https://doi.org/10.33271/nvngu/2022-4/117

V. Chubaievskyi[1],
orcid.org/0000-0001-8078-2652,
H. Blakyta[1],
orcid.org/0000-0002-4848-9912,
O. Bogma[1],
orcid.org/0000-0002-5637-6010,
I. Shtuler[2],
orcid.org/0000-0002-0852-8526,
T. Batrakova[3],
orcid.org/0000-0002-5710-9416

1 – State University of Trade and Economics, Kyiv, Ukraine,
e-mail: chubaievskyi_vi@knute.edu.ua
2 – National Academy of Management, Kyiv, Ukraine
3 – Zaporizhzhia National University, Zaporizhzhia, Ukraine

PROTECTION OF INFORMATION RESOURCES AS AN INTEGRAL PART OF ECONOMIC SECURITY OF THE ENTERPRISE

Purpose. To build a mathematical model and algorithms for optimizing the losses that the company may suffer from information threats and the costs necessary to prevent these losses.

Methodology. General and special methods of cognition were used to perform scientific research: comparative analysis, logical generalization and systematization, mathematical abstraction, system-oriented analysis.

Findings. A mathematical model and optimization algorithms are proposed for using an improved methodological approach to the formation of information security of the enterprise in terms of minimizing costs and losses. This allows one not only to analyze threats and determine the weight of factors' influence but also to determine effective tactics and strategies to minimize their consequences.

Originality. During the research, a mathematical model and algorithms of optimization of losses from information threats and expenses of the enterprise for their neutralization are created. It also allows us to predict the likely consequences of probable threats. Methodological approaches to the formation of the optimal level of costs to maintain the appropriate level of security have been improved. It is shown that the analysis of information risks and threats of assessment of financial and economic stability of the enterprise to information danger should be accompanied by comparison in a dynamic mode of the corresponding economic indicators. The introduction of a methodological approach to comparing the real and optimal values of the integrated indicator of resilience allows managers to assess trends and directions of projected information threats and the need to allocate sufficient resources for protection.

Practical value. The results of the study can be used by practitioners to implement effective management of information risks and neutralize their impact on economic indicators of the enterprise and by scientists to develop strategies and methods to neutralize information threats to financial and economic stability, production and economic stability and organizational and economic stability, the latest methods of enterprise risk management.

Keywords: *information security of the enterprise, mathematical model, algorithm, integrated indicator, enterprise stability*

Introduction. In modern conditions of rapid changes in the field of information technology and its use to cause economic damage, management of economic information protection is becoming extremely important.

Information technology is an integral component of modern life; it determines the efficiency of production but also requires considerable attention to information and economic security of the enterprise.

Thus, this study is interdisciplinary, as the digital dimension of threats must be linked and treated as an economic risk.

Literature review. The research [1] reveals the essence of information protection and information security (IS) of enterprises. The main threats to IS, reasons and preconditions for loss of commercial information are classified. In [2] it is pointed out that in Ukraine the growing threats to IS due to "national peculiarities of management, such as lack of proper legal framework, use of unlicensed accounting software (Software), neglect of automated workplace protection rules, lack of accounting specialist's basics of cybersecurity". In [3] the experience of developed countries in building a system of IS enterprises is studied and the directions of its implementation in Ukrainian realities are indicated. The article [4] points out the difference between IS and cybersecurity of enterprises, the issues of organization of accounting information systems at enterprises are considered. The authors [5, 6] investigate the institutional foundations of insurance protection against cyberattacks and developed mechanisms for this protection. There are many areas that need to be defended for a modern enterprise and new ones are emerging. For example, in [7] the features of protection against the threats of the industrial Internet of Things are considered. This modern direction of IT activity promotes the development of production processes, forms a new virtual work environment, can significantly increase production productivity. However, it also represents significant opportunities for attackers [7]. Legal and regulatory aspects of enterprises are considered in [8]. This set of issues is also being studied by foreign scientists. Thus, it was found that the generation of competitive advantage is the drivers of the level of private sector investment in IS [9]. In [10], they analyze how the benefits of information segmentation and the comparison of benefits and costs contribute to investing in IS. Using the Gordon-Leb analytical model, a set of sufficient conditions for information segmentation is formed to reduce overall investment in IS. [11] proposes an approach to estimating the IS of small and medium enterprises in the cloud environment, which uses a framework that forms an index of the achieved level of IS in the corresponding cloud computing environment. In [12], the variants of the risk-oriented approach of the analysis of IS are analyzed. In [13], logistic regression was used to predict the risk of hosts from malicious software. The use of CAARS to assess software adaptability and threat assessment is described in [14]. The work is devoted to testing information and communication networks of enterprises from threats [15]. The use of the simulation approach and the model of current risk assessment on information communication systems is investigated in [16]. The threats to IS can increase significantly in modern hybrid warfare [17].

The topic of the work is related to the formation of a methodological approach to optimizing the probable losses from information threats and cyber-attacks and the costs to prevent them.

Unsolved aspects of the problem. At present, there is no comprehensive methodology linking forms and methods of information threats, cyber-attacks with direct economic consequences for the company in monetary terms, i. e. losses, and there is no proposal for mathematical modeling to optimize probable losses and costs to prevent them.

The purpose of the article is to offer a mathematical model and algorithms for optimizing the losses that can be incurred by the company from information threats and the costs necessary to prevent these losses.

Methods. Creating a system of information protection of economic information of the enterprise, on the one hand, requires financial resources. On the other hand, information threats that have not been neutralized will undoubtedly have economic consequences for the company. Since both aspects have a monetary dimension, this is the basis for comparison and optimization on a monetary scale.

Therefore, it becomes important to propose a mathematical model and algorithm that would optimize the cost of information protection of the enterprise while minimizing probable losses.

Mathematical methods of set theory, fuzzy logic and fuzzy relations, probability theory [18], context-dependent binary relations and graph theory were used in the study [19]. The use of such different mathematical methods is due to the fact that the factors that determine threats are different in nature: deterministic, stochastic, fuzzy and even verbal, and others.

Analytical research on threats of different types and directions has established that the factors that determine them are such samples of overlapping data. That is, the same factor or group of them can identify several threats. This problem of set theory is studied in detail in [19, 20].

It is proposed to define the whole set of these factors as a single space of variables Y, and the spaces of variables that define individual threats and, accordingly, are fragments of the general space of variables Y, to denote as $y_1, y_2, y_3, ..., y_n$.

This determines the possibility of the following mathematical formalization

$$y_1, y_2, y_3, \ldots, y_n \subsetneq Y.$$

Analytical research can prove that $y_1, y_2, y_3, ..., y_n$ are eigenvalues of the set Y.

And, in the general case, these local sets meet the condition

$$y_1 \cap y_2 \cap y_3 \ldots \cap y_n.$$

Set theory being used, a single space of variables Y can be defined as a superset, and $y_1, y_2, y_3, ..., y_n$ are subsets.

None of the subsets $y_1, y_2, y_3, ..., y_n$ contains empty elements and is a superset. However, each of the sets of parameters μ_i for each i^{th} risk factor may contain an empty set.

Moreover, this is true by definition

$$\{\mu_i\} \in y_i.$$

However, each of the sets of parameters for each risk factor is not an empty set

$$\{\mu_i\} \notin \varnothing.$$

For a superset of the space of variables Y then the following must be fulfilled

$$Y - \sum_{1}^{n} y_i = \varnothing.$$

Thus, the use of this apparatus of set theory makes it possible to form the above restrictions.

These constraints preclude actions on variable space operations that can lead to multicollinear optimization errors.

In particular, from the point of view of applied economics, this will eliminate the cost of neutralizing one threat, when these costs can simultaneously neutralize a group of threats, including the specified one.

In each subspace of variables y_i in the next step of the algorithm are determined deterministic y_i^d stochastic y_i^s and fuzzy y_i^f subspaces of variables that do not intersect.

These subspaces correspond to the response functions f_i^d, f_i^s, f_i^f [18], which form the response surface, on which one of the standard methods (steep ascent, steep ascent, etc.) is the search for the extremum of the cost function. The software of these standard methods is also standard.

To analyze the level and direction of possible losses, an assessment of the financial and economic resilience of the enterprise to the impact of threats is performed. Part of this influence, its tools are information threats. These threats are assessed by the degree of their contribution (weight).

The use of system-oriented approach allowed forming the basic principles or requirements, from a practical point of view, of building an information system to protect, first of all, economic information:

1. Integration of data of various formats from various information sources.

2. Providing opportunities for system development. A modular approach is used for this. The modular approach allows building capacity of the system without radical restructuring of its architecture. This approach is provided by the gradual integration into the system of new modules.

3. Independence of digital solutions from individual manufacturers of hardware or ancillary software.

4. Scalability of the information system. The increase in the number of users and auxiliary devices should be provided by the envisaged possibility of increasing computing resources.

5. The possibility of extended adaptability of the system to the software development kit of different manufacturers. The information system can be flexibly adapted to various industrial protocols, development tools, auxiliary utilities, and so on.

6. Ability to connect video surveillance systems, regardless of their location, hardware or auxiliary software.

7. Control of operation of equipment and auxiliary software.

8. Monitoring and recording of cash transactions.

Analytical study on the main directions of the formation of information threats in terms of their implementation showed that it is a violation of: confidentiality; system integrity; availability of information.

The risk of breach of confidentiality is due to unauthorized access to information, the disclosure of which is unacceptable.

The risk of integrity is associated with tampering or damage to data.

The risk of impaired availability is associated with reduced performance of the information system or its elements, blocking access to data.

These risks are due to improper characteristics of the information system, the external environment, the actions of staff, and so on.

All of the above can lead to a negative impact on the functioning of the enterprise, namely:

- interruptions in the work of automated control systems;
- loss of information intended solely for official use;
- inaccuracy of tax, financial and other reports;
- unauthorized access to the information space of the enterprise and its automated management systems;
- the possibility of disclosing false or partially false information, and others.

Disclosure of false or partially false information about the operation of the enterprise may lead to:

- depreciation of the cost of capital of the enterprise;
- significant increase in the cost of external loans;
- difficulties in business relations with contractors;
- non-performance of contracts;
- reducing the effectiveness of management decisions;
- loss of intellectual property resources;
- deterioration of conditions for the sale of products or services, etc.

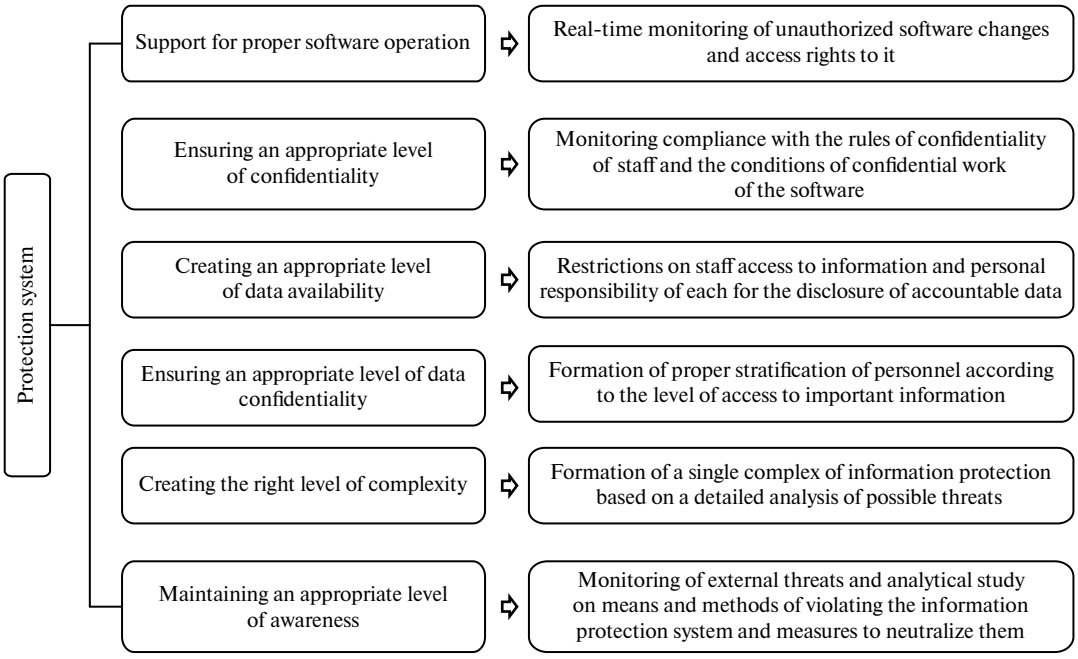

Fig. 1. Components of enterprise information protection systems

According to the Internet Security Threat Report [21] and based on the Cyberthreat Defense Report [22], the formation of threats in the field of economic information of enterprises in the period for which the analysis was conducted, took place through:

- use of unlicensed, improperly certified and verified software;
- improper user authentication;
- improper protection of used equipment;
- inadequate awareness of the peculiarities of work in conditions of information danger and training of personnel on information security;
- neglect of information discipline by the staff of the enterprise;
- improper compliance with the basic requirements and rules of data storage and backup;
- inadequate monitoring of external threats;
- absence of a specialist responsible for information protection at the enterprise;
- lack of control over the delimitation of access rights to information, etc.

This analysis became the basis for the formation of a list of components of the integrated system of protection of economic information of the enterprise (Fig. 1) in accordance with the standard ISO/IEC 27001:2013 [22]. Each of the modules of the integral system performs a range of tasks, outlined and schematically presented in Fig. 1.

The specified system of protection of economic information of the enterprise is a methodological basis both for the corresponding organization of service of protection, and for formation of the automated environment of an estimation of levels of threats, probable losses in real time.

The implementation of the system of protection of economic information of the enterprise in the form of an algorithm for managing the optimization of costs and losses is presented in Fig. 2.

The cost and loss optimization management algorithm implements in practice the methodology of synthesis of two scientific disciplines, has two components of subsystems that synergistically reinforce each other: information and economic.

Results. Assessment of financial and economic stability of the enterprise to information threats should be accompanied by a dynamic comparison of relevant economic indicators.

Coefficients of financial and economic stability of the enterprise were chosen as such indicators. This is due to the fact that the information threat must be presented to economists in a form they understand to identify the direction in which the threat operates or will operate. This will allow a more relevant choice of hazard neutralization methods (Fig. 2).

An example of assessing the financial and economic resilience of the enterprise to the impact of threats, the share of impact in which information threats are assessed by the degree of their severity, is demonstrated by the analysis of the maritime industry in Table 1.

These coefficients of financial and economic stability of the enterprise form the corresponding integrated indicator of

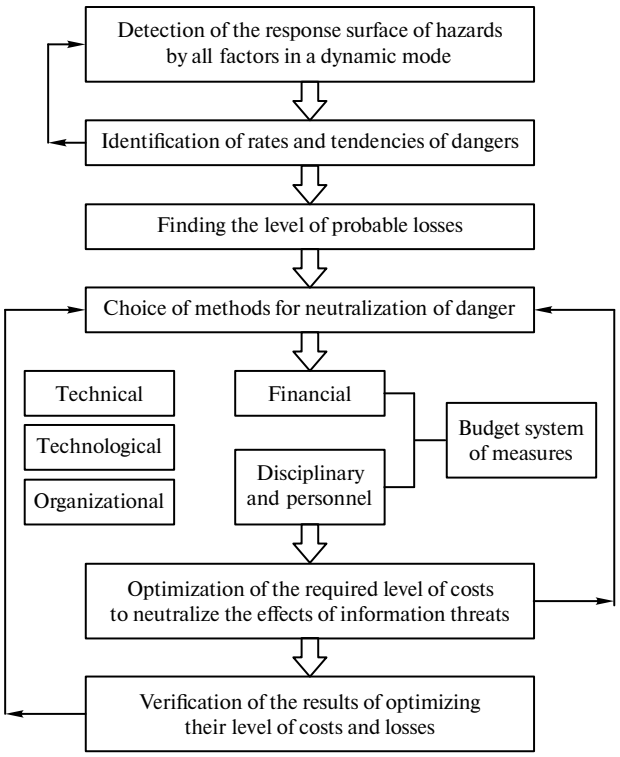

Fig. 2. Cost and loss optimization management algorithm

Table 1

Assessment of financial and economic stability of the enterprise to information threats

Indicator	Actual value	Expected value	Threat level		Weight
			Past period	Current period	
Equity concentration ratio	0.68	0.72	0.01	0.012	0.15
Coefficient of financial dependence	1.43	1.48	0.01	0.012	0.10
Equity maneuverability ratio	0.08	0.10	0.01	0.012	0.05
Rated capital concentration ratio	0.33	0.35	0.01	0.011	0.05
Coefficient of long-term investment structure	0.11	0.11	0.01	0.010	0.10
Ratio of long-term borrowings	0.08	0.08	0.01	0.010	0.10
Rated to equity ratio	0.43	0.45	0.01	0.011	0.10
Absolute liquidity ratio	0.01	0.01	0.01	0.010	0.05
Rapid liquidity ratio	0.54	0.58	0.01	0.011	0.15
Coefficient of coverage	1.23	1.29	0.01	0.012	0.15

Table 2

Comparison of real and optimal values of the integrated stability index

Indicator		Weight	Value	Result	Optimal value
External indicators of stability		0.28	0.392	0.314	0.325
Internal indicators of stability	Financial and economic stability	0.25	0.948	0.237	0.250
	Production and economic stability	0.19	0.769	0.146	0.150
	Organizational and economic stability	0.14	0.821	0.115	0.120
Integral indicator of stability				0.812	0.845

financial and economic stability. This integrated indicator of financial and economic stability together with the corresponding indicators of industrial and economic stability and organizational and economic stability form an integrated indicator of stability (Table 2).

Comparisons of the real and optimal values of the integrated indicator of sustainability allow managers to assess the effectiveness of measures and verify the results of optimizing its level of costs and losses (Fig. 2).

In Fig. 3 an example is given in the graphical form of intermediate results of cost optimization in accordance with the required level of information security for a real enterprise. The level of information security coincides with the abscissa in the direction – on the right there is an increase in this indicator.

For greater clarity, the costs of achieving a certain level of information security are divided into groups, namely: "Costs for monitoring information hazards", "Preventive costs", "Total costs" (Fig. 3).

Cost item "Costs for monitoring information hazards" is unchanged for increasing or decreasing the level of information hazards and its contribution to total costs is not very significant.

Cost item "Preventive costs" indicates a tendency to increase these costs to achieve a higher level of information security.

The article "Losses" has a smoothed hyperbolic character approximately to the intersection with the line "extremum" and then linearized to the intersection with the abscissa.

In the general case, these costs are approximated by a power function. The degree of their growth depends on various factors: the level of threats, the difference between the optimal and actual values of the integrated indicator of the stability of the enterprise, the level of its profits, and so on.

The resulting graph "Total costs" is parabolic, i.e. with a guaranteed presence of extremum. The total cost is minimized along the line indicated in Fig. 3 as "Extreme".

The search for this extremum is in accordance with the developed algorithm that implements the mathematical model presented above.

To illustrate (Fig. 4) the data of the calculation of the search for the extreme level of losses and costs of one of the enterprises of the maritime industry.

In this case, the response surface of the mathematical model of finding the extremum of the level of losses and costs is three-dimensional, which allows its graphical representation.

In the general case, the measurements may be greater.

In fact, some graphs presented in Fig. 3 are sections in the corresponding projections of the three-dimensional components of the figure shown in Fig. 4.

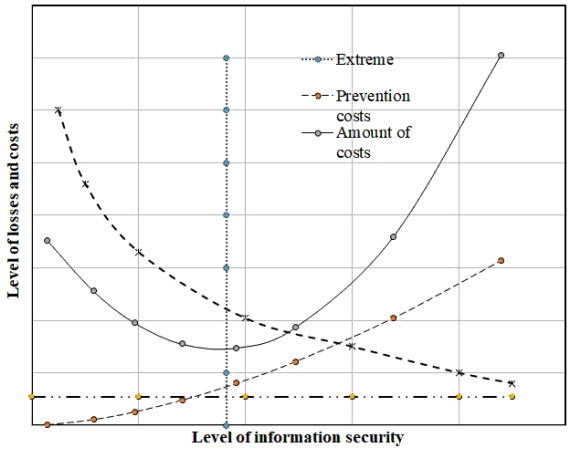

Fig. 3. Cost optimization in accordance with the required level of information security

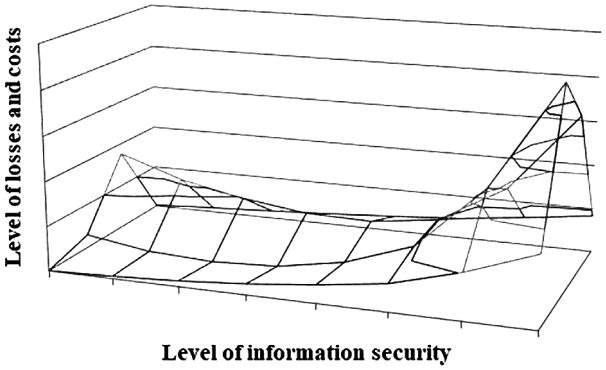

Fig. 4. Three-dimensional response surface of a mathematical model for finding the extreme level of losses and costs

These graphical representations illustrate the actions of algorithms for finding the optimal value of costs to neutralize information risks and give a visual representation of the company's management, economists, the reasons of the information security manager to clearly justify the cost of information security and bring them to the appropriate level.

Conclusions. In the process of research, a mathematical model and algorithms for optimizing the losses that can be incurred by the company from information threats and the costs necessary to prevent these losses.

The use of a system-oriented approach allowed forming the basic principles of building an information system for the protection of primarily economic information. Analytical research of the main directions of threat formation has proved that it is a violation of confidentiality; system integrity; availability of information.

This analysis became the basis for the formation of a list of components of the integrated system of protection of economic information of the enterprise and the implementation of this system in the form of a cost-loss and loss management algorithm.

Methodical approaches of formation of an optimum level of expenses are offered.

It is shown that the analysis of information risks and threats of assessment of financial and economic stability of the enterprise to information danger should be accompanied by comparison in the dynamic mode of the corresponding economic indicators.

Namely, these indicators are: financial and economic stability of the enterprise, production and economic stability and organizational and economic stability. These indicators form an integrated indicator of the stability of the enterprise.

The introduction of a methodological approach to comparing the real and optimal values of the integrated indicator of enterprise sustainability allows management to assess the effectiveness of measures and verify the results of optimization in accordance with reasonable levels of costs and losses.

The impact of threats on the dynamics of these indicators allows the company's management to assess the main trends and directions of the projected information threats and reasonably consider the need to allocate the necessary resources to protect economic and other information.

The practical implementation of the proposed methodological approach, the developed mathematical model and algorithms was carried out on the example of maritime enterprises.

The study will establish that the results of the mathematical model and algorithms for optimizing losses and costs should be presented in graphical form, which allows achieving relevant results in assessing the levels of risks and costs to specialists in various specialties, identifying areas and consequences of information threats.

Prospects for further research include the development of an automated environment for assessing the levels of threats, probable losses in real time.

References.

1. Bekhter, L. (2020). Threats of information security and protection of information as a component of economic security of agricultural enterprises. *Agrosvit*, *12*, 66-70. https://doi.org/10.32702/2306-6792.2020.12.66.

2. Popivniak, Yu. M. (2019). Cybersecurity and Protection of Accounting Data under Conditions of Modern Information Technology. *Business-Inform*, *8*, 150-157.

3. Lapinska, Ye. I. (2019). External experience in the protection of information in the field of enterprise and its use in Ukraine. *State and regions, 3*(65), 174-177. https://doi.org/10.32840/1813-338X-2019-3-28.

4. Viter, S. A., & Svitlyshyn, I. I. (2017). Protection of accounting information and cyber security of the enterprise. *Economy and society*, *3*, 497-502.

5. Shkarlet, S., Dorosh, M., Druzhynin, O., Voitsekhovska, M., & Bohdan, I. (2021). Modeling of Information Security Management System in the Project, (pp. 364-376). In Shkarlet, S., Morozov, A., & Palagin, A. (Eds) (2021). *Mathematical Modeling and Simulation of Systems (MODS'2020). MODS 2020. Advances in Intelligent Systems and Computing*, (Vol. 1265). Springer, Cham. https://doi.org/10.1007/978-3-030-58124-4_35.

6. Prykaziuk, N., & Gumenyuk, L. (2020). Cyber-insurance as an important tool of enterprise protection in the digitization economy. *Efektyvna ekonomika*, *4*. https://doi.org/10.32702/2307-2105-2020.4.6.

7. Sotnyk, I. N., & Zavrazhnyi, K. Yu. (2017). Approaches to provide information safety of the Industrial Internet of Things at the enterprise. *Marketing and innovation management, 3*, 176-178. https://doi.org/10.21272/mmi.2017.3-17.

8. Diorditsa, I. (2021). Administrative and legal content of the national cybersecurity system as a component of the national security system of Ukraine. *Actual problems of domestic jurisprudence,* (1), 79-83. https://doi.org/10.15421/392117.

9. Loe, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security, 9*, 133-153. https://doi.org/10.4236/jis.2018.92010.

10. 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.

11. Rupra, S., & Omamo, A. (2020). A Cloud Computing Security Assessment Framework for Small and Medium Enterprises. *Journal of Information Security*, *11*, 201-224. https://doi.org/10.4236/jis.2020.114014.

12. Savelieva, T. V., Panasko, O. M., & Prigodyuk, O. M. (2018). Analysis of methods and means to implement a risk-oriented approach in the context of providing enterprise information security. *Bulletin of Cherkasy State Technological University*, (1), 81-89. https://doi.org/10.24025/2306-4412.1.2018.153279.

13. Halakhov, Y. M., & Sobchuk, V. V. (2019). Development of models of cyber-attacks in the plane enterprise information security. *Telecommunication and information technologies*, *4*, 12-24. https://doi.org/10.31673/2412-4338.2019.041224.

14. Vakun, O., Hrabchuk, I., & Zakharchuk, V. (2019). Adaptability of Software for Reporting to User Requirements. *Modern Economics*, *13*(2019), 49-54. https://doi.org/10.31521/modecon.V13(2019)-07.

15. Maraj, A., Jakupi, G., Rogova, E., & Grajqevci, X. (2017). Testing of network security systems through DoS attacks, *2017, 6th Mediterranean Conference on Embedded Computing (MECO), Bar,* 17030164. https://doi.org/10.1109/MECO.2017.7977239.

16. Lakhno, V., Kryvoruchko, O., Mohylnyi, H., Semenov, M., Kiryeyev, I., Matiievskyi, V., & Donchenko, V. (2019). Model of indicator of current risk of threats realization on the information communication system of transport. *International Journal of Civil Engineering and Technology, 10*(02), 1-9.

17. Hrabchuk, I. L. (2018). Organization of protection of accounting information in a hybrid war. *Problems of Theory and Methodology of Accounting Control and Analysis, 3*(41), 20-24. https://doi.org/10.26642/pbo-2018-3(41)-20-24.

18. Bazaluk, O., Kotenko, S., & Nitsenko, V. (2021). Entropy as an Objective Function of Optimization Multimodal Transportations. *Entropy*, *23*(8), 946. https://doi.org/10.3390/e23080946.

19. Kotenko, S., Nitsenko, V., Hanzhurenko, I., & Havrysh, V. (2020). The Mathematical Modeling Stages of Combining the Carriage of Goods for Indefinite, Fuzzy and Stochastic Parameters. *International Journal of Integrated Engineering*, *12*(7), 173-180. https://doi.org/10.30880/ijie.2020.12.07.019.

20. CyberEdge Group (2021). *Cyberthreat Defense Report*. Retrieved from https://cyber-edge.com/cdr/.

21. Symantec (2019). 2019 *Internet Security Threat Report: Executive Summary*, (Vol. 24). Retrieved from https://docs.broadcom.com/doc/istr-24-executive-summary-en.
22. EY Global (2018). *Is cybersecurity about more than protection?* Retrieved from https://www.ey.com/en_gl/consulting/global-information-security-survey-2018-2019.

Захист інформаційних ресурсів як невід'ємна складова економічної безпеки підприємства

В. І. Чубаєвський[1], *Г. В. Блакита*[1], *О. С. Богма*[1], *І. Ю. Штулер*[2], *Т. І. Батракова*[3]

1 – Державний торговельно-економічний університет, м. Київ, Україна, e-mail: chubaievskyi_vi@knute.edu.ua
2 – Вищий навчальний заклад «Національна академія управління», м. Київ, Україна
3 – Запорізький національний університет, м. Запоріжжя, Україна

Мета. Побудувати математичну модель і алгоритми оптимізації збитків, що може понести підприємство від інформаційних загроз, та необхідних для запобігання вказаним збиткам витрат.

Методика. Для виконання наукового дослідження використані загальні та спеціальні методи пізнання: порівняльного аналізу; логічного узагальнення й систематизації; математичного абстрагування; системно-орієнтованого аналізу.

Результати. Запропонована математична модель і алгоритми оптимізації за використання вдосконаленого методологічного підходу до формування системи інформаційного захисту підприємства з точки зору мінімізації витрат і збитків. Це дозволяє не тільки проаналізувати загрози та визначити вагу впливу їх чинників, але й визначити ефективну тактику та стратегію мінімізації їх наслідків.

Наукова новизна. Під час дослідження створена математична модель і алгоритми оптимізації збитків від інформаційних загроз і витрат підприємства для їх нейтралізації. Це дозволяє також прогнозувати ймовірні наслідки вірогідних загроз. Удосконалені методичні підходи формування оптимального рівня витрат на підтримку належного рівня безпеки. Показано, що аналіз інформаційних ризиків і загроз оцінки фінансово-економічної стійкості підприємства до інформаційної небезпеки має супроводжуватися співставленням у динамічному режимі відповідних економічних показників. Упровадження методологічного підходу до порівняння реального та оптимального значень інтегрального показника стійкості надає можливість менеджерам підприємства оцінити тренди й напрями дії прогнозованих інформаційних загроз і необхідність виділення достатніх ресурсів для захисту.

Практична значимість. Результати дослідження можуть бути використані практиками для впровадження ефективного управління інформаційними ризиками й нейтралізації їх впливу на економічні показники підприємства та науковцями для розробки стратегій і методів знешкодження інформаційних загроз фінансово-економічної стійкості підприємства, виробничо-економічної стійкості та організаційно-економічної стійкості, а також для розробки новітніх методів управління ризиками підприємства.

Ключові слова: *інформаційна безпека підприємства, математична модель, алгоритм, інтегральний показник, стійкість підприємства*

The manuscript was submitted 07.07.22.