Organizational and Economic Provision of Corporate Information Effective Protection

Valery Lakhno[1], Bissenbay Satzhanov[2], Abzal Tabylov[2], Vitaliy Chubaievsyi[3], and Serhii Kaminskyi[3]

[1]*National University of Life and Environmental Sciences of Ukraine, 15 Heroyiv Oborony str., Kyiv, 03041, Ukraine*
[2]*Yessenov University, microdistrict 32, Aktau, 130000, Kazakhstan*
[3]*State University of Trade and Economics, 19 Kyoto str., Kyiv, 02156, Ukraine*

Abstract

The model that describes the procedure for formalizing the task of optimizing the Information Security System (ISS) of a business entity (company) has been further developed. At the same time, unlike existing approaches, the emphasis in the proposed solution is on mathematical, algorithmic, and computer support for the decision-making procedure in the task of organizational and economic support for the effective protection of corporate information in the context of the company's Information Security (IS) management tasks. It enables the defense side to effectively determine the parameters of organizational management of the company's information security infrastructure. The contour of the Decision Support System (DSS) in the process of the company's information security infrastructure development was considered. In the context of a qualified experts' shortage in the field of information security of companies, additions to the model were proposed that allow taking into account the impact of human resources of experts in information security issues on the management of the company's information security infrastructure. Recommendations were offered and the corresponding application software—DSS was described. The use of such DSS will help one to minimize the risks associated with the lack of qualified IS experts in many companies.

Keywords

Information protection, information security, organizational and economic support, infrastructure management, decision support system, risk minimization.

1. Introduction

In the conditions of globalization, cooperation, and competition, not a single company (regardless of the field of activity) can function without a developed structure of information technologies and systems (hereinafter, respectively, IT and IS), which ensure the success and efficiency of both making individual management decisions and efficiency of company business processes as a whole. The dynamic growth of the IT infrastructure of companies has long overcome the first stage of the traditional expansion of the scale of hardware and software complexes used to automate the collection, storage, processing, transmission, and receipt of information. In modern conditions, the priority has become not so much the quantity and quality of IT and IS used in the business processes of business entities, but the reliability and completeness of the information that contributes to the adoption of optimal management decisions.

Traditional IS for large companies has been replaced by corporate IS (hereinafter referred to as CIS). However, the rapid development of IT and IS companies has given rise to such an acute problem as ensuring the information security (hereinafter referred to as IS) of companies and the safety of their Information Resources (hereinafter referred to as InR). The use by the attacking side of increasingly complex methods for implementing cyber-attack scenarios has led to the fact that any CIS already at the time of its

CPITS 2023: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: lva964@gmail.com (V. Lakhno); satzhanov1959@mail.ru (B. Satzhanov); tabylov62@mail.ru (A. Tabylov); chubaievskyi_vi@knute.edu.ua (V. Chubaievsyi); s.kaminskyj@knute.edu.ua (S. Kaminskyi)
ORCID: 0000-0001-9695-4543 (V. Lakhno); 0000-0001-9811-9963 (B. Satzhanov); 0000-0002-2040-8228 (A. Tabylov); 0000-0001-8078-2652 (V. Chubaievsyi); 0000-0002-4884-1517 (S. Kaminskyi)

operation requires the adoption of appropriate measures aimed at protecting corporate information. Consequently, each enterprise must ensure a high degree of protection of commercial information, and the integrity of its InR [1].

Continuous organizational and economic support of the company's information security procedures can minimize business risks, maximize return on investment, facilitate business opportunities, and enhance the company's commercial image and competitive advantages [1, 2, 33–36].

To ensure effective protection of InR and stable management of information security, companies must not only periodically assess information security, but also constantly analyze the processes for their CIS.

While the process of information security effectiveness measurement is recognized as an important element of an information security management system, many gaps and challenges remain. Since information security is a complex and multifaceted system with a large amount of data, specialists in the information security departments of companies are often overloaded with current work. And, therefore, they cannot develop effective processes for assessing the current state of the company's information security.

As practice shows, information security specialists mainly focus on technical goals. At the same time, only a small part of them can perform a comprehensive assessment of the effectiveness of the company's information security, including work on organizational and economic support for the effective protection of corporate information. World experience undeniably proves that a simple increase in the number of means and measures to protect information (hereinafter referred to as IS) does not always give a tangible effect [2].

Moreover, in several situations [3, 37], the implementation of such a scenario only increases the workload of the personnel involved in the information security of the company. Moreover, errors in the planning of resources allocated for ensuring the information security of companies lead to the fact that expensive protection of InR with little value or significance for business processes results in damage. Such damage may not always be financially obvious. In some cases, the extent of reputational damage is many times greater than the financial losses from the loss of information [4]. The same can be said about the insufficiently effective protection of valuable InR companies. For example, according to [5], the presence in a company of leaks of important internal information used in business processes in volumes >20% can lead to the fact that the company will become bankrupt with a probability of 60%. Moreover, according to [5, 6, 38–39], more than 90% of companies that were deprived of access to their own InR for periods of >10 days stopped their economic activities with a high degree of probability.

Summarizing the above, there is a certain contradiction. So, on the one hand, significant costs for the Information Security System (ISS) are an obligatory component of the costs of almost all business entities. On the other hand, it is just as necessary to solve the problem related to optimizing the costs of building an effective information security system and organizing efficient processes in CIS. The conclusions drawn predetermine the relevance of this study, aimed at improving the methods and models of organizational support for IT infrastructure management processes in the information security system of companies.

2. Literature Review and Analysis

It is shown in [7, 8] that the increasing intensity and more complex scenarios of cyber-attacks make relevant not only the permanent improvement of the hardware and software systems of the information security system but also dictate the need to take other measures. Such measures, in particular, include measures aimed at improving the organizational and economic support for the effective protection of corporate information of business entities. According to [9, 10], it is necessary to provide the protection side with effective intelligent systems that can facilitate the rather routine work of managing the information security of companies.

The need for prompt decision-making related to organizational and economic support and management of corporate information protection has made promising research on the development of Decision Support Systems (DSS) [11, 12] in this area. In these works, as well as in [13, 14], it is shown that in the framework of the creation of such DSS, new methods, models, algorithms, and Application Software (AS) used to solve such problems are being developed accordingly. The authors of the considered works, however, do not give weighty arguments proving the effectiveness of the widespread use of such DSS for most business entities. The experience of using DSS in

IS management tasks for individual companies is considered in [15, 16]. However, as noted in [16, 17], the existing commercial DSS in the tasks of providing information security to companies are of a closed nature. The authors state that the acquisition by individual small companies of this class of DSS is associated with significant financial costs. Non-commercial DSS existing on the application software market in IS tasks do not have sufficient functionality [17].

As shown in [18–20], the issues of complex implementation of DSS in the tasks of organizational and economic support for the effective protection of corporate information in the context of information security management tasks have not been systematically considered.

More than half of all cyber-attacks are aimed at small companies and enterprises [21]. Despite such depressing statistics, as shown in [22], a significant part of the management of small and medium-sized companies continues to believe that information security is an extra cost item. This opinion should be partly based on the shortage of qualified human resources involved in information security. Thus, small companies experience more problems in monitoring the effectiveness of information security. As shown in [23, 24], the use of formal and complex procedures focused on anticipating and predicting information security incidents has become a common practice for such small companies.

Taking into account the conclusions made by the authors in [13, 15, 17–20, 24], the problem of systemic implementation of intelligent DSS in the tasks of organizational and economic support and information security management of companies remains unresolved. Mathematical-algorithmic and computer support of the decision-making procedure and qualitative expert assessment allow solving the problems of organizational and economic support of effective protection of corporate information in the context of information security management tasks in the most efficient way. Thus, conceptually innovative approaches can be based on the paradigm of the integrated implementation of DSS in the tasks of organizational and economic support for the effective protection of corporate information in the context of the tasks of IS management of companies.

The above reasons make the subject of our study relevant. In our opinion, it is advisable to focus on the implementation of such DSS in small companies, where the situation with information security seems to be the most critical.

3. The Purpose of the Work and the Objectives of the Study

The purpose of the work is to develop a model of organizational and economic support and management of information security companies.

To achieve the goal of the work, it is necessary to solve the following tasks:

- to develop a model of organizational and economic support and IS management of companies, taking into account the minimization of risks associated with the lack of qualified IS experts.
- to develop and test a DSS for the organizational, economic support, and management of information security of companies, which will allow the protection side to rationally use methods and information security.

4. Methods and Models

It is noted in [25, 26] that in the context of the global digitalization of the economy, many companies are faced with a shortage of qualified cybersecurity specialists. And if most of the InR threats can be blocked by hardware and technical information protection systems, then the issues of organizational and economic support for the effective protection of corporate information still have to be solved by information security analysts. And here much depends on the qualifications and experience of the work of a particular specialist. In our opinion, the direction associated with the widespread introduction into practice of solving problems of organizational and economic support of corporate information protection systems of intelligent DSS may turn out to be quite effective, see Fig. 1.

Such systems are capable of performing rather routine and time-consuming computational and analytical tasks, for example, related to optimizing the resolution of individual information security facilities along the contours of the company's information security. Also, this kind of DSS will allow you to quickly make decisions when redistributing information security in the face of dynamic confrontation with the attacking side [27, 28].

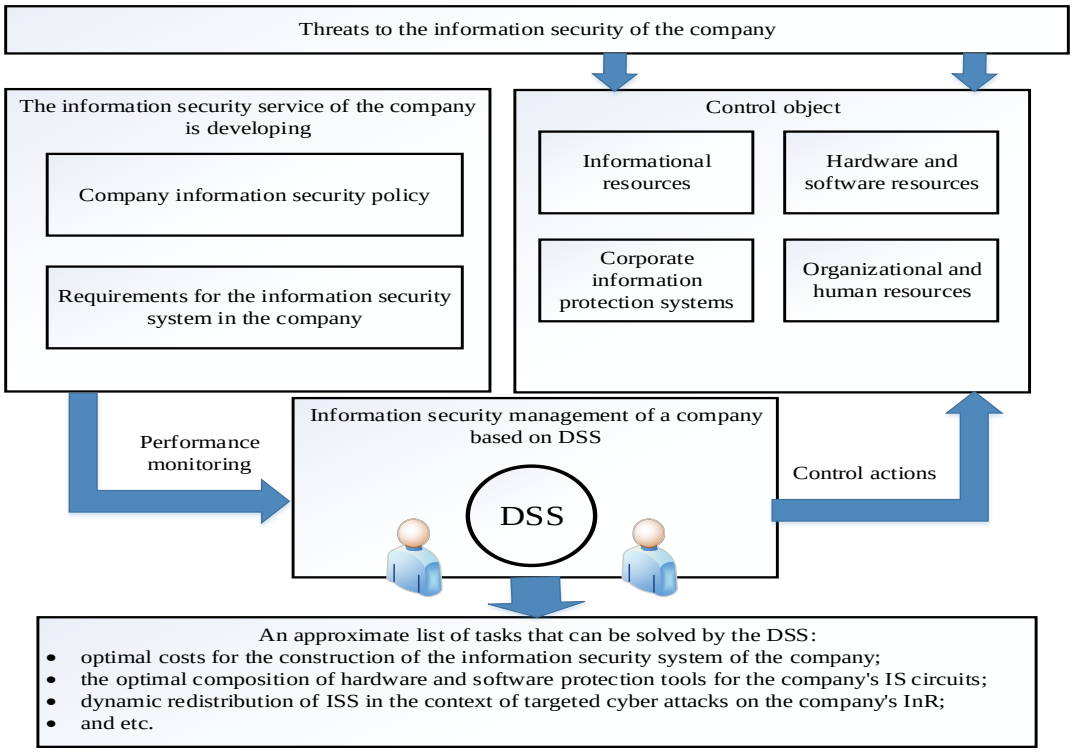

Figure 1: Structural diagram of the DSS in the tasks of ensuring the company's information security

A common practice in the Information Security Management System (hereinafter referred to as the ISMS) of companies is the delegation of some of the tasks that require sufficiently high qualifications to external experts. However, external experts are usually auditors who evaluate information security metrics through document reviews, observations, and interviews with staff. This approach has a positive effect when it is required to assess the technical vulnerabilities of the CIS and risks (which auditors usually identify using penetration tests and analysis of information security events (incidents). At this stage, complex calculations and complex technical tests are not needed. At this stage, it may be sufficient to present the results of such tests and analyses to the management of the company. Based on such analysis and audit findings, management can assess the importance of specific measures to be taken to ensure the protection of corporate information. However, this approach becomes less effective when it comes to the need for technical and economic calculations in the tasks of providing enterprise information security.

For example, such tasks include multicriteria optimization tasks related to the search:

- optimal costs for the construction of the information security system of the company.
- the optimal composition of hardware and software protection tools for the company's IS circuits.

dynamic redistribution of information security in the context of targeted cyber-attacks on the company's InR, etc.

In such situations, in our opinion, it is advisable to shift routine calculations and the search for mathematical solutions to these optimization problems to the DSS. With this approach, the processes of analyzing information security audit data and the results of mathematical and economic modeling using DSS, and in some cases risk forecasting, are presented to the company's management. Based on this data, management decides on the necessary corrective actions aimed at achieving the desired target level of information security. Moreover, we note that the results of mathematical and economic modeling and risk forecasting when using DSS are devoid of a subjective component, and are not tied to the qualifications of both internal and external auditors. In this case, we fully follow the well-established plan-do-check-act approach. The use of DSS makes this approach more flexible, operational, and continuous.

As the number and complexity of attack scenarios grow, information security becomes one of the main management tasks of company management. This is because we have to consider

the management of a complex system. Moreover, wrong decisions regarding the information security of a company can lead to a decrease in the performance of all business processes. When the company's information security specialists are competent and able to provide a high level of information security and protection, in most cases they act effectively in solving the problems of planning and investment activities in information security. Thus, the overall efficiency of a company's business processes most often depends on the consistency between information security planning and business planning.

Solving problems related to the optimization of the information security system of a company includes the following steps [14, 28]:

1. determine the parameters of organizational management of IT infrastructure and information security.
2. to minimize the cost of building ISS.
3. choose the optimal amount of investment in the company's information security.
4. eliminate (or minimize) the possibility of information leaks in the company.

The computational core of the DSS can take on all the calculations for the search for local or global extrema of the objective functions.

For example, when searching for a solution to the problem of minimizing financial costs for information security, you can use a function of the form:

$$C = \sum_{i=1}^{n}\sum_{j=1}^{m} C_{ij} \cdot \alpha_{ij} + \sum_{i=1}^{n} C_i \cdot \beta_i \to \min, \qquad (1)$$

where is $i = \overline{1,n}; \quad j = \overline{1,m}$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} s_j \cdot m_{ij} \cdot \alpha_{ij} \geq PL_{dc}, \sum_{i=1}^{n} \alpha_{ij} = 1, \forall j \in J, \qquad (2)$$

where C_{ij} is the number of costs for protecting the j^{th} resource with the help of the i^{th} ISS; C_i is the number of costs for the set of InR with the help of the i^{th} ISS; $I = \{i_1,...,i_n\}; J = \{j_1,..., j_m\}$ – accordingly, the set of information security in the company and the set of InR, which are subject to protection; m_{ij} assessment of the effectiveness of protecting the j^{th} resource with the help of the i^{th} ISS; s_j is the factor of the importance of the j^{th} resource in the complex assessment of the information security system of the company; α_{ij} – a binary value, if $\alpha_{ij} = 1$ else i^{th} ISS is selected to protect the j^{th} resource, $\alpha_{ij} = 0$ then i^{th} ISS is used to protect only against potential threats; β_i – binary value, if $\beta_i = 1$ then i^{th} ISS can be used, if $\beta_i = 0$, then not; PL_{cd} is the level of protection at the cost of information security in the amount of (C) and threats (D).

If we are talking about the need to maximize the degree of protection of the company's InR, then we can use the following objective function:

$$PL_C = \sum_{i=1}^{n}\sum_{j=1}^{m} s_j \cdot m_{ij} \cdot \alpha_{ij} \to \max, \qquad (3)$$

subject to the following boundary conditions:

$$C = \sum_{i=1}^{n}\sum_{j=1}^{m} C_{ij} \cdot \alpha_{ij} + \sum_{i=1}^{n} C_i \cdot \beta_i \leq C_d, \qquad (4)$$

$$\sum_{i=1}^{n} \alpha_{ij} = 1, \forall j \in J,$$

where $\alpha_{ij} \in \{0;1\}, \beta_{ij} \in \{0;1\}.$

The high dynamics of changes in the landscape of cyber threats and the external environment for modern companies that build many of their business processes on the use of IT and IS dictates its characteristics in the formation of a personnel policy for information security specialists. The purpose of this study is not a detailed study of the problem of the effectiveness of the use of human resources for information security in companies. We just want to emphasize that this is still little studied and requires the close attention of company leaders.

In general, the set that formalizes the shortage of human resources in the field of information security of the company can be represented as follows:

$$PE = \{J, \Pr, M, D\} \qquad (5)$$

where J is the set of InR of the company that requires attention from the staff in the context of information security; $\Pr$ – a set of properties that an employee dealing with information security issues for a specific InR should possess; M is motivation to constantly improve the level of their professional qualifications; D is set of threats that require the response of a highly qualified employee.

Of course, this formalization of the model does not take into account all aspects of the problem of the shortage of staff of IS specialists in companies, but it illustrates the importance of the task of including intelligent DSS in the business process loop, ready to take on some of the rather routine work that person has to perform in the daily practice of providing IS in a company.

The procedure for considering actual threats and risks associated with the implementation of these threats also requires separate modeling and assessment.

5. DSS Software Product "DSS Investing in Cybersecurity"

The models described above have been implemented in several software products. For example, in the DSS "DSS investing in cybersecurity" [29, 30].

DSS "DSS investing in cybersecurity" is intended for the online selection of optimal strategies for investing in the company's information security tools. This task is solved in the context of improving the security of corporate information systems with the help of innovative technologies based on the use of intelligent decision support systems in the protection circuits of CIS.

The interface for experts to work with DSS "DSS investing in cybersecurity" was developed on ASP.NET Core MVC, see Figs. 2–4.

For example, Figs. 2 and 3 show the results of solving the optimization problem described by the objective (1) and boundary conditions (2). In addition to graphical output, the DSS also generates textual output, shown at the top of the screen.

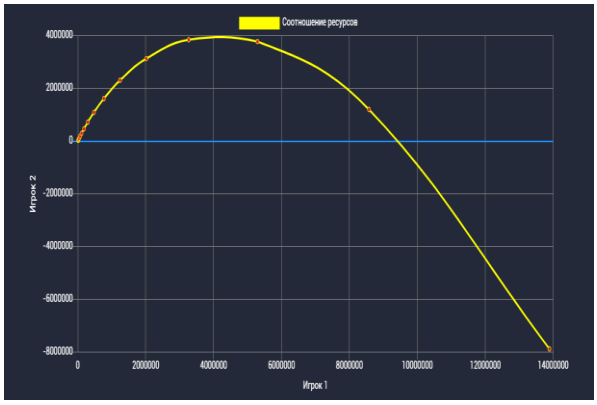

Figure 2: An example of visualization of graphs as a result of solving an optimization problem using DSS "DSS investing in cybersecurity"

In Fig. 2 Curve line 2 (shown in yellow) shows the trajectory of the distribution of financial resources with a clear optimum. The extreme value on the curve corresponds to the size of the company's financial resources, which will be sufficient to minimize IS threats.

Since the calculations are iterative, in the following figure (see Fig. 3) you can see the number of steps that were required to find the optimum, for example, when using the solution method based on the genetic algorithm [31, 32].

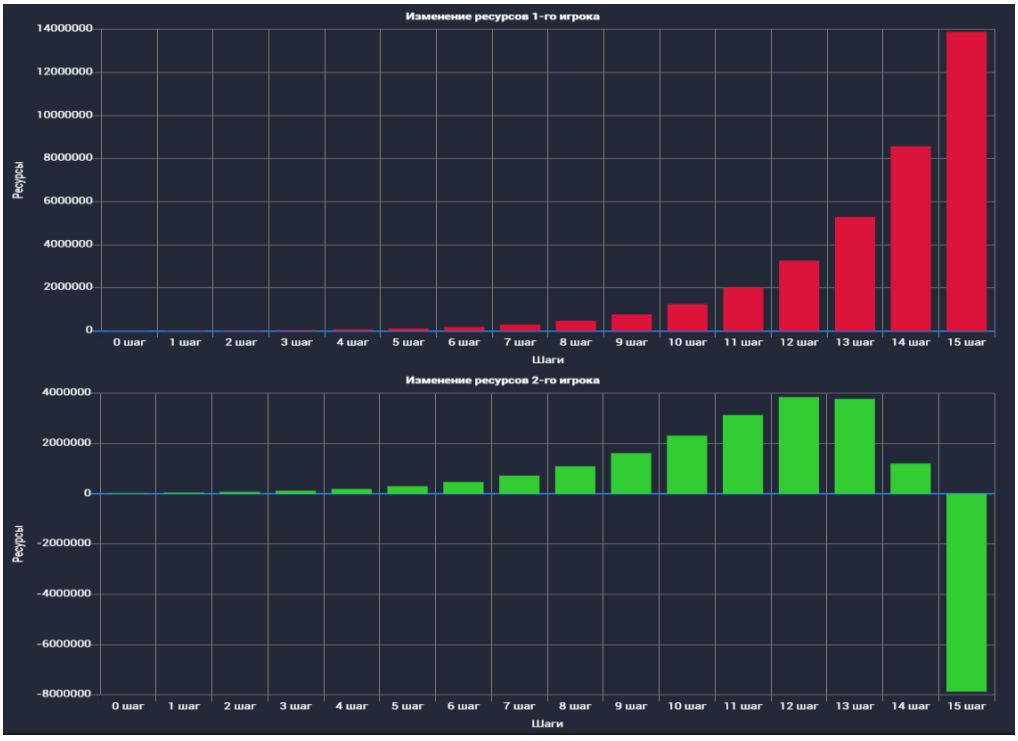

Figure 3: Visualization of graphs of the number of iterations in the course of finding the optimal solution using DSS "DSS investing in cybersecurity"

Fig. 4 shows an example of visualizing the intermediate results of evaluating the effectiveness of a company's information security system using the DSS investing in cybersecurity

DSS. This solution was obtained using a modified hierarchy analysis method. Fig. 4 shows the results of a comparative analysis using three types of antivirus software as an example: Avast, ESET NOD32, and Windows Defender. Software is compared on three parameters—cost efficiency complexity. The DSS investing in cybersecurity DSS relieves the evaluation and selection procedure of subjectivity, based only on a clear algorithmic comparison of all advantages and disadvantages. Similar procedures can be performed concerning other types of hardware and software systems of information security systems—firewalls, intrusion detection systems, access control systems, etc.

Figure 4: An example of visualization of intermediate results of assessing the effectiveness of the company's information security system using DSS "DSS investing in cybersecurity"

Without prioritizing the development of a set of models for solving multi-criteria optimization problems related to ensuring the company's information security as a priority of this study, we note that these tasks can be effective only based on a synergistic combination of expert experience and cybernetic modeling. Which together ensures prompt decision-making regarding the provision of information security for the company.

6. Discussion

If the DSS is entrusted with solving problems related to the optimization of information security, then information security specialists within the company can focus on solving organizational problems.

Such tasks include, for example, data backup activities; isolation of information systems most sensitive to threats; safe and secure destruction of devices and data; centralized system management and configuration management, etc.

We also note that it is much easier for information security specialists in the company itself than for external specialists to track personnel who have malicious motives. The assistance of the DSS is also not required in solving problems related to the motivation and readiness of employees to participate in IS training processes.

DSS can also be effective in risk analysis and assessment, business continuity plans, and

incident response, as well as to increase the efficiency of CIS recovery procedures.

The data of mathematical and economic modeling with the help of DSS are transferred to the company's management for decision-making at the strategic level of information security management. The main task of management in such a situation is to ensure a reasonable approach to the formation of an information security policy. Successful implementation of the information security policy requires continuous vertical and horizontal communication and coordination of the needs of all stakeholders—information security specialists, network administrators, management, etc.

Thus, organizational and economic support for the effective protection of corporate information becomes an integral part of information security management procedures. Such a synergistic approach demonstrates an adequate level of the company's information security maturity. The use of DSS can be identified and developed as a separate IS business function. Moreover, this business function, in conjunction with traditional approaches, will allow you to more quickly identify the weak links in the company's information security.

7. Conclusions

The model that describes the procedure for formalizing the task of optimizing the ISS of a business entity (company) has been further developed.

Unlike existing approaches, the focus of this study is on the mathematical-algorithmic and computer support of the decision-making procedure in matters of organizational and economic support for the effective protection of corporate information in the context of the tasks of IS management of companies.

The proposed approach enables the defense side to most effectively determine the parameters of organizational management of the company's information security infrastructure.

The contour of the DSS in the process of developing the company's information security infrastructure is considered. In the context of a shortage of qualified experts in the field of information security of companies, additions to existing mathematical models are proposed. The proposed additions make it possible to take into account the impact of the human resources of experts in information security issues on the management of the company's information security infrastructure. Recommendations are offered and the corresponding application software—DSS is described. The use of this DSS will help minimize the risks associated with the lack of qualified IS experts in many companies.

8. References

[1] J. H. Beales III, T. J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, U. Chi. L. Rev. 75(109) (2008).

[2] V. Astapenya, et al., Last Mile Technique for a Wireless Delivery System using an Accelerating Lens, in: IEEE International Conference on Problems of Infocommunications. Science and Technology (2020). doi: 10.1109/ picst51311.2020.9467886

[3] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, (2021). doi: 10.1109/picst54195.2021.9772181

[4] E. Amir, S. Levi, T. Livne, Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets, Review of Accounting Studies 23(3) (2018) 1177–1206.

[5] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[6] V. Astapenya, et al., Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems, in: 8th International Conference on Problems of Infocommunications, Science and Technology (2021) 174–178. doi: 10.1109/PICST54195.2021.9772161

[7] D. I. Dogaru, I. Dumitrache, Cyber Attacks of a Power Grid Analysis using a Deep Neural Network Approach, Journal of Control Engineering and Applied Informatics 21(1) (2019) 42–50.

[8] V. Krundyshev, M. Kalinin, Hybrid Neural Network Framework for Detection of Cyber Attacks at Smart Infrastructures, in: Proceedings of the 12th International

Conference on Security of Information and Networks (2019) 1–7.
[9] Y. Iskanderov, M. Pautov, Comprehensive Intelligent Information Security Management System (CIISMS) for Supply Networks: The Actor-Network Perspective, in: Proceedings of the Computational Methods in Systems and Software (2020) 130–142.
[10] I. H. Sarker, et al., Cybersecurity Data Science: An Overview from Machine Learning Perspective. Journal of Big Data 7(1) (2020) 1–29.
[11] B. Akhmetov, et al., Development of Sectoral Intellectualized Expert Systems and decision Making Support Systems in Cybersecurity, in: Proceedings of the Computational Methods in Systems and Software (2018) 162–171.
[12] H. Naseer, S. B. Maynard, K. C. Desouza, Demystifying Analytical Information Processing Capability: The Case of Cybersecurity Incident Response, Decision Support Systems 143 (2021) 113476.
[13] A. Couce-Vieira, D. R. Insua, A. Kosgodagan, Assessing and Forecasting Cybersecurity Impacts, Decision Analysis 17(4) (2020) 356–374.
[14] N. N. Akimov, et al., Mathematical Model of the Decision Support System for Ensuring Cybersecurity of the IED of the APCS of NPP. In Information Systems and Technologies IST-2020 (2020) 36–40.
[15] N. Tissir, S. El Kafhali, N. Aboutabit, Cybersecurity Management in Cloud Computing: Semantic Literature Review and Conceptual Framework Proposal, Journal of Reliable Intelligent Environments 7(2) (2021) 69–84.
[16] S. E. Donaldson, et al., Measuring a Cybersecurity Program. In Enterprise Cybersecurity (2015) 213–229. doi: 10.1007/978-1-4302-6083-7_12
[17] M. Ekstedt, et al., Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management, in: IEEE 19th International Enterprise Distributed Object Computing Workshop (2015) 152–155. doi: 10.1109/edocw.2015.40
[18] N. M. Radziwill, M. C. Benton, Cybersecurity cost of quality: Managing the costs of cybersecurity risk management (2017). arXiv:1707.02653.
[19] S. Al-Dhahri, M. Al-Sarti, A. Abdul, Information security management system, International Journal of Computer Applications 158(7) (2017) 29–33.
[20] V. A. Lakhno, Development of a Support System for Managing the Cyber Security, Radioelectronics, Informatics, Management 2 (2017) 109–116.
[21] Business Advantage. The State of Industrial Cybersecurity 2017 (2017). URL: https://go.kaspersky.com/rs/802-IJN-240/images/ICSWHITE PAPER.pdf
[22] Senseon. The State of Cyber Security—SME Report 2019. URL: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2019/08/White_paper_ 1.pdf%0A
[23] G. Cassar, B. Gibson, Forecast Rationality in Small Firms, Journal of Small Business Management 45(3) (2007) 283–302.
[24] S. E. Chang, C. B. Ho, Organizational Factors to the Effectiveness of Implementing Information Security Management, Industrial Management & Data Systems (2006).
[25] D. N. Burrell, An Exploration of the Cybersecurity Workforce Shortage, in: Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (2020) 1072–1081.
[26] T. Ohta, et al., Cybersecurity Solutions for Major International Events. Fujitsu Scientific & Technical Journal, 54(4) (2018) 57–65.
[27] K. Prislan, A. Mihelič, I. Bernik, A Real-World Information Security Performance Assessment using a Multidimensional Socio-Technical Approach, PloS one 15(9) (2020) e0238739.
[28] I. Bernik, K. Prislan, Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation, PloS one 11(9) (2016) e0163050. doi: 10.1371/journal. pone.0163050
[29] B. Akhmetov, et al., Conceptual Diagram of an Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems, Journal of Theoretical and Applied Information Technology 99(18) (2021) 4297–4310.
[30] V. Lakhno, et al., Model for Supporting Decisions of Investors, Taking into Consideration Multifactoriality and Turnover, Communications in Computer and Information Science 1388 (2021) 525–535. doi: 10.1007/978-3-030-71503-8_40
[31] A. Kalizhanova, et al., Optimization Model of Adaptive Decision Taking Support System

for Distributed Systems Cyber Security Facilities Placement, International Journal of Electronics and Telecommunications, 66(3) (2020) 493–498. doi: 10.24425/ijet.2020.134004
[32] V. Lakhno, et al., Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm, Lecture Notes in Networks and Systems 228 (2021) 41–53. doi: 10.1007/978-3-030-77448-6_5
[33] V. Lakhno, et al., Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing 1324 (2021). doi: 10.1007/978-3-030-68154-8_42
[34] V. Lakhno, et al., Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm, Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies 131 (2023). doi: 10.1007/978-981-19-1844-5_2
[35] T. V. Eaton, J. H. Grenier, D. Layman, Accounting and Cybersecurity Risk Management, Current Issues in Auditing 13(2) (2019) C1–C9.
[36] A. Al-Moshaigeh, D. Dickins, J. L. Higgs, Cybersecurity Risks and Controls: Is the AICPA's SOC for Cybersecurity a Solution? The CPA Journal 89(6) (2019) 36–41.
[37] M. A. Mamoshina, A. I. Demidenko, Organizational Support of the IT Infrastructure Management Process in the Information Security System at the Enterprise. In Actual Problems of Social and Humanitarian Research in Economics and Management (2018) 367–373.
[38] B. Alhayani, et al., Best Ways Computation Intelligent of Face Cyber Attacks. Materials Today (2021).