

O. Rozhenko¹,
orcid.org/0000-0002-9358-5436
T. Beridze^{*2},
orcid.org/0000-0003-2509-3242,
O. Galitsyna³,
orcid.org/0000-0003-0560-755X,
Yu. Gladka³,
orcid.org/0000-0001-5819-7465,
A. Buhra²,
orcid.org/0000-0003-3978-3404,
V. Galitsyn³,
orcid.org/0009-0005-4530-6323

1 – Klaipeda University, Klaipeda, Republic of Lithuania
2 – Kryvyi Rih National University, Kryvyi Rih, Ukraine
3 – Kyiv National Economics University named after Vadym
Hetman, Kyiv, Ukraine
* Corresponding author e-mail: beridzet2016@gmail.com

IMPERATIVES OF INFORMATION PROTECTION IN THE STRUCTURE OF ECONOMIC SECURITY OF AN ENTERPRISE

Purpose. Construction of a multifactorial mathematical model of information protection based on the corresponding properties of its components – cyber immunities.

Methodology. In the process of research, the methodology of system-parametric modeling was applied when forming the parameters of the impact on the integral indicator – information protection in the configuration of the security economic components of the enterprise. The principles of system research were used, namely, emergence, definition of the integral parameter. Accordingly, comparative analysis was used to determine the place and role of information protection in the security structure of the enterprise.

Findings. The main scientific and practical views on modeling the information protection at the enterprise as a component of its economic security are analyzed and researched. The possibility and feasibility of forming a generalizing parameter, which is determined as a whole on components with corresponding properties with the corresponding properties, are substantiated. It is determined that the general property of information protection is the degree of compliance of the parameters of local properties – cyber immunities with their specified values.

Originality. The definition of “cyber immunity” as a fuse of information threats when determining information protection is proposed. A multifactorial mathematical model of the integral indicator of information security has been formed. Based on the optimization of the values of local cyber immunities, its corresponding cost has been minimized.

Practical value. The practice of applying the proposed methodology allows improving methods for combating information threats to the security component of an enterprise. Mathematical modeling of the integral parameter of cyber immunity – information protection is aimed at building a multifactor model. Analysis of the model makes it possible to determine the property of integral cyber immunity as a set of properties of local cyber immunities. Moreover, there is a possibility of increasing the relevant structure in order to anticipate the emergence of new threats. The use of a static multiplicative structure of the mathematical model made it possible to implement these requirements. It can be assumed that the application of this approach will protect the economic security management of the enterprise from information threats.

Keywords: *cyber immunity, multifactor mathematical model, information protection, economic security, optimization*

Introduction. The modern world of digital technologies is steadily moving forward, bringing with it not only new opportunities, but also a number of challenges, including the issue of information protection. The effective activity of an enterprise is based on the sustainable growth of the results of its activities. The external and internal environment affects its functioning. The impact is both negative and positive. The formation of a protected information space is one of the tasks of building the security component of an enterprise. Modern conditions for the operation of manufacturing enterprises are characterized by the existence of a high probability of threats to economic security. Neutralization of threats to economic security or their elimination are moving from the direction of organizational, financial and cost measures that increase due to the dynamics of uncertainty in the external environment to information

threats. Modern scientific judgments regarding the definitions of economic security of an enterprise should take into account the expediency of including information protection in the security component. The presence of information protection in the structure of the security component of an enterprise provides a certain immunity from relations carrying different-level threats. Thus, there is an urgency to analyze the content of the concept of the category of cyber immunity in the structure of the security component of the enterprise. Cyber immunity can be considered a component of an integral indicator – information protection. The study of the enterprise as a system object, which has both internal and external threats, indicates their impact on economic security. In the context of modern information protection of the enterprise, it has become obvious that the approach, which is based exclusively on reactive measures, is no longer effective. It is necessary to move to active methods that will allow detecting and preventing threats at the early stages, rather than reacting to them after they

occur. The presence of cyber immunity will allow one to secure the corresponding local threats in the activities of the enterprise. Assuming that the economic security of the enterprise is a synthesis of the corresponding components, then, accordingly, information protection should be synthesized by the corresponding components. That is, we can consider cyber immunity as a thorough approach to information protection in the structure of the economic security of the enterprise. Using the components of information protection, namely the corresponding cyber immunity, there is an expediency in building a mathematical model of the process of implementing the information protection indicator, which can be considered integral cyber immunity. An approach to mathematical modeling of the formation of information protection is proposed by choosing a static multiplicative structure of the model with the subsequent identification of parameters. This allows adapting the model to real conditions. It is relevant and appropriate to take into account the cost-target indicators of the properties of the components of information protection. The formed mathematical model allowed formulating an economic criterion for minimizing the costs of information security at given values of the corresponding properties. The effectiveness of the proposed approach is argued using the example of using a two-factor mathematical model of a synthesized information security indicator. The modern world of digital technologies is steadily moving forward, bringing with it not only new opportunities, but also a number of challenges, among which the issue of information security is one of the most relevant.

Literature review. In general, solving cybersecurity problems at the state level is based on the relevant legislative document [1]. The current conditions of the functioning of enterprises affect the efficiency of their management. Threats that create a negative impact on the activities of the enterprise require their resolution. Modern conditions encourage solving a number of problems that directly affect the efficiency of the business process at the enterprise. Today, the issues of ensuring enterprise security are decisive. The importance of creating a safe future based on the concept of cyber immunity is growing due to the continuous development of information threats. Thus, scientists Babichev A. V., Samorodov B. V. investigate the problems of ensuring the security component of the enterprise on the basis of the information component. Thus, scientists Babichev A. V., Samorodov B. V. investigate the problems of information security. The authors identify information security components of the enterprise. Using CASE technologies, they analyze the information components of the security system [2]. The author, V. Hnatenko, proposes to systematically investigate information security as part of economic security. The scientist pays attention to the formation of the mutual influence of the information security space and the economic security of the state [3].

The issue of the role of information security in the overall financial and economic system of the relevant enterprise was analyzed in detail by the authors Machak T., Dubina O. and Yurchenko S. The researchers have identified factors influencing the economic security of an enterprise from the point of view of information security [4]. Organizational issues regarding the

protection of the information component of the enterprise were developed by scientist Zakharov O. The scientist developed a model of complex information support, which has two components. The formed components are aimed at the information protection of the economic security system of the enterprise [5]. One of the significant levers for protecting an enterprise is insurance in general and cyber insurance separately, noted by the authors Prykazyuk N. V., Gumenyuk L. S. They note that cyber insurance minimizes cyber risks [6]. Information segmentation is considered relevant to attract investments in cybersecurity. Gordon A., Loeb P. and Zhou Lei base their conclusions on the use of the Gordon-Loeb model. The scientists prove the feasibility of such investment in order to prevent threats to the enterprise's activities [7]. A number of authors study in detail the relationship between the cost indicators of information security directly with the economic security of an enterprise. Thus, Nekhay V. A. and Nekhay V. V. analyzed in detail the possible risks to the information and communication system of the enterprise. In addition, the scientists investigated, with a certain circle of scientists, the definition of the concept of "information security" [8]. The study by Shashina M. V., Volodin V. V. is noteworthy. The authors have determined the place of the information component in the structure of the economic security of the enterprise. The scientist has shown the relationship between the costs of the information security component of an enterprise and the level of its security. [9]. The most significant and detailed research should be considered the research by Chubaevsky V., Blakya G., Bogma O., Shtuler I., Batrakova T. The scientific research proposes the formation of a mathematical model and a corresponding algorithm. The authors offer a solution to the optimization problem regarding the balance of losses and costs for neutralizing information threats. [10]. Puriy G. M. defines information as resource potential. The scientist studies information systems in the context of the competitiveness of the enterprise. The emphasis is on the ability of information systems to track the main indicators of the enterprise's activity in real time [11]. The use of information resources used in management processes is analyzed by scientists Onopko A.S. and Zhygalkevych Zh.M. The authors systematized existing software products at different stages of enterprise management. The feasibility of using modern software products is proven [12]. The author, Pankratova O., conducted research on the impact of digitalization on enterprise performance indicators. She noted a positive impact that allowed for significant savings [13]. Currently, there is an opinion among the scientific community about the feasibility of rethinking the role of digitalization of society in general and in economic processes separately. Thus, Holoborodko A. explores general methodological approaches to the digital economy as an economy as a whole. The author focuses on digital technologies. He proves that it is these technologies that are the basis of the development of society and innovations in the economy. The author emphasizes that the general digitalization of society, the expansion of the digital space has affected business processes [14]. Scientists Puzenteilo P.R., Gumenyuk O.O. study the technological processes of the digital economy. The authors focus on the transformation processes

that accompany the development of the national economy on the basis of digitalization [15]. The author Beridze T.M. investigated the information components in the strategic management system of the enterprise. The algorithmic support of the information system of statistical monitoring and its adaptation to the enterprises of the mining complex are presented [16]. Scientists Piletska S. T., Korytko T. Yu., Tkachenko E. V. comprehensively investigated the assessment of economic security. The scientists proposed a model that took into account the main components that, in their opinion, reflect the security component [17]. The scientist Konkolewsky, H. focuses on the issue of the digital economy and the future of social security. The author analyzes the challenges that the digital economy poses to the social security of citizens and institutions [18].

The practice of approaches to protecting the information space abroad attracts attention. Thus, Estonia is known for its developed digital infrastructure and legislative framework, which provides a high level of security for IT companies and their clients. In Estonia, considerable attention is paid to training citizens in the field of cybersecurity. Of course, a positive step would be to introduce such experience at the national level.

Obviously, the modernization of the modern economy is the main prerequisite for reducing social risks and threats. Currently, there is a need to carefully study possible ways to transform economic processes by using new approaches. The issues of economic security of the enterprise remain relevant. The modern development of digitalization is characterized by the emergence of new threats to the effective functioning of enterprises. This encourages the scientific and practical environment to actualize the problems of building information protection for the activities of the enterprise. Without reducing the level of scientific research in this direction, it should be noted that the aspect of the value-target orientation of information protection in the structure of the economic security of the enterprise has not been sufficiently studied.

Unsolved aspects of the problem. The importance of building secure business processes based on the concept of information protection is growing due to the continuous development of informatization threats. The multifaceted nature of research confirms the relevance of the issue. Numerous studies devoted to information protection in the field of economic processes investigate the impact of informatization on their respective components. Modeling in the cost dimension of indicators regarding informatization danger and its elimination currently requires increased research among scientists. It is proposed to consider information protection as a set of relevant properties – cyber immunities, and information protection itself as integral cyber immunity. Mathematical modeling of information protection as integral cyber immunity is proposed to be built taking into account the properties of local cyber immunities. The general property of information protection is the degree of correspondence of the parameters of local properties – cyber immunities to their specified values.

Purpose. The aim of the article is to form a multifactorial mathematical model of information protection based on the corresponding properties of its components – cyber immunity

Results. The multifactor model of information protection refers to the dependence F that connects the information protection P with its input (r_1, \dots, r_n) – the vector of local components of cyber immunity.

$$R = R(r_1, r_2, \dots, r_n). \quad (1)$$

It is clear that information protection is influenced by many factors. Moreover, the influence of factors is different in the “strength” of their action. Therefore, to form a multifactor mathematical model of information protection, it is necessary to determine the degree of influence of each local component.

Analysis of the multifactor model of information protection assumes analytical dependence of the values of local parameters. Thus, this gives grounds to define the formed model, which represents a multiplicative structure. Therefore, model (1) will be formed as follows

$$R = \prod_{i=1}^n r_i^{c_i}. \quad (2)$$

The essence of the components c_1, \dots, c_n is not important at this time, only the multiplicativeness of the structure is important. It is also necessary to analyze the properties of the specified structure of the model (2). According to the requirements, the following restrictions on the features of information protection must be met

$$0 \leq R \leq 1; \quad 0 \leq r_i \leq 1, \quad (i = 1, 2, \dots, n). \quad (3)$$

Moreover, let

$$\hat{r}_i = 1, \quad (i = 1, 2, \dots, n). \quad (4)$$

Then

$$R = \lim_{n \rightarrow \infty} k \prod_{i=1}^n \hat{r}_i^{c_i} = k \lim_{n \rightarrow \infty} \prod_{i=1}^n \hat{r}_i^{c_i} = k \cdot 1 = k. \quad (5)$$

Taking into account (4) and according to (5), it follows that

$$R = 1. \quad (6)$$

Considering (5 and 6), we have

$$k = 1. \quad (7)$$

Considering (7), the multifactor information security model (2) will be represented as

$$R = r_1^{c_1} \cdot r_2^{c_2} \cdot \dots \cdot r_n^{c_n}. \quad (8)$$

To determine the parameters $c(i)$, it is advisable to find the logarithm of the analytical expression presented in (8)

$$\ln R = \ln(r_1^{c_1} \cdot r_2^{c_2} \cdot \dots \cdot r_n^{c_n}); \quad (9)$$

$$\ln P = c_1 \cdot \ln r_1 + c_2 \cdot \ln r_2 + \dots + c_n \cdot \ln r_n.$$

In the given analytical expression (9), we are looking for the derivative that is partial with respect to the variable p_i .

$$\frac{\partial \ln PR}{\partial r_i} = \frac{\partial}{\partial r_i} (c_1 \ln r_1 + \dots + c_i \ln r_i + \dots + c_n \ln r_n) = \frac{c_i}{p_i}; \quad (10)$$

$$\frac{\partial R}{\partial r_i} = R \frac{c_i}{r_i}.$$

Therefore, the analysis of formula (10) allows us to investigate the sensitivity of the information protection attribute R to the local component of cyber immunity.

Information about the identification of the two-factor information protection model

No.	R	r_1	r_2	y	x_1	x_2	R_m
1	0.9	0.86	0.95	-0.1054	-0.1508	-0.0513	0.8989
2	0.86	0.87	0.85	-0.1508	-0.1393	-0.1625	0.8353
3	0.85	0.91	0.89	-0.1625	-0.0943	-0.1165	0.8812
4	0.89	0.95	0.87	-0.1165	-0.0513	-0.1393	0.8847
5	0.91	0.96	0.91	-0.0943	-0.0408	-0.0943	0.9178
6	0.93	0.95	0.95	-0.0726	-0.0513	-0.0513	0.9416
7	0.9	0.93	0.92	-0.1054	-0.0726	-0.0834	0.9113
8	0.89	0.91	0.91	-0.1165	-0.0943	-0.0943	0.8952
9	0.9	0.92	0.89	-0.1054	-0.0834	-0.1165	0.8857
10	0.91	0.98	0.89	-0.0943	-0.0202	-0.1165	0.9122

$$0.7 < r_{RR_m} < 0.9,$$

we can note that there is a “high” relationship between the variables.

Thus, we can note that formula (30) meets the requirements for the formation of a two-factor mathematical model. It contains the appropriate components and allows us to determine quantitative parameters regarding information security protection.

The function that determines the cost of information protection relative to the corresponding values of the local components of the cyberimmunities of software and hardware has the form

$$S = s_1 \cdot r_1 + s_2 \cdot r_2, \tag{31}$$

where S is the cost of information protection; s_1, s_2 are the specific costs of local components: software and hardware.

The task of optimizing the two-factor model is to minimize the cost of integral cyber immunity, i.e.

$$S = s_1 \cdot r_1 + s_2 \cdot r_2 \rightarrow \min;_{p_1, p_2}$$

$$R = r_1^{c_1} r_2^{c_2} = \text{const.}$$

The cost of integral cyber immunity will be determined as a function of one variable, namely, the local cyber immunity of the software.

$$S = s_1 r_1 + s_2 \left(\frac{r}{r_1^{c_1}} \right)^{\frac{1}{c_2}},$$

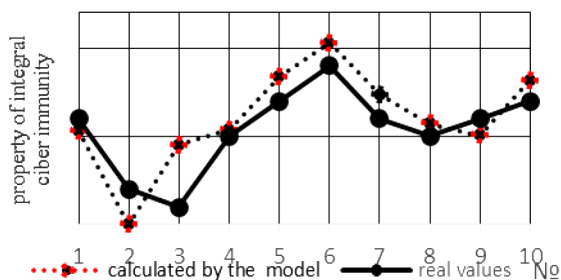


Fig. 1. Graphs of real values of information protection indicators and those calculated using the model (30)

or

$$S(r_1) = s_1 r_1 + s_2 R^{\frac{1}{c_2}} r_1^{-\frac{c_1}{c_2}}. \tag{32}$$

The minimum value of the integral cost indicator of cyberimmunity, represented by (32), is solved analytically. To find the minimum value of the integral cost indicator of cyberimmunity, we will use the necessary condition [20].

We determine the minimum value of the integral cost of cyber immunity by the corresponding analytical relation

$$S_{\min} = S1 \left(\frac{s_1 c_2 R^{\frac{1}{c_2}}}{s_2 c_1} \right)^{\frac{c_1+c_2}{c_2}} + S_2 R^{\frac{1}{c_2}} \left(\frac{s_1 c_2 R^{\frac{1}{c_2}}}{s_2 c_1} \right)^{-\frac{c_1}{c_2}}. \tag{33}$$

It should be noted that the properties of local cyber immunities must be in the interval $[0;1]$, i.e. satisfy the constraints

$$0 \leq r \leq 1.$$

Thus, the condition must be fulfilled

$$r_{1,opt} = \left(\frac{s_2 c_1 R^{\frac{1}{c_2}}}{s_1 c_2} \right)^{\frac{c_2}{c_1+c_2}} \leq 1. \tag{34}$$

Condition (34) imposes a restriction on the ratio of eigenvalues. Indeed, for the property $p_{1,opt}$ there must be

$$\left(\frac{s_2 c_1 R^{\frac{1}{c_2}}}{s_1 c_2} \right)^{\frac{c_2}{c_1+c_2}} \leq 1; \quad \frac{s_2 c_1 R^{\frac{1}{c_2}}}{s_1 c_2} \leq 1; \quad \frac{s_2}{s_1} \leq \frac{c_2}{c_1} P^{-\frac{1}{c_2}}. \tag{35}$$

Similarly, for the property $p_{2,opt}$

$$\frac{s_2}{s_1} \leq \frac{c_2}{c_1} R^{\frac{-1}{c_1+c_2}}. \tag{36}$$

We assume the following parameter values

$$R = 0.9; \quad s_1 = 1; \quad s_2 = 1.5. \tag{37}$$

We check inequality according to the data

$$\frac{c_1}{c_2} R^{\frac{1}{c_2}} = 0.568; \quad \frac{c_1}{c_2} R^{-\frac{1}{c_1}} = 0.825; \quad \frac{s_1}{s_2} = 0.666,$$

that is, the inequality is satisfied.

Next, we calculate the optimal values of the local components of the informatization of Noah's software and TP according to

$$r_{1opt} = 0.908; \quad r_{2opt} = 0.9018. \quad (38)$$

In this case, the minimum cost according to (33) was

$$S_{min} = 2.28636. \quad (39)$$

Thus, it is established that for the given values of parameters (37) using the mathematical model (33), the minimum cost of integral informatization of Noah is the value (39).

Of course, if conditions (35) or (36) were not met, it would be necessary to change the ratio of specific values.

Conclusions. In the conditions of rapid growth and implementation of IT technologies, the issue of comprehensive protection of the obtained results arises with all its acuteness. Taking into account that the action of viruses that destroy the functioning of digital systems is complex in nature, that is, it affects all systems, a new concept appears that has a biological basis – cyber immunity. At the same time, information protection naturally means integral (total) protection from local negative influences. Therefore, it is necessary to improve the methods for combating information threats. Therefore, mathematical modeling of integral cyber immunity – information protection was aimed at building such a model, with the help of which it is possible to determine the property of integral cyber immunity as a set of properties of local cyber immunities. Moreover, there is a possibility of increasing the corresponding structure in order to take into account the emergence of new threats. The use of a static multiplicative structure of the mathematical model made it possible to implement these requirements. Based on the multifactor model of the integral indicator of information protection, its corresponding value was minimized based on the optimization of the values of local cyber immunities. Its parameters were identified in accordance with the given statistical material. Numerical calculations confirmed the obtained result regarding the reduction of the cost of information protection – integral cyber immunity.

References.

1. Cabinet of Ministers of Ukraine (2023). *Resolution "Order of the Cabinet of Ministers of Ukraine dated December 19, 2023 No. 1163 "On approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine"*. Retrieved from <https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini>
2. Babichev, A. V., & Samorodov, B. V. (2023). Conceptual model for assessing and analyzing the information component of an enterprise's economic security. *Problemy ekonomiky*, 3(57), 157-167. <https://doi.org/10.32983/2222-0712-2023-3-157-167>
3. Hnatenko, V. (2020). Information and economic security as a factor of stable development of the state. *Publichne uriaduvannia*, 5(25), 63-74. [https://doi.org/10.32689/2617-2224-2020-5\(25\)-63-74](https://doi.org/10.32689/2617-2224-2020-5(25)-63-74)
4. Machak, T., Dubyna, O., & Yurchenko, S. (2024). Information support for the management of the enterprise's economic security system and its improvement. *Ekonomika ta suspil'stvo*, 61. <https://doi.org/10.32782/2524-0072/2024-61-66>
5. Zakharov, O. I. (n.d.). *Information support for the management of the enterprise's economic security system*. Retrieved from https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf

6. Prykaziuk, N., & Gumenyuk, L. (2020). Cyber-insurance as an important tool of enterprise protection in the digitization economy. *Efektivna ekonomika*, 4. <https://doi.org/10.32702/2307-2105-2020.4.6>
7. Gordon, A., Loeb, P., & Zhou, L. (2021). Information Segmentation and Investing in Cybersecurity. *Journal of Information Security*, 12, 115-136. <https://doi.org/10.4236/jis.2021.121006>
8. Nekhai, V. A., & Nekhai, V. V. (2017). Information security as a component of economic security of enterprises. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriya: Ekonomika i menedzhment*, 24(2), 137-140.
9. Shashyna, M. V., & Volodin, V. V. (2016). The information component of the economic security of an enterprise. *Efektivna ekonomika*, 10.
10. Chubaevskiy, V., Blakyt, H., Bohma, O., Shtuler, Y., & Batrakova, T. (2022). Protection of information resources as an integral component of the economic security of an enterprise. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu* (4), 117-121. <https://doi.org/10.33271/nvngu/2022-4/117>
11. Puriy, H. M. (2019). Information systems and technologies in the management of the enterprise activity. *Efektivna ekonomika*, 6. <https://doi.org/10.32702/2307-2105-2019.6.56>
12. Onopko, A. S., & Zhyhalkevych, Zh. M. (2017). Application of information technologies in the management of the enterprise. *Aktual'ni problemy ekonomiky ta upravlinnia*, 11.
13. Pankratova, O. (2021). Digitalization as a modern trend in management development. *Ekonomika ta suspil'stvo*, 33. <https://doi.org/10.32782/2524-0072/2021-33-55>
14. Hodoborod'ko, A. Yu. (2022). Digital economy: approaches and features of development. *Biznes inform*, 9, 10-16. <https://doi.org/10.32983/2222-4459-2022-9-10-18>
15. Putsentjelo, P. R., & Humeniuk, O. O. (2018). Digital economy as the newest vector of reconstruction of the traditional economy. *Innovatsijna ekonomika*, 5-6(75), 131-143.
16. Beridze, T. M. (2016). *Statistical monitoring in the enterprise strategic management. Private enterprise Shcherbatykh O. V., Kremenchuk: Ukraine*. ISBN 978-617-639-087-9.
17. Piletska, S. T., Korytko, T. Iu., & Tkachenko, Ye. V. (2021). Model of integrated assessment of economic security of the enterprise. *Ekonomichnyi Visnyk Donbasu*, 3(65), 56-65. [https://doi.org/10.12958/1817-3772-2021-3\(65\)-56-65](https://doi.org/10.12958/1817-3772-2021-3(65)-56-65)
18. Konkolewsky, H. (2017). Digital economy and the future of social security. *Administration*, 65(4), 21-30. <https://doi.org/10.1515/ad-min-2017-0031>
19. Yerina, A. M. (2013). Statistical modeling of dynamic processes with saturation effect. *Modelivannia ta informatsijni systemy v ekonomits*, 89, 62-68.
20. *MATLAB Global Optimization Toolbox User's Guide R2020a*. (2020). The MathWorks, Inc. 878 Retrieved from <https://dokumen.pub/matlab-global-optimization-toolbox-users-guide-r2020anbsped.html>

Імперативи інформаційного захисту в структурі економічної безпеки підприємства

О. В. Роженко¹, Т. М. Берідзе*², О. В. Галицина³,
Ю. А. Гладка³, А. В. Бугра², В. Є. Галицин³

1 – Клайпедський університет, м. Клайпеда, Литовська Республіка

2 – Криворізький національний університет, м. Кривий Ріг, Україна

3 – Київський національний економічний університет імені Вадима Гетьмана, м. Київ, Україна

* Автор-кореспондент e-mail: beridzet2016@gmail.com

Мета. Побудова багатofакторної математичної моделі інформаційного захисту за відповідними властивостями її складових – кіберіунітетів.

Методика. У процесі дослідження застосована методологія системно-параметричного моделювання при формуванні параметрів впливу на інтегральний показник – інформаційний захист у структурі економічної безпеки підприємства. Використані принципи системного дослідження,

а саме емерджентності, формування інтегрального показника. Відповідно використана методика порівняльного аналізу при визначенні місця й ролі у структурі економічної безпеки підприємства.

Результати. Проаналізовані й досліджені основні підходи до формування інформаційного захисту на підприємстві як складової його економічної безпеки. Обґрунтовані можливість і доцільність формування інтегрального показника, що формується на основі складових із відповідними властивостями. Визначено, що загальна властивість інформаційного захисту – ступінь відповідності параметрів локальних властивостей-кіберіунітетів їх заданим значенням.

Наукова новизна. Запропонована дефініція «кіберіунітет» як запобіжник інформаційних загроз при визначенні інформаційного захисту. Сформована багатофакторна математична модель інтегрального показника інформаційного захисту, проведена мінімізація його відповідної вартості на основі оптимізації величин локальних кіберіунітетів.

Практична значимість. Практика застосування

запропонованої методики дозволяє удосконалити методи боротьби з інформаційними загрозами щодо безпекової складової підприємства. Математичне моделювання інтегрального показника кіберіунітету – інформаційного захисту спрямоване на побудову такої моделі, на засадах якої можна визначити властивість інтегрального кіберіунітету як сукупності властивостей локальних кіберіунітетів. Існує можливість нарощувати відповідні складові структури з метою урахування появи нових загроз. Застосування статичної мультиплікативної структури математичної моделі дало змогу реалізувати відповідні можливості. Вбачається, що застосування такого підходу дозволить забезпечити управління економічною безпекою підприємства від інформаційних загроз.

Ключові слова: кіберіунітет, багатофакторна математична модель, інформаційний захист, економічна безпека, оптимізація

The manuscript was submitted 15.02.25.