DOI: 10.55643/fcaptp.6.47.2022.3936

Viacheslav Blikhar
D.Sc. in Philosophy, Professor, Director of the Institute of Management, Psychology and Security, Lviv State University of Internal Affairs, Lviv, Ukraine;
e-mail: blikharv@ukr.net
ORCID: 0000-0001-7545-9009
(Corresponding author)

Mikhailo Tsymbaliuk
D.Sc of Law, Professor, People's Deputy of Ukraine, Verkhovna Rada of Ukraine, Kyiv, Ukraine;
ORCID: 0000-0003-3965-3175

Halyna Hreshchuk
D.Sc. in Economics, Associate Professor, Head of the Department of Law, Lviv National Environmental University, Lviv, Ukraine;
ORCID: 0000-0001-5629-8828

Ruslana Dostdar
PhD in Law, Associate Professor of the Department of Maritime and Commercial Law, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine;
ORCID: 0000-0001-8614-7561

Tetiana Kokhaniuk
PhD in Law, Head of the Department of Organization of Educational and Scientific Training, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0002-1303-4272

Iryna Krykavska
Candidate of Juridical Sciences, Senior lecturer at the Department of Administrative and Information Law, Educational-Scientific Institute of Law, Psyhology and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine;
ORCID: 0000-0002-6108-2447

Received: 05/12/2022
Accepted: 19/12/2022
Published: 30/12/2022

CURRENT STATE AND DEVELOPMENT TRENDS OF INTERNATIONAL LAW IN THE CONTEXT OF ECONOMIC AND LEGAL ANALYSIS OF FINANCIAL MEASURES TO COMBAT CYBERCRIME IN THE GLOBAL ENVIRONMENT

ABSTRACT

The purpose of the article is to study the theoretical foundations and applied recommendations for the development of international law in the context of economic and legal analysis of financial measures to combat cybercrime in the global environment. Based on the results of the research, it was found that the development of international law is under the influence of significant destabilizing factors of a legal, political, economic and social nature and has a significant impact on the financial and economic system of the country because a specific share of cybercrimes is related to the commission of offences in the financial and economic system. The low level of effectiveness of international law in regulating legal relations financial and economic nature in cyberspace was revealed. The intensification of economic crime has been proven in the virtual environment has been proven. As a result of research carried out by the countries of the European Union and Ukraine regarding the identification of trends in the international legal regulation of the system of financial measures against cyber risks and modern cyber threats, as well as the formation of methods and measures for combating economic cybercrime, it was established that among the countries selected for analysis, three groups are distinguished, characterized by common signs: highly developed countries (Austria, Belgium, Denmark, Ireland, Luxembourg, the Netherlands, Germany, Portugal, Finland, Sweden), where the high indicators of ensuring the protection of cyberspace against criminal encroachments of a financial and economic nature are positioned, however, there are certain problems that need to be solved; developing countries (Slovenia, Estonia, Spain, Latvia, Lithuania, Malta, Poland, France, Slovakia, the Czech Republic), where high indicators of cyberspace protection are positioned, however, there are certain problems that need to be solved; developing countries (Bulgaria, Greece, Italy, Cyprus, Romania, Hungary, Croatia, Ukraine), in which there are significant problems of ensuring cyber security and economic and legal regulation of systemic counteraction to cyber risks and cyber threats, arising in the financial and economic sphere. Ways to strengthen the influence of international law on the system of financial countermeasures against cybercrime are proposed, namely: improvement of international law norms on increasing the level of cyber security of the financial and economic sphere of the state based on the innovative development of information technologies and the convergence of artificial intelligence technologies; strengthening of international legal regulation of economic aspects of activity and protection of producers of information and communication technologies; strengthening the protection of information flows containing information on the implementation of financial and economic transactions in cyberspace.

Keywords: financial and economic legal relations, legal norms, international law, legal obligations, economic crime in cyberspace, cyber security, cyber risks, cyber threats, globalization

JEL Classification: K33

INTRODUCTION

The strengthening of the processes of globalization, mega-regionalization and geopoliticization led to the emergence of new challenges, threats and dangers of a socio-economic, legal and socio-political nature, as a result of which national borders merged and a single global system of world economic relations was formed. It is obvious that the progressive development of the system of international relations has created prerequisites for the intensification of the development of the virtual environment, which is involved in the implementation of the bulk of financial and economic transactions and in the processes of interaction between the subjects of such relations at the international level, as a result of which there is a rapid improvement of cyberspace and its direct participation in globalization processes international financial and economic system. However, along with the positive qualities of digitalization of society at all levels of development, cyber-space has become an object of criminal encroachments and is increasingly used by criminals to commit illegal acts, which requires effective prevention and countermeasures. One of the ways to effectively solve existing problems is international law, which is able to regulate existing problematic aspects of the protection of cyberspace from risks and threats of a financial and economic nature. Undoubtedly, modern transformations deepen the inequality of the position of the countries of the world and cause lobbying of the interests of highly developed countries and violation of the interests of developing countries. As a result, in the modern global space, the problems of legal regulation of the interests of all participants in world relations and the need to protect their national interests in the financial and economic sphere under conditions of equality, democracy and mutual respect are becoming more acute. Under such conditions, the expediency of researching the state and development trends of international law as the main tool for regulating relations financial and economic nature at the global level, taking into account the intensification of the development of cyberspace and digital tools, as well as counteracting the spread of economic crime in the virtual environment, is actualized.

LITERATURE REVIEW

The issues of international law research in the context of economic and legal analysis of financial measures of counteracting cybercrime in the global environment have become actualized under the influence of deepening globalization processes and the emergence of new factors of society's existence. The intensive development of digital technologies has accelerated this process, as a result of which cyberspace has turned into a platform for the implementation of the bulk of financial and economic operations on a global scale and is often used for illegal actions. The emergence of cyber risks and cyber threats, as well as the emergence of interstate conflicts, go beyond national borders and require an effective system of legal regulation because domestic capabilities do not allow to fully counteract destabilizing and negative factors. In view of the above, the problems of researching the harmonization of national legislation with the norms of international law, that regulate legal relations in the financial and economic sphere, become particularly acute and urgent.

It becomes obvious that the development of international law under the influence of the processes of globalization and internationalization takes place with the participation of a number of intergovernmental and international organizations and transnational corporations, which are actively involved in the production of norms of international law that acts as a regulator of international relations, including in cyberspace, the intensification of the development of which, according to G. Valori [1], is caused by the emergence of new cyber opportunities. At the same time, the scientist claims that the growing trends in economic cybercrime determine the deepening of research in the direction of identifying problematic aspects of the regulation of legal relations in cyberspace, which cannot be carried out only within one country. Therefore, the author places the main emphasis on the necessity and urgency of normalizing financial and economic legal relations in cyberspace with the help of international law, because it has been established that destructive changes in cyberspace threaten not only the functioning financial and economic system of the country, but also business structures and, especially in the conditions of the spread of the COVID-19 pandemic, the population of the country due to the need to protect personal and commercial data and the need to create new software that can withstand the challenges and dangers of modern times. As a result, such needs require adequate international protection of innovative developments, which can be achieved thanks to highly developed international law.

Moreover, L. Vigul [2] established that the functioning of cyberspace requires a clear demarcation and observance of the main principles of sovereignty and the prohibition of interference of one country in the affairs of other countries, and the regulation of legal relations in this direction requires strict external regulation and compliance with legal norms, international treaties and other regulatory and legislative acts.

In-depth studies in the sphere of the influence of international law on the functioning of cyberspace were conducted by T. Moulin [3, p. 423], who established a sufficiently high level of the inconsistency of the norms of international law with the global mechanism for regulating legal relations in cyberspace, related to financial and economic transactions. At the same

time, the scientist emphasizes the need to resolve problematic aspects of cyber threats and suggests a clear demarcation of territoriality and militarization of cyberspace, which, according to P. Bargiacchi [4], can be achieved precisely by applying international legal norms and regulating the rules of cyber behaviour of participants in legal relations. In this context, the need for the formation of a general legal basis for the application of the norms of international law for the regulation of financial and economic legal relations in cyberspace is actualized. In view of such trends, C. Eggett [5] suggests implementing a systematic consistency of elements of international law with the norms of national legal systems, which regulate relations in the financial and economic sphere, which will allow for the formation of a single effective mechanism for counteracting financial and economic risks and threats in cyberspace.

It is obvious that in modern conditions, the development of international law is influenced by significant destabilizing factors, and the intensification of financial and economic operations in the virtual environment further deepens the need to increase its effectiveness, which is confirmed by scientific research of M. Adams and M. Reiss [6], who proved the unsettled issues of safe exploitation of social media in the grey zone and the principles of ensuring effective counteraction to information warfare using virtual technologies and revealed a sufficiently low level of legal regulation of the problems of prevention of cyberattacks, from which the financial and economic sphere of the state constantly suffers.

A similar position is held by J. Kulesza and R. Weber [7], who, studying the problems of legal regulation of cyberspace at the international level, came to the conclusion of the need to improve international law in order to strengthen legal control over financial and economic operations in the virtual environment.

Instead, M. Ülgül, Yu. Çinar, M. Öztarsu and others [8] are convinced that the problem of regulating financial and economic legal relations in cyberspace with the help of international law is currently being actively considered by the scientific community, and the main developments are aimed at ensuring a significant level of the ability of international law to timely detect and prevent risks and threats that intensify in cyberspace. T. Maurer [9] proved the variability of the development of international law and the significant influence on it of individual states that initiate the creation of certain legal norms in order to protect their own national interests.

It becomes obvious that this behaviour of individual subjects is unacceptable at the level of international economic relations, therefore, in order to protect their own interests, dissatisfied countries resort to actions that contradict the established norms and rules. M. Schmitt [10] believes that cyberspace in the conditions of globalization, mega-regionalization and geopoliticization turns into an object of criminal encroachments, where some countries try to harm others, as a result of which the development of cybercrime is intensified, which acquires a threatening scale and spreads at a rapid pace, which requires the immediate adoption of appropriate decisions regarding containment and minimization of negative manifestations of criminal acts.

M. Schmitt's opinion is shared by S. Alshdaifar who, apart from stated above, emphasizes the importance of international organizations and regional associations in the process of forming the norms of international law which regulate the financial and economic legal relations in the sphere of cyber security. J. Odermatt [12] proves the importance of the position of the countries of the European Union, which have integrated their own national legal systems into the European one, which has a significant impact on the functioning parameters of the global legal system.

Investigating trends in the spread of cybercrime, in the financial and economic sphere V. Havlovskyi [13, p. 108] associates this destructive phenomenon with intentional illegal acts carried out using computer technologies in cyberspace with financial resources. At the same time, significant difficulties are observed in the study of cybercrime in the legal dimension, since, as noted by O. Tataryn and V. Havlovskyi [14, p. 195], in most countries the current national legislation does not clearly define the categorical apparatus in this direction, and the debatable issues regarding the classification of cybercrime and its statistics are still the subject of active discussion both at the national and international levels.

It is obvious that the system of international law in the unstable conditions of globalization and intensification of the spread of cybercrime to the financial and economic sphere needs to be improved in the direction of taking into account the impact of global cyberspace challenges and normalizing financial and economic legal relations that regulate the identification of problematic aspects of the unification and harmonization of international law norms with European and national legislation of the countries of the world.

AIMS AND OBJECTIVES

The purpose of the article is an analytical assessment of the state and trends in the development of international law in the context of economic and legal analysis of financial measures to combat cybercrime in a global environment. Achieving the set goal involves solving the tasks of identifying the problems of the influence of international law on the regulation of

DOI: 10.55643/fcaptp.6.47.2022.3936

financial and economic legal relations in cyberspace; analysis of the dynamics of the Global Cyber Security Index, the State Instability Index and cybercrime indicators in Ukraine; determination of strategic priorities for the development of international law in the context of globalization in the context of its impact on the system of financial measures to combat cybercrime.

METHODS

The methodological base of the research consists of the main methods of economic analysis and fundamental research. Determination of the essence of international law, cybercrime in the financial and economic sphere and cyberspace was carried out using the methods of analysis, synthesis, scientific abstraction, observation and system analysis; analytical assessments of cyber security, state instability, and cybercrime indicators were carried out using comparison methods, statistical analysis, and multivariate cluster analysis based on the k-means method (using the Statistica software package, 7.0); identification of the problems of the influence of international law on the system of financial measures to combat cybercrime was carried out by applying a functional and systemic approach; the formation of the results of the conducted research and conclusions was carried out with the help of methods of generalization and systematization.

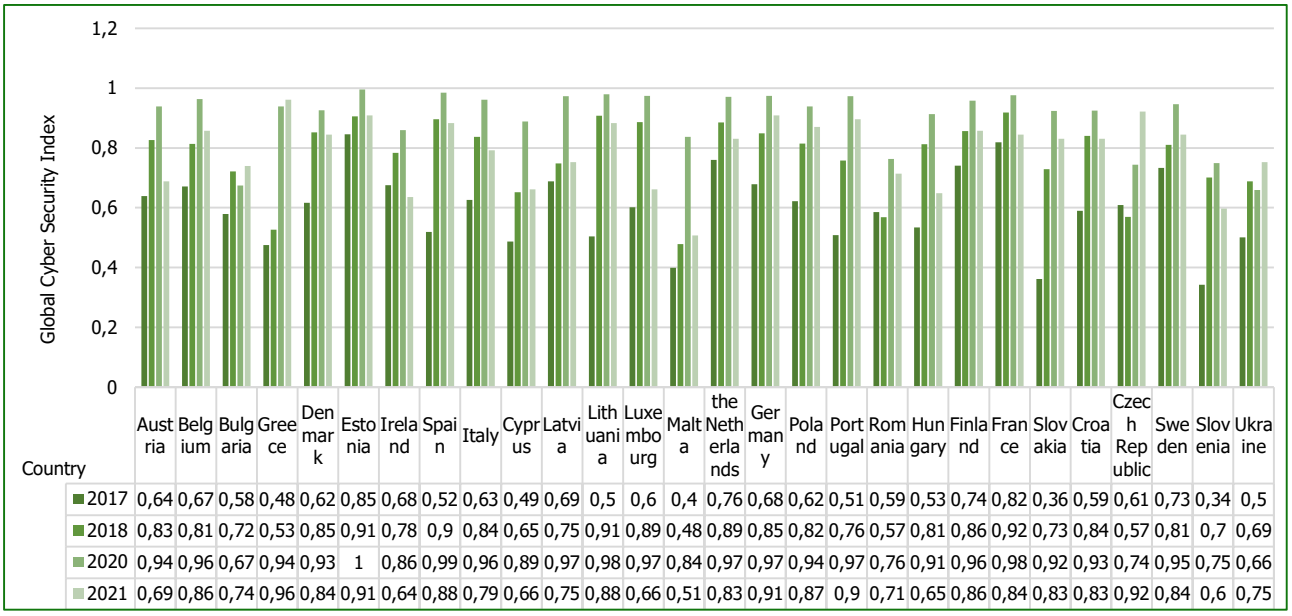
RESULTS

The strengthening of socio-economic, legal and socio-political instability and uncertainty on the European continent is due to the emergence of the latest risks and threats to the existence of the world community. The processes of globalization, geopoliticization and European integration intensified significant changes in national legal systems and led to the formation of a single global legal system with the aim of ensuring the strengthening of democracy, and the preservation of the territorial integrity and inviolability of each country. However, the events that shook the world community in 2022 as a result of the full-scale military invasion of the russian federation on the territory of Ukraine reformatted all existing international relations and required the search for effective methods of solving problems.

Obviously, the established procedures for the functioning of international law in the context of the regulation of financial measures to combat cybercrime need to be revised and improved, which is caused by the need to quickly normalize negative phenomena and processes and ensure stability, security and peace on the European continent. The existing system of international law, which is positioned by the single organizational and legal principles of functioning, in a certain way determines the principles of relations in the globalized world, however, as practice shows, it is unable to guarantee security, peace and the inviolability of the territorial integrity of countries. Undoubtedly, the existing system of international law is also not able to ensure the defined priorities in relation to the regulation of financial and economic international relations in cyberspace.

This is evidenced by the parameters of empirical studies of the main indicators of cyber security in the section of the countries of the European Union for the period of 2017–2021 (Figure 1), which prove a higher level of legal protection and security of cyberspace in those countries that belong to the highly developed ones, and countries of the transitive type, to which Ukraine belongs, show significantly lower values of the Global Cyber Security Index.

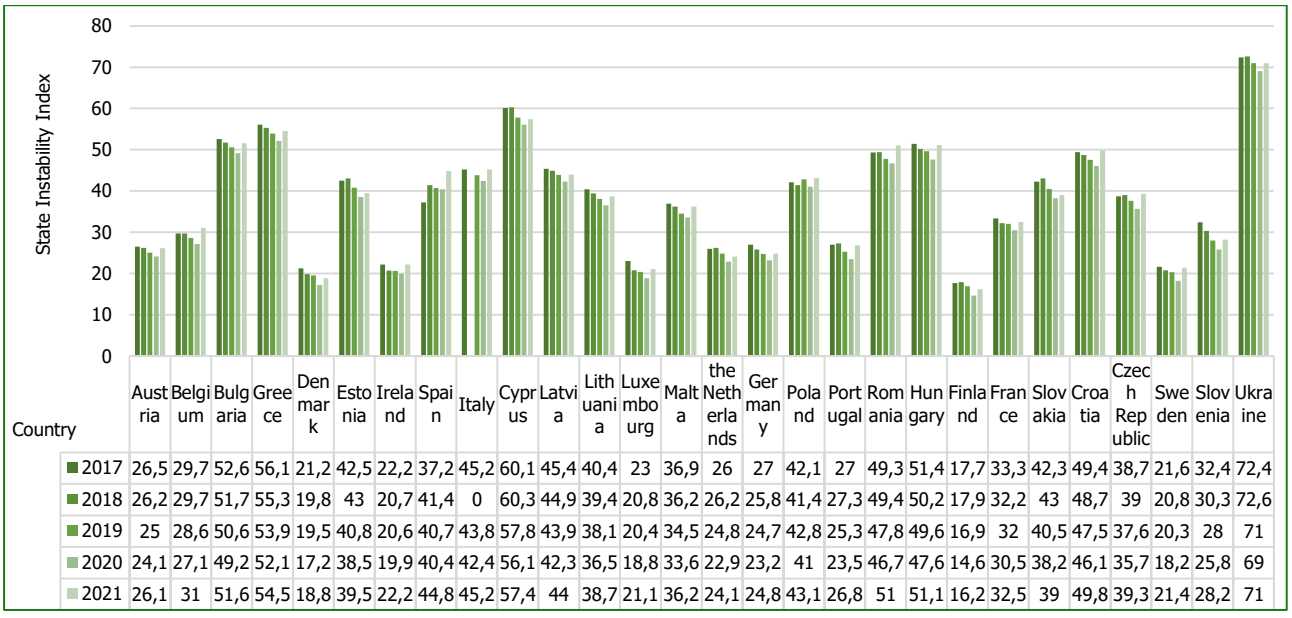
At the same time, it is worth noting the average value of the Global Cyber Security Index, which was observed in Ukraine throughout the analyzed period (0.50–0.75). It is obvious that domestic legislation regulating organizational and legal relations financial and economic nature in the field of cybercrime is not perfect and effective, as its norms often do not correspond to the provisions of international law and are not able to protect the country's national interests in cyberspace. We note that similar trends are observed in relation to countries that are at the stage of transformational restructuring and have not completed the processes of structural changes in the legal system.



Country	Austria	Belgium	Bulgaria	Greece	Denmark	Estonia	Ireland	Spain	Italy	Cyprus	Latvia	Lithuania	Luxembourg	Malta	the Netherlands	Germany	Poland	Portugal	Romania	Hungary	Finland	France	Slovakia	Croatia	Czech Republic	Sweden	Slovenia	Ukraine
2017	0,64	0,67	0,58	0,48	0,62	0,85	0,68	0,52	0,63	0,49	0,69	0,5	0,6	0,4	0,76	0,68	0,62	0,51	0,59	0,53	0,74	0,82	0,36	0,59	0,61	0,73	0,34	0,5
2018	0,83	0,81	0,72	0,53	0,85	0,91	0,78	0,9	0,84	0,65	0,75	0,91	0,89	0,48	0,89	0,85	0,82	0,76	0,57	0,81	0,86	0,92	0,73	0,84	0,57	0,81	0,7	0,69
2020	0,94	0,96	0,67	0,94	0,93	1	0,86	0,99	0,96	0,89	0,97	0,98	0,97	0,84	0,97	0,97	0,94	0,97	0,76	0,91	0,96	0,98	0,92	0,93	0,74	0,95	0,75	0,66
2021	0,69	0,86	0,74	0,96	0,84	0,91	0,64	0,88	0,79	0,66	0,75	0,88	0,66	0,51	0,83	0,91	0,87	0,9	0,71	0,65	0,86	0,84	0,83	0,83	0,92	0,84	0,6	0,75

Figure 1. Dynamics of the Global Cyber Security Index in the countries of the European Union and in Ukraine in 2017–2021. *(Source: calculated on the basis of: [15–18])*

The State Instability Index (SII) is a sufficiently significant indicator that reflects the state of the country in the legal, financial, economic, political and social spheres and vulnerability to the influence of external and internal destabilizing factors. According to the results of the studies of the dynamics of the index of state instability in the countries of the European Union and in Ukraine in 2017–2021 (Fig. 2), the trends are observed, according to which Ukraine was recognized as the most unstable among the countries of the analyzed group (SII: 69–73), Cyprus (SII: 56–60), Greece (SII: 52–56) and Bulgaria (SII: 49–53), the legal systems of which are partially harmonized with the norms of international law and require significant improvement in terms of regulation of financial and economic legal relations. On the other hand, the highest level of state stability was recorded in Finland (SII: 15–18), Denmark (SII: 17–21), Ireland (SII: 20–22), Luxembourg (SII: 19–23) and Sweden (SII: 18 –22), where the introduction of high standards of development of legal systems and observance of legal norms is observed.



Country	Austria	Belgium	Bulgaria	Greece	Denmark	Estonia	Ireland	Spain	Italy	Cyprus	Latvia	Lithuania	Luxembourg	Malta	the Netherlands	Germany	Poland	Portugal	Romania	Hungary	Finland	France	Slovakia	Croatia	Czech Republic	Sweden	Slovenia	Ukraine
2017	26,5	29,7	52,6	56,1	21,2	42,5	22,2	37,2	45,2	60,1	45,4	40,4	23	36,9	26	27	42,1	27	49,3	51,4	17,7	33,3	42,3	49,4	38,7	21,6	32,4	72,4
2018	26,2	29,7	51,7	55,3	19,8	43	20,7	41,4	0	60,3	44,9	39,4	20,8	36,2	26,2	25,8	41,4	27,3	49,4	50,2	17,9	32,2	43	48,7	39	20,8	30,3	72,6
2019	25	28,6	50,6	53,9	19,5	40,8	20,6	40,7	43,8	57,8	43,9	38,1	20,4	34,5	24,8	24,7	42,8	25,3	47,8	49,6	16,9	32	40,5	47,5	37,6	20,3	28	71
2020	24,1	27,1	49,2	52,1	17,2	38,5	19,9	40,4	42,4	56,1	42,3	36,5	18,8	33,6	22,9	23,2	41	23,5	46,7	47,6	14,6	30,5	38,2	46,1	35,7	18,2	25,8	69
2021	26,1	31	51,6	54,5	18,8	39,5	22,2	44,8	45,2	57,4	44	38,7	21,1	36,2	24,1	24,8	43,1	26,8	51	51,1	16,2	32,5	39	49,8	39,3	21,4	28,2	71

Figure 2. Dynamics of the State Instability Index in the countries of the European Union and in Ukraine in 2017–2021. *(Source:* calculated on the basis of: [19–23])

Deepening the research of the countries of the European Union and Ukraine according to the indicators of the Global Cyber Security Index and the State Instability Index in 2017–2021 should be carried out by grouping them based on multivariate

DOI: 10.55643/fcaptp.6.47.2022.3936

cluster analysis (k-means method, Statistica software package, 7.0) in order to identify common development trends and problems of ensuring the harmonization of national legal systems with the norms of international law, and systematize the obtained results in Table. 1.

Table 1. Grouping of the countries of the European Union and Ukraine according to the indicators of the Global Cyber Security Index and the State Instability Index in 2017-2021. *(Source: calculated on the basis of: [15–18; 19–23])*

Global Cyber Security Index			State Instability Index		
№	**Country**	**Cluster number**	**№**	**Country**	**Cluster number**
1.	Austria	1	1.	Austria	1
2.	Belgium		2.	Belgium	
3.	Denmark		3.	Denmark	
4.	Ireland		4.	Estonia	
5.	Luxembourg		5.	Ireland	
6.	the Netherlands		6.	Spain	
7.	Germany		7.	Italy	
8.	Portugal		8.	Latvia	
9.	Finland		9.	Lithuania	
10.	Sweden		10.	Luxembourg	
11.	Slovenia		11.	the Netherlands	
12.	Estonia	2	12.	Germany	
13.	Spain		13.	Poland	
14.	Latvia		14.	Portugal	
15.	Lithuania		15.	Finland	
16.	Malta		16.	France	
17.	Poland		17.	Croatia	
18.	France		18.	Sweden	
19.	Slovakia		19.	Cyprus	2
20.	Czech Republic		20.	Malta	
21.	Bulgaria	3	21.	Hungary	
22.	Greece		22.	Slovakia	
23.	Italy		23.	Slovenia	
24.	Cyprus		24.	Bulgaria	3
25.	Romania		25.	Greece	
26.	Hungary		26.	Romania	
27.	Croatia		27.	Czech Republic	
28.	Ukraine		28.	Ukraine	

From the results of the research, it can be concluded that according to both indicators, the countries of the European Union are divided into three groups: highly developed, countries with an average level of development, and countries of the transitive type, which are developing.

According to the Global Cyber Security Index, the first group includes countries such as Austria, Belgium, Denmark, Ireland, Luxembourg, the Netherlands, Germany, Portugal, Finland, Sweden and Slovenia, which managed to build an effective national system of financial measures for combating cybercrime and achieved sufficiently high levels of security in cyber-space.

The second group consists of Estonia, Spain, Latvia, Lithuania, Malta, Poland, France, Slovakia and the Czech Republic, where a sufficiently effective economic and legal mechanism for combating cyber risks and cyber threats has been formed, the national legislation is harmonized with international, however, there are certain inaccuracies and inconsistencies of national legislation with the norms of international law regarding the formation of a complex of financial measures to combat cybercrime, that require due attention.

The third group includes Bulgaria, Greece, Italy, Cyprus, Romania, Hungary, Croatia, and Ukraine, which are considered countries of the transitive type, and the national legal systems require substantial revision and harmonization with international law.

As for the results of clustering according to the State Instability Index, there are three groups of countries characterized by common features of ensuring the stability of the state's functioning.

The first group includes Austria, Belgium, Denmark, Estonia, Ireland, Spain, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Germany, Poland, Portugal, Finland, France, Croatia and Sweden, where low indicators of state instability index were recorded, which testify the appropriate level of counteraction to existing challenges and dangers of economic and legal nature, and the legal system is capable of ensuring the functioning of high-quality mechanisms for effective counteraction to risks and threats, arising in the financial and economic sphere. The second group consists of Cyprus, Malta, Hungary, Slovakia and Slovenia, which demonstrate not too high development indicators, however, the level of state stability is assessed as mediocre. The third group includes Bulgaria, Greece, Romania, the Czech Republic and Ukraine, which have significant problems in ensuring the stability of the functioning of state economic and legal mechanisms, and national legal systems need significant improvement in terms of forming financial measures to counter cybercrime.

A clear example of the existence of problematic issues of state regulation of legal relations economic and legal relations in cyberspace is the growing trend of cybercrime in Ukraine, which testifies to the low indicators of the application of international law in the system of counteraction to financial and economic cyber risks and cyber threats. According to the data reported by the National Police of Ukraine [24–27], the total number of detected cybercrimes during 2017–2021 has a tendency to increase (Figure 3). Moreover, a particularly sharp increase in the number of cybercrimes was recorded in 2021 (by 91.22% compared to 2020), due to quarantine restrictions connected with the spread of the COVID-19 pandemic and the transition to financial and economic operations in cyberspace using modern digital tools.

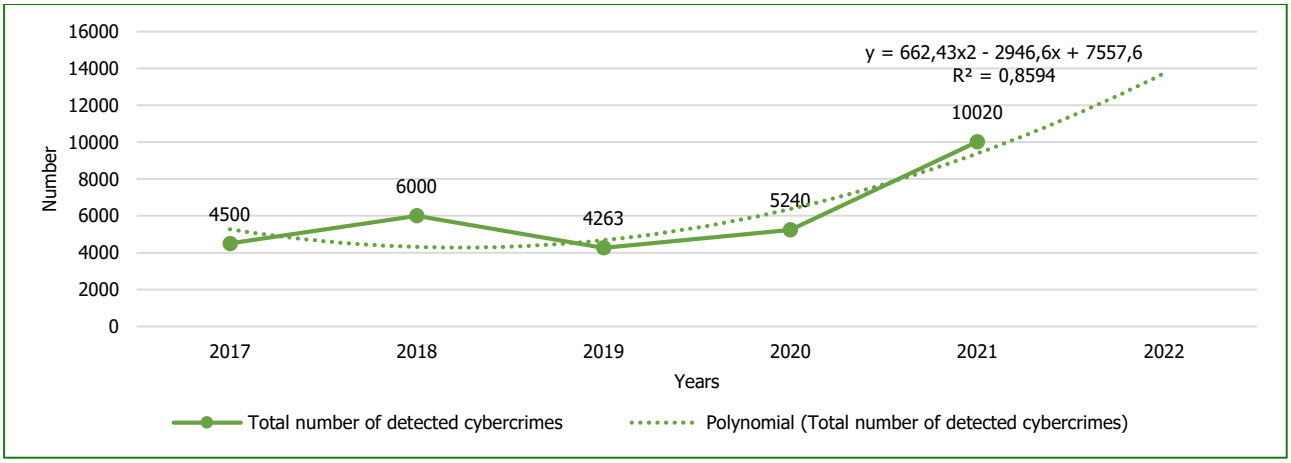


Figure 3. Dynamics of cybercrime indicators in Ukraine in 2017–2022 (2022 – forecast estimates). *(Source: calculated on the basis of: [24–27])*

At the same time, forecast estimates of the number of cybercrimes for 2022 testify to the deepening of negative trends, and a possible increase in the number of illegal acts financial and economic nature in cyberspace is predicted at the level of 13,900 crimes.

Moreover, if we conduct an analytical study of the main trends in the number of detected cybercrimes in the financial and banking sector of Ukraine, in the field of computer systems and the facts of online fraud, it is possible to identify significant growth trends in each of the types of cybercrimes. It is worth noting that the indicators of the number of cybercrimes committed in the banking sector have reached critically high values, from 1,330 crimes in 2017 to 3,049 crimes in 2021. In addition, the number of online frauds is growing at a particularly high rate, as a result of which the volume of losses of financial resources is increasing both economic entities and natural persons, the exact size of which cannot be estimated in modern conditions due to the lack of tools for recording such actions with official statistics.

It is obvious that the existing system of international law is not capable of effectively resisting the financial and economic risks and threats arising in cyberspace, therefore there is a need to create effective mechanisms for counteracting cybercrime based on the improvement of international law. The main ways of strengthening the influence of international law

DOI: 10.55643/fcaptp.6.47.2022.3936

on the system financial measures of counteracting cybercrime can be as follows: (1) improvement of the norms of international law in terms of the formation of an economic and legal mechanism for increasing the level of cyber security, taking into account the pace of innovative development of information technologies and the convergence of artificial intelligence technologies; (2) strengthening international regulation of activities and protection of producers of information and communication technologies; (3) strengthening the legal protection of information flows regarding financial and economic transactions in cyberspace and the mechanism for regulating the digitalization of cybercrime investigations.

The results of the conducted studies confirm the problematic functioning of the international law system in the unstable conditions of modern times and prove the need for its improvement in terms of regulating financial and economic legal relations in cyberspace.

DISCUSSION

The study of the theoretical and applied foundations of the development of international law in the context of the economic and legal analysis of financial measures to combat cybercrime in the global environment allow to form the main problems, among which the most significant are as follows: a low level of cyber security and economic and legal regulation of systemic counteraction to cyber risks and cyber threats; lack of formation of a single global system of international law in terms of normalizing financial measures to counter cyberattacks; inconsistency of national systems of financial measures to combat cybercrime with the norms of international law, their multiformat and versatility; lack of a clear unified economic and legal definition of the categorical apparatus for regulating financial and economic legal relations in cyberspace; the lack of formation of the economic and legal mechanism for the implementation of financial measures to combat cybercrime at the international level and the limitation of international legal regulation of problematic aspects of the creation and functioning of specialized units to combat cybercrime in various countries of the world.

Conducted research using analytical data made it possible to reveal the level of effectiveness of regulation of financial and economic legal relations in cyberspace by international law and to establish that highly developed countries position higher standards of security of financial transactions carried out in a virtual environment while developing countries are unable to ensure the implementation of basic measures counteracting cyber risks and cyber threats, as a result of which the processes of the spread of cybercrime on their territory are intensifying, which is confirmed by empirical estimates of the level of growth of cybercrime in the financial and economic sphere on the example of Ukraine.

The outlined trends indicate the existence of significant problems in the development of international law in the context of the study of financial measures to combat cybercrime in the global environment, which need to be solved.

CONCLUSIONS

Thus, as a result of the conducted studies of the theoretical and applied foundations of the development of international law in the context of economic and legal analysis of financial measures to combat cybercrime in the global environment, it can be stated that the existing system of international law is not able to effectively resist modern challenges, dangers, risks and threats of a financial and economic nature, which occur in cyberspace. It was established that the essence of international law is a set of generally recognized national and international legal norms that ensure effective interstate interaction, as well as regulation of relations in various spheres of social, political, and economic life. The actualization of the development and growing trends in the functioning of cyberspace, which, in addition to its positive effect, poses a significant threat to the spread of economic crime using the virtual environment has been proven. Empirical studies have revealed the peculiarities of the application of international law by European countries in the formation of national mechanisms for combating economic crime in cyberspace, on the basis of which it has been found that highly developed countries are able to provide a higher level of protection against cyber risks and cyber threats in the financial and economic sphere than countries that are developing It has been established that the financial and banking sector of the country is most significantly affected by the commission of cybercrimes on a global and national scale, and in the conditions of the spread of the COVID-19 pandemic and the introduction of restrictive quarantine measures, economic crime in the direction of committing online fraud has intensified. The need to improve international law in terms of regulating legal relations regarding the formation of financial measures to combat cybercrime has been proven, which is the perspective of our further research.

REFERENCES

1. Valori, G.E. (2022). Cyberspece and intelligence: Threats to intelligence business and personal data will increase in 2022. *Modern Diplomacy*. URL: https://moderndiplomacy.eu/2022/03/01/cyberspace-and-intelligence-threats-to-intelligence-business-and-personal-data-will-increase-in-2022/.
2. Vihul, L. (2018). The Application of International Law in Cyberspace: State of Play. *United Nation. Office for Disarmament Affairs*. URL: https://www.un.org/disarmament/ar/update/the-application-of-international-law-in-cyberspace-state-of-play/.
3. Moulin, T. (2020). Reviving the Principle of Non–Intervention in Cyberspace: The Path Forward. *Journal of Conflict and Security Law*. Vol. 25. Issue 3. P. 423–447. https://doi.org/10.1093/jcsl/kraa011.
4. Bargiacchi, P. (2020). Cyberspace and International Law. *International Workshop at Dokuz Eylul University*. P. 1–12. URL: https://www.academia.edu/44350226/CYBERSPACE_AND_INTERNATIONAL_LAW.
5. Eggett, C. (2019). The Rolle of Principles and General Principles in the Constitutional Processes of International Law. *Netherlands International Law Review*. Vol. 66. P. 197–217. https://doi.org/10.1007/s40802-019-00139-1.
6. Adams, M.J., & Reiss, M. (2018). International Law and Cyberspace: Evolving Views. *Cybersecurity and Deterrence*. URL: https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views.
7. Kulesza, J., & Weber, R. H. (2021). Protecting the Internet with International Law. *Computer Law & Security Review*. Vol. 40. https://doi.org/10.1016/j.clsr.2021.105531.
8. Ülgül, M., Çinar, Yu., Öztarsu, M.F., Vilić, V., Varpahovskis, E., & Erendor, M.E. (2020). Contemporary Issues in International Relations. *Cambridge Scholars Publishing*. URL: https://www.researchgate.net/publication/340249638.
9. Maurer, T. (2016). "Proxies" and Cyberspace. *Journal of Conflict and Security Law*. Vol. 21. Iss. 3. P. 383–403. https://doi.org/10.1093/jcsl/krw015.
10. Schmitt, M. N. (2020). Taming the Lawless Void: Tracking the evolution of International Law Rules for Cyberspace. *Texas National Security Review*. Vol. 3. Iss. 3. P. 32–47.
11. Alshdaifar, S. A. (2017). A visible Theme in the History of International Law: International or Global. *International Journal of Public Law and Policy*. Vol. 6. Iss. 1. P. 54–77. URL: https://ssrn.com/abstract=3037856.
12. Odermatt, J. (2021). International Law and the European Union. *Cambridge University Press*. https://doi.org/10.1017/9781108895705.
13. Havlovskyi, V. D. (2019). Analiz stanu kiberzlochynnosti v Ukraini [Analysis of the state of cybercrime in Ukraine]. Information and law.
14. Tataryn, O. V., & Havlovskyi, V. D. (2021). Orhanizovana kiberzlochynnist v Ukraini: problemy formuvannia ofitsiinoi statystky ta yii analizu [Organized cybercrime in Ukraine: problems of forming official statistics and their analysis]. Information and law. https://doi.org/10.37750/2616-6798.2021.4(39).249306.
15. Global Cybersecurity Index (GCI) 2017. URL: https://www.cybersecobservatory.com/wp-content/uploads/2017/07/D-STR-GCI.01-2017-R1-PDF-E.pdf.
16. Global Cybersecurity Index (GCI) 2018. URL: https://www.itu.int/en/publications/ITU-D/pages/publications.aspx?parent=D-STR-GCI.01-2018&media=electronic.
17. Global Cybersecurity Index (GCI) 2020. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
18. Global Cybersecurity Index (GCI) 2021. URL: https://www.itu.int/en/publications/ITU-D/pages/publications.aspx?parent=D-STR-GCI.01-2021&media=electronic.
19. Fragile States Index Annual Report 2017. URL: https://fragilestatesindex.org/2017/05/14/fragile-states-index-2017-annual-report/.
20. Fragile States Index Annual Report 2018. URL: https://fragilestatesindex.org/2018/04/24/fragile-states-index-2018-annual-report/.
21. Fragile States Index Annual Report 2019. URL: https://fragilestatesindex.org/2019/04/07/fragile-states-index-2019-annual-report/.
22. Fragile States Index Annual Report 2020. URL: https://fragilestatesindex.org/2020/05/08/fragile-states-index-2020-annual-report/.

DOI: 10.55643/fcaptp.6.47.2022.3936

23. Fragile States Index Annual Report 2021. URL: https://fragilestatesindex.org/2021/05/20/fragile-states-index-2021-annual-report/.

24. Zvit Natsionalnoi politsii Ukrainy pro rezultaty roboty u 2018 rotsi [Report of the National Police of Ukraine on the results of work in 2018]. URL: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf (in Ukrainian).

25. Zvit Natsionalnoi politsii Ukrainy pro rezultaty roboty u 2019 rotsi [Report of the National Police of Ukraine on the results of work in 2019]. URL: https://www2.npu.gov.ua/assets/userfiles/files/zvity/zvit_NPU_2019.pdf (in Ukrainian).

26. Zvit Natsionalnoi politsii Ukrainy pro rezultaty roboty u 2020 rotsi [Report of the National Police of Ukraine on the results of work in 2020]. URL: https://www.kmu.gov.ua/news/zvit-nacionalnoyi-policiyi-ukrayini-pro-rezultati-roboti-u-2020-roci (in Ukrainian).

27. Zvit Natsionalnoi politsii Ukrainy pro rezultaty roboty u 2017 rotsi [Report of the National Police of Ukraine on the results of work in 2017]. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/Zvit_NPU_2021_.pdf (in Ukrainian).

Бліхар В., Цимбалюк М., Грещук Г., Достдар Р., Коханюк Т., Крикавська І.

СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ МІЖНАРОДНОГО ПРАВА В КОНТЕКСТІ ЕКОНОМІКО-ПРАВОВОГО АНАЛІЗУ ФІНАНСОВИХ ЗАХОДІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В ГЛОБАЛЬНОМУ СЕРЕДОВИЩІ

Метою статті є дослідження теоретичних засад та прикладних рекомендацій щодо розвитку міжнародного права в контексті економіко-правового аналізу фінансових заходів протидії кіберзлочинності в глобальному середовищі. На підставі результатів проведеного дослідження виявлено, що розвиток міжнародного права відбувається під впливом значних дестабілізуючих чинників правового, політичного, економічного та суспільного характеру й має значний уплив на фінансово-економічну систему країни, адже питома частка кіберзлочинів пов'язана зі вчиненням правопорушень у фінансово-економічній системі. Виявлено низький рівень ефективності міжнародного права при регулюванні правовідносин фінансово-економічного характеру в кіберпросторі. Доведено активізацію економічної злочинності у віртуальному середовищі. У результаті проведених досліджень країн Європейського Союзу та України щодо виявлення тенденцій міжнародного правового регулювання системи фінансових заходів протидії кіберризикам і кіберзагрозам сучасності, а також формування методів і заходів ведення боротьби з економічною кіберзлочинністю встановлено, що серед обраних для аналізу країн виділяється три групи, які характеризуються спільними ознаками: високорозвинуті країни (Австрія, Бельгія, Данія, Ірландія, Люксембург, Нідерланди, Німеччина, Португалія, Фінляндія, Швеція), які забезпечують високі стандарти міжнародного правового регулювання досліджуваної сфери; країни з посереднім рівнем розвитку (Словенія, Естонія, Іспанія, Латвія, Литва, Мальта, Польща, Франція, Словаччина, Чехія), де позиціонуються високі показники забезпечення захисту кіберпростору від злочинних посягань фінансово-економічного характеру, проте існують певні проблеми, що потребують вирішення; країни, що розвиваються (Болгарія, Греція, Італія, Кіпр, Румунія, Угорщина, Хорватія, Україна), у яких є істотні проблеми забезпечення кібербезпеки та економіко-правового регулювання системної протидії кіберризикам і кіберзагрозам, що виникають у фінансово-економічній сфері. Запропоновано шляхи посилення впливу міжнародного права на систему фінансових заходів протидії кіберзлочинності, а саме: удосконалення норм міжнародного права щодо підвищення рівня кібербезпеки фінансово-економічної сфери держави на основі інноваційного розвитку інформаційних технологій та конвергенції технологій штучного інтелекту; посилення міжнародного правового регулювання економічних аспектів діяльності та захисту виробників інформаційно-комунікаційних технологій; посилення захисту інформаційних потоків, що містять відомості про здійснення фінансово-економічних операцій, у кіберпросторі.

Ключові слова: фінансово-економічні правовідносини, норми права, міжнародне право, правові зобов'язання, економічна злочинність у кіберпросторі, кібербезпека, кіберризики, кіберзагрози, глобалізація

JEL Класифікація: K33