

DOI: <https://doi.org/10.34069/AI/2023.69.09.28>

How to Cite:

Trzonkowski, K., Khalina, O., Kolisnichenko, P., Rozumovych, N., & Zhyhulin, O. (2023). Information systems for financial and economic security in the face of cyberthreats: study of characteristics in the context of modern administrative and legal mechanism. *Amazonia Investiga*, 12(69), 315-324. <https://doi.org/10.34069/AI/2023.69.09.28>


## Information systems for financial and economic security in the face of cyberthreats: study of characteristics in the context of modern administrative and legal mechanism

**Sistemas de información para la seguridad financiera y económica frente a las ciberamenazas: estudio de características en el contexto del moderno mecanismo administrativo-legal**

Received: August 1, 2023

Accepted: September 20, 2023

Written by:


**Konrad Trzonkowski<sup>1</sup>** <https://orcid.org/0000-0002-3129-5732>**Olena Khalina<sup>2</sup>** <https://orcid.org/0000-0002-4086-6314>**Paulina Kolisnichenko<sup>3</sup>** <https://orcid.org/0000-0001-6730-1236>**Nataliia Rozumovych<sup>4</sup>** <https://orcid.org/0000-0003-4498-725X>**Oleksandr Zhyhulin<sup>5</sup>** <https://orcid.org/0000-0003-1532-2806>


### Abstract


The aim of the article was to study the characteristics of the formation of an information system to implement the administrative and legal mechanism to ensure financial and economic security under the influence of cyber threats. The research methodology involved the use of hierarchical and pairwise comparison analysis, as well as the method of expert analysis, with the help of academic documentary sources. As a result of the study, the main cyber threats in the information system of the administrative and legal mechanism for ensuring financial and economic security were identified and ordered according to their level of influence. This order will allow the management apparatus to understand, at least in theory, the hierarchy of importance of existing threats and subsequently use the latter to build information systems. Everything allows to conclude that, by analyzing the obtained results, a methodical approach to the assessment of cyber threats to financial and economic security was formed. However, the

### Resumen


El objetivo del artículo fue estudiar las características de la formación de un sistema de información para implementar el mecanismo administrativo y legal para garantizar la seguridad financiera y económica, bajo la influencia de las ciberamenazas. La metodología de investigación implicó el uso de análisis jerárquico y de comparación por pares, así como el método de análisis de expertos, con ayuda de fuentes documentales de carácter académico. Como resultado del estudio, se identificaron y ordenaron las principales ciberamenazas en el sistema de información del mecanismo administrativo y legal para garantizar la seguridad financiera y económica, de acuerdo con su nivel de influencia. Este orden permitirá que el aparato de gestión comprenda, al menos en teoría, la jerarquía de importancia de las amenazas existentes y, posteriormente, utilice estas últimas para construir sistemas de información. Todo permite concluir que, al analizar los resultados obtenidos, se formó un enfoque metódico para la evaluación de las

<sup>1</sup> WSHIU Academy of Applied Sciences, Poznan, Poland.  WoS Researcher ID: JGE-3283-2023

<sup>2</sup> Ukrainian Academy of Printing, Ukraine, Lviv, Ukraine.  WoS Researcher ID: FDC-7854-2022

<sup>3</sup> Vice Rector for International Cooperation, WSHIU Academy of Applied Sciences, Poznan, Poland.  WoS Researcher ID: IWE-0198-2023

<sup>4</sup> King Danulo University, Ivano-Frankivsk, Ukraine.  WoS Researcher ID: DQA-6944-2022

<sup>5</sup> Odesa National University of Technology, Odesa, Ukraine.  WoS Researcher ID: JQI-0228-2023

study has its limitations, as for the formation of the above-mentioned information systems, a small number of cyber threats were adopted, which are also characteristic for a particular country like Ukraine.

**Keywords:** Financial and Economic Security, Information Systems, Administrative and Legal Mechanism, Financial Markets, Cyber Threats.

## Introduction

Historically, financial security primarily revolved around the accumulation and preservation of wealth, often in physical forms like gold or property. As economies evolved, so did the concept of financial security. The development of banking systems, stock markets, and various financial instruments allowed for more diversified means of securing and growing wealth. In modern times, financial security also encompasses aspects like insurance, pension plans, and access to credit, which help individuals and businesses manage risk and uncertainty.

Different approaches have been adopted to ensure economic and financial security over time. Governments play a crucial role through policies that regulate financial markets, provide social security, and manage economic cycles. Meanwhile, individual strategies may include savings, investments, and insurance. The digital age has introduced new dimensions to financial security, including cyber security and the management of digital assets. The continuous evolution of these concepts reflects the dynamic nature of economies and the ever-changing challenges and opportunities they present.

One of the fundamental factors of the independence of a sovereign state in modern economic conditions is the state of its financial and economic security. Due to the rapid changes in market conditions in global financial markets and the interconnected system of economic relations in the structure of the world economy, the state of the domestic financial sector is becoming increasingly difficult to control, given the instability of the internal and external environment. In such a situation, there is a need for a comprehensive preventive assessment of external and internal factors that directly or indirectly affect the country's financial sector. The development of the economy can be ensured by expanding relationships between national and

amenazas cibernéticas a la seguridad financiera y económica. Sin embargo, el estudio tiene sus limitaciones, ya que para la formación de los sistemas de información antes mencionados, se adoptó un número reducido de ciberamenazas, que también son características de un país como Ucrania en particular.

**Palabras clave:** Seguridad Financiera y Económica, Sistemas de Información, Mecanismo Administrativo y Legal, Mercados Financieros, Amenazas Cibernéticas.

international financial and credit institutions and integration into the world market.

Financial and economic security is ensuring such development of the financial and economic system and financial relations, as well as processes in the economy, in which the necessary financial conditions are created for the socio-economic and financial stability of the country, maintaining the integrity and unity of the financial system (including monetary, budgetary, credit), tax and currency system), successfully overcoming internal and external threats in the financial sector.

The financial system must have a certain margin of safety in case of unforeseen and extraordinary circumstances, so that government authorities can quickly and timely respond to the emergence of any threats and, if possible, prevent, neutralize or minimize potential socio-economic losses.

In the current conditions of economic development, strengthening of integration and globalization processes, the issue of ensuring the national security of the state comes to the fore. Financial and economic security is its most important component, without which it is almost impossible to solve any of the problems facing the state. Recently, the financial and economic safety of different states has been influenced by a number of external and internal threats: monetary crises, geopolitical situation, the influence of the activities of international organizations, inflationary processes, instability of the legal system, etc.

The lack of financial resources leads to the inability of the financial system to provide the state with financial resources sufficient to perform its internal and external functions and generally poses a threat to national security.

The formation and practical implementation of an effective mechanism for ensuring financial and economic security presupposes, first of all, the identification of factors influencing the state of financial security, external and internal threats, and the study of the interconnectedness of the individual components of this structure, which is complex in internal structure and hierarchical composition.

Cyberthreats in modern society are gaining significant scale. Now, a successful hacker attack can cut off power to an area or country, lead to a bank robbery, or destroy a successful organization.

Based on these definitions, we offer the author's understanding: "cyberthreats" are illegal, punishable actions of subjects of information legal relations that create a danger to the vital interests of an individual, society and the state as a whole, the implementation of which depends on the proper functioning of information, telecommunication and information-telecommunication systems, as well as relations on the creation, collection, receipt, storage, use, distribution, protection, protection of information.

#### **Theoretical Framework or literature review**

Financial and economic security is a state of protecting the economic interests of an individual, company or state from internal and external threats, ensuring the stability and sustainability of the financial system, as well as the ability to effectively withstand various types of economic risks. This includes measures to prevent financial crises, ensure the stability of the national currency, and protect against fraud, corruption and other illegal activities.

Cyber threats are potential or actual security threats that arise in the digital space. These could be attacks on computer systems, networks or personal data. Problems of ensuring financial and economic security and countering cyber threats attract the attention of scientists due to the growing relevance of cybersecurity in a world where financial and economic systems are increasingly dependent on digital technologies. This field of study combines not only the technical aspects of information systems security, but also a deep understanding of economic processes, making it multidisciplinary and important for modern research. The topic has also grown in importance in the context of global cyber threats that threaten economic stability and security at the national and international levels.

In the contemporary landscape of financial and economic security, the convergence of administrative, legal, and technological dimensions becomes pivotal in navigating the challenges posed by modern cyberthreats. This literature review delves into key studies that illuminate various aspects of this multifaceted domain.

The legal aspects of reforming public management for financial and economic security in Ukraine are scrutinized by Dragan et al., (2023). This study positions legal considerations as instrumental in shaping effective administrative mechanisms to counter evolving threats, particularly in the context of European integration.

Raghutla and Chittedi (2021) provide an insightful analysis into how financial development fuels economic growth in emerging markets. Their study highlights the critical role of financial policies, market development, and regulatory frameworks in shaping economic resilience. This research underlines the importance of robust financial systems, which are essential for safeguarding economies against various threats, including those of a cyber nature. The findings suggest that a well-developed financial sector is better equipped to handle the complexities and challenges posed by cyberthreats, underlining the symbiotic relationship between financial stability and cybersecurity. Albalawi and Almaiah (2022) delve into the cybersecurity challenges prevalent in IoT environments, shedding light on the vulnerabilities and attack vectors that are increasingly becoming a concern for financial information systems. The study assesses various mitigation techniques, emphasizing their applicability in protecting sensitive financial data. This research is particularly relevant in understanding how IoT, a rapidly growing dimension in financial technology, can be safeguarded against cyber intrusions that threaten financial stability.

Fakiha (2022) examines the effectiveness of forensic firewalls in defending against cyberattacks. The study's focus on the protective capabilities of these firewalls offers valuable insights into their role in safeguarding devices and, by extension, the financial information they contain. Jing et al., (2014) present a comprehensive perspective on the security challenges in the Internet of Things, with a focus on how these challenges impact financial data integrity and privacy. Their findings are crucial in understanding the broader implications of IoT

security for the financial sector, emphasizing the need for robust security protocols and innovative solutions to safeguard financial systems in an increasingly interconnected world.

Rushchyshyn, Medynska, Nikonenko, Kostak, and Ivanova (2021), in their work published in *Business: Theory and Practice*, examine the regulatory and legal components in ensuring a state's financial security. Their analysis is crucial for understanding the legal frameworks and regulatory mechanisms that underpin the financial security of nations, particularly in mitigating and responding to cyberthreats.

The work of Iskayan et al., (2022) highlights the importance of the information environment factor in assessing the economic security of a country. The authors analyze how digital technologies and information systems affect the economic stability and security of nations, pointing out the complexity and interdependence of these factors in the world. On the other hand, Al Azzam's (2019) study focuses on the importance of international cooperation in countering cybercrime. Al Azzam reviews existing international cooperation mechanisms and suggests ways to modernize them to effectively address the global challenges posed by cybercrime. This research shows the shortcomings of current systems and highlights the need for more coordinated and comprehensive approaches.

Benigno et al., (2013) explores financial crises and macro-prudential policies in the *Journal of International Economics*. His research offers insights into how macroeconomic tools and policies can be utilized to prevent or mitigate financial crises, a perspective that is essential when considering the systemic risks posed by cyber threats to financial systems. Syshchuk and Teteruk (2018) focus on the European Union's monetary and financial mechanism of anti-crisis regulation. Their study, provides an in-depth look at how the EU has developed mechanisms to manage financial crises, offering a model that can be considered in the context of managing cyber risks. Jovovic et al., (2017) discuss the concept of sustainable regional development in the *Journal of International Studies*, emphasizing the institutional aspects, policies, and prospects. This research is significant for understanding the broader context in which financial and economic security operates, including the sustainability of regional development in the face of evolving cyberthreats.

Stankevičienė, Sviderskė, and Miečinskienė (2014) in their article in *Business: Theory and Practice* compare country risk, sustainability, and economic safety indices. This comparison is valuable for assessing how different countries manage economic safety and risks, including those related to cybersecurity. Soni et al., (2021), in *Technological Forecasting and Social Change*, explore technological interventions in social business. Their research is pertinent for understanding how technological advancements can be leveraged to enhance financial and economic security while also recognizing the new challenges and risks these technologies bring, especially in cybersecurity. Finally, Alvarez, Di Caprio, and Santos-Arteaga (2016), in their study in *Technological and Economic Development of Economy*, discuss technological assimilation and divergence during times of crisis. This study is relevant for understanding how technology can both contribute to and mitigate the impacts of economic crises, with particular relevance to cybersecurity threats.

The human factors in cyber defense are addressed by Vieane et al., (2016), emphasizing the importance of addressing gaps in cybersecurity through an understanding of human behavior. This perspective adds a crucial layer to the technological aspects of financial and economic security. Gordieiev et al., (2021) propose the concept of using eye-tracking technology to assess and ensure cybersecurity, functional safety, and usability.

Sylkin et al., (2020) contribute to the methodology of forming a model for assessing the level of financial security, providing a structured approach that can guide policymakers and administrators in evaluating and enhancing financial resilience. Kryshtanovych et al., (2023) present an intelligent multi-stage model for countering the impact of disinformation on the cybersecurity system. This forward-looking study recognizes the evolving nature of threats and the importance of adaptive models in safeguarding financial and economic systems.

In synthesis, these studies collectively underscore the intricate interplay of administrative, legal, and technological elements in the pursuit of robust financial and economic security. The literature sets the stage for the current research, which seeks to contribute novel insights into the implementation of an information system tailored to counter modern cyberthreats and fortify the administrative-legal mechanisms safeguarding financial integrity.

## Methodology

The methodological basis of the study is the theoretical and methodological provisions for ensuring the financial and economic security of the state in the context of countering modern cyberthreats.

To fully understand the process of improving the financial and economic security of the state in the context of countering modern cyberthreats, we used the modern methods of hierarchical analysis and pairwise comparison method and also expert analysis method.

In the hierarchical analysis method, the even comparison procedure is applied to pairs of homogeneous elements. Heterogeneous elements are divided into interconnected groups (clusters) containing homogeneous elements. In the hierarchical analysis method, it is possible to create matrices of paired comparisons based on any ratio scales used for the measured properties of the objects being compared. In similar variants, expert assessment is replaced by the ratio of two corresponding dimensions. The resulting scale derived from the paired comparison matrix containing estimates of the actual measurements will be similar to that which can be obtained by normalizing to the unit of the corresponding measurements.

These methods make it possible to systematically and objectively assess the impact of various cyber threats and determine which of them should be paid special attention to when planning measures to ensure financial and economic security. The said methods were used to compare and contrast certain cyber threats in such a way as to ascertain from expert opinion which negative impact is more dominant than the other. For this purpose, there is a point rating scale according to the procedure. If it significantly exceeds, then more points; if not significantly, then less. In total, more than 30 experts from the field of financial and economic security were involved. 20 experts from the field of cybersecurity were also involved. A survey was conducted through the Delphi method.

Research hypothesis: to propose a methodological approach to ordering cyber threats in such a way that it is possible to establish the most significant ones in the context of ensuring financial and economic security, and which ones are not.

## Results and Discussion

The formation and effective implementation of a cybersecurity policy, within the framework of which a set of measures to predict and counter cyber threats is developed, is a necessary condition for the development of a knowledge society. In the context of the globalization of information processes and their integration into various spheres of public life, the leadership of the leading countries of the world pays increased attention to the creation and improvement of effective systems for protecting critical infrastructure from external and internal cyberthreats.

It should be noted that in many leading countries of the world, national cybersecurity systems have already been formed as the most optimal organizational structures that can quickly accumulate the forces and resources of competent government authorities with the involvement of public authorities to counter cyberthreats.

Cyberthreats in modern society are gaining significant scale. Now, a successful hacker attack can cut off power to an area or country, lead to a bank robbery, or destroy a successful organization. In order to carry out correct and effective measures to prevent cyber threats and eliminate their negative consequences, their legitimization is first of all necessary - the development and consolidation of a legislative definition in order to avoid differences in the application of this category, as well as conflicts with other legal acts, determination of their content, uniformity of law enforcement practice.

In the context of our research, for the formation of information systems for the implementation of the administrative and legal mechanism for ensuring financial and economic security under the influence of modern cyberthreats, it is important to highlight the key cyberthreats that have the greatest impact. For better understanding and specification, all threats will refer to a specific country - Ukraine. The reason for choosing this country was that the authors and experts who were chosen for the study live in Ukraine and are specialists in the field of cyberthreats and cyber security in Ukraine. Thus, according to the expert opinion, the experts identified key cyberthreats in the information system of the administrative and legal mechanism for ensuring financial and economic security of Ukraine (Table.1).

**Table 1.**

*Key cyberthreats in the information system of the administrative and legal mechanism for ensuring financial and economic security of Ukraine*

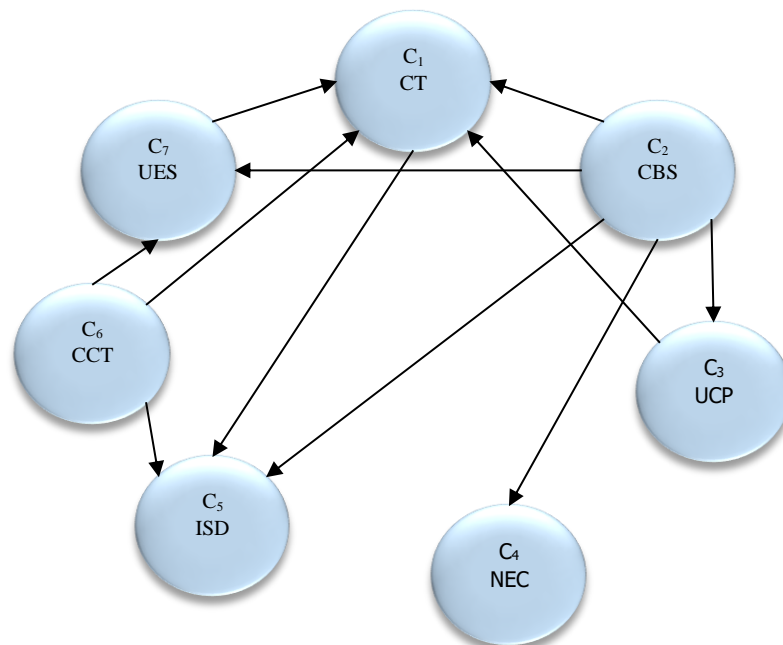
№	The name of the cyber threat	Mnemonic name
1	The activation of cyber terrorism caused by military actions	CT
2	Development of cybercrime in the banking sector	CBS
3	Unsystematic measures of cyber protection of critical information infrastructure	UCP
4	Noncompliance of the state's electronic communications infrastructure, its level of development and security with modern requirements	NEC
5	Insufficient effectiveness of the subjects of the security and defense sector of Ukraine in countering cyberthreats of a military, criminal, terrorist and other nature	ISD
6	Emergence of content cyberthreats	CCT
7	Threats to the integrity of the economic space	UES

Source: (Formed by authors)

Taking the constructed graph as a basis, we construct a binary dependence matrix A for the set of vertices C1 as follows (1):

$$a_{ij} = \begin{cases} 1, & \text{if criterion (vertex) } I \text{ depends on criterion (vertex) } J \\ 0 & \text{if criterion (vertex) } I \text{ does not depend on criterion (vertex) } J \end{cases} \quad (1)$$

Graph of connections between key cyberthreats in the information system of the administrative and legal mechanism for ensuring financial and economic security of Ukraine in Figure 1.



**Figure 1.** Graph of connections between key cyberthreats in the information system of the administrative and legal mechanism for ensuring financial and economic security of Ukraine **Formed by authors.**

According to the calculations performed and the generated matrix, the next step will be to create a binary dependency matrix (Table 2).

**Table 2.**  
Binary dependency matrix

		1	2	3	4	5	6	7
1	CT	CT	BP	UCP	NEC	ISD	CCT	UES
		SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:0	:0	:0	:0	:1	:0	:0
2	BP	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:1	:0	:1	:1	:1	:0	:1
3	UCP	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:1	:0	:0	:0	:0	:0	:0
4	NEC	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:1	:0	:0	:0	:0	:0	:0
5	ISD	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:0	:0	:0	:0	:0	:0	:0
6	CCT	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:1	:0	:0	:0	:1	:0	:1
7	UES	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS	SET AS
		NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER
		:1	:0	:0	:0	:0	:0	:0

Source: (Formed by authors)

This matrix is constructed in accordance with the relationship proposed below (2):

$$a_{ij} = \begin{cases} 1, & \text{when there is a relationship between cyberthreats} \\ 0 & \text{when there is no connection between cyberthreats} \end{cases} \quad (2)$$

Vertex  $z_j$  is formed from vertex  $C_i$  if in the graph (Fig. 1) there is a path leading from vertex  $C_i$  to vertex  $C_j$ . Such a peak is designated as achievable. Forming a subset of similar vertices through  $S(C_i)$ . Similarly, vertex  $C_i$  is the next corresponding vertex  $C_j$  if it reaches its maximum. Thus, the collection of vertices forms a subset  $P(C_i)$ .

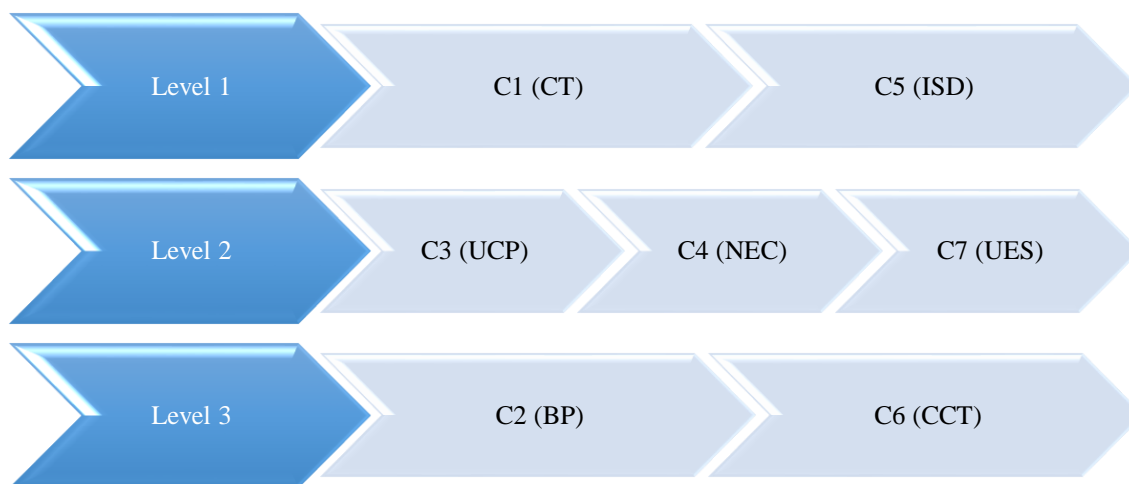
The final intersection of subsets of reachable vertices and predecessor vertices, which corresponds to subset (3):

$$R(C_i) = S(z_i) \cap P(z_i) \quad (3)$$

The vertices that do not reach any vertex of the set of remaining  $C1$  determine a certain level of the priority hierarchy of the actions of cyberthreats, the vector of which goes to these vertices. An additional condition is to ensure the equality shown in the formula (4)

$$P(C_i) = R(C_i) \quad (4)$$

Bypassing intermediate calculations, we ultimately obtain hierarchical levels of the impact of cyberthreats in the information system of the administrative and legal mechanism for ensuring financial and economic security of Ukraine (Fig.2).



**Figure 2.** The scheme of the hierarchy of the influence of cyberthreats in the information system of the administrative and legal mechanism for ensuring the financial and economic security of Ukraine.

Source: (developed by the authors)

Thus, we have determined that cyberthreats 2 and 5 have the greatest impact on the formation of information systems of the administrative and legal mechanism for ensuring financial and economic security. Accordingly, in order to formulate the most effective administrative and legal support, it is critical to take into account measures that would counteract or neutralize the impact of these particular cyberthreats. It should be noted that certain cyberthreats are specific to the realities of the Ukrainian financial and economic system, and therefore, when creating similar information systems of the administrative and legal mechanism for other countries, cyberthreats specific to each country should be identified.

### Conclusions

In the sum, in modern conditions, the influence of the global financial and economic system on an individual state is moving to a qualitatively new level. Given the leading role of finance in the modern economy, special attention is paid to management influences through financial mechanisms, using financial levers, financial incentives and financial goals. And globalization precisely creates the conditions for the establishment of special financial power, which, through the ownership of world money and the disposal of the cost of managing financial flows, allows one to influence both the entire global economic space and individual states.

As computers have moved to “resource sharing systems,” cybersecurity issues require significant resources, the development of appropriate strategies, mechanisms to combat cybercrime, and coordination among different market actors.

Approaches to cybersecurity and financial security are no longer technical, as they increasingly embrace legislative and policy issues tailored to the specific skills and practices of users shaped by the diversity of cultures and societies online and around the world. As the Internet has become more pervasive in life and the workplace, there is greater awareness that cybersecurity cannot simply be a response to emerging problems, but must prevent the threat of cybercrime to improve the resilience of any systems.

Modern realities of cybersecurity indicate a number of important problems that prevent the creation of an effective system for countering threats in cyberspace for financial and economic security. Such problems, first of all, include terminological uncertainty, lack of proper coordination of the activities of relevant departments, dependence on foreign-made software and technical products, and difficulties with staffing the relevant structural units. These factors only strengthen the identified cyberthreats and potentiate their manifestation.

The importance of ensuring financial and economic security in the context of protection modern methods of hierarchical analysis and pairwise comparison method against cyberthreats is becoming increasingly significant in the realities of the present world. This situation has led to active interest in the formation of specific information systems for the implementation of administrative and legal mechanisms to ensure financial and economic security. The study has its limitations, since for the formation of the above information systems, a limited number of cyberthreats were adopted,



which are also characteristic of a particular country. In the future, it is planned to expand the list and levels of influence of threats, which will be used to create more complete and integrated information systems for the implementation of the administrative and legal mechanism for ensuring financial and economic security under the influence of modern cyberthreats, both for Ukraine and for other countries.

Given the identified cyberthreats, we recommend that governments and organizations take specific steps to ensure better protection. First, interdepartmental coordination needs to be strengthened to ensure effective sharing of information and resources. Secondly, it is important to reduce dependence on foreign software and technical products by promoting the development of domestic alternatives. Finally, upskilling staff in cybersecurity is key to strengthening defenses against digital threats. The results of our study also point to potential directions for future cybersecurity research. First, it may be interesting to analyze the specific impacts of cyberthreats in different countries and regions, as they may differ depending on local conditions and policies. It is also important to explore new technologies that can help identify and counter cyber threats at an early stage. Finally, developing effective strategies to mitigate the damage from cyberattacks will be an important step in strengthening cybersecurity at the global level.

### Bibliographic references

- Al Azzam, F.A.F. (2019). The adequacy of the international cooperation means for combating cybercrime and ways to modernize it. *JANUS. NET e-journal of International Relations*, 10, 64-81. <https://doi.org/10.26619/1647-7251.10.1.5>
- Albalawi, A.M., & Almaiah, M.A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *Journal of Theoretical and Applied Information Technology*, 100(9), 2988-3011.
- Alvarez, I., Di Caprio, D., & Santos-Arteaga, F.J. (2016). Technological assimilation and divergence in time of crisis. *Technological and Economic Development of Economy*, 22(2), 254-273. <https://doi.org/10.3846/20294913.2015.1033663>
- Benigno, G., Chen, H., Otrók, C., Rebucci, A., & Young, E. R. (2013). Financial crises and macro-prudential policies. *Journal of International Economics*, 89(2), 453-470. <https://doi.org/10.1016/j.jinteco.2012.06.002>
- Dragan, I., Liakhovych, G., Inozemtseva, O., Marushchyn, Y., & Lyakhovych, U. (2023). Legal aspects of reforming public management of financial and economic security in Ukraine in the context of European integration. *Financial and Credit Activity Problems of Theory and Practice*, 1(48), 326-334. <https://doi.org/10.55643/fcaptop.1.48.2023.3961>
- 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/ijssse.120110>
- 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/ijssse.110409>
- Iskajyan, S.O., Kiseleva, I.A., Tramova, A.M., Timofeev, A.G., Mambetova, F.A., & Mustaev, M.M. (2022). Importance of the information environment factor in assessing a country's economic security in the digital economy. *International Journal of Safety and Security Engineering*, 12(6), 691-697. <https://doi.org/10.18280/ijssse.120604>
- Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, 20, 2481-2501. <https://doi.org/10.1007/s11276-014-0761-7>
- Jovovic, R., Draskovic, M., Delibasic, M., & Jovovic, M. (2017). The concept of sustainable regional development – institutional aspects, policies and prospects. *Journal of International Studies*, 10(1), 255-266. <https://doi.org/10.14254/2071-8330.2017/10-1/18>
- Kryshchanovych, 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. *International Journal of Safety and Security Engineering*, 28(1), 41-47. <https://doi.org/10.18280/isi.280105>
- Raghutla, C., & Chittedi, K.R. (2021). Financial development, real sector and economic growth: Evidence from emerging market economies. *International Journal of Finance & Economics*, 26(4), 6156-6167. <https://doi.org/10.1002/ijfe.2114>

- 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>
- Soni, G., Mangla, S. K., Singh, P., Dey, B. L., & Manoj, D. (2021). Technological interventions in social business: Mapping current research and establishing future research agenda. *Technological Forecasting and Social Change*, 169, 120818. <https://doi.org/10.1016/j.techfore.2021.120818>
- Stankevičienė, J., Sviderskė, T., & Miečinskienė, A. (2014). Comparison of country risk, sustainability and economic safety indices. *Business: Theory and Practice*, 15(1), 1-10. <https://doi.org/10.3846/btp.2014.01>
- Sylkin, O., Kryshchanovych, M., Bekh, Y., & Riabeka, O. (2020). Methodology of forming model for assessing the level financial security. *Management Theory and Studies for Rural Business and Infrastructure Development*, 42(3), 391-398. <https://doi.org/10.15544/mts.2020>
- Syshchuk, A., & Teteruk, O. (2018). Formation and development of the European Union monetary and financial mechanism of anti-crisis regulation. *Economic Journal of Lesia Ukrainka Eastern European National University*, 1(13), 157-164. <https://doi.org/10.29038/2411-4014-2018-01-157-164>
- 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>