КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

DOI 10.28925/2663-4023.2024.24.8189
UDC 004.056

Ivan Karpovich
PhD, Associate Professor, Associate Professor at the
Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering, Rivne, Ukraine
ORCID ID: 0000-0002-4601-0541
i.m.karpovich@nuwm.edu.ua

Olena Hladka
PhD, Associate Professor, Associate Professor at the
Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering, Rivne, Ukraine
ORCID ID: 0000-0003-4728-0663
o.m.hladka@nuwm.edu.ua

Anastasiia Tymrakevych
Student at the Institute of Cybernetics, Information Technologies and Engineering
National University of Water and Environmental Engineering, Rivne, Ukraine
tymrakevych_ak22@nuwm.edu.ua

METHODOLOGY FOR ASSESSING THE IMPACT OF INFORMATION THREATS IN THE CONDITIONS OF INFORMATION CONFRONTATION

Abstract. The problem of information confrontation as rivalry in the information sphere with the aim of influencing various aspects of social relations is extremely important in the period of hybrid war. The object of the study was to the models of the dissemination of information and models of information confrontation. The goal of the work is the determine the features of the dissemination of informational threats in the conditions of informational and psychological conflict using a mathematical model based on modern achievements of social psychology, and to find optimal modes of informational dissemination and means of neutralizing informational threats. Mathematical models are proposed that describe the processes of the dissemination of informational threats in the conditions of informational and psychological conflict based on the innovation diffusion model and rivalry models. It is assumed that two flows of information dissemination in society so that each individual can become a supporter of one or the other side. The peculiarities of the methods of choosing behavioral strategies by subjects of influence in the social network during information confrontations are analyzed. The conditions under which one of the parties to the conflict can achieve an advantage by systematically varying the characteristics of the process have been studied. Based on the analysis of mathematical models of the dissemination of information threats, meaningful characteristics are defined, the management of which will reduce or neutralize the impact of the flow of negative information. The presented mathematical models allow to make for both quantitative and qualitative analysis of the main characteristics of the dynamics of information confrontation. The prospects for further research may consist in the generalization of the proposed models for a larger number of information flows and taking into account the dynamics of changes over time in the intensity of information dissemination and other characteristics.

Keywords: informational security; informational and psychological confrontation; informational threat; dissemination of information; modeling of information influence.

INTRODUCTION

Information becomes the most important strategic resource that contributes to increasing the efficiency of practical activities in all spheres of life. According to some data, about a third of the planet’s population is covered by information networks, which are an effective tool for influencing public opinion and a powerful means of mobilizing citizens. At the same time, the existing technologies for spreading information (or false information, fakes) create ample opportunities for unfriendly groups or hostile states to promote their interests and realize their goals in all spheres of human life and society [1].

Significant changes in communication processes in the information space contributed to the birth of a new form of confrontation—hybrid war. Hybrid war combines political, economic, informational and other means for one state to achieve superiority over another [2].

An important role in the conduct of hybrid warfare is given to information confrontation as a rivalry between social systems or countries in the information sphere to influence various aspects of social relations and establish control over strategic resources. This is facilitated, in particular, by the high speed of the dissemination in information systems of content that contains destructive informational influence on society [3], [4]. Information conflicts have become an everyday phenomenon: election races, attempts at raiding attacks, promotion of goods or services in a competitive environment, etc. One of the extreme forms of information conflict is information war—a set of measures related to information influence on mass consciousness to change people's behavior and impose on them goals that do not correspond to their interests, as well as protection against such influences [5].

The object of study is the problems of information security, namely the processes of the dissemination of informational threats in the conditions of informational and psychological confrontation. The problems of information security are traditionally reduced mainly to the protection of information from unauthorized access, or to the issues of suppressing the spread of unwanted information by technical or other means. Along with this, one of the important tasks of ensuring information security, in addition to determining the sources, nature and mechanisms of the emergence and spread of socially significant information threats, is the search for methods of neutralizing these information threats or their mitigation by use of the scientifically based approaches.

The subject of study is the mathematical models that describe the processes of the dissemination of informational threats in the conditions of informational warfare.

Problem statement. The process of distribution of a new product (in our case, information threats) will be considered as an "epidemic", when people who have not yet become consumers of the innovation are "infected" by real consumers (influence of an internal factor), and are also exposed to external factors, in particular, advertising.

Analysis of recent research and publications. Among the large number of publications that analyze the main problems of information security (see, for example, [6]–[8] and the literature cited there), priority tasks of scientific research in the field of information security, along with scientific and technical problems, are considered humanitarian problems and problems of personnel provision of information security.

Given the relevance of various types of information confrontation, in which a significant number of social network users are involved, mathematical models based on modern achievements of social psychology should be used to increase the effectiveness of research on humanitarian issues [9]–[11].

Such models, in our opinion, are models for innovation diffusion [12], which describe the processes of the spread of innovations (introduction of new scientific and technical developments, ideas, inventions) in new conditions or new branches of production.

The purpose of the work is to study the peculiarities of the dissemination of informational threats in the conditions of informational and psychological confrontation based on the innovation diffusion model.

RESEARCH RESULTS

Construction of a mathematical model

Diffusion of innovations is considered to be the solution $N = N(t)$ of the Cauchy problem for the differential equation (1):

$$\frac{dN(t)}{dt} = f\left(t, N(t)\right) \tag{1}$$

with the initial condition $N(0) = N_0$. Here t is time; $N(t)$ is the scope of the dissemination of the innovation up to the moment t (which is usually determined by the number of active consumers of the innovative product); $f\left(t, N(t)\right)$ is a function that determines the shape of the diffusion curve and reflects certain assumptions about the nature of the innovation diffusion process. It is usually assumed that the function $N(t)$ is continuous and differentiable for all non-negative values of t, and the function $f\left(t, N(t)\right)$ is unimodal.

The right-hand side of equation (1) is often written in the form [13]:

$$f\left(t, N(t)\right) = g\left(t, N(t)\right)\left(M - N(t)\right) \tag{2}$$

Formula (2) assumes that the total number of potential consumers of innovation M is a social community (political, age, members of the Internet community) exposed to information threats, which consists in negative changes in its state during the transmission of important information through information channels, is constant. The rate of spread of the threat $\frac{dN(t)}{dt}$ at each moment of time is proportional to the volume of not yet covered members of the community $\left(M - N(t)\right)$. The function $g\left(t, N(t)\right)$ determines the speed of adaptation. It is interpreted as the motivation of a potential consumer to perceive new information, ideas, narratives, norms, etc. and in the simplest case can be specified by a linear function of $N(t)$:

$$g\left(t, N(t)\right) = a + bN(t) \tag{3}$$

Substituting the rate of adaptation (3) into formula (2) gives the following differential equation of the model:

$$\frac{dN(t)}{dt} = \left(a + bN(t)\right)\left(M - N(t)\right) \tag{4}$$

Parameters a and b in model (4) reflect, respectively, the extent of external and internal influences on the speed of adaptation and, therefore, on the speed of innovation diffusion. External influences on the speed of adaptation are determined by individuals’ need for innovation and the level of advertising communications (term $a\left(M - N(t)\right)$ in the right-hand side of equation (4)). The intensity of the advertising campaign can be determined by the number of information acts per unit of time.

A community exposed to an information threat is considered to be in an unlimited information field. This means that any not yet covered member of the community has the opportunity to receive and with a certain probability perceive information that is distributed through an external channel. The probability of receiving information can be determined, in particular, by the credibility of it or the source of dissemination. Internal influences on the speed of adaptation are determined by communications between members of the social community (as a result of which, the information contained in the informational threat is transmitted to members of the community that have not yet been covered)—this corresponds to the term $bN(t)\left(M-N(t)\right)$.

The solution of equation (4) with the initial condition $N(0)=N_0$ is the logistic function (5), which describes the dependence of the number of covered community members on time:

$$N(t)=\frac{M\left(a+bN_0\right)-a\left(M-N_0\right)e^{-(a+bM)t}}{a+bN_0+b\left(M-N_0\right)e^{-(a+bM)t}} \qquad (5)$$

As can be seen from (5), the value of the function $N(t)$ for $t>0$ increases monotonically and goes towards M , in other words, in a sufficiently long period of time ($t\to\infty$), all members of the group will be covered by negative information spread by the information threat.

Note that the calculations performed earlier in [14] for the analysis of the distribution of innovative software using the model in the form (5) are in good agreement with the actual data [15].

The analysis of the speed of the dissemination of informational threats shows that for some values of the model parameters it is possible to find the value of t_{kr}, which corresponds to the maximum speed of coverage of negative information of community members. Depending on the relationship between the parameters, the intensity of external sources of information threats may exceed the intensity of internal sources or vice versa. Under some conditions, these intensities can be equal. An increase in the parameter b (the intensity of interpersonal contacts) changes the value of t_{kr}, which is a consequence of the nonlinearity of the model (4), and leads to an increase in the value of $N(t_{kr})$.

Based on the parameters of the model, it is possible to calculate the overall efficiency of information dissemination or information threats—the ratio of the number of covered community members $N(t)$ to the number of informational acts:

$$E(t)=\frac{N(t)}{at}.$$

This characteristic makes it possible to find a point in time, starting from which further measures to spread information, counter-information or information threats become impractical.

Thus, the analysis of the mathematical model of the spread of information threats shows that, depending on the goals, available resources, time frames and behavioral characteristics, the participants of this process have certain opportunities for its organization in the desired direction. It should be noted that based on the methods of the theory of optimal management, optimal modes of information dissemination or means of neutralizing information threats, described by this model, can be found in terms of resources spent.

Let us consider the case of the simultaneous spread of several different types of information (information conflict), when a certain social community with the number of M is exposed to the influence of not one, but, for example, two information flows. Let two sources of different information simultaneously begin to spread it among the community at the moment of time $t=0$. In general, the information of the first type I_1 can be opposite in content to the information of the second type I_2.

We will build a mathematical model of information confrontation, assuming (analogous to the previous one) that each of the streams I_1 and I_2 spreads among the community through two information channels. The intensity of information dissemination through the external channel for I_1 is characterized by parameter a_1, and for I_2 by parameter a_2. The second (internal) channel is the interpersonal communication of members of the social community.

Here, the intensity of information dissemination for I_1 is determined by parameter b_1, and for I_2 by parameter b_2. As a result of such communication, the participants of the process who are already covered by a certain idea influence the members of the community who have not yet been covered, thereby contributing to the dissemination of information.

The rates of change in the number of supporters of the corresponding idea consist of the rates of external involvement (they are proportional to the products of the intensities a_1 and a_2 by the number of unreached community members, i.e., the values $a_1\left(M - N_1(t) - N_2(t)\right)$ and $a_2\left(M - N_1(t) - N_2(t)\right)$ respectively for I_1 and I_2) and rates of internal involvement (they are proportional to the product of the intensities b_1 and b_2 by the number of valid supporters $N_1(t)$ and $N_2(t)$ and the number of unreached community members, i.e., the values $b_1N_1(t)\left(M - N_1(t) - N_2(t)\right)$ and $b_2N_2(t)\left(M - N_1(t) - N_2(t)\right)$ respectively).

The number of members of the community not yet covered by the information influence is equal to $\left(M - N_1(t) - N_2(t)\right)$—from the total number of participants of M we subtract the number of persons $N_1(t) + N_2(t)$ covered by not one, but two types of information ($N_1(t)$ is the number of participants for whom information of type I_1 is the priority (correct); $N_2(t)$ is the number of participants who prefer information of type I_2).

As already noted, parameters a_1, a_2, b_1 and b_2 characterize not only the intensity of informational influence, but also the tendency to perceive it. Thus, the speed of perception of information by a part of the community not yet covered at time t depends on the value of these values, which have a probabilistic component. The effectiveness of the conducted special informational and psychological operation is evaluated by the probable number of elements of the social community, which under the influence of this influence changed its initial state [16].

Taking into account the formulated assumptions, we will obtain a model of information confrontation in the form (6):

$$\begin{aligned} \frac{dN_1}{dt} &= \left(a_1 + b_1N_1(t)\right)\left(M - N_1(t) - N_2(t)\right), \quad N_1(0) = N_{10}; \\ \frac{dN_2}{dt} &= \left(a_2 + b_2N_2(t)\right)\left(M - N_1(t) - N_2(t)\right), \quad N_2(0) = N_{20}. \end{aligned} \qquad (6)$$

Using the known parameter values and initial conditions, on the basis of model (6), it is possible to find important characteristics of the dynamics of information confrontation. The main one is the question of superiority, when by the time the community under study is fully covered by both types of information, one of the participants has managed to spread his information among a larger number of community members than the opponent.

Study of the model

Computer experiments with the proposed mathematical model were conducted. We varied different values of the model parameters a_1, a_2, b_1, b_2 in order to determine their influence on the results.

Calculations show that in the case of $b_1 = b_2$, when the intensity of the internal (interpersonal) propagation channels of I_1 and I_2 is the same, for the advantage of I_1 it is necessary that the inequality $a_1 > a_2$ be fulfilled (respectively, for the advantage of I_2 it is necessary that $a_1 < a_2$). That is, under these circumstances, the one who provides a stronger external information influence wins. The same criteria of information advantage are observed in the case when, for both types of information, the intensity of dissemination through internal channels is significantly lower than through external ones. If $a_1 = a_2$, that is, the intensities of the external channels of information dissemination I_1 and I_2 are the same, the advantage is given to the one whose information is more intensively disseminated through internal (interpersonal) channels (the ratio $b_1 > b_2$ is a guarantee of the advantage of the first party, and the ratio $b_1 < b_2$ is a guarantee of the advantage of the second party).

For fixed a_1, b_1 and relatively small values of b_1 compared to a_1 (that is, when $b_1 << a_1$ which means a strong advantage of the intensity of the propagation of I_1 through the external channel, compared to the internal), the condition for the advantage of I_1 is the ratio $a_1 > a_2$, despite the noticeable advantage in dissemination of information I_2 through the internal channel. At the same time, the analysis shows that in the opposite case, for relatively large values of b_1 (that is, when $b_1 >> a_1$), in order to achieve victory, the first party must have a significant advantage in spreading its information through the external channel ($a_2 << a_1$).

Thus, even a brief analysis shows that the parties to the conflict have various opportunities to achieve advantage by systematically varying the characteristics of the process. At the same time, the choice of the ratio between the capacities of external and internal information channels is of great importance.

Model (6) can be generalized to the case of conflict between not two, but more types of information I_i ($i = 1, 2, \ldots, k$), $k > 2$. In this case, it represents a system of k nonlinear differential equations:

$$\frac{dN_i}{dt} = f_i\left(a_i, b_i, N_i(t)\right), \quad N_i(0) = N_{i0}, \qquad (7)$$

where $N_i(t)$, $N_i(0)$ are the current and initial values of the number of followers of information I_i, and a_i, b_i are the intensity of its distribution through external and internal channels, respectively. The study of the dynamics of such a process depending on the parameter values can be the subject of a separate study.

The considered models do not take into account the heterogeneity of the social environment, the effects of forgetting or conscious resistance to informational threats, etc. However, according to the authors, taking into account the listed factors will not change the essence of the analyzed models.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

Based on the analysis of mathematical models of the spread of information threats and information rivalry, meaningful characteristics are defined, the management of which will allow optimizing the methods of their organization and will stimulate the flow of these processes in the direction required by their participants. Note that the analyzed processes, due to their nonlinearity under certain conditions, have modes of development that are difficult to predict.

The practical significance of the obtained results lies in the fact that the parameters of the proposed model were analyzed for the purpose of managing the processes under investigation, and practical recommendations were provided for countering hostile information threats.

Prospects for further research are to generalization of the proposed models for a larger number of information flows and taking into account the dynamics of changes over time in the intensity of information dissemination and other characteristics. Other problem statements about the dissemination of information threats are possible, which are based on the analyzed models, namely, the alternating influence of internal and external sources of information threats, the dependence of characteristics on time, etc.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Stephen, C. W. (2011). *Revealed: Air Force ordered software to manage army of fake virtual people*. https://www.filmsforaction.org/news/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people
2. Hrabar, I. H., Hryshchuk, R. V., & Molodetska, K. V. (2019). *Bezpekova synerhetyka: Kibernetychnyi ta informatsiinyi aspekty*. ZhNAEU.
3. Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physics Review Letters, 86(14).*
4. Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press.
5. Horbulin, V. P., Dodonov, O. H., & Lande, D. V. (2009). *Informatsiini operatsii ta bezpeka suspilstva: Zahrozy, protydiia, modeliuvannia*. Intertekhnolohiia.
6. Anosov, A. O., & Puzniak, Z. M. (2017). Informatsiino-oriientovana model yak realizatsiia metodyky vyiavlennia vplyvu na dostovirnist informatsii v informatsiinomu prostori. *Suchasnyi zakhyst informatsii, 4(32),* 55–59.
7. Hrechka, S. O. (2020). Naratyvni tekhnolohii modeliuvannia imidzhu Ukrainy v umovakh informatsiino-psykholohichnoho protyborstva. *Young Scientist, 8(84),* 183–189. https://doi.org/10.32839/2304-5809/2020-8-84-37
8. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: Sotsiotekhnichnyi aspekt*. DUT.
9. Barrett, C., Eubank, S., & Marathe, M. (2006). Modeling and simulation of large biological, information and socio-technical systems: An interaction based approach. *Interactive Computation*, 353–392.
10. Bin, H., & Zhang, D. (2007). Cellular – Automata Based Qualitative Simulation for Nonprofit Group Behavior. *JASSS, 10(1).*
11. Tatnall, A. (2010). Actor-Network Theory and Technology Innovation: Advancements and New Concepts. *Information Science Reference*.
12. Bass, F. (1969). A new product growth for model consumer durables. *Management Science, 15(3),* 215–227.
13. Mahajan, V., & Peterson, R. (1985). *Models for Innovation Diffusion*. Beverly Hills.
14. Karpovych, I. M., Hladka, O. M., & Ustymchyk, M. (2018). Modeliuvannia rynku prohramnoho zabezpechennia ta yoho osoblyvosti. *Visnyk Natsionalnoho universytetu vodnoho hospodarstva ta pryrodokorystuvannia, 2(82),* 249–258.
15. Maevsky, D. A., Maevskaya, E. J., Jekov, O. P., & Shapa, L. N. (2014). Verification of the software reliability models. *Reliability: Theory & Applications, 9(3(34)),* 14–23.
16. Dudatyev, A., Kupershtein, L., & Voitovych, O. (2023). Information Counterfeature: Models Of Implementation And Evaluation Of Information Operations. *Cybersecurity: Education, Science, Technique, 4(20),* 72–80. https://doi.org/10.28925/2663-4023.2023.20.7280

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Карпович Іван Миколайович
к.ф.-м.н., доцент, доцент кафедри комп'ютерних
технологій та економічної кібернетики
Національний університет водного господарства та
природокористування, Рівне, Україна
ORCID ID: 0000-0002-4601-0541
i.m.karpovich@nuwm.edu.ua

Гладка Олена Миколаївна
к.т.н., доцент, доцент кафедри комп'ютерних
технологій та економічної кібернетики
Національний університет водного господарства та
природокористування, Рівне, Україна
ORCID ID: 0000-0003-4728-0663
o.m.hladka@nuwm.edu.ua

Тимракевич Анастасія Олегівна
здобувачка вищої освіти
Навчально-наукового інституту кібернетики,
інформаційних технологій та інженерії
Національний університет водного господарства та
природокористування, Рівне, Україна
tymrakevych_ak22@nuwm.edu.ua

МЕТОДИКА ОЦІНЮВАННЯ ВПЛИВУ ІНФОРМАЦІЙНИХ ЗАГРОЗ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Анотація. Проблема інформаційного протиборства як суперництва в інформаційній сфері з метою впливу на різні аспекти суспільних відносин є надзвичайно важливою в період гібридної війни. Об'єкт дослідження — моделі розповсюдження інформації та моделі інформаційного протиборства. Метою роботи є визначення особливостей розповсюдження інформаційних загроз в умовах інформаційно-психологічного протиборства з використанням математичної моделі, що грунтується на сучасних досягненнях соціальної психології, та знаходження оптимальних режимів поширення інформації і засобів нейтралізації інформаційних загроз. Запропоновано математичні моделі, що описують процеси поширення інформаційних загроз в умовах інформаційно-психологічного протиборства на основі моделі дифузії інновацій та моделей суперництва. Передбачається, що у соціумі поширюються два потоки інформації так, що кожен індивід може стати прихильником однієї або іншої сторони. Проаналізовано особливості методів вибору поведінкових стратегій суб'єктами впливу у соціальній мережі під час інформаційних протиборств. Досліджено умови, за яких одна із сторін протиборства може досягати переваги, системно варіюючи характеристиками процесу. На основі аналізу математичних моделей поширення інформаційних загроз визначено змістовні характеристики, управління якими дозволить зменшити або нейтралізувати вплив потоку негативної інформації. Представлені математичні моделі дозволяють провести як кількісний, так і якісний аналіз основних характеристик динаміки інформаційного протиборства. Перспективи подальших досліджень можуть полягати в узагальненні запропонованих моделей для більшої кількості інформаційних потоків, врахуванні динаміки зміни з часом інтенсивності поширення інформації та інших характеристик.

Ключові слова: інформаційна безпека; інформаційно-психологічне протиборство; інформаційна загроза; поширення інформації; моделювання інформаційного впливу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stephen, C. W. (2011). *Revealed: Air Force ordered software to manage army of fake virtual people*. https://www.filmsforaction.org/news/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people
2. Hrabar, I. H., Hryshchuk, R. V., & Molodetska, K. V. (2019). *Bezpekova synerhetyka: Kibernetychnyi ta informatsiinyi aspekty*. ZhNAEU.
3. Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physics Review Letters, 86(14).*
4. Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press.
5. Horbulin, V. P., Dodonov, O. H., & Lande, D. V. (2009). *Informatsiini operatsii ta bezpeka suspilstva: Zahrozy, protydiia, modeliuvannia*. Intertekhnolohiia.
6. Anosov, A. O., & Puzniak, Z. M. (2017). Informatsiino-oriientovana model yak realizatsiia metodyky vyiavlennia vplyvu na dostovirnist informatsii v informatsiinomu prostori. *Suchasnyi zakhyst informatsii, 4(32),* 55–59.
7. Hrechka, S. O. (2020). Naratyvni tekhnolohii modeliuvannia imidzhu Ukrainy v umovakh informatsiino-psykholohichnoho protyborstva. *Young Scientist, 8(84),* 183–189. https://doi.org/10.32839/2304-5809/2020-8-84-37
8. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: Sotsiotekhnichnyi aspekt*. DUT.
9. Barrett, C., Eubank, S., & Marathe, M. (2006). Modeling and simulation of large biological, information and socio-technical systems: An interaction based approach. *Interactive Computation*, 353–392.
10. Bin, H., & Zhang, D. (2007). Cellular – Automata Based Qualitative Simulation for Nonprofit Group Behavior. *JASSS, 10(1).*
11. Tatnall, A. (2010). Actor-Network Theory and Technology Innovation: Advancements and New Concepts. *Information Science Reference*.
12. Bass, F. (1969). A new product growth for model consumer durables. *Management Science*, *15(3),* 215–227.
13. Mahajan, V., & Peterson, R. (1985). *Models for Innovation Diffusion*. Beverly Hills.
14. Karpovych, I. M., Hladka, O. M., & Ustymchyk, M. (2018). Modeliuvannia rynku prohramnoho zabezpechennia ta yoho osoblyvosti. *Visnyk Natsionalnoho universytetu vodnoho hospodarstva ta pryrodokorystuvannia*, *2(82),* 249–258.
15. Maevsky, D. A., Maevskaya, E. J., Jekov, O. P., & Shapa, L. N. (2014). Verification of the software reliability models. *Reliability: Theory & Applications*, *9(3(34)),* 14–23.
16. Dudatyev, A., Kupershtein, L., & Voitovych, O. (2023). Information Counterfeature: Models Of Implementation And Evaluation Of Information Operations. *Cybersecurity: Education, Science, Technique, 4(20),* 72–80. https://doi.org/10.28925/2663-4023.2023.20.7280