Economic Affairs, Vol. 68, No. 01s, pp. 61-71, February 2023
DOI: 10.46852/0424-2513.1s.2023.8

AESSRA

Research Paper

Formation of Business Cyber Security in Conditions of Instability of the Domestic Economy

Olena Skiban[1], Yaroslaw Kostetskyi[2*], Marta Danylovych-Kropyvnytska[3], Olga Cholyshkina[4] and Mykola Miroshnichenko[5]

[1]Ukrainian Academy of Printing, Lviv, Ukraine
[2]Dept. of Fundamental and Special Disciplines, Novovolynsk Educational and Scientific Institute of Economics and Management of West Ukrainian National University, Ternopil, Ukraine
[3]Dept. of Theoretical and Applied Economics, Lviv Polytechnic National University, Lviv, Ukraine
[4]Dept. of Computational Mathematics and Computer Modeling, Interregional Academy of Personnel Management, Kyiv, Ukraine
[5]Dept. of Computer Sciences, Dmytro Motornyi Tavria State Agrotechnological University, Melitopol, Zaporizhzhiaobl., Ukraine

*Corresponding author: yarkos09@gmail.com (**ORCID ID:** 0000-0001-5487-2996)

Received: 16-11-2022 **Revised:** 29-01-2023 **Accepted:** 03-02-2023

ABSTRACT

The strengthening of the destabilizing influence of modern challenges and dangers leads to the emergence of significant risks and threats to Ukraine's national security. It creates the need to protect the country's territorial integrity and sovereignty, for as much as the full-scale invasion of the Russian Federation into the territory of independent Ukraine caused an unprecedented crisis and critical conditions for the state's functioning. The influence of these challenges and dangers on business structures, which are often subject to unauthorized interference in their activities by cybercriminals, is especially noticeable under such circumstances, which makes it necessary to ensure a high level of business cyber security. The purpose of the academic paper is to study the theoretical and applied principles of ensuring business cyber security in conditions of the domestic economy's instability. The methodological base of the research comprises the following general scientific and special methods of economic analysis and scientific knowledge, namely: scientific abstraction, system analysis, synthesis, statistical analysis, comparison, analogies, classification, grouping, cluster analysis (based on the k-means method), graphic, tabular generalization and systematization. Based on the results of the conducted research, it can be stated that the cyber security of business in conditions of the domestic economy's instability is characterized by an excessive influence of cyber risks and cyber threats. It has been established that the effectiveness of ensuring business cyber security depends on the level of the country's development: highly developed countries have significantly higher cyber security indicators (USA: 0,919 - 1,000; Great Britain: 0,783 - 0,995; Germany: 0,679 – 0,974) than in developing countries (Moldova: 0,418 – 0,758; Belarus: 0,506 -0,592; Ukraine: 0,501 - 0,688). It has been proven that countries of the transitive type are unable to fully withstand the challenges and dangers of cyberspace, as a result of which business structures are exposed to malicious unauthorized encroachments by cybercriminals. The basic preventive and strategic measures to strengthen business cyber security are proposed, and the need for the codification of cyber law in Ukraine is substantiated.

HIGHLIGHTS

- It has been established that the effectiveness of ensuring business cyber security depends on the level of the country's development.
- It has been proven that countries of the transitive type are unable to fully withstand the challenges and dangers of cyberspace, as a result of which business structures are exposed to malicious unauthorized encroachments by cybercriminals.
- An increase in the number of cyberattacks on business entities conducted using ransomware in the period 2017–2022 was revealed.

Keywords: Cyber risks, cyber threats, cyber security, cyber space, cyber-crime, cyber-attacks, economic instability, business structures

How to cite this article: Skiban, O., Kostetskyi, Y., Danylovych-Kropyvnytska, M., Cholyshkina, O. and Miroshnichenko, M. (2023). Formation of Business Cyber Security in Conditions of Instability of the Domestic Economy. *Econ. Aff.*, **68**(01s): 61-71.

Source of Support: None; **Conflict of Interest:** None

The spread of globalization processes characterizes the current state of developing world economic relations. As a result, the merging of national borders is observed, and the transformations of social-economic and social-political processes into a single global world economic system, in which operations are carried out using the virtual environment on a global scale. The rapid development of cyberspace and its improvement is also due to countries' participation in the processes of globalization and geopoliticization, resulting in interstate conflicts. Their development causes economic instability and the emergence of cyber risks and cyber threats, which, in turn, contribute to the intensification of cyber-crime. Moreover, the intensification of the struggle for spheres of influence in cyberspace between the world power centers in order to fulfill their geopolitical interests has a particularly significant negative impact of the destabilizing factors of cyberspace's functioning on implementing operations within its borders by business structures whose activities are extremely vulnerable in conditions of financial, economic and social-political instability. It is obvious that the specified tendencies require the formation of an effective system for ensuring the cyber security of all economic agents and the creation of effective measures to minimize the impact of cyber risks and cyber threats,. Consequently, this extremely actualizes the research topic and requires an in-depth study of the outlined issues.

Literature Review

The issue of investigating business cyber security in conditions of the domestic economy's instability has been the subject of study by leading domestic and foreign scientists for a long period of time. After all, the intensification of cybercrime's development has reached a threatening scale and poses a serious obstacle to the security of the functioning of the state, society and business structures. Kuzmenko *et al.* (2022) claim that business structures in Ukraine are constantly subjected to cyberattacks. Their intensification increased significantly during the period of the full-scale invasion of the Russian Federation on the territory of Ukraine and the deployment of active hostilities in significant territories. Scientists have established that cyberattacks on enterprises belonging to critical infrastructure facilities are especially dangerous. Therefore, ensuring business cyber security should take into account measures and coordinated actions implemented at different levels of social relations: national, regional and international (Holovatyi, 2015). Cochran, 2022 believes that economic uncertainty and the presence of crisis situations stimulate the development and intensification of cyber risks and cyber threats, as a result of which the level of cyber security of business is significantly reduced.

In this context, Jabbari (2018) notes that in accordance with the provisions of international laws and regulations, the functioning of cyberspace and the implementation of operations within its limits are clearly regulated by the principles of sovereignty and jurisdiction. They constitute a ban on the intervention of some countries in the affairs of others, as well as the use of force methods impact. In addition, the scientist insists that states subject to unauthorized influence have the right to apply countermeasures, which, in fact, corresponds to the concept of implementing the principles of cyber security.

As for Ukraine, there are certain problems of ensuring business cyber security in this direction. Even despite the approval of the Cyber Security Strategy of Ukraine (the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cyber Security Strategy of Ukraine") and the implementation of its main provisions, it has not been possible to reduce the level of cyber-crime yet. According to this legal act, the Russian Federation is recognized as the greatest source of threats to international and national cyber security, forasmuch as it carries out information warfare, psychological influence, intelligence and subversive activities and other types of cyber-attacks. The issue of ensuring cyber security becomes even more urgent under such circumstances. This requires outlining the basic priority directions for cyberspace protection of national interests in cyberspace, the formation of effective countermeasures against existing and potential cyber risks and cyber threats, as well as the creation of favorable conditions for cyberspace's safe functioning.

At the same time, it is worth noting that the existing scientific heritage does not cover a single unified

approach to interpreting the essence of business cyber security. Moreover, there is still no single definition of the content of the category "cyber security". In particular, in the Cyber Security Strategy of Ukraine (the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cyber Security Strategy of Ukraine"), the essence of cyber security is defined as the state of protection of the state's national interests in cyberspace from unauthorized external influence by external subjects. Therefore, Mishra et al., 2022 note that cyber security should become a critical and priority issue in the system of ensuring the effective functioning of enterprises of various types, taking into account the strategic vectors of its provision at the national level. The team of authors headed by Ishchenko *et al.* (2021) dealt with issues of chemical safety in the context of environmental goals of sustainable development.

Zwilling *et al.* (2020) argue that business structures have a sufficiently high level of awareness of cyber threats and understand their importance and danger. However, they take only minimal measures to protect against cyber-attacks and to strengthen their cyber security, one of the good reasons for which is the high cost of acquiring cyber security tools. Wirth (2017) estimated the global costs on cyber security, which annually reach 100 billion US dollars, and the losses due to the implementation of cyber-attacks – 1 trillion US dollars. At the same time, the scientist established a shift in the vector of committing cyber-crimes from unauthorized interference in the work of stations and servers to obtaining confidential data. The scholar also emphasizes the activation of danger in cyberspace on the part of ransomware. At the same time, the researcher singles out certain features of ensuring cyber security in modern business, the most significant of which are as follows: (1) the need to form a data protection strategy of the business entity; (2) prevention of leakage of data and confidential information, the loss of which leads to financial failure and loss of business; (3) formation of an effective mechanism for combating cyber-attacks and cyber-threats; (4) activation of investment and innovation development of business cyber security technologies.

Supplementing previous researchers' viewpoints, Vasupula *et al.* (2021) state that ensuring business cyber security involves the formation of an effective mechanism to protect personal and confidential data from unauthorized influence by third parties on them with the aim of obtaining data without the user's consent, its disclosure and distribution. After all, as established by Guembe *et al.* (2022), in today's conditions, cyber-attacks take on a new form and are diversified with the wide use of artificial intelligence methods, which allow being less visible in cyberspace and causing more damage, and existing cyber security tools are unable to detect such cyber-attacks in time and effectively counteract them.

Li & Liu (2021) argue that it is meaningless to study the issue of cyber security only within the scope of protecting business from cyber-attacks. They insist on considering this issue not even at the national, but at the international level, taking into account the transnational nature of cyberspace's functioning and the scale of operations there. At the same time, scientists claim that the state of ensuring cyber security within a specific country depends on its economic stability and economic development indicators. After all, the financial and economic background is extremely significant, especially for countries characterized by financial, economic and social and political instability (Holovatyi, 2015). Moreover, Tam *et al.* (2021) investigated that the outlined hypothesis has the right to exist. Problems of ensuring cyber security should be considered and regulated at the state level, forasmuch as it has been found that small business entities are exposed to unauthorized influence and cyber-attacks not only from external attackers, but also from medium and large businesses. Thus, scientists believe that ensuring the cyber security of small businesses is a more complex problem and requires the legal intervention of the state (Kostiukevych, 2020).

It is obvious that the issues of ensuring business cyber security are multifaceted. A high level of unpredictability in the conditions of the influence of modern challenges and dangers characterizes them. Given these trends, Thomson, 2015, suggests paying considerable attention not only to studying cyber-attacks in the context of ensuring cyber security for business, but also to cyber espionage, as this problem has become extremely relevant under the influence of globalization and other modern challenges. Bullock *et al.* (2021), consider it, along

with cyber wars, cyber terrorism, cyber sabotage and cyber-crime, to be one of the most dangerous threats to business cyber security.

Liu *et al.* (2022) consider the emergence of cyber security threats through the prism of continuous and multi-format destructive impact on business processes. They claim that the amount of financing measures to ensure business cyber security at the level of the countries of the world has increased significantly in recent years. At the same time, the scholars note the difficulty of ensuring a sufficient level of cyber security due to the constant updating of tools for cyber-attacks and cyber-crimes, their constant improvement and the creation of new malicious programs. According to the data systematized by Richardson (2022), the most common threats to business cyber security in 2022 were as follows: (1) ransomware attacks; (2) phishing; (3) using encrypted malware; (4) fileless attacks; (5) using memory-based malware; (6) crypto fraud; (7) using IoT malware; (8) side-channel attacks. In addition, 43% of cyber-attacks' cases on a global scale are related to the Russian-Ukrainian armed military conflict, which proves the importance of the war in Ukraine on a global scale in all spheres of social relations.

It is obvious that the issue of ensuring business cyber security in current conditions is extremely relevant. It becomes especially acute in those countries where problems of a geopolitical nature are present, and there is the need to strengthen it, which requires in-depth research in this direction.

The purpose of the academic paper is to study the theoretical and applied principles of ensuring business cyber security in conditions of the domestic economy's instability.

METHODS

The methodological base of the research comprises the following general scientific and special methods of economic analysis and scientific knowledge, namely: scientific abstraction, system analysis and synthesis, which were used to clarify the essence of business cyber security and the features and problems of its provision. The method of statistical analysis, comparison and analogies was applied to carry out an empirical assessment of the current state and trends of business cyber security, as well as to analyze and monitor cyber risks and cyber threats. The method of classification, grouping and cluster analysis (based on the k-means method) was applied in order to identify common and distinctive features and peculiarities of business cyber security in countries with different levels of development. Graphical and tabular methods were used for visual display of the obtained research results. The method of generalization and systematization was applied for the purpose of forming conclusions.

The information base of the research consists of the scientific works of leading domestic and foreign scientists investigating the issues of ensuring business cyber security in the modern conditions of the domestic economy's instability, as well as the reporting data of international organizations for 2017–2021: Global Cyber Security Index according to the Global Cyber Security Index; Spending on cyber security worldwide from 2017 to 2021 (COVID-19) adjusted by the indicator of total expenditures on cyber security and Annual number of ransomware attacks worldwide from 2016 to first half 2022 according to the indicator of the total annual number of cyber-attacks using ransomware, conducted in global cyberspace and aimed at business entities.

RESULTS

The problems of ensuring the sustainable development of Ukraine's economy are caused by the negative impact of factors of the external and internal environment, which are related to the processes of globalization, geopoliticization and aspirations to integrate into the world economic and legal space. Increasing instability of the domestic economy is a consequence of the destructive changes taking place in various spheres of state activity. It is obvious that modern challenges, along with the positive impact on economic processes, also cause negative trends, one of which is mainstreaming the activities of the subjects of economic relations in cyberspace. As a result, processes and operations of a financial-economic and social-political nature take place, causing significant damage to society and economic agents.

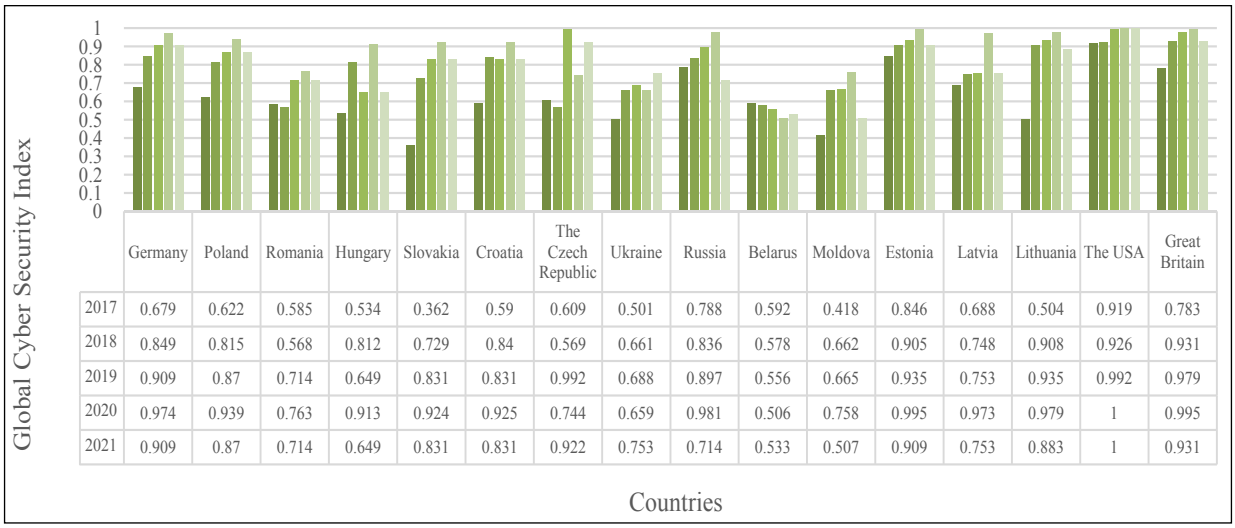
Conducted studies of theoretical viewpoints on the issue of the domestic economy's instability make it possible to single out various problems of ensuring the protection of national interests of the state, one

of which is the excessive vulnerability of business structures to challenges and dangers arising in cyberspace and destabilizing their activities. The specified tendencies require increased attention to ensuring cyber security at various levels of relations and conducting in-depth research in this direction.

The domestic cyber defense system is currently very weak and needs a complex of efficient measures to strengthen it, as shown by analytical evaluations of the primary approaches to studying the problem of ensuring business cyber security in the context of economic instability and Ukraine's military resistance to the armed aggression of the Russian Federation. Leading domestic scientists and economists claim that ensuring business cyber security depends significantly on the country's level of development and its ability to counter cyber risks, cyber threats and cyber-attacks effectively. Moreover, the assessments of countries based on the Global Cyber Security Index during 2017–2021 (Fig. 1) allow us to identify the country's ability to identify threats, create a powerful cyber security system, and intensify the educational component regarding the cyber awareness of the public and business structures in the field of cyber security. The results of the conducted empirical studies indicate a different level of effectiveness of the business cyber security system in the countries selected for analysis. In particular, such countries as the United States, the United Kingdom, and Germany are more effective in combating cyber threats and cyber risks and are able to provide the highest level of cyber security, as evidenced by the values of the Global Cyber Security Index, which in the United States are in the range of 0,919 - 1,000; in Great Britain, it is within 0,783 - 0,995; in Germany, it is in the range of 0,679 - 0,974.

At the same time, the worst situation regarding the provision of cyber security is revealed in Moldova (GCSI: 0,418 - 0,758), Belarus (GCSI: 0,506 – 0,592) and Ukraine (GCSI: 0,501 – 0,688), where the existing domestic systems for ensuring cyber security are too weak, and the financing of measures countering cyber risk and cyber threats is characterized by low volumes. In addition, it is worth noting the significant values of the Global Cyber Security Index indicator in Russia, which is at the level of 0,714 - 0,981 during the analyzed period, which, admittedly, is a significant achievement of the country and poses a significant threat to other countries. It is not surprising that, in recent years, Russia has been regarded as the main source of cyber hazards and threats, and the majority of cyberattacks originate from within its borders.

The outlined tendencies indicate the ambiguity of solving the problem of ensuring business cyber security in the countries selected for analysis. In order to identify common and distinctive features, we suggest grouping these countries according to the Global Cyber Security Index and establishing their inherent features. The necessary calculations will be conducted using the technology of cluster analysis, which will be built on the basis of the



	Germany	Poland	Romania	Hungary	Slovakia	Croatia	The Czech Republic	Ukraine	Russia	Belarus	Moldova	Estonia	Latvia	Lithuania	The USA	Great Britain
2017	0.679	0.622	0.585	0.534	0.362	0.59	0.609	0.501	0.788	0.592	0.418	0.846	0.688	0.504	0.919	0.783
2018	0.849	0.815	0.568	0.812	0.729	0.84	0.569	0.661	0.836	0.578	0.662	0.905	0.748	0.908	0.926	0.931
2019	0.909	0.87	0.714	0.649	0.831	0.831	0.992	0.688	0.897	0.556	0.665	0.935	0.753	0.935	0.992	0.979
2020	0.974	0.939	0.763	0.913	0.924	0.925	0.744	0.659	0.981	0.506	0.758	0.995	0.973	0.979	1	0.995
2021	0.909	0.87	0.714	0.649	0.831	0.831	0.922	0.753	0.714	0.533	0.507	0.909	0.753	0.883	1	0.931

Compiled based on: Global Cyber Security Index 2017–2021.

Fig. 1: Dynamics of the Global Cyber Security Index in some European countries

k-means method. The obtained results will be systematized in Table 1.

Table 1: Grouping of some European countries according to the Global Cyber Security Index in 2017–2021

№	Country	Euclidean distance	Cluster number
1	The USA	0,121	
2	Great Britain	0,064	
3	Germany	0,025	
4	Poland	0,050	
5	Croatia	0,069	1
6	Russia	0,077	
7	Estonia	0,068	
8	Latvia	0,098	
9	Lithuania	0,097	
10	Slovakia	0,088	2
11	The Czech Republic	0,088	
12.	Romania	0,069	
13	Hungary	0,111	
14	Ukraine	0,064	3
15	Belarus	0,123	
16		0,076	

Compiled based on: Global Moldova Cyber Security Index 2017–2021.

As evidenced by the results of clustering some European countries according to the Global Cyber Security Index, in 2017–2021 there is a trend that the countries of the selected group are divided into three clusters, which are characterized by both common and distinctive features of ensuring business cyber security. In particular, the first group includes such highly developed and technologically innovative countries as the USA, Great Britain, Germany, Poland, Croatia, Estonia, Latvia and Lithuania. These countries attach great importance at the state level to the issue of ensuring business cyber security, support projects of innovative and technological development of means and measures to counter cyber risks and cyber threats, as a result of which they manage to fight effectively against cyber-attacks. In addition to the mentioned European countries, the first cluster includes Russia; Global Cyber Security Index indicators in this country are quite high, indicating a significant level of business protection. Moreover, Russia has long been engaged in thorough research in the field of cyber security and is capable, despite positive results, of creating a variety of malicious software with the help of which it exerts a significant negative illegal and unauthorized influence on other countries' systems and facilities. The world community recognizes Russia as the most dangerous producer and distributor of malicious software in today's conditions.

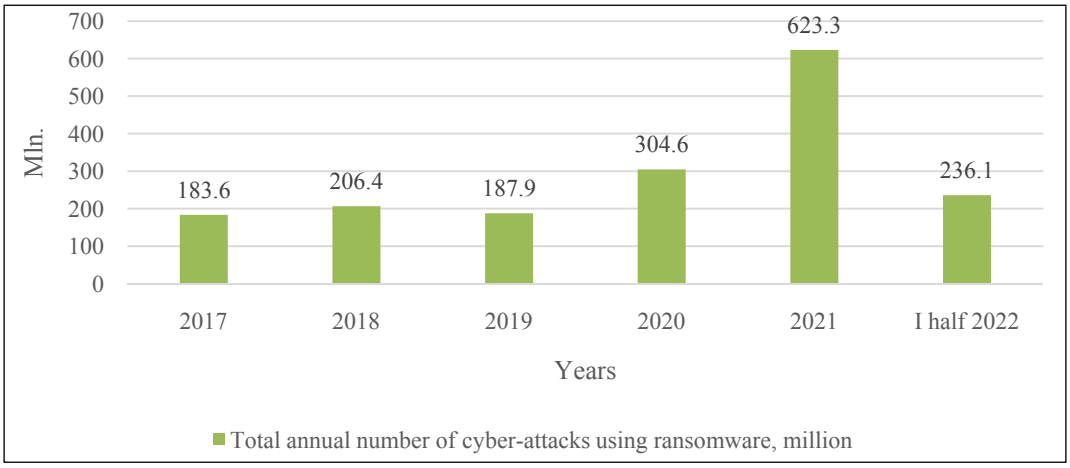
The second group of countries consists of Slovakia and the Czech Republic. The system of ensuring business cyber security in these countries is developed at a sufficiently high organizational and methodical level and there is significant potential for strengthening business cyber security. However, there are certain problems with regard to timely countermeasures against cyber-attacks.

The third group includes the countries of the post-Soviet space, which have been undergoing transformational restructuring for a long enough time (Romania, Hungary, Ukraine, Belarus and Moldova). The business cyber security system of these states does not meet established global requirements and standards and needs significant improvement.

At the same time, it should be noted that most European countries, as well as the USA, are consolidating efforts to jointly ensure business cyber security. After all, the challenges of the spread of cyber-crime and the emergence of new cyber risks and cyber threats are updated every day. Therefore, the issue of financing cyber security at the international level, as well as monitoring the state of its parameters, is of particular importance. In particular, we consider it expedient to monitor the dynamics of the total number of cyberattacks using ransomware in Fig. 2, which are carried out in global cyberspace annually and cause significant damage to business entities.

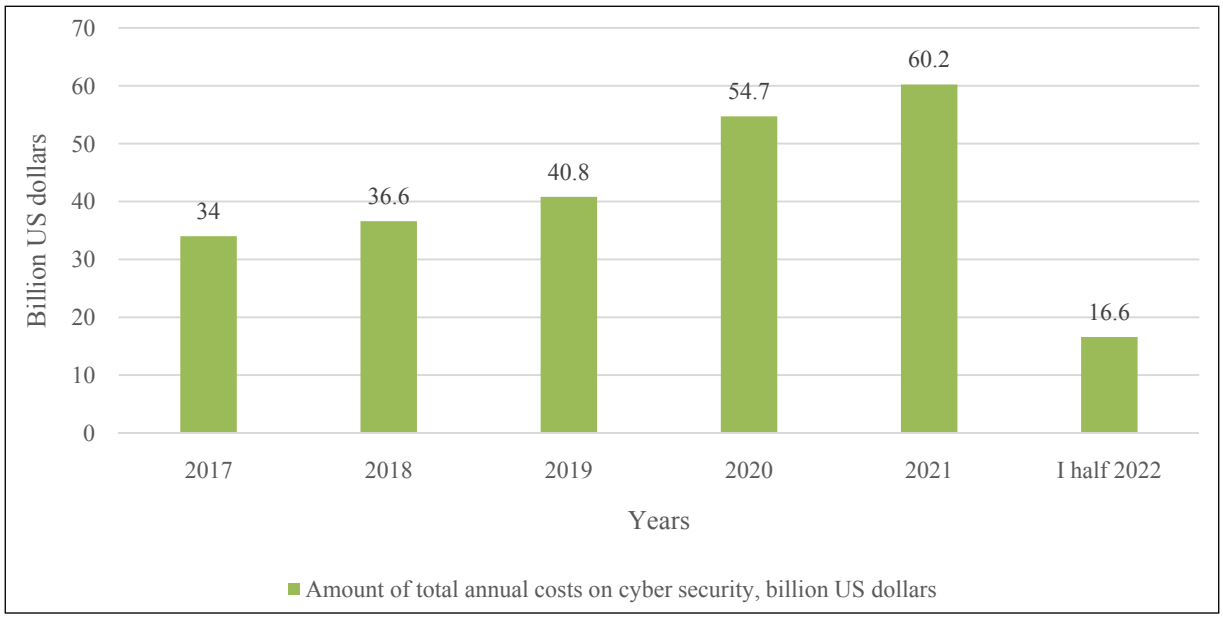
As evidenced by the results of the conducted research, indicators of the total annual number of cyber-attacks using ransomware, conducted in global cyberspace and aimed at business entities, have significant growing trends. An annual increase in their number is observed from 183,6 million in 2017 to 623,3 million in 2021, which proves the need to pay particular attention to the issues of ensuring business cyber security.

It is worth noting that some progress in this direction has already been made, as evidenced by the indicators of the total annual costs for cyber



Compiled based on: Annual number of ransomware attacks worldwide from 2016 to first half 2022.

Fig. 2: Dynamics of the total annual number of cyber-attacks using ransomware carried out in global cyberspace and aimed at business entities in 2017-2022



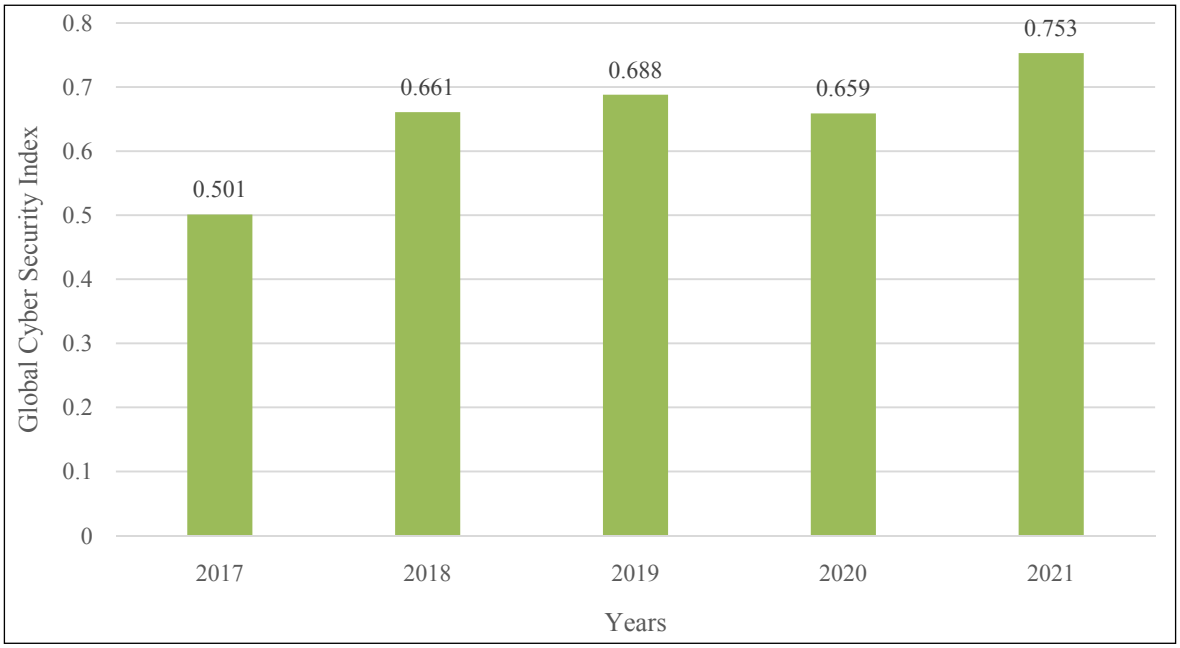
Compiled based on: Spending on cyber security worldwide from 2017 to 2021 (COVID-19) adjusted.

Fig. 3: Dynamics of total annual costs for cyber security in 2017–2022

security, the dynamics of which during 2017–2022 are shown in Fig. 3.

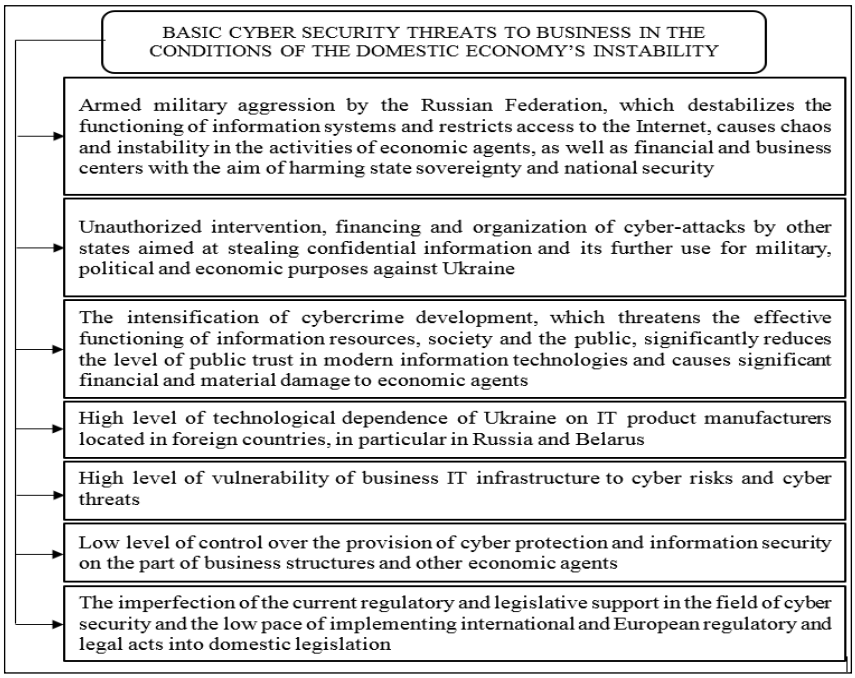
The data reflected in Fig. 3 show that the amount of spending on cyber security is increasing every year at the international level. In particular, it amounted to 34 billion US dollars in 2017, and it reached the mark of 60,2 billion US dollars in 2021 (rate of change is 77,06%).

As for Ukraine, it is worth noting that the situation is extremely difficult to ensure an adequate level of cyber security there. As evidenced by the data systematized in Fig. 4, the level of the Global Cyber Security Index ranges from 0,501 to 0,753. This is a sufficiently low value and it indicates the excessive vulnerability of domestic business to challenges and dangers in cyberspace. However, it is important to note the positive, albeit minor, but significant strengthening of cyber security in Ukraine in 2021. It took place under the influence of the aggravating the problem of the activation of petty fraud in cyberspace as a result of the introduction of quarantine restrictions caused by spreading the COVID-19 pandemic and the transition of a significant number of financial transactions to



Compiled based on: Global Cyber Security Index, 2017–2021.

Fig. 4: Status and tendencies of changes in the Global Cyber Security Index in Ukraine in 2017–2021



Author's development.

Fig. 5: The basic threats to business cyber security in conditions of the domestic economy's instability

virtual space. It is obvious that the domestic system of ensuring business cyber security coped with existing challenges and managed to develop and implement effective countermeasures.

At the same time, significant problems of ensuring business cyber security still remain relevant and require searching for solutions. Regrettably, in today's conditions, the influence of cyber risks and cyber threats on the activities of business structures is constantly increasing, the main of which should be systematized in Fig. 5. At the same time, it should be noted that the most significant cyber

risks and cyber threats to business in conditions of instability of the domestic economy include Russia's war against Ukraine, the intensification of cyber-crime development, a significant level of technological dependence on external manufacturers of IT products, and a low level of control over the provision of cyber protection and information security on the part of business structures. Moreover, the existing state of regulatory and legislative support in Ukraine doesn't make it possible to fully regulate the issue of ensuring business cyber security, and the cyber law system, in our opinion, needs codification.

Undoubtedly, the spectrum of business cyber security threats is extremely large. It differs in instrumental use, specifics of implementation, degree of complexity, conditions of initialization and remoteness of implementation, parameters of the automation process, manifestations and direction. Currently, business entities are most often affected by such cyber threats as: (1) DDoS and DoS attacks aimed at external vulnerabilities of enterprise systems; (2) phishing emails containing malicious files and links; (3) focus on the human factor, which leads to the tendency of employees to leak information or deliberately ignore the rules for handling sensitive data.

It is obvious that serious problems of ensuring business cyber security exist not only in Ukraine and other countries of the transitive type, but also in highly developed countries. Therefore, the need for a joint fight at the international level with the manifestations of malicious acts in cyberspace becomes important.

DISCUSSION

Formation of a set of measures to effectively counteract cyber risks and cyber threats, as well as ensure the smooth functioning of the business cyber security system requires the development of preventive measures, the list of which must include:

- formation of a system of indicators and determination of their parameters for detecting and implementing monitoring and assessment of cyber risks and cyber threats (analysis of network infrastructure; introduction of a system of access, storage and transfer of information resources in a protected "cloud"; creation of backup copies of confidential information);
- creation and implementation of a response plan to cyber-attacks (planning of the procedure for the timely recovery of business processes, data and IT systems in the event of a cyber-attack, prompt response to cyber-attacks, rapid elimination of the consequences of cyber-attacks);
- ensuring a high level of security of cooperation (checks of partners and suppliers regarding cyber security, strict control over access of partners and suppliers to company resources);
- control over specialists' cyber awareness performing the functions of ensuring business cyber security (constant retraining and advancing their qualifications);
- implementation of constant monitoring of the state and changes in tendencies in the world regarding cyber security (regular diagnosis of cyber security threats and vulnerabilities, improvement of the process of ensuring the confidentiality and integrity of information resources).

At the same time, the consolidation of the international community's efforts and the effective exchange of positive experience in ensuring cyber security on a global scale are becoming extremely significant. After all, cybercrime has acquired a transnational character and spreads at an extremely fast pace. At the same time, it makes no sense to be limited only to current measures, but it is necessary to form strategic priorities for ensuring business cyber security. In particular, the cyber law system in Ukraine is too weak and needs codification. Only comprehensive implementation of the proposed measures on a global scale will allow achieving the desired results.

CONCLUSION

Thus, the conducted studies of the theoretical and applied principles of ensuring business cyber security in conditions of the domestic economy's instability provide grounds for the conclusion that the current state of business cyber security is characterized by an excessive influence of cyber risks and cyber threats, which reduces the effectiveness of business structures and leads to the loss of confidential information. Based on the

conducted research, it was possible to establish that the effectiveness of ensuring business cyber security is higher in highly developed countries (USA, GCSI: 0,919–1,000; Great Britain, GCSI: 0,783–0,995; Germany, GCSI: 0,679–0,974). Along with this, developing countries (Moldova, GCSI: 0,418–0,758; Belarus, GCSI: 0,506–0,592; Ukraine, GCSI: 0,501–0,688) are unable to fully withstand the challenges and dangers of cyberspace, as a result of which business structures are very often the objects of malicious unauthorized encroachments. Growing tendencies in the total annual number of cyber-attacks using ransomware, carried out in global cyberspace and aimed at business entities, were identified, the volumes of which in the period of 2017–2022 increased from 183,6 million in 2017 to 623,3 million in 2021. The need to strengthen business cyber security and increase financing measures to ensure it has been proven, which is quite successfully implemented at the international level; however, in Ukraine, additional attention is required. After all, the detected cyber threats are extremely significant and have a destructive effect on business activities. The basic measures to strengthen business cyber security have been proposed. They are as follows: the formation of a system of indicators and the determination of their parameters for detecting and implementing monitoring and assessment of cyber risks and cyber threats; creation and implementation of a cyber-attack response plan; ensuring a high level of cooperation security; monitoring the cyber awareness of specialists performing the functions of ensuring business cyber security and carrying out constant monitoring of the state and changes in tendencies in the world regarding cyber security. At the same time, the need for codification of cyber law in Ukraine has been established.

REFERENCES

Annual number of ransomware attacks worldwide from 2016 to first half 2022. Statista. Available at: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

Bullock, J.A., Haddow, G.D. and Coppola, D.P. 2021. Cyber security and critical infrastructure protection. *Introduction to Homeland Security (Sixth Edition)*, pp. 425–497. Available at: https://doi.org/10.1016/B978-0-12-817137-0.00008-0

Cochran, C. 2022. Economic uncertainty is increasing cyber security risks. *Help Net Security*. Available at: https://www.helpnetsecurity.com/2022/10/17/economic-uncertainty-increasing-cybersecurity-risks/

Global Cyber Security Index 2017. ITU. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Global Cyber Security Index 2018. ITU. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Global Cyber Security Index 2020. ITU. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Global Cyber Security Index 2021. ITU. Available at: https://www.itu.int/en/publications/ITU-D/pages/publications.aspx?parent=D-STR-GCI.01-2021&media=electronic

Guembe, B., Azeta, A., Masra, S., Osamor, V.C., Fernandes-Sanz, L. and Pospelova, V. 2022. The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, **36**(1). Available at: https://doi.org/10.1080/08839514.2022.2037254

Holovatyi, M. 2014. Multiculturalism as a means of nations and countries interethnic unity achieving. *Economic Annals-**XXI***(11-12): 15-18.

Holovatyi, M. 2015. The state and society: The conceptual foundations and social interaction in the context of formation and functioning of states. *Economic Annals,* **XXI**(9-10): 4-8.

Ishchenko, A., Stuchynska, N., Haiova, L. and Shchepanskiy, E. 2021. Chemical safety in the context of environmental goals of sustainable development. International Conference on Environmental Sustainability in Natural Resources Management, 15–16 October, 2021, Odesa, Ukraine, Volume 915. DOI 10.1088/1755-1315/915/1/012032

Jabbari, K. 2018. The Application of International Law in Cyberspace: State of Play. *Office for Disarmament Affairs United Nation*. Available at: https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

Kostiukevych, R., Mishchuk, H., Zhidebekkyzy, A., Nakonieczny, J. and Akimov, O. 2020. The impact of european integration processes on the investment potential and institutional maturity of rural communities. *Economics and Sociology*, **13**(3): 46-63.

Kuzmenko, O., Makliuk, O. and Chernyshova, O. 2022. Business Cyber Security in Time of War. *Economy and Society*, **44**: 1–6. Available at: DOI: https://doi.org/10.32782/2524-0072/2022-44-21

Li, Yu. and Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging Trends and recent developments. *Energy Reports*, **7**: 8176–8186.

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul–Haq, J. and Abbas, S. 2022. Cyber Security threats: A never-ending challenge for E-commerce. *Frontiers in Psychology*, **13**: 1–15. Available at: https://doi.org/10.3389/fpsyg.2022.927398

Mishra, A., Alzoubi, Ye.I., Gill, A.Q. and Anwar, M.J. 2022. Cyber security Enterprises Policies: A Comparative Study. *Sensors*, **22**(2): 538. Available at: https://doi.org/10.3390/s22020538

On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cyber security Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 № 447/2021. Available at: https://zakon.rada.gov.ua/laws/show/447/2021?find=1&text= %D0%BA%D1%96%D0%B1%D0%B5%D1%80% D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0#w1_1

Richardson, M.A. 2022. Top Cyber security Threats in 2022 that Business Are Worried About. Spiceworks. Available at: https://www.spiceworks.com/it-security/security-general/articles/top-cyber-threats-to-watch-out-for/

Spending on cyber security worldwide from 2017 to 2021 (COVID-19) adjusted. Statista. Available at: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/

Tam, T., Rao, A. and Hall, J. 2021. The good, the bad and the missing: A Narrative review of cyber security implications for Australian Small Business. *Computers & Security*, **109**. Available at: https://doi.org/10.1016/j.cose.2021.102385

Thomson, J.R. 2015. Cyber Security, Cyber-attack and Cyber-espionage. *High Integrity Systems and Safety Management in Hazardous Industries*, pp. 45–53. Available at: https://doi.org/10.1016/B978-0-12-801996-2.00003-9

Vasupula, N.R., Munnangi, V. and Daggubati, S. 2021. Modern Privacy Risks and Protection Strategies in Data Analytics. Soft Computing and Signal Processing. *Advances in Intelligent Systems and Computing*, 1340. Springer, Singapore. Available at: https://doi.org/10.1007/978-981-16-1249-7_9

Wirth, A. 2017. The Economics of cyber security. *Biomedical Instrumentation & Technology*, **51**: 52–59. Available at: https://doi.org/10.2345/0899-8205-51.s6.5

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. 2020. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62 (1), 82–97. Available at: https://doi.org/10.1080/08874417.2020.1712269