with augmented reality is considered. The current state of this problem is investigated. The general process of face recognition and the basic concepts of augmented reality have been studied. The analysis of modern approaches to solving the face recognition problem is carried out, the strengths and weaknesses of the methods used have been found. A search is carried out for a method invariant to scaling, scene changes, head turns, changes in lighting, accessories, and changes in emotions. An algorithm, architecture, and the software system that solves the problem of face recognition in a video stream with the elements of augmented reality have been developed. A histogram of oriented gradients (HOG) is chosen as the method for face detection; face recognition functionality is developed on the basis of the convolutional neural network architecture – ResNet34. Experimental studies are carried out, the system has been tested on both one and several faces simultaneously. Estimate methods of the recognition quality for the developed software system are determined – the plotting of ROC-curves that show the dependence of the number of false positives on the detection accuracy (true positive rate) and measuring AUC. AUC =

DOI: 10.24025/2306-4412.3.2020.200277

0.95 has been achieved during recognition of one face, and AUC = 0.83 – during recognition of several faces (maximum 4).

Statement of the problem. *Investigation and analysis of existing approaches to building face-to-face recognition technology in augmented reality systems by analyzing models, methods and algorithms for human face recognition, identifying strengths and weaknesses of existing solutions, choosing the best combination of detection and recognition methods.*

Analysis of recent research and publications. *Approaches have been proposed for the formation of biometric face image templates that can be used for biometric verification or face identification. However, all recent facial recognition results have been obtained through the use of deep convolutional neural networks. In the work of Yu. V. Visilter et al., a convolutional neural network with a hash forest (ZNMHL), based on a convolutional network with a hash layer, has been obtained. J. Betty et al. have investigated how different factors influence recognition quality.*

The purpose of the article *is to prove the effectiveness of the proposed approach based on the histogram of directed gradients and convolutional neural network architecture ResNet34 for the problem of face recognition in a video stream in augmented reality systems.*

Presenting main material. *The basic concepts of augmented reality are analyzed. The process of face recognition is described. The description of the software for the solution of the problem is given and mathematical model is developed. The algorithm of work of the program of face recognition program developed by authors is detailed. The architecture of face recognition system in augmented reality video stream is designed.*

Results. *A software system designed to recognize human faces in augmented reality video streams has shown satisfactory results. The application correctly recognizes the face, available in the database, in different conditions of lighting, head rotation, with the presence of accessory ditches, the closure of some parts of the face, changes in emotions, etc., similarly for recognizing multiple faces at the same time. The system has been tested on 520 examples: 4 people separately and together in different combinations under different conditions of lighting, noise, interference, accessories, emotions.*

Conclusion. *Applying a neural network to the ResNet architecture with appropriate settings for detecting and recognizing human faces in augmented reality video streams is a good choice – this method is invariant to scaling, scene changes, head turns, light changes, accessories, and emotion changes. The system is a platform for further development. In particular, it is planned to conduct experimental studies using other methods of face recognition in a video stream and to perform a comparative analysis of the results, as well as to create a more convenient graphical interface of the program and adaptation for the mobile version.*

Keywords: *face recognition, augmented reality, image pre-processing, face detection, face landmarks estimation.*

DOI: 10.24025/2306-4412.3.2020.200277

УДК 519.233.5:004.81.056.6(045)

[0000-0003-2388-7321] **О. В. Салієва,** *асистент,*
e-mail: salieva8257@gmail.com
[0000-0002-6303-7703] **Ю. Є. Яремчук,** *д.т.н., професор*
e-mail: yurevyar@vntu.edu.ua
Вінницький національний технічний університет
вул. Хмельницьке шосе, 95, м. Вінниця, 21021, Україна

ДОСЛІДЖЕННЯ ДОСТОВІРНОСТІ ВПЛИВУ ЗАГРОЗ НА РІВЕНЬ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА РЕЗУЛЬТАТАМИ КОГНІТИВНОГО МОДЕЛЮВАННЯ

У роботі проведено дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури, визначеного за сценарним моделюванням на основі когнітивного підходу. Водночас застосовано апарат множинного регресійного аналізу, який дає можливість простежити зв'язок між загрозами та захищеністю досліджуваних систем, оцінивши ступінь ймовірного впливу. Сформовано аналітичні вирази лінійної кореляційної залежності між найвагомішими концептами кожної когнітивної моделі та захищеністю відповідної досліджуваної системи. З метою порівняння впливу загроз на захищеність об'єкта критичної інфраструктури та системи захисту інформації, отриманого за результатами когнітивного моделювання, визначено стандартизовані коефіцієнти регресії та коефіцієнти еластичності. Проведений аналіз отриманих значень цих показників дав змогу підтвердити достовірність впливу загроз на рівень захищеності досліджуваних систем.

Ключові слова: *інформаційна безпека, загрози безпеці, когнітивне моделювання, нечітка когнітивна карта, множинний регресійний аналіз.*

Вступ. Сучасний інформаційний простір зазнає впливу найрізноманітніших загроз, реалізація яких може призвести до вкрай негативних наслідків. Тому дослідження впливу загроз на рівень захищеності систем є актуальним та важливим науковим завданням, яке характеризується високим ступенем невизначеності та складністю строгої формалізації. Для його вирішення доцільно скористатися когнітивним підходом, який базується на побудові нечітких когнітивних карт [1-6]. Так, у роботі [7] автори запропонували методику оцінювання рівня інформаційної безпеки на основі нечіткої когнітивної моделі, яка складається із шести рівнів ієрархії.

Автор праці [8] для проведення аналізу та оцінювання ризиків інформаційній безпеці використав нечітку когнітивну карту і нечітку продукційну модель у складі нечіткої гібридної моделі.

У [9] розглянуто задачу підвищення достовірності оцінок показників забезпечення інформаційної безпеки на основі побудови когнітивних моделей, пов'язаних з процесом формування та розвитку різних типів загроз.

У роботах [10-12] запропоновано та проаналізовано когнітивні моделі для оцінювання рівня захищеності комп'ютерної мережі (КМ), системи захисту інформації (ЗІ) та об'єкта критичної інфраструктури (КІ) відповідно. Визначено найвагоміші загрози і проведено сценарне моделювання, в результаті якого встановлено відносну зміну рівня захищеності досліджуваних систем при впливі кожної із найвагоміших загроз. Достовірність отриманого результату впливу загроз на рівень захищеності КМ підтверджено у роботі [13]. Тому цікавим є проведення аналогічного дослідження відносно систем ЗІ та об'єкта КІ на основі множинного регресійного аналізу[14].

Метою дослідження є встановлення достовірності впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ, отриманого за результатами когнітивного моделювання.

Для досягнення поставленої мети необхідно вирішити такі ***завдання:***

– визначити експериментальні дані за сценарним моделюванням на основі когнітивного підходу;

– для кожної з когнітивних моделей знайти аналітичний вираз лінійної кореляцій-

DOI: 10.24025/2306-4412.3.2020.216251

ної залежності, яка існує між досліджуваними концептами;

– визначити коефіцієнти регресії та коефіцієнти еластичності;

– на основі значень коефіцієнта регресії та коефіцієнта еластичності порівняти вплив найвагоміших концептів на захищеність досліджуваних систем.

Визначення впливу загроз на рівень захищеності системи ЗІ на основі множинного регресійного аналізу

Розглянемо когнітивну модель, запропоновану у роботі [11], для визначення впливу загроз на рівень захищеності системи ЗІ (рисунок 1).

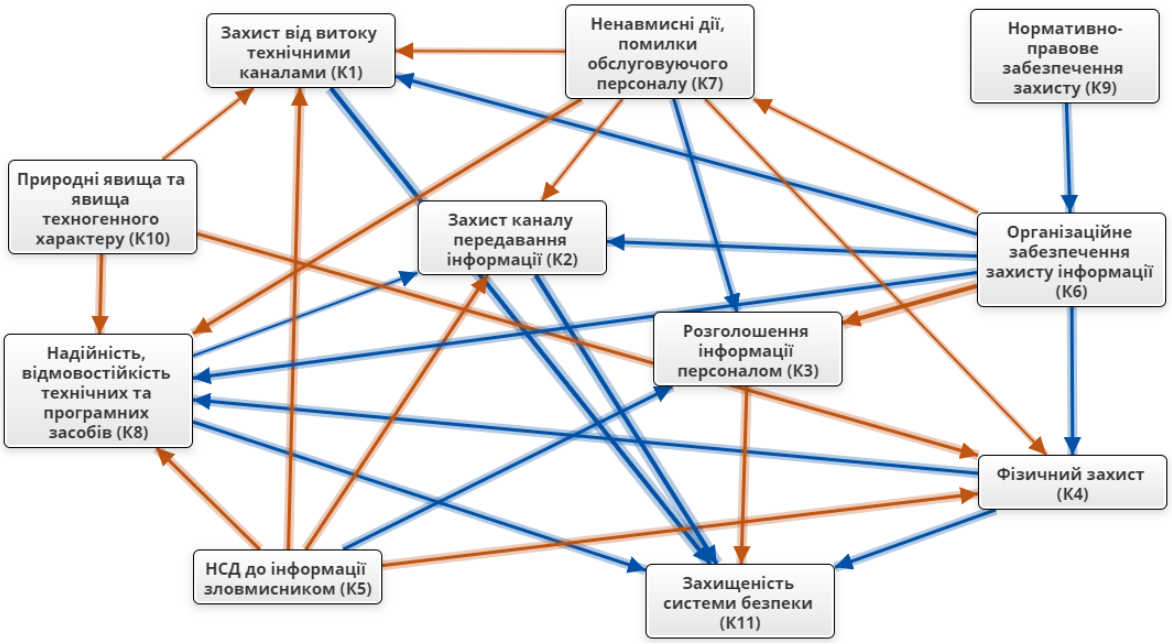


Рисунок 1 – Когнітивна модель дослідження стану захищеності системи ЗІ

У результаті дослідження цієї моделі було визначено її найвагоміші концепти: фізичний захист (K_4), НСД до інформації зловмисником (K_5) та організаційне забезпечення ЗІ (K_6). За допомогою сценарного моделювання встановлено, що при максимально негативному впливі кожного з цих концептів окремо захищеність системи безпеки (K_{11}) погіршиться відповідно на 0,26; 0,23 та 0,07.

Порівняємо вплив найвагоміших концептів на захищеність досліджуваної системи за допомогою регресійного аналізу [15].

Для досягнення поставленої мети змоделюємо десять різних сценаріїв, що відображають відносну зміну захищеності системи безпеки при заданих значеннях обраних концептів (таблиця 1).

Таблиця 1 – **Значення досліджуваних концептів, отримані в результаті сценарного моделювання**

i	K_{i4}	K_{i5}	K_{i6}	K_{i11}
1	1	1	1	0,08
2	0,9	-0,1	0,7	0,13
3	-0,1	-0,3	-0,1	-0,08
4	1	-0,2	1	0,16
5	-0,2	0,3	0,9	-0,04
6	0,8	0,2	-0,3	-0,01
7	1	-0,1	-0,2	0,06
8	-0,3	-0,5	0,8	0,01
9	0,7	0,8	0,9	0,05
10	0,5	-0,3	-0,1	0,02

DOI: 10.24025/2306-4412.3.2020.216251

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_{11} відносно K_4, K_5 та K_6).Позначимо:

$$Y = \begin{pmatrix} 0.08 \\ 0.13 \\ -0.08 \\ 0.16 \\ -0.04 \\ -0.01 \\ 0.06 \\ 0.01 \\ 0.05 \\ 0.02 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0.9 & -0.1 & 0.7 \\ 1 & -0.1 & -0.3 & -0.1 \\ 1 & 1 & -0.2 & 1 \\ 1 & -0.2 & 0.3 & 0.9 \\ 1 & 0.8 & 0.2 & -0.3 \\ 1 & 1 & -0.1 & -0.2 \\ 1 & -0.3 & -0.5 & 0.8 \\ 1 & 0.7 & 0.8 & 0.9 \\ 1 & 0.5 & -0.3 & -0.1 \end{pmatrix}.$$

Для зручності обчислень складемо допоміжну таблицю (таблиця 2).

Таблиця 2 – **Додаткові проміжні дані**

i	K_{i4}	K_{i5}	K_{i6}	y_i	K_{i4}^2	K_{i5}^2	K_{i6}^2	$K_{i4}K_{i5}$	$K_{i4}K_{i6}$	$K_{i5}K_{i6}$	y_iK_{i4}	y_iK_{i5}	y_iK_{i6}
1	1	1	1	0,08	1	1	1	1	1	1	0,08	0,08	0,08
2	0,9	-0,1	0,7	0,13	0,81	0,01	0,49	-0,09	0,63	-0,07	0,117	-0,013	0,091
3	-0,1	-0,3	-0,1	-0,08	0,01	0,09	0,01	0,03	0,01	0,03	0,008	0,024	0,008
4	1	-0,2	1	0,16	1	0,04	1	-0,2	1	-0,2	0,16	-0,032	0,16
5	-0,2	0,3	0,9	-0,04	0,04	0,09	0,81	-0,06	-0,18	0,27	0,008	-0,012	-0,036
6	0,8	0,2	-0,3	-0,01	0,64	0,04	0,09	0,16	-0,24	-0,06	-0,008	-0,002	0,003
7	1	-0,1	-0,2	0,06	1	0,01	0,04	-0,1	-0,2	0,02	0,06	-0,006	-0,012
8	-0,3	-0,5	0,8	0,01	0,09	0,25	0,64	0,15	-0,24	-0,4	-0,003	-0,005	0,008
9	0,7	0,8	0,9	0,05	0,49	0,64	0,81	0,56	0,63	0,72	0,035	0,04	0,045
10	0,5	-0,3	-0,1	0,02	0,25	0,09	0,01	-0,15	-0,05	0,03	0,01	-0,006	-0,002
$\sum$	5,3	0,8	4,6	0,38	5,33	2,26	4,9	1,3	2,36	1,34	0,47	0,07	0,345

Враховуючи дані таблиці 2, знайдемо $(K'K)^{-1}$:

$$(K'K)^{-1} = \begin{pmatrix} 10 & 5.3 & 0.8 & 4.6 \\ 5.3 & 5.33 & 1.3 & 2.36 \\ 0.8 & 1.3 & 2.26 & 1.34 \\ 4.6 & 2.36 & 1.34 & 4.9 \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} 0.34 & -0.28 & 0.18 & -0.24 \\ -0.28 & 0.48 & -0.23 & 0.095 \\ 0.18 & -0.23 & 0.65 & -0.23 \\ -0.24 & 0,095 & -0.23 & 0.44 \end{pmatrix}.$$

Перемножаючи цю матрицю на вектор

$$K'Y = \begin{pmatrix} 0.38 \\ 0.47 \\ 0.07 \\ 0.345 \end{pmatrix}, \text{ отримаємо } b = \begin{pmatrix} -0.07 \\ 0.14 \\ -0.08 \\ 0.092 \end{pmatrix}.$$

Таким чином, рівняння множинної регресії матиме вигляд

$$\hat{y} = -0.07 + 0.14K_4 - 0.08K_5 + 0.092K_6.$$

Для порівняння впливу кожного із найвагоміших концептів на захищеність системи ЗІ використаємо стандартизовані коефіцієнти регресії b'_j та коефіцієнти еластичності E_j $(j = 1, 2, \ldots, p)$:

$$b'_j = b_j \frac{s_{kj}}{s_y}, \qquad (1)$$

де $s_{kj}^2 = \frac{\sum (K_{ij} - \overline{K})^2}{i}$, $s_y^2 = \frac{\sum (y_i - \overline{y})^2}{i}$,

$$E_j = b_j \frac{\overline{K}_j}{\overline{y}}. \qquad (2)$$

Розрахуємо стандартизовані коефіцієнти регресії b'_j (1) і коефіцієнти еластичності E_j (2):

$$b'_1 = 0.14\frac{0.5}{0.07} = 1, \quad b'_2 = -0.08\frac{0.47}{0.07} = -0.54,$$

$$b'_3 = 0.092\frac{0.53}{0.07} = 0.7;$$

DOI: 10.24025/2306-4412.3.2020.216251

$$E_1 = 0.14\frac{0.53}{0.038} = 1.95, \quad E_2 = -0.08\frac{0.08}{0.038} = -0.17,$$

$$E_3 = 0.092\frac{0.46}{0.038} = 1.11.$$

Проаналізувавши значення отриманих показників, можна зробити висновок, що збільшення значень концептів фізичний захист (K_4) та організаційне забезпечення ЗІ (K_6) на одне S_{K4} або S_{K6} посилить у середньому захищеність системи ЗІ відповідно на S_y або на $0.7S_y$, а збільшення цих змінних на 1 % (від своїх середніх значень) приведе у середньому до підвищення рівня захищеності відповідно на 1,95 % та 1,11 %. Водночас збільшення значення концепту НСД до інформації зловмисником (K_5) на S_{K5} призведе до послаблення захищеності у середньому на $0.54S_y$, а збільшення цього концепту на 1 % (від своїх середніх значень) призведе у середньому до зниження рівня захищеності системи ЗІ на 0,17 %.

Таким чином, концепт фізичний захист (K_4) чинить більший вплив на захищеність системи ЗІ, ніж концепт організаційне забезпечення ЗІ (K_6), а концепт НСД до інформації зловмисником (K_5) має найменший вплив серед усіх найвагоміших концептів когнітивної моделі. Це, у свою чергу, підтверджує результати, отримані у роботі [11], внаслідок проведеного сценарного моделювання.

Визначення впливу загроз на рівень захищеності об'єкта КІ за допомогою множинного регресійного аналізу

Подібним чином проаналізуємо результати, отримані внаслідок дослідження когнітивної моделі для визначення рівня захищеності об'єкта КІ [12] (рисунок 2).

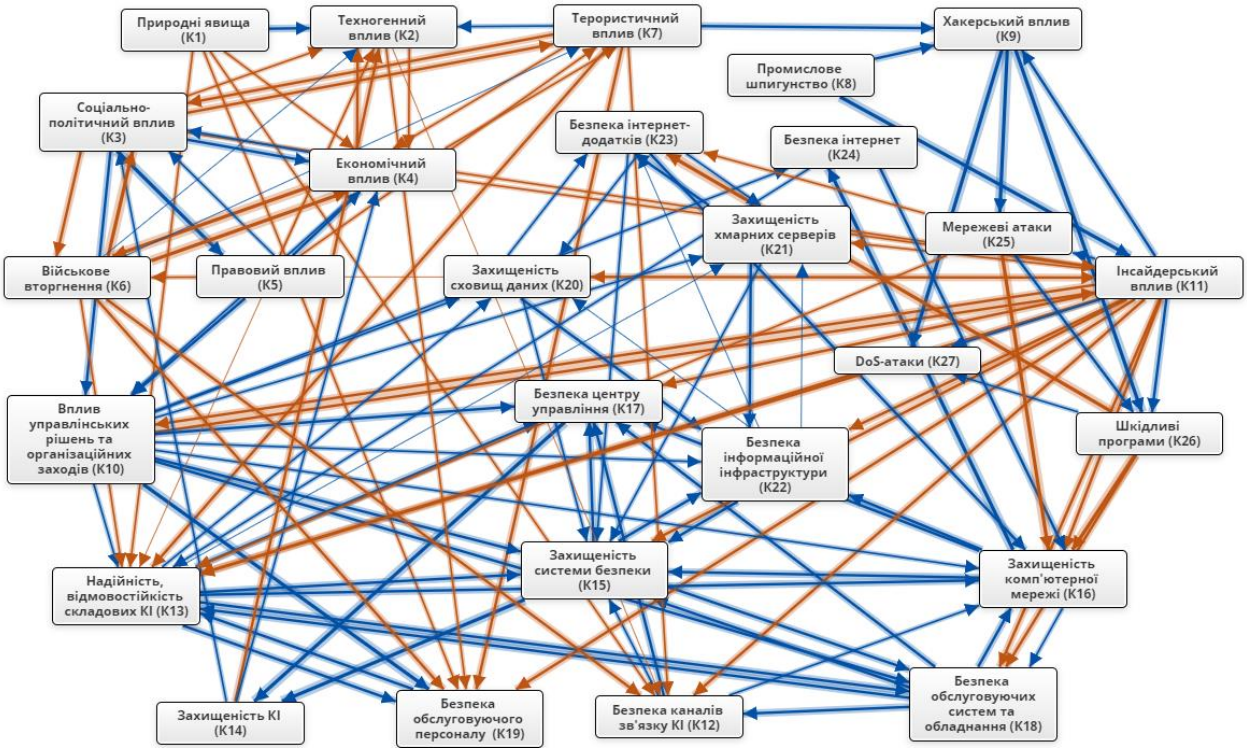


Рисунок 2 – Когнітивна модель для дослідження рівня захищеності об'єкта КІ

У цьому випадку найвагомішими концептами було визначено: інсайдерський вплив (K_{11}), захищеність системи безпеки (K_{15}) і захищеність КМ (K_{16}). Відзначимо, що при максимально негативному впливі кожного з цих концептів захищеність об'єкта КІ (K_{14}) погіршиться на 0,03; 0,44 та 0,06 відповідно.

З метою проведення дослідження змоделюємо 10 різних сценаріїв, що відображають відносну зміну захищеності об'єкта КІ при заданих значеннях найвагоміших концептів (таблиця 3).

DOI: 10.24025/2306-4412.3.2020.216251

Таблиця 3 – **Значення досліджуваних концептів, отримані в результаті сценарного моделювання**

i	K_{i11}	K_{i15}	K_{i16}	K_{i14}
1	-1	1	1	0,02
2	-0,5	-0,7	0,8	-0,31
3	1	0,6	-0,9	-0,11
4	-0,2	-0,9	-0,7	-0,41
5	-0,1	-0,6	-0,2	-0,32
6	-0,9	-1	-1	-0,41
7	0,4	0,3	0,1	-0,11
8	0,6	-0,5	-0,1	-0,36
9	-0,8	-0,4	-0,9	-0,26
10	0,3	-0,8	-0,9	-0,44

Припускаючи, що між концептами існує лінійна кореляційна залежність, знайдемо її аналітичний вираз (рівняння регресії K_{14} відносно K_{11}, K_{15} та K_{16}). Здійснимо позначення:

$$Y = \begin{pmatrix} 0.02 \\ -0.31 \\ -0.11 \\ -0.41 \\ -0.32 \\ -0.41 \\ -0.11 \\ -0.36 \\ -0.26 \\ -0.44 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & -0.5 & -0.7 & 0.8 \\ 1 & 1 & 0.6 & -0.9 \\ 1 & -0,2 & -0.9 & -0,7 \\ 1 & -0.1 & -0.6 & -0.2 \\ 1 & -0.9 & -1 & -1 \\ 1 & 0.4 & 0.3 & 0.1 \\ 1 & 0.6 & -0.5 & -0.1 \\ 1 & -0.8 & -0.4 & -0.9 \\ 1 & 0.3 & -0.8 & -0.9 \end{pmatrix}.$$

Для зручності обчислень складемо допоміжну таблицю (таблиця 4).

Таблиця 4 – **Додаткові проміжні дані**

i	K_{i11}	K_{i15}	K_{i16}	y_i	K_{i11}^2	K_{i15}^2	K_{i16}^2	$K_{i11}K_{i15}$	$K_{i11}K_{i16}$	$K_{i15}K_{i16}$	y_iK_{i11}	y_iK_{i15}	y_iK_{i16}
1	-1	1	1	0,02	1	1	1	-1	-1	1	-0,02	0,02	0,02
2	-0,5	-0,7	0,8	-0,31	0,25	0,49	0,64	0,35	-0,4	-0,56	0,155	0,217	-0,248
3	1	0,6	-0,9	-0,11	1	0,36	0,81	0,6	-0,9	-0,54	-0,09	-0,054	0,099
4	-0,2	-0,9	-0,7	-0,41	0,04	0,81	0,49	0,18	0,14	0,63	0,08	0,36	0,287
5	-0,1	-0,6	-0,2	-0,32	0,01	0,36	0,04	0,06	0,02	0,12	0,032	0,192	0,064
6	-0,9	-1	-1	-0,41	0,81	1	1	0,9	0,9	1	0,369	0,41	0,41
7	0,4	0,3	0,1	-0,11	0,16	0,09	0,01	0,12	0,04	0,03	-0,044	-0,033	-0,011
8	0,6	-0,5	-0,1	-0,36	0,36	0,25	0,01	-0,3	-0,06	0,05	-0,216	0,18	0,036
9	-0,8	-0,4	-0,9	-0,26	0,64	0,16	0,81	0,32	0,72	0,36	0,208	0,104	0,234
10	0,3	-0,8	-0,9	-0,44	0,09	0,64	0,81	-0,24	-0,27	0,72	-0,132	0,352	0,396
$\sum$	-1,2	-3	-2,8	-2,71	4,36	5,16	5,62	0,99	-0,81	2,81	0,342	1,748	1,287

DOI: 10.24025/2306-4412.3.2020.216251

Таким чином, отримаємо обернену матрицю:

$$(K'K)^{-1} = \begin{pmatrix} 10 & -1.2 & -3 & -2.8 \\ -1.2 & 4.36 & 0.99 & -0.81 \\ -3 & 0.99 & 5.16 & 2.81 \\ -2.8 & -0.81 & 2.81 & 5.62 \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} 0.13 & 0.035 & 0.043 & 0.049 \\ 0.035 & 0.28 & -0.088 & 0.1 \\ 0.043 & -0.088 & 0.32 & -0.15 \\ 0.049 & 0{,}1 & -0.15 & 0.29 \end{pmatrix}.$$

Перемножаючи цю матрицю на вектор

$$K'Y = \begin{pmatrix} -2.71 \\ 0.342 \\ 1.748 \\ 1.287 \end{pmatrix}, \text{ матимемо } b = \begin{pmatrix} -0.2 \\ -0.024 \\ 0.22 \\ 0.016 \end{pmatrix}.$$

Отже, складемо рівняння множинної регресії:

$$\hat{y} = -0.2 - 0.024K_{11} + 0.22K_{15} + 0.016K_{16}.$$

За допомогою формул (1)-(2) розрахуємо стандартизовані коефіцієнти регресії b'_j та коефіцієнти еластичності E_j:

$$b'_1 = -0.024\frac{0.65}{0.14} = -0{,}11, \quad b'_2 = 0.22\frac{0.65}{0.14} = 1.02,$$

$$b'_3 = 0.016\frac{0.69}{0.14} = 0.08;$$

$$E_1 = -0.024\frac{-0.12}{-0.271} = -0.01, \quad E_2 = 0.22\frac{-0.3}{-0.271} = 0.24,$$

$$E_3 = 0.016\frac{-0.28}{-0.271} = 0.017.$$

Аналіз розрахованих коефіцієнтів показав, що збільшення значень концептів захищеність системи безпеки (K_{15}) та захищеність КМ (K_{16}) на одне S_{K15} або S_{K16} посилить у середньому захищеність об'єкта КІ відповідно на $1.02S_y$ або на $0.08S_y$, а збільшення цих змінних на 1 % (від своїх середніх значень) приведе у середньому до підвищення рівня захищеності відповідно на 0,24 % та 0,017 %. Водночас збільшення інсайдерського впливу (K_{11}) на S_{K11} призведе до послаблення захищеності в середньому на $0.11S_y$, а збільшення цього концепту на 1 % (від своїх середніх значень) призведе у середньому до зниження рівня захищеності об'єкта КІ на 0,01 %.

Отримані дані підтверджують достовірність результатів, отриманих за сценарним моделюванням у роботі [12], а саме: встановлено, що захищеність системи безпеки (K_{15}) чинить більший вплив на захищеність КІ, ніж захищеність КМ (K_{16}), у той час як зростання інсайдерського впливу (K_{11}) найменшою мірою відобразиться на захищеності КІ.

Результати досліджень. На основі множинного регресійного аналізу визначено вплив найвагоміших загроз на рівень захищеності системи ЗІ та об'єкта КІ.

Зокрема, при дослідженні когнітивної моделі системи ЗІ встановлено, що збільшення значень концептів фізичний захист (K_4) та організаційне забезпечення ЗІ (K_6) на 1 % (від своїх середніх значень) приведе у середньому до підвищення рівня захищеності відповідно на 1,95 % та 1,11 %. Водночас збільшення значення концепту НСД до інформації зловмисником (K_5) знизить у середньому рівень захищеності на 0,17 %.

У свою чергу, дослідження когнітивної моделі об'єкта КІ показало, що підвищення захищеності системи безпеки (K_{15}) та КМ (K_{16}) на 1 % (від своїх середніх значень) підсилить у середньому рівень захищеності відповідно на 0,24 % та 0,017 %, а зростання інсайдерського впливу (K_{11}) призведе до зниження рівня захищеності об'єкта КІ на 0,01 %.

Зазначені результати підтверджують достовірність впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ, отриманого за результатами когнітивного моделювання.

Обговорення результатів. Аналізуючи отримані результати з наявними у роботі [13], слід відзначити, що вони дають можливість дослідити достовірність впливу загроз лише для КМ, у той час як результати цієї роботи підтверджують вірогідність впливу загроз для системи ЗІ та об'єкта КІ. Порівнюючи отримані результати з наявними у роботах [11] та [12], слід також зазначити, що в них визначався вплив загроз на захищеність системи ЗІ та об'єкта КІ на основі сценарного моделювання, тоді як у цьому дослідженні підтверджено достовірність впливу загроз на рівень захищеності досліджуваних систем на основі апарату множинного регресійного аналізу, що у

DOI: 10.24025/2306-4412.3.2020.216251

цілому підвищило рівень достовірності впливу визначених загроз. Окрім того, результати цієї роботи дають можливість спрогнозувати розвиток ситуації для прийняття вчасних та ефективних управлінських рішень, спрямованих на підвищення захищеності системи ЗІ та об'єкта КІ.

Висновки. Таким чином, на основі множинного регресійного аналізу було доведено достовірність впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ, визначеного за результатами когнітивного моделювання. Для кожної із когнітивних моделей знайдено аналітичний вираз лінійної кореляційної залежності, яка існує між найвагомішими її концептами та захищеністю відповідної системи. Розраховано стандартизовані коефіцієнти регресії, які показують, на скільки величин зміниться в середньому залежна змінна при збільшенні тільки однієї незалежної змінної, та коефіцієнти еластичності, за допомогою яких простежується, на скільки відсотків (від середнього значення) зміниться у середньому залежна змінна при збільшенні незалежної змінної на 1 %. Проведений аналіз отриманих значень визначених показників дав змогу підтвердити достовірність впливу загроз на рівень захищеності досліджуваних систем.

Наукова новизна роботи полягає у використанні когнітивних моделей для дослідження впливу загроз на рівень захищеності системи ЗІ та об'єкта КІ.

Практичною цінністю роботи є можливість застосування отриманих результатів для підвищення рівня захищеності досліджуваних систем.

Перспективним є подальше дослідження еволюційного розвитку усієї системи ЗІ при впливі на неї потенційних загроз на основі імпульсного моделювання.

Список використаних джерел

[1] B. Kosko, "Fuzzy cognitive maps", *International Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65-75, 1986.

[2] В. Б. Силов, *Принятие стратегических решений в нечеткой обстановке.* Москва, Россия: ИНПРО, РЕС, 1995.

[3] В. В. Борисов, В. В. Круглов, и А. С. Федулов, *Нечеткие модели и сети*, 2-е изд., стереотип. Москва, Россия: Горячая линия, Телеком, 2012.

[4] О. П. Кузнецов, А. А. Кулинич, и А. В. Марковский, "Анализ влияний при управлении слабоструктурированными ситуациями на основе когнитивных карт", *Человеческий фактор в управлении*, с. 313-344, 2006.

[5] E. Papageorgiou, and I. Salmeron, "Review of fuzzy cognitive maps research during the last decade", *IEEE Trans. on Fuzzy Systems*, vol. 21, no. 1, pp. 66-79, 2013.

[6] А. С. Федулов, "Нечеткие реляционные когнитивные карты", *Известия РАН. Теория и системы управления,* № 1, с. 120-132, 2005.

[7] И. М. Ажмухамедов, и О. М. Князева, "Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности", *Прикаспийский журнал: управление и высокие технологии*, № 3 (31), с. 24-39, 2015.

[8] Е. А. Зюзикова, "Использование нечеткой гибридной модели для анализа рисков информационной безопасности", *Научный журнал «Студенческий»*, № 11 (31), с. 5-7, 2018.

[9] Ш. Г. Магомедов, "Оценка степени влияния сопутствующих факторов на показатели информационной безопасности", *Российский технологический журнал,* т. 5, № 2, с. 47-56, 2017.

[10] О. В. Салієва,та Ю. Є. Яремчук, "Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі", *Реєстрація, зберігання і обробка даних*, т. 21, № 4, с. 28-39, 2019.

[11] О. В. Салієва, та Ю. Є. Яремчук, "Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання", *Безпека інформації*, № 1, с. 42-49, 2020.

[12] О. В. Салієва, та Ю. Є. Яремчук, "Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури", *Безпека інформації*, т. 26, № 2, с. 64-73, 2020.

[13] О. В. Салієва, та Ю. Є. Яремчук, "Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі,

DOI: 10.24025/2306-4412.3.2020.216251

визначеного за сценарним моделюванням на основі когнітивного підходу", *Вісник Вінницького політехнічного інституту,* № 4, с. 98-104, 2020.

[14] Р. М. Літнарович, *Побудова і дослідження математичної моделі за джерелами експериментальних даних методами регресійного аналізу*. Рівне, Україна: МЕГУ, 2011.

[15] Н. Ш. Кремер, *Теория вероятностей и математическая статистика*. Москва, Россия: Юрайт, 2019.

References

[1] B. Kosko, "Fuzzy cognitive maps", *International Journal of Man-Machine Studies*, vol. 24, no. 1, pp. 65-75, 1986.

[2] V. B. Silov, *Strategic decision-making in a fuzzy environment*. Moscow, Russia: INPRO, RES, 1995. [in Russian].

[3] V. V. Borisov, V. V. Kruglov, and A. S. Fedulov, *Fuzzy models and networks*, 2nd ed., Stereotype. Moscow, Russia: Goryachaya liniya. Telekom, 2012. [in Russian].

[4] O. P. Kuznetsov, A. A. Kulinich, and A. V. Markovskiy, "Analysis of influences in the management of weakly structured situations based on cognitive maps", *The human factor in management*, pp. 313-344, 2006. [in Russian].

[5] E. Papageorgiou, and I. Salmeron, "Review of fuzzy cognitive maps research during the last decade", *IEEE Trans. on Fuzzy Systems*, vol. 21, no. 1, pp. 66-79, 2013.

[6] A. S. Fedulov, "Fuzzy relational cognitive maps", *Izvestiya RAN. Teoriyaisistemyupravleniya*, no. 1, pp. 120-132, 2005. [in Russian].

[7] I. M. Azhmukhamedov, and O. M. Knyazeva, "Assessment of the state of security of the organization's data in the context of the possibility of implementing threats to information security", *Prikaspiyski yzhurnal: upravleniye i vysokiye tekhnologii*, no. 3 (31), pp. 24-39, 2015. [in Russian].

[8] E. A. Zyuzikova, "Using a fuzzy hybrid model for the analysis of information security risks", *Nauchnyy zhurnal "Studencheskiy"*, no. 11 (31), pp. 5-7, 2018. [in Russian].

[9] Sh. G. Magomedov, "Assessment of the degree of influence of accompanying factors on information security indicators", *Rossiyskiy tekhnologicheskiy zhurnal*, vol. 5, no. 2, pp. 47-56, 2017. [in Russian].

[10] O. V. Saliieva, and Yu. E. Yaremchuk, "Development of a cognitive model for the analysis of the impact of threats on the level of security of a computer network", *Reiestratsiia, zberihannia i obrobka danykh*, vol. 21, no. 4, pp. 28-39, 2019. [in Ukrainian].

[11] O. V. Saliieva, and Yu. E. Yaremchuk, "Determination of the level of security of the information protection system based on cognitive modeling", *Bezpeka informatsii*, no. 1, pp. 42-49, 2020. [in Ukrainian].

[12] O. V. Saliieva, and Yu. E. Yaremchuk, "Cognitive model for studying the level of security of a critical infrastructure object", *Bezpeka informatsii*, vol. 26, no. 2, pp. 64-73, 2020. [in Ukrainian].

[13] O. V. Saliieva, and Yu. E. Yaremchuk, "Study of the reliability of the impact of threats on the level of security of a computer network, determined by scenario modeling based on a cognitive approach", *Visnyk Vinnytskoho politekhnichnoho instytutu*, no. 4, pp. 98-104, 2020. [in Ukrainian].

[14] R. M. Litnarovych, *Construction and research of a mathematical model based on sources of experimental data by regression analysis*, Rivne, Ukraine: MEGU, 2011. [in Ukrainian].

[15] N. Sh. Kremer, *Probability theory and mathematical statistics*, Moscow, Russia: Yurayt, 2019. [in Russian].

DOI: 10.24025/2306-4412.3.2020.216251

O. V. Saliieva, *assistant,*
e-mail: salieva8257@gmail.com
Yu. E. Yaremchuk, *D.Sc., professor*
e-mail: yurevyar@vntu.edu.ua
Vinnytsia National Technical University,
Khmelnytske Shosse, 95, Vinnytsia, Ukraine

STUDY OF THE RELIABILITY OF THE IMPACT OF THREATS ON THE LEVEL OF SECURITY OF THE INFORMATION PROTECTION SYSTEM AND THE OBJECT OF CRITICAL INFRASTRUCTURE BASED ON THE RESULTS OF COGNITIVE MODELING

The rapid development of information technology has led to new challenges and threats to information security. Therefore, it is important to solve the problem of ensuring the proper level of security of systems when exposed to potential threats. Particular attention is paid to the safety of critical infrastructure and information protection systems, violations of the functioning of which can lead to large-scale consequences of a negative nature.

In this regard, the study of the reliability of the impact of threats on the level of security of the information protection system and the object of critical infrastructure determined by the script modeling on the basis of cognitive approach has been conducted. At the same time, the multiple regression analysis apparatus is used, which allows to trace the link between threats and the security of the investigated systems, assessing the degree of likely impact.

To achieve this goal, based on the researched cognitive models to assess the level of security of information protection systems and the object of critical infrastructure, analytical expressions of linear correlational dependence between the most important concepts of each model separately and the protection of the relevant systems are formed. In order to compare the impact of threats on the security of the information protection system and the object of critical infrastructure, standardized regression coefficients are defined, which show how much values the dependent variable will change on average while increasing only one independent variable and the elasticity ratios by which the average dependent variable will change by one percent. The analysis of the obtained values of these indicators has allowed to confirm the accuracy of the results obtained as a result of script modeling on a cognitive approach.

Keywords: *information security, security threats, cognitive modeling, fuzzy cognitive map, multiple regression analysis.*

DOI: 10.24025/2306-4412.3.2020.216251

УДК 628.3.034.2:628.16.065.2

[0000-0002-5937-167X] **Т. В. Солодовнік,** *к.х.н., доцент*,
e-mail: solodovniktetana@gmail.com
[0000-0001-9469-8240] **І. К. Якименко,** *аспірант*
e-mail: yakimenko97@ukr.net
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ДОСЛІДЖЕННЯ ТА УДОСКОНАЛЕННЯ ФЛОКУЛЯЦІЙНО-КОАГУЛЯЦІЙНИХ ПРОЦЕСІВ ОЧИЩЕННЯ ЗАБАРВЛЕНИХ ПРОМИСЛОВИХ СТОКІВ

Проаналізовано проблеми, які виникають у процесі очищення промислових стічних вод, а також методи їх очищення від різного типу забруднювачів. У ході роботи досліджено вплив застосування природних флокулянтів, які використовували сумісно з типовим коагулянтом, на ступінь та швидкість очищення модельних розчинів, які містять різні типи барвників та зважені частинки. Встановлено переваги та недоліки різних типів природних флокулянтів на прикладі хітозану та альгінату натрію при їх сумісній дії з традиційним коагулянтом – алюмінієм сірчанокислим. При проведенні досліджень з підбору найбільш ефективних реагентів у процесі очищення конкретної стічної води, а також для визначення їх оптимальних доз використовувався метод Джар-тесту. Дослідження складу мутних та забарвлених модельних зразків води проводилося з використанням сучасних методів аналізу: спектрофотометрії та нефелометрії.

Ключові слова: *стічні води, очищення, коагуляція, кольоровість, мутність, коагулянти, флокулянти.*

Вступ. Відомо, що стічні води, які утворюються в результаті діяльності промислових підприємств, характеризуються великими об’ємами утворення, нестійким хімічним складом, вони є небезпечними джерелами забруднення природних вод, а також чинять антропогенне навантаження на навколишнє середовище. В зв’язку з тим, що промислові стоки утворюються несистематично, це створює певні технологічні перешкоди для їх утилізації. Вже доведено, що одним із пріоритетних завдань у вирішенні питання утилізації та знешкодження стічних вод має бути створення оптимального методу очищення для кожного виду виробничих стічних вод. Як приклад можна розглянути підприємства легкої промисловості, де забруднення водоймищ відбувається внаслідок безперервної роботи текстильних фабрик і комбінатів, виробничих дільниць з дублення шкіри тощо.

Щороку одна фабрика витрачає в середньому 350 млн $м^3$ води. Стічні води такого підприємства характеризуються основними забруднюючими речовинами, такими як: миючі засоби (50–120 мг/$дм^3$), завислі речовини (250–400 мг/$дм^3$), барвники, сульфати, фосфати, хлориди, сполуки важких та кольорових металів, легкоспливаючі агресивні речовини.

На території України розташовано близько 28 текстильних комбінатів, кожен з яких щороку витрачає близько 400 млн л води, і з кожним роком ця кількість збільшується, очищення ж цих вод проводять на застарілих очисних станціях, що, в свою чергу, не може гарантувати якісного очищення. В зв’язку з цим актуальним є питання розробки й удосконалення методів очищення стічних вод текстильних підприємств на території України з використанням природних та екологічно безпечних реагентів.

Склад стічних вод та їх властивості оцінюють за результатами санітарно-хімічного аналізу, що включає, поряд зі стандартними хімічними тестами, ряд фізичних, фізико-хімічних і санітарно-бактеріологічних визначень. Мутність – властивість води, яка обумовлена присутністю в ній завислих речовин органічного і мінерального походження. Мутність тісно пов’язана з іншими властивостями води, перш за все, з кольоровістю, запахом і присмаком. Кольоровість – один із органолептичних показників якості стічних вод. Наявність інтенсивної кольоровості різних відтінків – свідоцтво присутності виробничих стічних вод. Для пофарбованих стічних вод визначають інтенсивність кольоровості за розведенням до безкольорової, наприклад 1:400, 1:250 і т. д. [1].

DOI: 10.24025/2306-4412.3.2020.213912

Барвники – органічні сполуки, що характеризуються здатністю інтенсивно поглинати та перетворювати енергію електромагнітних випромінювань (світлову енергію) у видимій і ближніх ультрафіолетових та інфрачервоних областях спектра і застосовані для надання цієї властивості іншим тілам. Водорозчинні барвники, що мають найбільше значення у формуванні складу стічних вод, широко застосовують у легкій промисловості, фарбувально-оброблювальному, текстильному, трикотажному, прядильно-нитковому, трикотажно-панчішному, хутряному, валяльно-войлочному виробництвах. Більша кількість барвників надходить у стічні води від анілінфарбувальної промисловості. Очищення стічних вод від барвників проводять різними методами. В основному застосовують хімічні, фізико-хімічні та біологічні методи.

Вивчення робіт сучасних науковців вказує на постійний розвиток та удосконалення методів очищення стічних вод від барвників у напрямі підвищення їх ефективності, спрощення у виконанні, а також пошуку більш дешевих та безпечних реагентів [2]. Для видалення різного типу барвників зі стічних вод розробляються нові методики та синтезуються нові типи коагулянтів, флокулянтів та адсорбентів.

Дослідниками [3] було розроблено адсорбент на основі нановолокон із поліетилсульфону, який призначений для видалення барвників, та доведено його ефективність на прикладі сорбції барвника метиленового синього з водних розчинів.

Автори [4] досліджували особливості процесів вилучення барвників, а саме бром фенолового синього, при використанні технології флотоекстракції. Відповідно до термодинамічних розрахунків було встановлено, що формування комплексу між іонами барвника та ПАР відбувається самочинно і не потребує накладання зовнішніх сил.

Згідно з проведеним оглядом та аналізом літературних джерел, які включають патенти, монографії та статті зарубіжних і вітчизняних авторів, встановлено, що процес коагуляції, який відбувається за рахунок адсорбційних властивостей коагулянтів та флокулянтів, широко застосовується в технологіях очищення як природних, так і промислових стічних вод від колоїдних частинок, радіонуклідів, фосфатів, барвників і завислих речовин. Встановлено, що найбільш поширеними у використанні є коагулянти, такі як алюміній та заліза сульфати, хлоругід, ферум та алюміній хлорид, і флокулянти, такі як хітозан, насіння Моринги олійної та альгінат натрію [5-10].

Нині розглядаються перспективи вивчення властивостей промислових коагулянтів на основі алюмінію, оскільки вони характеризуються кращими реакційними властивостями та мають менший вплив на пришвидшення корозії апаратури, ніж залізовмісні коагулянти, та комплексну дію коагулянтів з природними флокулянтами, адже вони є екологічно чистими реагентами та більш ефективними, ніж синтетичні, для видалення різних типів барвників.

Процес коагуляції на практиці складається з коагуляції, флокуляції та сепарації. Після коагуляції дестабілізовані колоїди й інші осади утворюють малі агломерати, які потім мають зростати в більші, міцні й компактні пластівці. Цей процес називається флокуляцією і визначається як процес контакту й адгезії, при якому дисперсні частинки потім мають бути відділені методом відстоювання, флотації або фільтрування. Також взято до уваги те, що процес коагуляції сумісний з такими видами очищення, як біологічне, озонування, знезараження та мембранні фільтри, що спрощує його застосування в технологічних схемах [11-14]. При виборі технології очищення стічних вод потрібно також звертати увагу на такі чинники, як кількість і характер забруднень, їх подальше використання, необхідність ступеня очищення тощо.

Метою дослідження є визначення закономірностей та способів удосконалення коагуляційно-флокуляційного очищення при використанні природних флокулянтів сумісно з традиційним коагулянтом.

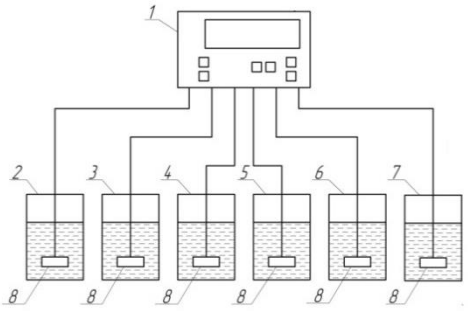
Матеріали та методи дослідження. Об’єктами дослідження були модельні розчини, подібні до стічних вод текстильних підприємств, з середнім ступенем забарвлення і середнім вмістом зважених частинок (вміст барвників та зважених частинок становить 200 мг/дм^3). Для отримання модельних розчинів використовували барвники різних типів, а саме: активний синій, прямий чорний та дисперсний червоно-коричневий. Біла глина косметична застосовувалась для створення мутності. Як реагенти використовували 10 % розчин алюмінійвмісного коагулянту ($Al_2(SO_4)_3 \cdot 18H_2O$), а також 1 % розчини природних флокулянтів: альгінату натрію та хітозану зі ступенем деацетилювання 82 %.

DOI: 10.24025/2306-4412.3.2020.213912

Визначення кольоровості та мутності досліджуваних зразків проводили з використанням спектрофотометра Ulab 102 та мутноміра ТВ 1000W за стандартними методиками [15]. Вимірювання pH розчинів проводили за допомогою іономіра лабораторного І-160МІ.

Для визначення оптимальної дози коагулянту та флокулянтів (Ме/дм^3) застосовували метод пробної коагуляції, так званий «Джар-тест» (JAR-test). Цей метод імітує виробничий процес, що дає змогу визначити ефективну дозу реагентів і оптимальні умови, які потрібні для утворення та осадження пластівців або спливання їх у вигляді осаду. Дослідження води проводиться після відстоювання. За даними досліджень якості обробленої води, що проводилися після відстоювання, обираються та доза реагентів і час, що сприяють утворенню більш щільного осаду з високими седиментаційними властивостями [1].

Для методу пробної коагуляції використовували стаціонарну установку, удосконалену в лабораторії дослідження води кафедри хімічних технологій та водоочищення ЧДТУ [16], схему якої зображено на рисунку 1.



1 – флокулятор Kemira 2000; 2-7 – лабораторні стакани об'ємом 1 дм^3; 8 – механічні мішалки

Рисунок 1 – Лабораторна установка для проведення Джар-тесту

Результати досліджень та їх обговорення

Визначення оптимальної дози коагулянту. Одним із завдань науково-дослідної роботи було визначення мінімальної робочої дози (Ме/дм^3) коагулянту на лабораторній установці (рисунок 1). Шість лабораторних стаканів були заповнені досліджуваними модельними розчинами, в які одночасно було введено коагулянт зі збільшенням дози від 20 до 70 мг/дм^3 з кроком в 10 мг/дм^3. Інтенсивне перемішування зі швидкістю 140 об/хв., що проводили впродовж трьох хвилин, відповідає стадії гідролізу коагулянту. З метою утворення пластівців швидкість перемішування була знижена до 50 об/хв і залишалася сталою впродовж 10 хв.

Осадження пластівців у вигляді осаду відбувається на останній стадії процесу, тобто протягом періоду седиментації. Оцінювання якості очищення зразків на вміст залишкових концентрацій забруднюючих речовин було проведено через 60, 120 та 180 хв після початку седиментації шляхом відбору проб з кожного стакана на одній і тій же глибині відстояного шару.

В процесі візуального спостереження за утворенням та осіданням осаду було встановлено оптимальну дозу коагулянту, яка визначалася для кожного з досліджуваних барвників у присутності зважених частинок. Отримані результати зображено у вигляді гістограм (рисунки 2, 3), які свідчать про те, що найменша доза коагулянту, яка необхідна для ефективного очищення забарвлених розчинів прямим, активним та дисперсним барвниками у присутності зважених частинок каоліну, відповідно становить 40, 50 та 40 мг/дм^3 а ефективне осадження відбувається впродовж двох годин.

Визначення оптимальної дози флокулянтів. Наступним завданням дослідження було визначення оптимальної дози флокулянтів (альгінату натрію і хітозану) при їх комплексній дії з коагулянтом. Для цього шість скляних стаканів було заповнено однаковим об'ємом досліджуваного модельного розчину, і в кожен із них додано оптимальну дозу коагулянту, яку було визначено на попередньому етапі. Перед зменшенням швидкості перемішування до 50 об/хв. в стакани було додано 1 % розчин флокулянта – хітозану від 1 до 20 см^3, що відповідає вмісту хітозану від 10 до 200 мг/дм^3, при цьому перший стакан залишався контрольним. Оцінювання якості очищення проводили через 60, 120 та 180 хв після початку процесу седиментації.

Аналогічно проводили визначення оптимальної дози флокулянта – альгінату натрію. Для цього було додано 1 % розчин флокулянта від 1 до 20 см^3, що відповідає вмісту діючої речовини від 10 до 200 мг/дм^3, при цьому контрольним залишали перший стакан.

DOI: 10.24025/2306-4412.3.2020.213912

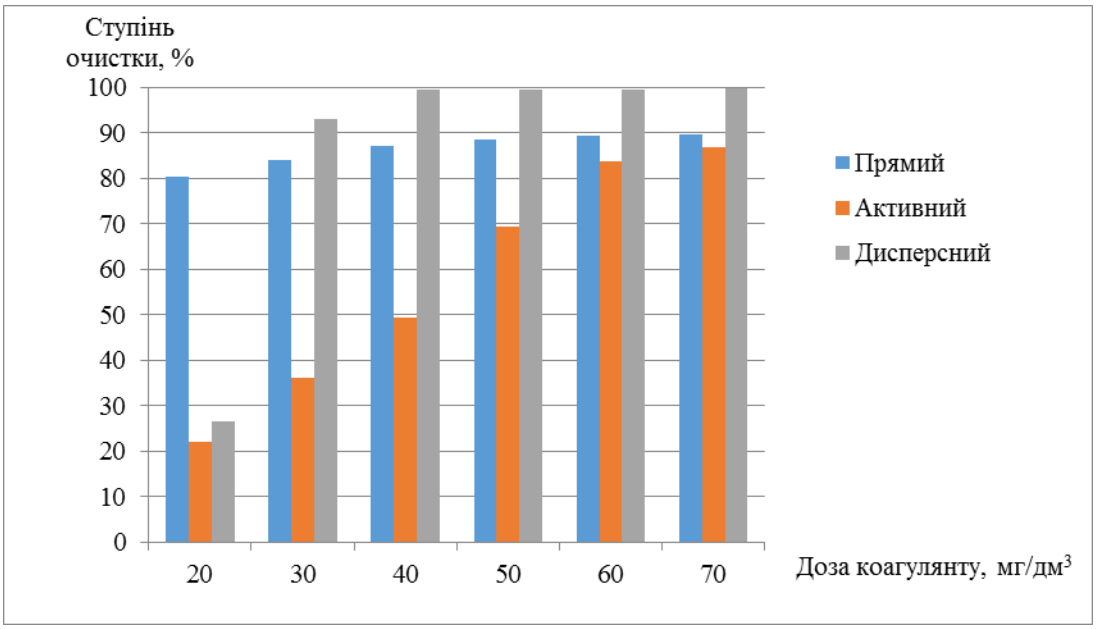


Рисунок 2 – Залежність ступеня очистки забарвлених модельних розчинів від барвників у присутності зважених частинок каоліну від дози коагулянту

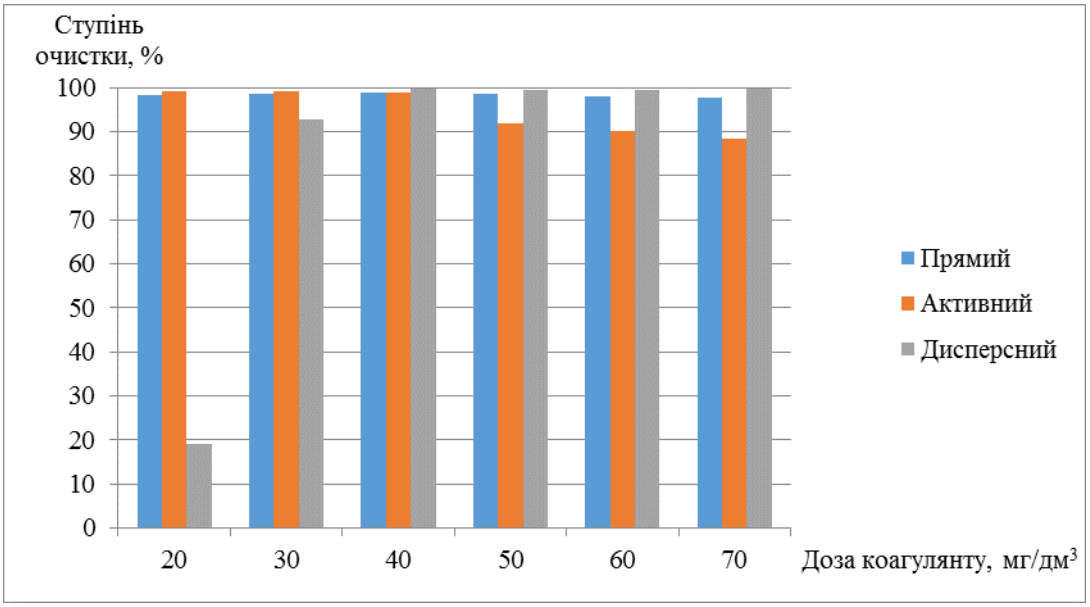


Рисунок 3 – Залежність ступеня очистки забарвлених модельних розчинів від мутності у присутності зважених частинок каоліну від дози коагулянту

Результати експериментального визначення оптимальної дози флокулянтів зображено у вигляді гістограм (рисунки 4, 5). Оптимальна доза флокулянтів становить: для хітозану – 50 мг/дм^3 при очищенні розчинів, забарвлених прямим барвником, та 10 мг/дм^3 для розчинів, забарвлених активним і дисперсним барвниками. Для альгінату натрію – 50 мг/дм^3 при очищенні розчинів, забарвлених прямим барвником, і 10 мг/дм^3 для розчинів, забарвлених активним і дисперсним барвниками.

Також встановлено, що при застосуванні хітозану було досягнуто більш високої ефективності очищення забарвлених розчинів, ніж при використанні альгінату натрію. Цей факт можна пояснити тим, що хітозан, завдяки наявності в його структурі великої кількості гідроксидних та амонійних функціональних груп, сприяє утворенню більш міцних і компактних агломератів, а це, в свою чергу, пришвидшує їх осадження.

DOI: 10.24025/2306-4412.3.2020.213912

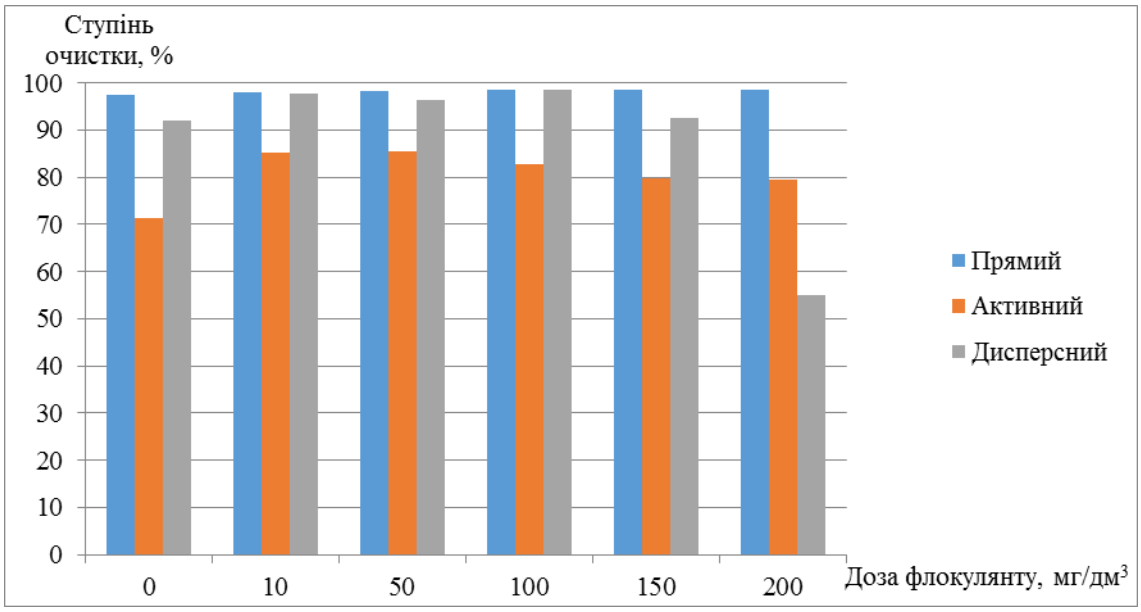


Рисунок 4 – Залежність ступеня очистки забарвлених модельних розчинів від барвників у присутності зважених частинок каоліну від дози флокулянту – хітозану (з визначеною на попередньому етапі досліджень оптимальною дозою коагулянту для кожного барвника)

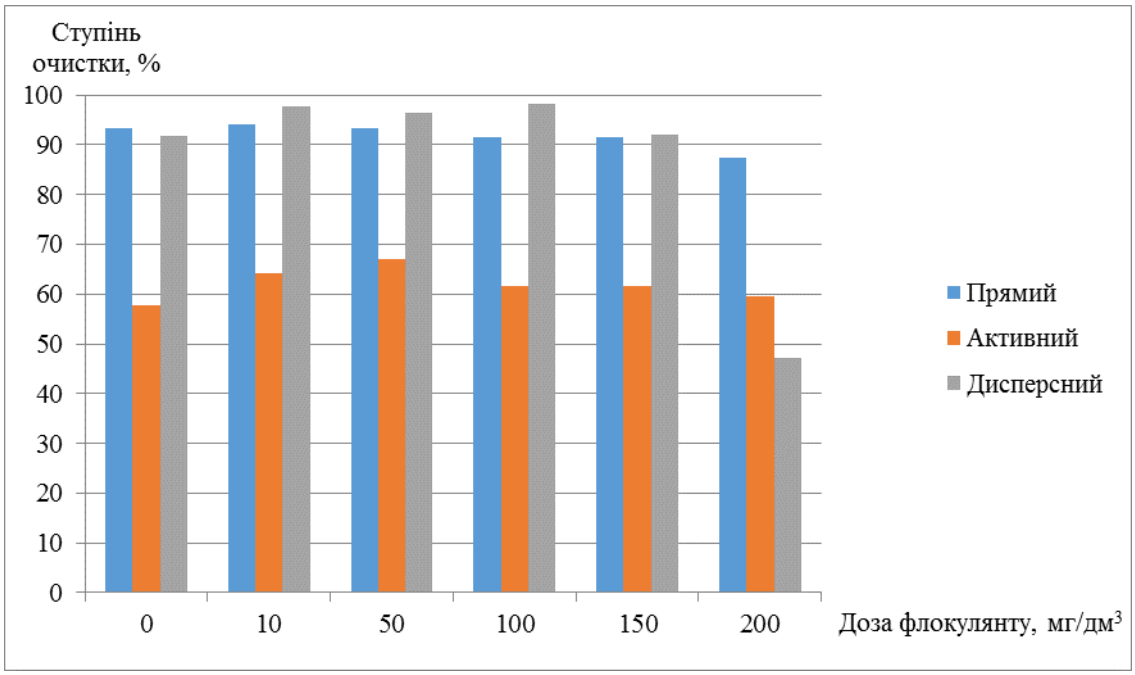


Рисунок 5 – Залежність ступеня очистки забарвлених модельних розчинів від барвників у присутності зважених частинок каоліну від дози флокулянту – альгінату натрію (з визначеною на попередньому етапі досліджень оптимальною дозою коагулянту для кожного барвника)

Під час здійснення коагуляційного процесу проводили контроль за зміною pH розчинів до та після додавання реагентів. Отримані дані, які наведено в таблиці 1, показують, що при додаванні алюмінію сірчанокислого pH розчинів змінюється з нейтрального до кислого, але залишається в межах ефективної дії коагулянту (від 4 до 8). Таким чином забезпечується максимальний ступінь використання алюмінійвмісного коагулянту.

DOI: 10.24025/2306-4412.3.2020.213912

Таблиця 1 – **Зміна pH забарвлених модельних зразків після додавання коагулянту алюмінію сірчанокислого технічного $Al_2(SO_4)_3 \cdot 18H_2O$**

pH / Доза Al^{3+}	Прямий чорний	Активний синій	Дисперсний коричневий
Початкова	8,077	7,777	7,850
20	7,37	7,081	7,056
30	7,025	7,071	6,570
40	6,721	7,063	5,979
50	6,371	5,905	5,045
60	5,652	5,064	4,463
70	4,804	4,635	4,356

Висновки. Таким чином, при проведенні цієї експериментальної роботи було проаналізовано процес очищення модельних розчинів, наближених до стічних вод текстильного підприємства, методами коагуляції та флокуляції. В роботі використовували коагулянт на основі алюмінію, а саме: алюміній сірчанокислий технічний $Al_2(SO_4)_3 \cdot 18\ H_2O$, як флокулянти було застосовано природні біополімери: хітозан зі ступенем деацетилювання 82 % та альгінат натрію, а також проведено їх порівняльний аналіз.

На першому етапі дослідження було встановлено оптимальну дозу коагулянту для мутних розчинів, забарвлених прямим чорним – 40 мг/дм^3, активним синім – 50 мг/дм^3 та дисперсним коричневим – 40 мг/дм^3.

На наступному етапі було визначено оптимальні дози флокулянтів (альгінату натрію та хітозану) при їх комплексній дії з оптимальною дозою коагулянту для кожного барвника. Встановлено, що більш ефективного ступеня очищення можна досягти при додаванні до коагулянту флокулянтів, а саме: при очищенні мутних розчинів, забарвлених прямим чорним, оптимальна доза– 10 мг/дм^3 для альгінату натрію або 50 мг/дм^3 для хітозану, при забарвленні активним синім та дисперсним коричневим – 50 мг/дм^3 для альгінату натрію або 10 мг/дм^3 для хітозану.

При проведенні порівняльного аналізу дії флокулянтів встановлено, що природний біополімер хітозан є більш ефективним для використання в комплексі з коагулянтом $Al_2(SO_4)_3 \cdot 18\ H_2O$, ніж альгінат натрію, а осад, який утворюється, є більш щільним та характеризується більшою агрегатною стійкістю.

Доведено, що додавання флокулянтів до традиційних коагулянтів збільшує ефективність очищення та пришвидшує осадження утворених агломератів. Досліджено, що ступінь очищення мутних вод, забруднених барвниками, напряму залежить від концентрації коагулянту та флокулянта, ступеня забрудненості води, а також від тривалості осадження, що дає можливість моделювати оптимальні умови для якісного й ефективного очищення забруднених стічних вод, враховуючи їх якісний і кількісний склад.

Список використаних джерел

[1] Ю. В. Воронов, и С. В. Яковлев, *Водоотведение и очистка сточных вод*: учебник для вузов. Москва, Россия: Изд-во Ассоциации строит. вузов, 2006.

[2] Т. В. Солодовнік, Н. М. Толстопалова, Н. М. Фоміна, та І. К. Якименко, "Дослідження процесів очищення забарвлених розчинів при використанні неорганічних коагулянтів та природного флокулянту", *Вісник Черкаського державного технологічного університету*, № 3, с. 108-117, 2019.

[3] Shahin Homaeigohar, Ahnaf Usman Zillohu, Ramzy Abdelaziz, Mehdi Keshavarz Hedayati, and Mady Elbahri, "A novel nanohybrid nanofibrous adsorbent for water purification from dye pollutants", *Materials (Basel)*, vol. 9, no. 10, pp. 1-16, 2016.

[4] T. Obushenko, N. Tolstopalova, O. Kulesha, and I. Astrelin, "Thermodynamic studies bromphenol blue removal from water using solvent sublation", *Chemistry & Chemical Technology*, vol. 10, no. 4, pp. 515-518, 2016.

[5] M. S. Hossain, F. Omar, Aj Asis, R. T. Bachmann, M. Z. Islam Sarker, and M. O. Ab Kadir, "Effective treatment of palm oil mill effluent using FeSO4.7H2O waste from titanium oxide industry: Coagulation adsorption isotherm and

DOI: 10.24025/2306-4412.3.2020.213912

kinetics studies", *Journal of Cleaner Production*, 2019, doi: https://doi.org/10.1016/j.jclepro.2019.02.069.

[6] І. К. Якименко, та Т. В. Солодовнік, "Дослідження процесу коагуляції та процесу очищення мутних та забарвлених розчинів при використанні різного типу коагулянтів", на *VII Міжнар. конф. студентів, аспірантів та молодих вчених з хімії та хімічної технології*: зб. тез доп. (м. Київ, 11-13 квіт. 2018 р.), с. 169.

[7] С. С. Душкін, М. В. Дегтяр, С. С. Душкін, та М. В. Дегтяр, "Спосіб очищення води від дисперсних домішок", *патент 112556 UA, МПК: C02F 1/00*, заявл. 23.05.2016; опубл. 26.12.2016, Бюл. № 24, 2016.

[8] А. В. Іванченко, Д. О. Єлатонцев, та Л. О. Артеменко, "Спосіб глибокої доочистки стічних вод від фосфатів та завислих речовин", *патент 116645 UA, МПК: C02F 1/52, C02F 1/58*, заявл. 26.12.2016; опубл. 25.05.2017, Бюл. № 10, 2017.

[9] J. Dotto, M. R. Fagundes-Klen, M. T. Veit, S. M. Palácio, and R. Bergamasco, "Performance of different coagulants in the coagulation/flocculation process of textile wastewater", *Journal of Cleaner Production*, 2018, doi: https://doi.org/10.1016/j.jclepro.2018.10.112.

[10] E. GilPavasa, I. Dobrosz-Gómez, and M. Á. Gómez-García, "Optimization of sequential chemical coagulation – electrooxidation process for the treatment of an industrial textile wastewater", *Journal of Water Process Engineering*, vol. 22, pp. 73-79, 2018, doi: https://doi.org/10.1016/ j.jwpe.2018.01.005.

[11] F. W. Pontius, "Chitosan as a drinking water treatment coagulant", *American Journal of Civil Engineering*, vol. 4, iss. 5, pp. 205-215, 2016.

[12] E. Güneş, E. Demir, Y. Güneş, and A. Hanedar, "Characterization and treatment alternatives of industrial container and drum cleaning wastewater: Comparison of Fenton-like process and combined coagu-?ation/oxidation processes", *Separation and Purification Technology*, 2018, doi: https://doi.org/10.1016/j.seppur.2018.07.060.

[13] Feng Qian, Mengchang He, Jieyun Wu, Huibing Yu, and Liang Duan, "Insight into removal of dissolved organic matter in post pharmaceutical wastewater by coagulation-UV/H_2O_2", *Journal of Environmental Sciences*, vol. 76, pp. 329-338, February 2019, doi: 10.1016/j.jes.2018.05.025.

[14] Z.-Q. Liu, L. You, X. Xiong, Q. Wang, Y. Yan, J. Tu, Y.-H. Cui, X.-Y. Li, G. Wen, and X. Wu, "Potential of the integration of coagulation and ozonation as a pretreatment of reverse osmosis concentrate from coal gasification wastewater reclamation", *Chemosphere*, 2019, doi: https://doi.org/10.1016/j.chemosphere.2019.01.187.

[15] Т. В. Солодовнік, *Аналітична хімія: практикум*: навч. посіб., вид. 2-ге, доп. Черкаси, Україна: ЧДТУ, 2019.

[16] T. V. Solodovnik, H. S. Stolyarenko, and A. A. Slis, "Prospects of using complex coagulation systems based on chitosan in water treatment processes", in *V Int. Water Forume "Water Resources and Climate"*, part 2. Minsk, Republic of Blarus, 2017, pp. 87-90.

References

[1] Yu. V. Voronov, and S. V. Yakovlev, *Water disposal and wastewater treatment*. Moscow, Russia: Izd-vo Assotsiatsii stroit. vuzov, 2006 [in Russian].

[2] T. V. Solodovnik, N. M. Tolstopalova, N. M. Fomina, and I. K. Yakymenko, "Researching the processes of colored solutions cleaning using inorganic coagulants and natural floculant", *Visnyk Cherkaskogo derzhavnogo tekhnologichnogo universytetu*, no. 3, pp. 108-117, 2019 [in Ukrainian].

[3] Shahin Homaeigohar, Ahnaf Usman Zillohu, Ramzy Abdelaziz, Mehdi Keshavarz Hedayati, and Mady Elbahri, "A novel nanohybrid nanofibrous adsorbent for water purification from dye pollutants", *Materials (Basel)*, vol. 9, no. 10, pp. 1-16, 2016.

[4] T. Obushenko, N. Tolstopalova, O. Kulesha, and I. Astrelin, "Thermodynamic studies bromphenol blue removal from water using solvent sublation", *Chemistry & Chemical Technology*, vol. 10, no. 4, pp. 515-518, 2016.

[5] M. S. Hossain, F. Omar, Aj Asis, R. T. Bachmann, M. Z. Islam Sarker, and M. O. Ab Kadir, "Effective treatment of palm oil mill effluent using FeSO4.7H2O waste from titanium oxide industry: Coagulation adsorption isotherm and kinetics studies", *Journal of Cleaner Production*, 2019, doi: https://doi.org/10.1016/j.jclepro.2019.02.069.

DOI: 10.24025/2306-4412.3.2020.213912

[6] I. K. Yakymenko, and T. V. Solodovnik, "Investigation of the coagulation process and the process of purification of turbid and colored solutions using different types of coagulants", in *7th Int. Conf. of students, graduate students and young scientists in chemistry and chemical technology*, (Kyiv, Ukraine, April 2018), p. 169 [in Ukrainian].

[7] S. S. Dushkin, M. V. Degtyar, S. S. Dushkin, and M. V. Degtyar, "The method of water purification from dispersed impurities", *Ukr. patent 112556, MKP: C02F 1/00*, Appl. 23.05.2016, Publ. 26.12.2016, Bulletin no. 24 [in Ukrainian].

[8] A. V. Ivanchenko, D. O. Yelatontsev, and L. O. Artemenko, "The method of deep wastewater treatment from phosphates and suspended solids", *Ukr. patent 116645, MKP: C02F 1/52, C02F 1/58*., Appl. 26.12.2016; Publ. 25.05.2017, Bulletin no. 10 [in Ukrainian].

[9] J. Dotto, M. R. Fagundes-Klen, M. T. Veit, S. M. Palácio, and R. Bergamasco, "Performance of different coagulants in the coagulation/flocculation process of textile wastewater", *Journal of Cleaner Production*, 2018, doi: https://doi.org/ 10.1016/j.jclepro.2018.10.112.

[10] E. GilPavasa, I. Dobrosz-Gómez, and M. Á. Gómez-García, "Optimization of sequential chemical coagulation – electro-oxidation process for the treatment of an industrial textile wastewater", *Journal of Water Process Engineering*, vol. 22, pp. 73-79, 2018, doi: https://doi.org/ 10.1016/ j.jwpe.2018.01.005.

[11] F. W. Pontius, "Chitosan as a drinking water treatment coagulant", *American Journal of Civil Engineering*, vol. 4, iss. 5, pp. 205-215, 2016.

[12] E. Güneş, E. Demir, Y. Güneş, and A. Hanedar, "Characterization and treatment alternatives of industrial container and drum cleaning wastewater: Comparison of Fenton-like process and combined coagulation /oxidation processes", *Separation and Purification Technology*, 2018, doi: https://doi.org/10.1016/j.seppur.2018.07.060.

[13] Feng Qian, Mengchang He, Jieyun Wu, Huibing Yu, and Liang Duan, "Insight into removal of dissolved organic matter in post pharmaceutical wastewater by coagulation-UV/H_2O_2", *Journal of Environmental Sciences*, vol. 76, pp. 329-338, February 2019, doi: 10.1016/j.jes.2018.05.025.

[14] Z.-Q. Liu, L. You, X. Xiong, Q. Wang, Y. Yan, J. Tu, Y.-H. Cui, X.-Y. Li, G. Wen, and X. Wu, "Potential of the integration of coagulation and ozonation as a pretreatment of reverse osmosis concentrate from coal gasification wastewater reclamation", *Chemosphere*, 2019, doi: https://doi.org/ 10.1016/j.chemosphere.2019.01.187.

[15] T. V. Solodovnik, *Analytical chemistry: manual*, 2nd ed., suppl., Cherkasy, Ukraine: ChDTU, 2019 [in Ukrainian].

[16] T. V. Solodovnik, H. S. Stolyarenko, and A. A. Slis, "Prospects of using complex coagulation systems based on chitosan in water treatment processes", in *V Int. Water Forume "Water Resources and Climate"*, part 2. Minsk, Republic of Belarus, 2017, pp. 87-90.

T. V. Solodovnik, *Ph.D., assistant professor,*
e-mail: solodovniktetana@gmail.com
I. K. Yakymenko, *postgraduate student*
e-mail: yakimenko97@ukr.net
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

RESEARCH AND IMPROVEMENT OF FLOCCULATION-COAGULATION PROCESSES OF PURIFICATION OF COLORED INDUSTRIAL WASTES

Contaminated wastewater from industrial enterprises significantly reduces drinking water volumes. Together with untreated wastewater from textile, chemical or metalworking enterprises, toxic substances, harmful to the health of fish, animals and humans, enter the reservoirs. Dyes used in dyeing processes are typical contaminants of wastewater in textile industry. The wide range of composition and insufficient treatment of these waters has a negative impact on the condition of water bodies,

DOI: 10.24025/2306-4412.3.2020.213912

and that is why it is necessary to carefully justify the choice of the optimal method of purification. The coagulation process, which occurs due to adhesive properties of coagulants and flocculants, is widely used in technologies for treatment of both natural and industrial wastewaters from colloidal particles, radionuclides, phosphates, dyes and suspended solids. Today, one of the promising areas of research of coagulation and flocculation processes consists in the use of natural and environmentally friendly reagents with high adsorption and adhesion properties.

While carrying out this experimental work, the staff of the Department of Chemical Technology and Water Treatment has conducted studies of the impact of model solutions containing different types of dyes and in the presence of suspended particles on purification processes, the use of natural flocculants, together with a typical coagulant, on the degree of purification and the speed of agglomerates precipitation. The advantages and disadvantages of different types of natural flocculants have been established on the example of chitosan and sodium alginate, when combined with a traditional coagulant – aluminum sulfate. When conducting research on the selection of the most effective reagents in the process of purification of specific wastewater, as well as determining their optimal doses, the Jar test method has been used. The essence of this technique is that in laboratory conditions the simulation of the process of flake formation, which is typical for industrial plants of wastewater purification, is carried out. The study on the composition of turbid and colored model samples of water has been carried out using modern methods of analysis: spectrophotometry, and nephelometry.

Keywords: *wastewater, purification, coagulation, color, turbidity, coagulants, flocculants.*

DOI: 10.24025/2306-4412.3.2020.213912