DOI: 10.55643/fcaptp.2.55.2024.4298

MECHANISM FOR INFORMATION SUPPORTING THE FINANCIAL AND ECONOMIC SECURITY OF INFORMATION AND TELECOMMUNICATION ENTERPRISES UNDER THE INFLUENCE OF MODERN CYBER THREATS

Myroslav Kryshtanovych
D.Sc. in Public Administration, Professor of the Department of Pedagogy and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine;
e-mail: mf0077@ukr.net
ORCID: 0000-0003-1750-6385
(Corresponding author)

Oleg Batiuk
Doctor of Legal Sciences, Professor of the Department of State Security, Lesya Ukrainka Volyn National University, Lutsk, Ukraine;
ORCID: 0000-0002-2291-4247

Tetiana Panfilova
D.Sc. in History, Associate Professor of the Department of State Policy and Governance, Lviv Polytechnic National University, Lviv, Ukraine;
ORCID: 0000-0002-7924-8716

Vitalii Burnatnyi
Vice-commandant of fire support rapid response Border Command Post, 15th mobile border guard detachment Chief of Staff, Kyiv, Ukraine;
ORCID: 0000-0001-9496-5708

Kostiantyn Sporyshev
PhD in Technical Sciences, Associate Professor, Doctoral Student of adjunct and doctoral studies, National Academy of the National Guard of Ukraine, Kharkiv, Ukraine;
ORCID: 0000-0003-4737-9698

Received: 02/01/2024
Accepted: 10/04/2024
Published: 30/04/2024

ABSTRACT

The main purpose of the article is to develop a modern mechanism for information support of financial and economic security under the influence of the most significant cyber threats. As part of the study, the importance and weight of this type of threat to financial and economic security as a cyberspatial action has been proven. The object of the study is open socio-economic systems engaged in information and telecommunications activities on the territory of Ukraine under martial law. It is substantiated that in a state of war, the increased influence of modern cyber threats significantly reduces the level of financial and economic security. The research methodology involves the use of a diverse number of methods, the main of which are: the method of system analysis, expert analysis, the Delphi method, modelling and the analytical-hierarchical process. As a result of the study, changes were identified in the dynamics of key performance indicators of institutions in the field of information and telecommunication services, which have a direct impact on ensuring financial and economic security. The need to improve information support in order to improve the level of security has been proven. A modern mechanism for information support of financial and economic security has been developed, which, unlike similar ones, focuses on the principles of countering cyber threats. The key most significant cyber threats to institutions in the field of information and telecommunication services today, under martial law, have been identified. Their ordering made it possible to better understand which measures should be applied first and which should not. The proposed approach to streamlining cyber threats forms the information basis for effectively ensuring financial and economic security in modern conditions.

Keywords: information support, information basis, financial and economic security, information and telecommunication activities, military status, countering cyber threats, financial performance indicators

JEL Classification: L96, C61, K24

INTRODUCTION

Today, information is of key importance for ensuring financial and economic security, especially in the context of developing the security of modern open socio-economic systems. In the era of Industry 4.0, which is gradually moving into Industry 5.0, digitalization and integration of cyber-physical systems are becoming the foundation for the development of economics and management. Consequently, information has turned from a simple application to the main activity into a full-fledged resource, which determines the level of financial and economic security. Moreover, if previously information served only to meet the needs of the main subjects of ensuring financial and economic security, today it is also a tool for increasing its level.

It should be noted that modern threats, especially under martial law, as is the case in Ukraine, are acquiring new forms and intensity. Cyber threats are becoming a major concern as they can lead to disruptions in critical information infrastructures, disruption

of financial flows, loss of confidential data, and destabilization of economic systems in general. Thus, the cyber threat has become the number one concern for most open socio-economic systems in Ukraine.

After two years of full-scale war in Ukraine, it is no secret that information and telecommunications services enterprises are especially vulnerable to cyber threats. This is because they store and process huge amounts of data, including confidential information. Hacking, DDoS attacks, phishing, spyware - all this can lead not only to financial losses but also to loss of trust from customers and partners. Consequently, this has an effect on ensuring financial and economic security. It should be noted that the transformation of traditional threats into cyber threats occurs due to the constant increase in business dependence on information technology. This leads to the fact that vulnerabilities in IT systems can have a disproportionate impact on the overall performance of an information and telecommunications services enterprise. Taking these factors into account, we can make the statement that research and development of mechanisms for protecting against modern cyber threats and ensuring financial and economic security are extremely relevant. This is important not only for Ukraine but also for the entire world community since cyber threats know no borders and can affect the stability of economic systems at the global level. Especially when most enterprises of information and telecommunication services in Ukraine are trying to move their databases outside the country as part of strengthening the security of their own functioning.

LITERATURE REVIEW

The issue of ensuring the financial and economic security of modern enterprises has never been in short supply among scientists and practitioners. This also applies to threats. Research in this area emphasizes the importance of developing effective strategies and mechanisms for ensuring financial and economic security in the context of the growing cyber threat. Fakiha (2021) examines organizations' security strategies to defend against cyberattacks, emphasizing the need for integrated security approaches. Satish Babu and Krishna Mohan (2022) present an intelligent multi-objective evolutionary model for securing cyber-physical systems, indicating the need for highly adaptive technological solutions.

Therefore, another position of Haber et al. (2018) focus on predicting the level of financial security of a country, using Ukraine as an example. This highlights the importance of analytical tools in identifying and responding to potential economic threats. Abdalrahman and Varol (2019) explore defence against cyberattacks in the context of the Internet of Things, focusing on emerging challenges in the field of financial and economic security.

The work of Rushchyshyn et al. (2021) analyze the regulatory and legal components of ensuring the financial security of the state, emphasizing the importance of legislative support in this area. Vieane et al. (2016) draw attention to human factors in cyber defence as critical to understanding and managing financial security.

Silva et al. (2017) conducted a thorough investigation into the thermal performance of outdoor telecommunication cabinets. Their study emphasizes the importance of maintaining optimal operating conditions for telecommunications equipment, which is vital for ensuring uninterrupted service, especially in times of war where infrastructure might be at risk. The authors' approach in characterizing thermal performance highlights the need for robust and resilient infrastructure in maintaining the operational integrity of telecommunication enterprises against environmental and man-made challenges, including cyber threats.

The work of Stankevičienė, Krivka, and Liučvaitienė (2009) offers valuable insights into the theoretical and practical aspects of human resource management strategies, with a specific focus on the Lithuanian telecommunication sector. Their research underscores the critical role of effective human resource strategies in navigating complex and rapidly changing business environments. This is particularly relevant in the context of cyber threats and war conditions, where the agility and resilience of the workforce are as crucial as technological solutions in ensuring enterprise security.

Skačkauskienė and Kiselevskaja (2014) explored the system of indicators for evaluating employee motivation within telecommunication enterprises. Their study reveals that employee motivation is a key factor in the successful operation of telecommunication companies. In scenarios of heightened cyber threats and wartime conditions, motivated and engaged employees are essential for maintaining vigilant and responsive operations. The authors' focus on motivational aspects provides a crucial dimension to understanding how human factors contribute to the resilience and security of telecommunication enterprises.

Eian et al. (2020) examine cyberattacks in the era of COVID-19 and possible solutions, highlighting the connection between global events and changes in cyber threats. The work of Sylkin et al. (2019) models the process of applying anti-crisis management in the system of ensuring the financial security of an enterprise, pointing out the importance of flexible management strategies for facing economic challenges.

DOI: 10.55643/fcaptp.2.55.2024.4298

Fülöp et al. (2022) discuss the impact of fintech accounting and Industry 4.0 on the accounting profession, showing how technological innovation can affect economic security. Finally, a study by Biliomistniy et al. (2017) analyzes the influence of external and internal factors on the financial security of an enterprise, emphasizing the complexity of the interaction of various aspects of financial stability.

At the same time, it should be noted that in modern scientific and practical literature, scientists identify a number of problems, which we have summarized and presented in Figure 1.

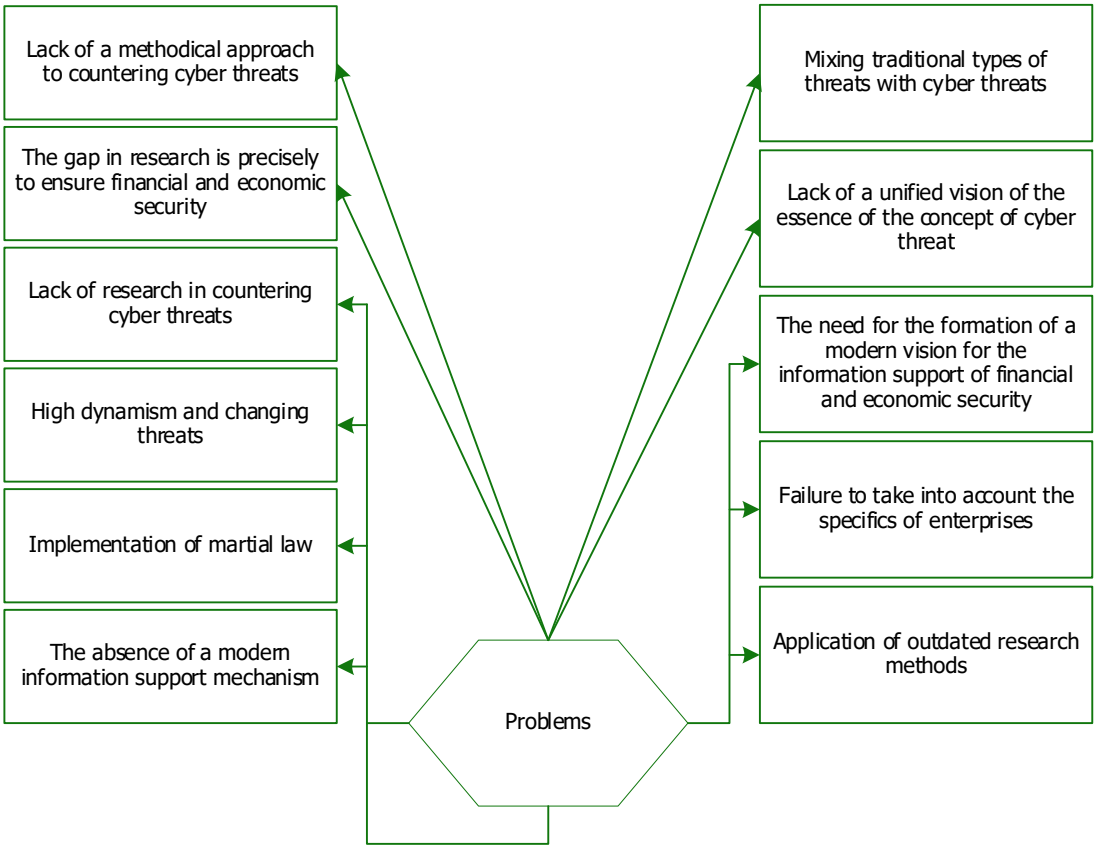


Figure 1. Key problems in the literature on the research topic.

A review of the literature demonstrates the variety of approaches and strategies that exist in the field of financial, economic security and cyber defence, highlighting the complexity and diversity of this topic. Our research is aimed at improving the approach to the information provision of financial and economic security specifically for the enterprises of information and telecommunication activities.

AIMS AND OBJECTIVES

The aim of the article is to develop a modern mechanism for information support for the financial and economic security of enterprises under the influence of the most significant cyber threats. Consequently, the object of study is open socio-economic systems engaged in information and telecommunications activities on the territory of Ukraine under martial law. To achieve these goals, the manuscript presents a methodological approach to identifying and streamlining cyber threats should be presented in order to satisfy the information needs of subjects of financial and economic security of information and telecommunications enterprises.

METHODS

The research methodology consists of many key methods, which together when correctly combined, allow the authors of the article to achieve the set goal (Figure 2).

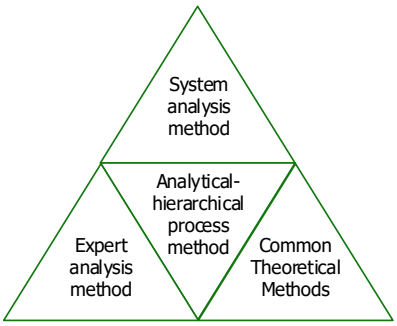


Figure 2. Structure of research methodology.

The system analysis method and the Saati analytical-hierarchical process method are important tools for analyzing complex problems, such as the ordering of key cyber threats to the financial and economic security of enterprises in the field of information and telecommunication services. Therefore, the system analysis method is used for the comprehensive study and analysis of large and complex systems. It allows you to determine how different components of a system interact with each other and how these interactions affect the overall functionality and efficiency of the system. In the context of our research, this method was used to identify and analyze various aspects of cyber threats, as well as to understand their potential impact on the financial and economic security of enterprises.

The Saati Analytical Hierarchical Process Method is a technique developed by Thomas Saati for decision-making in complex situations, allowing decision-making to be systematized and quantified. The AIP method uses a hierarchical structure to break down a problem into smaller, understandable parts, which are then evaluated and compared with each other. In our case, it was used to rank cyber threats based on their significance and impact on financial and economic security, allowing us to effectively identify threats that require the most attention and resources to counter. In addition to this, we used a graph method, which involves generating a graph of possible connections between certain cyber threats.

The method of expert analysis in our research is to attract qualified specialists in the field of information and telecommunication services to assess and analyze cyber threats. Thirty people were invited to participate, representing specific companies or organizations and having significant experience and deep knowledge in this field. These experts provided valuable contributions based on their professional expertise, which contributed to an in-depth analysis of cyber threats and their impact on the financial and economic security of enterprises.

The Delphi method we applied is a structured communication process designed to collect systematic expert opinions. Participants in the process, anonymous to each other, underwent several rounds of interviews. During each round, experts gave their answers to questions independently, after which they received a summary of the answers of other participants. This process helped to identify consensus and common understanding among participants about key aspects of the issue.

At the initial stage of the survey, experts were asked to determine a list of cyber threats that, in their opinion, have the greatest impact on the financial and economic security of industry enterprises. The responses received were analyzed to identify the most frequently mentioned threats. At the next stage, participants were asked to evaluate and optimize the list of cyber threats based on the updated information. This approach made it possible to focus on the most relevant and significant cyber threats as of winter 2023, related to ensuring the financial and economic security of enterprises in the field of information and telecommunication services.

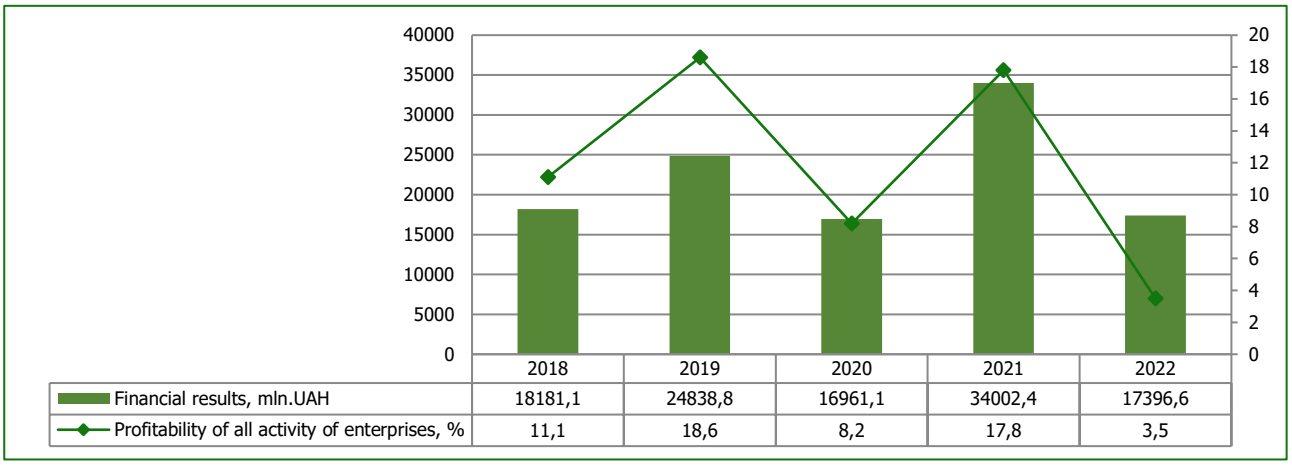
RESULTS

The essence of the concept of "information" in the context of ensuring the financial and economic security of an enterprise is the collection, analysis and use of data that allows the enterprise to predict risks, minimize threats and effectively manage resources to achieve stability and profitability. Information assurance in this context means the systematic collection and processing of data that is important for financial stability, such as market trends, financial performance, competitive information, regulatory changes, etc.

The purpose of information support for financial and economic security is to meet the needs of security subjects, i.e., management of the enterprise and its employees in reliable, up-to-date and complete information. This helps in making informed decisions, reducing the impact of negative factors on the activities of the enterprise and increasing competitiveness and economic stability.

DOI: 10.55643/fcaptp.2.55.2024.4298

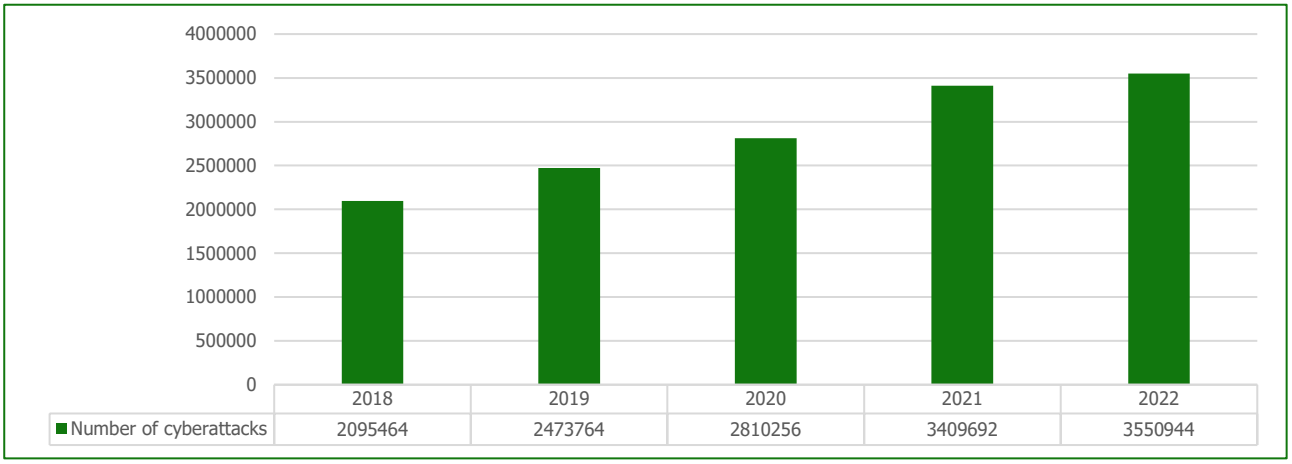
Martial law, declared in response to military aggression, has a significant impact on all aspects of the country's economic life. It leads to political and economic instability, which negatively affects the investment climate and business confidence. Also important is the factor of uncertainty, which constrains potential investment and business expansion. Additionally, ongoing cyberattacks, especially those targeting critical infrastructure such as telecommunications, require significant costs to improve cybersecurity and restore damaged systems. This could include upgrading equipment, implementing more sophisticated security systems, and even compensating customers for losses resulting from service interruptions. All this leads to an increase in operating costs and, accordingly, a decrease in profitability. It should also be taken into account that under martial law there is an increased need for strict compliance with safety standards and restrictions imposed by the government, which may lead to a further increase in administrative and operational costs. All these factors together influence the level of financial and economic security of these enterprises. They are forced to adapt to new realities, implementing strategies aimed at minimizing risks and maintaining stability in an unpredictable and hostile external environment (Figure 3).



	2018	2019	2020	2021	2022
Financial results, mln.UAH	18181,1	24838,8	16961,1	34002,4	17396,6
Profitability of all activity of enterprises, %	11,1	18,6	8,2	17,8	3,5

Figure 3. Dynamics of the main indicators of the financial and economic activity of enterprises of information and telecommunication services in Ukraine, for 2018-2022, units.

In the context of martial law, cyberspace becomes an additional front of conflict. Russian Federation, using cyber-attacks as part of its military strategy, is trying to damage the Ukrainian economy and reduce trust in government structures. This includes attacks on critical infrastructure such as telecommunications networks and financial systems, aiming to destabilize economies and wreak havoc on societies. At the same time, digital illiteracy among the population and workers of these enterprises also plays a significant role in vulnerability to cyber-attacks. Lack of cybersecurity skills and knowledge makes systems easier targets for hackers. Even basic cyberattack methods, such as phishing or malware, can be effective if workers don't know how to identify and prevent them. Considering these aspects, the increase in the number of cyber-attacks is understandable in light of the current political and technological situation in Ukraine. This creates a need to strengthen security at all levels (Figure 4).



	2018	2019	2020	2021	2022
Number of cyberattacks	2095464	2473764	2810256	3409692	3550944

Figure 4. Dynamics of cyber-attacks on information and telecommunication services enterprises in Ukraine that harmed financial and economic activity in 2018-2022, units.

One of the key problems of the growth of cyber-attacks is ineffective information support. The lack of information and data leads to the inability to respond promptly. It is necessary to build a modern mechanism of information support for the financial and economic security of enterprises of information and telecommunication services in Ukraine (Figure 5).

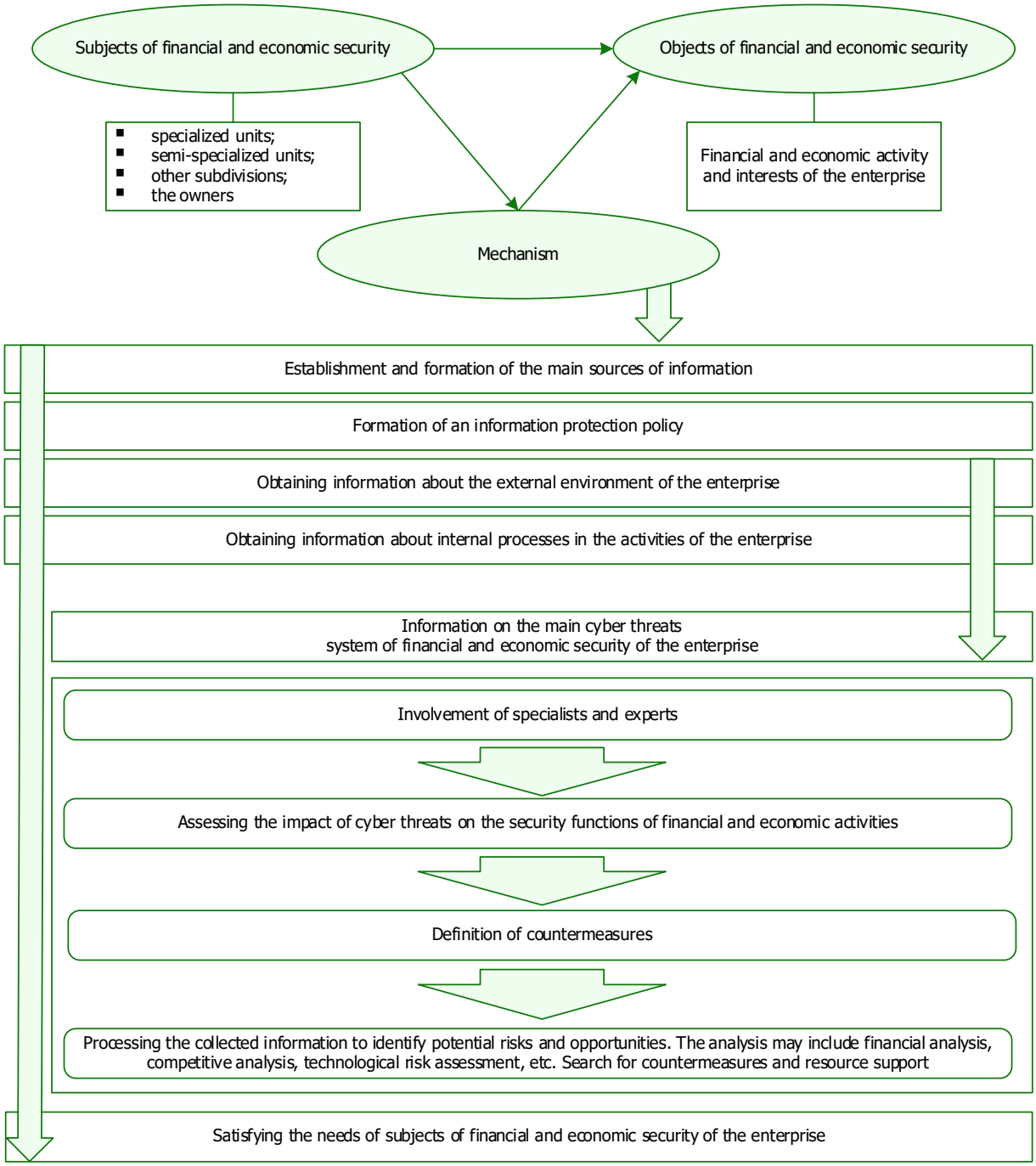


Figure 5. Mechanism of information support of financial and economic security of enterprises of information and telecommunication services in Ukraine.

Let us present the author's vision of the approach to this part of the mechanism.

Based on the results of the expert analysis and through the Delphi method, the following list of the most significant cyber threats in the system of ensuring financial and economic security of enterprises of information and telecommunication services in Ukraine was determined:

1. DDoS attacks (distributed denial of service attacks). These attacks overload servers or networks, which can lead to service interruptions and data loss.

DOI: 10.55643/fcaptp.2.55.2024.4298

2. Distribution of malware (viruses, Trojans). Malware can be used to steal data, spy on, or even destroy data on a business's infrastructure.
3. Attacks due to unprotected access points. Unsecured or poorly secured network access points can become a route for hackers to infiltrate corporate systems.
4. Insider threats. These are threats from employees that can intentionally or accidentally lead to data loss or leakage.
5. Ransomware (ransom demand). This is a type of malware that blocks access to the system or files and demands a ransom to unlock them.
6. Phishing attacks. This is one of the most common forms of cybercrime and involves the use of deceptive email messages to steal sensitive information such as logins, passwords or banking information.
7. Data leakage due to weak security measures. Poor data management and a lack of effective security measures can lead to the leakage of sensitive information.
8. Threats associated with cloud computing: Cloud services can be vulnerable to cyber-attacks, especially if they are not properly secured or configured.

Each cyber threat is assigned a mathematical designation, which together will form the following subset:$W=\{W_1; W_2; W_3; W_4; W_5; W_6; W_7; W_8\}$.

Construction of a graph of connections between cyber threats for the financial and economic security of enterprises of information and telecommunication services using the graph theory method involves the use of cyber threats as the vertices of the graph. Each of these threats, such as phishing attacks, DDoS attacks, and malware distribution, is a separate peak. The connections between these threats, defined through their relationships and interdependencies, form the edges of the graph. The weight of each edge can reflect the ability to move from one threat to another or the degree of impact of one threat on another. It is also important to consider the direction of the connections, which can be unidirectional or bidirectional depending on the nature of the interaction between threats. The constructed graph creates the necessary basis for further calculations (Figure 6).

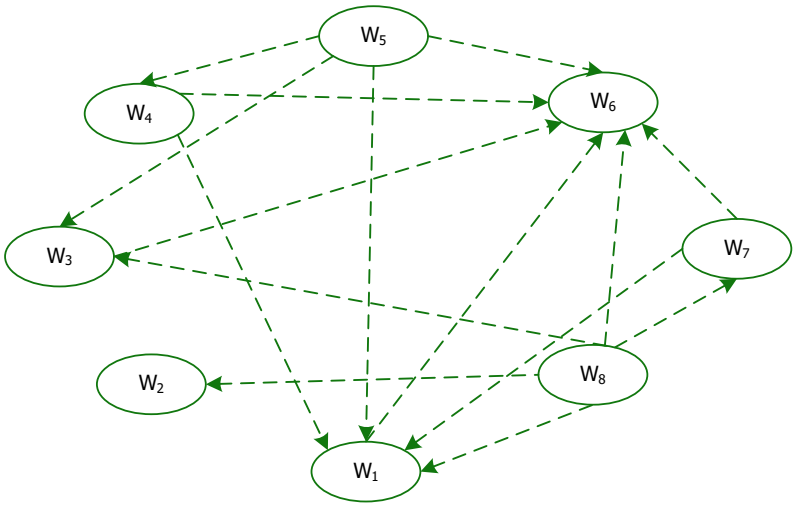


Figure 6. Graph of connections between certain cyber threats to the financial and economic security of enterprises of information and telecommunication services in Ukraine.

The next step is to build, based on the generated graph, a binary dependency matrix of size 8x8. Moreover, if, according to the graph, the arrow goes over and there is a dependence, we denote it as 1, if not, then 0. Thus, we fill in the matrix and present the result in Figure 7.

	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8
W_1	0	0	0	0	0	1	0	0
W_2	0	0	0	0	0	0	0	0
W_3	0	0	0	0	0	1	0	0
W_4	1	0	0	0	0	1	0	0
W_5	1	0	1	1	0	1	0	0
W_6	0	0	0	0	0	0	0	0
W_7	0	1	0	0	0	1	0	0
W_8	1	1	1	0	0	1	1	0

Figure 7. The filled-in binary matrix of dependence between the identified cyber threats to the financial and economic security of information and telecommunication services enterprises of Ukraine.

In cybersecurity, if a path can be determined between two cyber threats Wi and Wj in the corresponding graph, then cyber threat Wj is considered accessible from cyber threat Wi. This means that Wj is within the radius of influence or reach of Wi. Accordingly, we can define a group of such interrelated cyber threats, which we denote as S(Wi). Similarly, when a cyber threat Wi is the starting point of a path leading to Wj, then wi is considered to be an antecedent or predecessor to wj. In this context, the arrow arcs in the graph illustrate the dependency between cyber threats, where the exit from one cyber threat indicates its impact on the next. According to this scheme, the set of all cyber threats that serve as predecessors in the graph forms a subset P(Wi). Moreover, their cross-section is R(Wi) and if it is equal to P(Wi), then this is the priority level of the cyber threat.

It should be noted that the diagonal in the reach matrix will always be 1. Filling the diagonal with ones helps ensure the internal consistency of the matrix. This means that comparisons between different elements can be made sequentially, based on the assumption that each element is equal to itself (Figure 8).

	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8
W_1	1	0	0	0	0	1	0	0
W_2	0	1	0	0	0	0	0	0
W_3	0	0	1	0	0	1	0	0
W_4	1	0	0	1	0	1	0	0
W_5	1	0	1	1	1	1	0	0
W_6	0	0	0	0	0	1	0	0
W_7	0	1	0	0	0	1	1	0
W_8	1	1	1	0	0	1	1	1

Figure 8. The filled-in binary matrix of reachability between the identified cyber threats to the financial and economic security of information and telecommunication services enterprises of Ukraine.

DOI: 10.55643/fcaptp.2.55.2024.4298

Next, we build an iterative matrix for determining the lowest level of impact of cyber threats on the financial and economic security of enterprises of information and telecommunication services in Ukraine. As can be seen from Figure 9, the lowest level will be the cyber threat w_5 and W_8.

	S(Wi)	P(Wi)	R(Wi)
W_1	1;6	1;4;5;8	1
W_2	2	2;7;8	2
W_3	3;6	3;5;8	3
W_4	1;4;6	4;6	4
W_5	1;3;4;5;6	5	5
W_6	6	1;3;4;5;6;7;8	6
W_7	2;6;7	7;8	7
W_8	1;2;3;6;7;8	8	8

Figure 9. The iterative matrix for determining the lowest level of impact of cyber threats on the financial and economic security of enterprises of information and telecommunication services in Ukraine has been filled in.

It should be noted that what is presented in Figure 8 is repeated until all levels of cyber threats are determined. Skipping those intermediate calculations due to their similarity and uniformity, we present an iterative table of the levels of impact of cyber threats on the financial and economic security of enterprises of information and telecommunication services in Ukraine (Table 1).

Table 1. Ordering cyber threats and their corresponding countermeasures based on the results of the analysis.

Action level	Threat	Countermeasures
1 - High	W_6. Phishing attacks	Train employees to recognize phishing emails. Installing filters for spam and fraudulent messages. Implementation of two-factor authentication for access to corporate systems.
2	W_1. DDoS attacks W_2. Distribution of malware	Using specialized services to mitigate DDoS attacks, such as Cloudflare or Akamai. Training employees in the basics of cyber hygiene and threat awareness.
3	W_3. Attacks due to unprotected access points W_4. Insider threats W_7. Data leakage due to weak security measures	Application of powerful authentication and encryption methods for wireless networks. Implement a least privilege and access control policy. Implementation of data management policies and procedures.
4-Low	W_5. Ransomware (ransom demand) W_8. Threats associated with cloud computing	Regular data backup. Using encryption and authentication for cloud services.

The key to countering cyber threats effectively lies not only in technical solutions and staff education but also in economically viable strategies that include regular updates to security policies and procedures. This approach is financially prudent, particularly for entities with limited budgets, as it maximizes the use of existing resources without necessitating additional personnel costs. The findings of this study are particularly relevant for financial and economic security stakeholders, offering them cost-effective means to respond to threats and minimize potential financial damage. It's crucial to emphasize that the proposed provisioning mechanism is cost-effective, as it leverages existing resources efficiently, avoiding the need for significant new financial investments. However, the successful implementation of this mechanism does require a baseline level of technical infrastructure, which might entail some initial capital expenditure. This investment is justified by the

need for continual monitoring, analysis, and response to evolving cyber threats, a necessity that becomes even more critical in wartime scenarios. The initial financial outlay for technical equipment is offset by the long-term benefits of being able to identify, neutralize, and adapt to new cyber threats, thereby ensuring the stability and resilience of information and telecommunication systems.

In summary, the proposed information support mechanism stands out by focusing on proactive and economically efficient cyber threat countermeasures, rather than solely on passive protection. This proactive approach not only addresses current threats but also anticipates future challenges, which is essential for long-term financial and information security. The mechanism's economic advantage lies in its ability to optimize current resource utilization, thus minimizing the need for additional financial investment while maximizing security outcomes.

DISCUSSION

In the context of the discussion of the obtained results, it should be noted that when compared with other works, it can be seen that each of them has its own specificity and emphasis. For example, some of them focus on assessing and countering specific cyber threats in specific industries, while others explore methodological approaches to managing financial and economic security at different levels. For example, a study by Rajaonah et al. (2017) focuses on the importance of trust and security of information systems, which is key to protecting critical infrastructure, while our work focuses on specific strategies for ensuring financial and economic security under martial law. Similarly, Franchuk et al. (2020) explore ways to counter threats to the financial security of high-tech enterprises, while our work brings a new dimension to understanding these challenges in the field of information and telecommunication services. This demonstrates a more specific approach to cyber threats, which is particularly relevant in a state of war.

We believe that we extend the framework defined by Gordieiev et al. (2021), who explore the application of eye-tracking technology to assess and ensure financial and economic security, showing how these technologies can be integrated into broader security strategies.

Tsuchiya et al. (2018) propose an innovative approach to the use of network firewall technology in the context of Industry 4.0 industrial systems, which demonstrates the importance of developing specialized solutions for cyber protection in various industries. It can be argued that this complements to a certain extent our work, which focuses on information and telecommunication services, showing a wide range of application areas for ensuring financial and economic security. A study by Srinivas et al. (2019) highlights the importance of government regulation in cybersecurity, suggesting frameworks, standards, and guidelines that can be used to improve security. This places our research in the context of the wider policy and regulatory environment, which is important for understanding and implementing effective mechanisms for ensuring financial and economic security.

The work of Fakiha (2022) focuses on the effectiveness of using forensic firewalls in protecting devices from cyber-attacks. This study provides important information about specific technologies that can be integrated into our proposed approach to ensure financial and economic security. Finally, Kryshtanovych et al. (2023) present the development of a smart multi-level model to counter the impact of disinformation on a cybersecurity system. This is particularly relevant for our study, as it demonstrates the importance of a comprehensive approach to countering not only the technical but also the social aspects of cyber threats.

We present the key principles of the original research results obtained by us (Table 2).

Table 2. The key principles of the original research results obtained by us.

№	Result	The essence of the result obtained
1	Analysis of financial and economic activity of enterprises of information and telecommunication services	Changes in the dynamics of key performance indicators of institutions in the field of information and telecommunication services that have a direct impact on ensuring financial and economic security are analyzed and determined
2	A new approach to the construction of the mechanism	A modern mechanism for information support of financial and economic security has been developed, which, unlike similar ones, focuses on countering cyber threats
3	A modern vision of the main cyber threats	The key, most significant cyber threats to institutions in the field of information and telecommunication services today, under martial law, have been identified
4	Methodical approach	The proposed approach to streamlining cyber threats forms the information basis for effectively ensuring financial and economic security in modern conditions

DOI: 10.55643/fcaptp.2.55.2024.4298

Consequently, our research is focused on developing a mechanism for information support of financial and economic security of information and telecommunications services enterprises in the context of cyber threats, especially under martial law. These results not only expand the understanding of the current situation in the field of information and telecommunication services but also make an important contribution to the practical provision of security in this area.

CONCLUSIONS

To summarize, it should be noted that the research has provided significant progress in the development of a mechanism for information support of financial and economic security, especially in the context of modern cyber threats, which have become especially relevant under martial law in Ukraine. The importance of this study lies in the fact that it identifies and analyzes specific cyber threats that have a direct impact on the financial and economic security of institutions operating in the field of information and telecommunication services in terms of the constructed mechanism. At the same time, innovativeness is revealed through the development of an approach to countering cyber threats. This approach focuses not only on identifying existing cyber threats but also on analyzing and predicting potential future challenges. The innovation lies in the fact that the specifics of martial law are taken into account, imposing additional restrictions and requirements on security systems.

It was presented how it is possible to satisfy the information needs of subjects of financial and economic security of information and telecommunications enterprises. This approach is part of the author's vision of a modern information support mechanism. The research employs a combination of methods like system analysis, expert analysis, the Delphi method, modelling, and the analytical-hierarchical process. This varied methodology ensures a comprehensive and multifaceted understanding of the issues at hand. A significant part of the approach is identifying the most pressing cyber threats, especially under conditions like martial law. This involves not only recognizing these threats but also prioritizing them in terms of which should be addressed first based on their impact and likelihood.

However, there are some limitations to consider. First of all, the study focuses on enterprises in only one industry and in only one country, which cannot fully reflect the global situation in ensuring financial and economic security. Also, given the rapid pace of technology development and the changing nature of cyber threats, there is a risk that the developed methods and recommendations will quickly become obsolete.

Prospects for further research include expanding the scope of the study to cover different types of organizations and countries, as well as adapting the developed mechanism to changing conditions and new types of cyber threats. It is also important to constantly update and improve information support, taking into account the new needs of financial and economic security subjects. It is recommended in the future to actively exchange knowledge with colleagues from different countries and industries on a given topic, as collaboration can contribute to a deeper understanding of challenges and the development of more effective solutions. An integral part of successful work is constant self-education and participation in professional conferences and seminars, which allows you to keep abreast of the latest research and trends in this field. Only real practice of working with information and cyberware will help ensure financial and economic security.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Data curation: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Formal Analysis: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Methodology: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Software: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Resources: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Supervision: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova*
Validation: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova*
Investigation: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Visualization: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*
Project administration: *Myroslav Kryshtanovych, Oleg Batiuk*
Writing – review & editing: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova*
Writing – original draft: *Myroslav Kryshtanovych, Oleg Batiuk, Tetiana Panfilova, Vitalii Burnatnyi, Kostiantyn Sporyshev*

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Abdalrahman, G. A., & Varol, H. (2019). Defending against cyber-attacks on the Internet of things. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 1-6. http://doi.org/10.1109/ISDFS.2019.8757478
2. Biliomistniy, O., Bilomistna, I., & Galushko, Y. (2017). Influence external and internal factors to financial security of enterprise. *Financial and Credic Activity: Problems of Theory and Practice 1*(22), 105-111. https://doi.org/10.18371/fcaptp.v1i22.109935
3. Eian, I.C., Yong, L.K., Li, M.Y.X., Qi, Y.H., & Fatima, Z. (2020). Cyber attacks in the era of COVID-19 and possible solution domains. *Preprints, 2020*, 2020090630. http://doi.org/10.20944/preprints202009.0630.v1
4. Fakiha, B. (2021). Business organization security strategies to cyber security threats. *International Journal of Safety and Security Engineering, 11*(1), 101-104. https://doi.org/10.18280/ijsse.110111
5. Fakiha, B. (2022). Effectiveness of forensic firewall in protection of devices from cyberattacks. *International Journal of Safety and Security Engineering, 12*(1), 77-82. https://doi.org/10.18280/ijsse.120110
6. Franchuk, V., Omelchuk, O., Melnyk, S., Kelman, M., & Mykytyuk, O. (2020). Identification the ways of counteraction of the threats to the financial security of high-tech enterprises. *Business: Theory and Practice, 21*(1), 1-9. https://doi.org/10.3846/btp.2020.11215
7. Fülöp, M. T., Topor, D. I., Ionescu, C. A., Căpușneanu, S., Breaz, T. O., & Stanescu, S. G. (2022). Fintech accounting and Industry 4.0: future-proofing or threats to the accounting profession? *Journal of Business Economics and Management, 23*(5), 997–1015. https://doi.org/10.3846/jbem.2022.17695
8. Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., & Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. *International Journal of Safety and Security Engineering, 11*(4), 361-367. https://doi.org/10.18280/ijsse.110409
9. Haber, J., Bukhtiarova, A., Chorna, S., & Lastremska, O. (2018). Forecasting the level of financial security of the country on the example of Ukraine. *Investment Management and Financial Innovations, 15*(3), 304-317. https://doi.org/10.21511/imfi.15(3).2018.25
10. Kryshtanovych, M., Lyubomudrova, N., Bondar, H., Motornyy, V., & Kuchmenko, V. (2023). An intelligent multi-stage model for countering the impact of disinformation on the cybersecurity system. *Ingénierie des Systèmes d'Information, 28*(1), 41-47. https://doi.org/10.18280/isi.280105
11. Rajaonah, B. (2017). A view of trust and information system security under the perspective of critical infrastructure protection. *Ingénierie des Systèmes d'Information, 22*(1), 109-133. https://doi.org/10.3166/ISI.22.1.109-133
12. Rushchyshyn, N., Medynska, T., Nikonenko, U., Kostak, Z., & Ivanova, R. (2021). Regulatory and legal component in ensuring state's financial security. *Business: Theory and Practice, 22*(2), 232-240. https://doi.org/10.3846/btp.2021.13580
13. Satish Babu, J., & Krishna Mohan, G. (2022). An intelligent multi-objective evolutionary model for establishing security in cyber-physical systems. *Ingénierie des Systèmes d'Information, 27*(2), 213-221. https://doi.org/10.18280/isi.270205
14. Silva, P.D., Pires, L., Patrício, C., & Gaspar, P.D. (2017). Characterization of the Thermal Performance of an Outdoor Telecommunication Cabinet. *International Journal of Energy Production and Management, 2*(1), 106-117. https://doi.org/10.2495/EQ-V2-N1-106-117
15. Skačkauskienė, I., & Kiselevskaja, A. (2014). A system of indicators for evaluating the motivation of employees for work in telecommunication enterprises. *Business: Theory and Practice, 15*(3), 245-253. https://doi.org/10.3846/btp.2014.24
16. Srinivas, J., Das, A.K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188. https://doi.org/10.1016/j.future.2018.09.063
17. Stankevičienė, A., Krivka, A., & Liučvaitienė, A. (2009). The theoretical and practical aspects of human resource management strategy development: A case of Lithuanian telecommunication sector. *Business: Theory and Practice, 10*(4), 276-284. https://doi.org/10.3846/1648-0627.2009.10.276-284
18. Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., & Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. *Business: Theory and Practice*, *20*, 446-455. https://doi.org/10.3846/btp.2019.41
19. Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A., & Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. *Journal of Industrial Engineering and Management (JIEM), 11*(2), 318-333. http://dx.doi.org/10.3926/jiem.2534

DOI: 10.55643/fcaptp.2.55.2024.4298

20. Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., & Wickens, C. (2016). Addressing human factors gaps in cyber defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60*(1), 770-773. https://doi.org/10.1177/1541931213601176

Криштанович М., Батюк О., Панфілова Т., Бурнатний В., Споришев К.

МЕХАНІЗМ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ В УМОВАХ ВПЛИВУ СУЧАСНИХ КІБЕРЗАГРОЗ

Основною метою дослідження є розроблення сучасного механізму інформаційного забезпечення фінансово-економічної безпеки в умовах впливу найбільш вагомих кіберзагроз. У рамках проведеного дослідження доведено важливість і вагомість такого впливу загроз фінансово-економічній безпеці як кіберпросторового характеру дії. Об'єктом дослідження обрано відкриті соціально-економічні системи, що займаються інформаційно-телекомунікаційною діяльністю на території України в умовах воєнного стану. Обґрунтовано, що при воєнному стані посилений вплив сучасних кіберзагроз суттєво знижує рівень фінансово-економічної безпеки. Методологія дослідження передбачає застосування різноманітної кількості методів, основними серед яких є: метод системного аналізу, експертного аналізу, методі Дельфі, моделювання й аналітично-ієрархічного процесу. У результаті проведеного дослідження визначено зміни в динаміці ключових показників діяльності установ у царині інформаційно-телекомунікаційних послуг, які мають безпосередній вплив на забезпечення фінансово-економічної безпеки. Доведено потребу в удосконаленні інформаційного забезпечення з метою підвищення рівня безпеки. Розроблено сучасний механізм інформаційного забезпечення фінансово-економічної безпеки, який, на відміну від подібних, акцентує увагу на засадах протидії кіберзагрозам. Визначено ключові, найбільш вагомі сьогодні, в умовах воєнного стану, кіберзагрози для установ у царині інформаційно-телекомунікаційних послуг. Їх упорядкування дозволило краще зрозуміти, яких заходів слід уживати першочергово, а яких ні. Запропонований підхід до впорядкування кіберзагроз формує інформаційне підґрунтя для ефективного забезпечення фінансово-економічної безпеки в сучасних умовах.

Ключові слова: інформаційне забезпечення, інформаційне підґрунтя, фінансово-економічна безпека, інформаційно-телекомунікаційна діяльність, воєнний стан, протидія кіберзагрозам, фінансові показники діяльності

JEL Класифікація: L96, C61, K24