УДК 338:351
DOI: 10.60022/1(1)-1SD

Buriak A.
PhD (Economics), Associate Professor, Associate Professor of the International Economic Relations and Tourism Department
National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine
Буряк А. А.
к.е.н., доцент, доцент кафедри міжнародних економічних відносин та туризму
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна,
ORCID: 0000-0002-0814-7459

Levchenko I.
PhD (Economics), Associate Professor, Associate Professor of the International Economic Relations and Tourism Department,
National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine
Левченко І. В.
доктор філософії, доцент кафедри міжнародних економічних відносин та туризму
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна,
ORCID: 0000-0001-7068-8320

THE ROLE OF INTERNATIONAL ORGANIZATIONS IN THE FORMATION OF A SECURITY-ORIENTED INFORMATION ENVIRONMENT AND THE IMPLEMENTATION OF STRATEGIES FOR ENSURING THE ECONOMIC AND ECOLOGICAL SECURITY OF UKRAINE

Abstract. *The role of international organizations in the formation of a security-oriented information environment and the implementation of strategies for ensuring the economic and ecological security of Ukraine are investigated in the article. A change in the vector of security threats has been determined, which requires a rethinking of traditional strategies for ensuring Ukraine's information, economic and ecological security and the development of new approaches to ensuring stability and protection.*

It has been proven that the development of information technologies and the spread of digital space have increased the need to coordinate the efforts of the international community in the security sphere. The growth of potential threats associated with the use of dual-purpose information technologies is substantiated, which stimulates the need for a coordinated international approach to their control and regulation. It was determined that such international organizations as the UN, NATO, OSCE play a key role in the formation of information security, develop strategies and mechanisms for responding to threats, improve information protection methods, and contribute to the regulation and development of standards in cyberspace.

The need for the development of international standards of information, economic and ecological security and the use of modern technologies in order to ensure stability and security in the international space has been revealed. The main measures within the framework of the program of extended partnership with NATO, with the help of which Ukraine will have the opportunity to ensure operational planning in the early stages of conflicts, to expand the dialogue in the field of intelligence information exchange, including on the prevention of cyber-attacks, as well as to participate in cyber defense exercises, are substantiated. provided for program participants, receive positions in the International Military Headquarters of NATO and other command structures of the alliance to gain management experience in the field of information, economic and environmental security.

The main prospects for further scientific research in this direction are the study of the problem of ensuring informational, economic and ecological security at various levels – regional, national, international, sub regional and transatlantic, which concerns the aspirations of individual world actors to control political and economic processes in large territories with the help of special information operations.

Key words: *security-oriented information environment, economic security of Ukraine, ecological security of society, international organizations, ecological threats, ecocide.*

РОЛЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У ФОРМУВАННІ БЕЗПЕКООРІЄНТОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ТА РЕАЛІЗАЦІЇ СТРАТЕГІЙ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ Й ЕКОЛОГІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *У статті досліджено роль міжнародних організацій у формуванні безпекоорієнтованого інформаційного середовища та реалізації стратегій забезпечення економічної й екологічної безпеки України. Визначено зміну вектору безпекових загроз, що вимагає переосмислення традиційних стратегій забезпечення інформаційної, економічної й екологічної безпеки України та розробки нових підходів до забезпечення*

стабільності та захисту.

Доведено, що розвиток інформаційних технологій і поширення цифрового простору підвищили необхідність координації зусиль міжнародної спільноти у безпековій сфері. Обґрунтовано зростання потенційних загроз, пов'язаних із використанням інформаційних технологій подвійного призначення, що стимулює необхідність узгодженого міжнародного підходу до їх контролю та регулювання. Визначено, що такі міжнародні організації, як ООН, НАТО, ОБСЄ відіграють ключову роль у формуванні інформаційної безпеки, розробляють стратегії та механізми реагування на загрози, вдосконалюють методи захисту інформації, сприяють регулюванню та розвитку стандартів у кіберпросторі.

Виявлено необхідність розвитку міжнародних стандартів інформаційної, економічної та екологічної безпеки та застосування сучасних технологій з метою забезпечення стабільності та безпеки у міжнародному просторі. Обґрунтовано основні заходи в рамках програми розширеного партнерства із НАТО, за допомогою яких Україна матиме можливість забезпечувати оперативне планування на ранніх стадіях конфліктів, розширити діалог у сфері обміну розвідувальною інформацією, у тому числі й щодо попередження кібератак, а також брати участь у навчаннях з кібероборони, передбачених для учасників програми, отримувати посади у Міжнародному військовому штабі НАТО та інших командних структурах альянсу для набуття досвіду управління у сфері інформаційної, економічної та екологічної безпеки.

Основними перспективами подальших наукових досліджень у даному напрямку є дослідження проблеми забезпечення інформаційної, економічної та екологічної безпеки на різних рівнях – регіональному, національному, міжнародному, субрегіональному та трансатлантичному, що стосується прагнень окремих світових акторів контролювати політичні та економічні процеси на значних територіях за допомогою спеціальних інформаційних операцій.

Ключові слова: *безпекоорієнтоване інформаційне середовище, економічна безпека України, екологічна безпека суспільства, міжнародні організації, екозагрози, екоцид.*

Formulation of the problem. In today's world, international organizations are revising their policies and approaches to ensuring international informational, economic and ecological security. The change in the vector of security threats, in particular information threats, requires a rethinking of traditional strategies and the development of new approaches to ensuring stability and protection.

In particular, today, international organizations are actively cooperating to combat information risks. They jointly develop strategies and policies as information security becomes a key aspect of international relations. The development of information technologies and the spread of digital space have increased the need to coordinate the efforts of the international community in this area.

The growth of potential threats associated with the use of dual-purpose information technologies stimulates the need for a coordinated international approach to their control and regulation. Countries and international organizations are focusing on developing joint strategies that will help prevent the negative consequences of using such technologies for military purposes and other threats.

Analysis of recent research and publications. The development of research in the field of informational, economic and ecological security and their concepts is associated with a critical rethinking of traditional approaches to understanding these concepts. Thus, many domestic and foreign experts and researchers paid attention to the problems of information, economic and ecological security, such as J. Andrusek, J. Burton, K. Booth, B. Danylyshyn [1], L. Jones, M. Kahler, F. Knight, V. Onyshchenko, S. Onyshchenko [2 – 3], Yu. Holik [4]; they developed concepts of power in security relations, theories of new-generation information wars, and analyzed the practice of using information weapons in conflicts. These researchers actively studied the characteristics of information security, developed a definition of this concept, and also conducted an analysis of trends in international cooperation in the field of information security at the level of international organizations and in the leading states of the world. These scientists also focused attention on the institutional foundations of informational, economic and ecological security, considered international mechanisms for countering information challenges for the international security system, and studied methods of protection against such threats. Their research and analysis became an important addition to the general understanding of informational, economic and ecological security in the context of international relations and global security.

However, in our opinion, in the conditions of modern challenges and threats, it is urgent to expand the role of international organizations in the formation of a security-oriented information environment and the implementation of strategies for ensuring the economic and ecological security of Ukraine, which determined the choice of the research, its purpose and tasks.

The purpose of the article is to study the role of international organizations in the formation of a security-oriented information environment and the implementation of strategies for ensuring the economic and ecological security of Ukraine.

The main material of the study. International cooperation in the field of information security requires not only reactive measures, but also active planning, cooperation and development of strategies that would consider the rapid

development of technologies and the variability of threats.

Thus, modern digitalization of the economy and the development of innovative technologies significantly change the paradigm of international relations and require governmental and non-governmental international organizations to adapt to new conditions. This modernization includes responding to challenges related to the digital transformation of the economy and public administration, as well as to changes in international security, including hybrid conflicts using information technology and psychological influence.

International relations and security organizations are actively working to adapt to these new realities. They develop strategies and mechanisms for responding to threats, improve information protection methods, and contribute to the regulation and development of standards in cyberspace.

The growing number of hybrid conflicts in which information technology plays a significant role also forces these organizations to work on improving the methods of detecting, analyzing and responding to such threats. Therefore, modern international governmental and non-governmental organizations are actively developing their strategy to effectively counter new challenges in the field of information security [5].

Indeed, modern challenges in the field of information security require integrated approaches and joint efforts from the international community. International organizations, such as the UN, NATO, OSCE and others, play a key role in shaping information security and cooperation in this area.

At the level of international security organizations, decisions are made aimed at ensuring security and stability in the face of ever-increasing information threats. These decisions are based on the principles of international law and common goals of all participants. They define strategies, joint initiatives and response mechanisms to modern threats and challenges related to information security.

By broadly representing and considering the positions and interests of various international actors, these organizations work to create mechanisms aimed at joint action to ensure information security on a global scale. This approach contributes to solving problems in the field of information security and contributes to maintaining peace and stability in the international community.

It is worth noting that the experts identified important issues and trends in the field of international information security through discussions at the sessions of the UN General Assembly. The resolutions «The role of science and technology in the context of international security and disarmament» and «Achievements in the field of informatization and telecommunications in the context of international security» created a basis for the discussion of important aspects that determine the modern policy of information security. These resolutions contained provisions on the dual use of information and communication technologies in the civil and military spheres, the use of scientific and technical achievements in the modernization of modern weapons, as well as the importance of countering destructive influences. This shows awareness of the need to develop international information security standards and use modern technologies to ensure stability and security. Such documents [6] reflect the recognition of the importance of joint efforts of states, the private sector, scientific institutions and civil society to achieve the goal of increasing the effectiveness of international cooperation in the field of information security. The UN, through the discussion of such issues, summarizes common approaches and strategies that can serve as a basis for further action in this area.

The discussion of the draft Convention on International Information Security at the session of the UN General Assembly reflected different views of the states on the definition of concepts, assessment of potential information threats and organizational support of international cooperation in this area.

A Group of Governmental Experts was created to reach a consensus on the wording of the Convention. Her task was to conduct a competent analysis of information security problems, develop international principles for regulating communication networks, in particular, considering the fact that innovative technologies can be used for attacks on the basic systems of states and communities.

However, the competition between the approaches of different countries to the basic principles of the convention caused its disapproval and postponement of the discussion to the future. Different views on how international information security should be regulated complicated the process of agreeing on the text of the convention.

The resolution «Encouraging responsible behavior of states in cyberspace in the context of international security», adopted at the session of the UN General Assembly with the support of the majority of member states, reflects the need to create a safe, stable and peaceful information and communication environment in cyberspace. This resolution determines that the establishment of trusting relations between states in cyberspace is an important condition for ensuring international security. It also emphasizes the need to expand the capabilities of states to cooperate and use high technologies to reduce the risk of conflicts in the cyber sphere.

This resolution also states that while the responsibility for ensuring security in cyberspace rests with states, the participation of the private sector, academic institutions and civil society can contribute to more effective international cooperation.

In the context of this resolution, a new format of the Group of Governmental Experts was created at the UN level, considering the geographical representation of states. This group can make a significant contribution to strengthening international information security through the development of recommendations and the establishment of mechanisms to encourage responsible behavior of states in cyberspace.

Thus, NATO has identified cyberspace as a key environment for information warfare and gives high priority to information security. The organization has created NATO Centers of Excellence in its member countries, which are multinational institutes for developing information security strategies and promoting interstate cooperation in this area.

The NATO Information Security Center, founded in Estonia, was created at the initiative of the Estonian authorities and the first sponsor countries. It is not part of NATO's military command or structure. Instead, its staff and funding are provided by sponsoring nations and member states of the organization. This Center is important for the exchange of experience in information protection, the development and implementation of strategies to counter information threats, as well as cooperation with other organizations such as the European Defense Agency and the Cyber Security Research Center in Germany.

Thus, the Center's experts, together with the Red Cross and the US Cyber Command, presented the documents «Guidelines of international law that can be applied during cyber warfare» and «Tallinn Guidelines 2.0». These documents are the basic principles for conducting information warfare and correspond to the provisions of modern international law regulating operations in the information space.

The documents stipulate that countries carrying out information attacks are responsible for their actions against other countries. They call for a ban on the use of force in the information space, as information attacks can lead to the destruction of infrastructure, digital data and life support systems of states and affect the civilian population, which can be considered war crimes.

This classification of information warfare as «armed conflicts» recognizes the use of countermeasures in response to cyberattacks as legitimate. However, it should be emphasized that the expert report is the independent opinion of the authors and, unlike official NATO documents, has a recommendatory nature [7].

The analysis of NATO's information security policy shows the initiative of Estonia as a NATO member state in cooperation with the countries participating in the Eastern Partnership Program, in particular with Ukraine and Georgia, in the field of information security. Joint measures that have been implemented have included training of personnel, technical advice and the supply of equipment to combat information threats.

In the conditions of the full-scale invasion of the Russian Federation in Ukraine, as well as during the conflict in the East of Ukraine and the illegal occupation of Crimea, the Minister of Defense of Estonia called on NATO partners to provide financial assistance to Ukraine in the context of aggressive cyber-attacks of the Russian Federation against Ukraine. Estonia also transferred 100,000 euros to the NATO trust fund to support Ukraine's information security and organized training for Ukrainian cyber security specialists.

It is important to note that Ukraine can become an important partner in cooperation with the Center due to its experience in countering Russian cyber threats and negative informational influence, which poses a threat not only to democratic processes in the European region, but also at the international level.

Ukraine's joining the NATO Enhanced Capability Partnership initiative is an important step aimed at expanding cooperation with NATO in the field of information security. This can be useful when solving crisis situations and carrying out peacekeeping missions.

As part of the expanded partnership program, Ukraine will have the opportunity to provide operational planning in the early stages of conflicts, expand dialogue in the field of intelligence exchange, including the prevention of cyber-attacks. Also, Ukraine will be able to participate in cyber defense exercises provided for program participants, as well as receive positions in the International Military Headquarters of NATO and other command structures of the alliance to gain management experience in the field of information security [8].

Ukraine's cooperation with NATO within the Comprehensive Assistance Package is an important step for improving the standards of military-political organization in the country. This aid package includes support through trust funds and the implementation of the Annual National Program, which is a tool for implementing reforms.

As part of this practical cooperation, the Decree on the approval of the Annual National Program under the auspices of the Ukraine-NATO Commission for 2022 was adopted. In addition, the Action Plan for the implementation of the Concept of Improving Public Information on the Euro-Atlantic Integration of Ukraine was adopted. These initiatives include the work of joint Ukraine-NATO working groups on military reform, defense-technical cooperation and information security, as well as cooperation on science and the environment [9].

The OSCE is an important forum for discussing contemporary security issues in Europe, North America and the independent states that emerged after the collapse of the USSR. Initially, this organization was created to support security, human rights, democracy and media development in areas of armed conflict, as well as to monitor the development of crisis situations.

With the emergence of hybrid conflicts, where special information operations and destructive information and psychological influences have become an integral part, the modernization of the OSCE policy has become urgent. The organization is considering proposals for correcting its priorities in the field of international information security, including the definition of concepts in this field, the creation of effective threat prevention mechanisms, compliance with international law in the field of information threats, the system for identifying the sources of such threats, as well as the coordination of international efforts to protect the Internet networks and increasing trust in the global information infrastructure.

The OSCE emphasizes the importance of information threats in today's world. She called on all interested parties to find solutions in the field of information security and achieve general and effective regulation of cyberspace based on international law [10].

The conference «A Common Approach to Cyber Security: Defining the Future Role of the OSCE» was an important step in defining the OSCE's strategy for information security. This conference discussed the problems of illegal use of cyberspace, as well as analyzed the relevant countermeasures of international and regional organizations, in particular, their impact on security in the OSCE region. The main topics of the conference included the potential of the OSCE in developing a comprehensive approach to information security, the exchange of experience between the countries of the region, the creation of norms and rules to regulate the behavior of states in cyberspace, as well as decision-making to strengthen information security in the region.

As a result of the conference, innovative recommendations on measures to strengthen trust in the field of information security were adopted. These recommendations provided for OSCE interaction with the private sector and providers of key infrastructure, joint approaches to information security management, aimed at increasing transparency and ensuring information security in the OSCE.

The OSCE's efforts in conducting interactive discussions proved to be key to addressing issues related to multilateral cyber diplomacy, the development of regional information security as a driving force for global progress, the impact of artificial intelligence on the security of information and communication technologies, and the protection of critical infrastructure. The conference focused on the fact that information and communication technologies have become a determining factor of economic and social progress in the modern world, opening up new opportunities in international relations. However, threats in cyberspace have led to a potential escalation of tensions between states due to misuse of networks, cyberattacks and breaches of privacy.

OSCE members emphasized the need to develop trust between participating states to reduce the risks of conflicts associated with the use of information and communication technologies [11]. The proactive approach of the organization could include research projects, analytical expert assessments and specialized programs aimed at specifying the issues of information security policy on the OSCE platform.

Conclusions. Summarizing the analysis of the activities of international organizations in the field of information security, it is important to note that their capabilities consist in the ability to promote a multilateral dialogue between international participants, consider the diverse positions of various subjects of global governance, and act as universal international platforms for coordinating views on solving current security issues.

The main problem is ensuring information security at various levels –sub regional, transatlantic, international, national and regional. This concerns the aspirations of individual global actors to control political processes in large territories with the help of special information operations. This management approach creates problems of information imbalance of power and can lead to violations of national information sovereignty, which is observed in Ukraine in the conditions of a full-scale invasion of the Russian Federation.

Understanding these problems and solving them requires joint efforts and cooperation at the international level, with the aim of developing norms and strategies aimed at ensuring security in the digital environment and protecting national sovereignty in this new information landscape.

Thus, the mixing of global and regional problems significantly affects the role and capabilities of international institutions in determining the direction of changes at the global level. This encourages these organizations to engage powerful mechanisms to solve problems related to global development.

At the same time, the hybrid nature of informational influences led to a change in the approaches of international organizations to policy in the field of information security. This requires the formation of new structures and strategies to effectively confront modern challenges aimed at ensuring security and stability. Such organizations must adapt to the changing information environment and develop innovative strategies aimed at protecting against new threats emerging in the digital space.

References

1. Danylyshyn B.M., Onyshchenko S.V., Maslii O.A. (2019). Socio-economic security: modern approach to ensuring the socio-economic development of the region. Ekonomika i rehion, vol. 4(75), pp. 6–13.

2. Onyshchenko, V., Onyshchenko, S., Verhal, K., Buriak, A. (2022). The Energy Efficiency of the Digital Economy. In: Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (eds) Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering, vol 299. Springer, Cham. Available at: https://doi.org/10.1007/978-3-031-17385-1_64 (accessed March 13, 2024).

3. Onyshchenko S.V., Masliy O.A., Buriak A.A. (2023). Threats and risks of ecological and economic security of Ukraine in the conditions of war. XVII International Scientific Conference «Monitoring of Geological Processes and Ecological Condition of the Environment», 7-10 November 2023, Kyiv, Ukraine. Mon23-072. Available at: https://reposit.nupp.edu.ua/bitstream/PoltNTU/13700/1/2023_11_Mon23-072.pdf (accessed March 13, 2024).

4. Holik Yu., Maksiuta N. (2020). Establishment of a network for the public atmospheric air monitoring and informing the population. Technology audit and production reserves, vol. 4/3(54), pp. 36–40. DOI: https://doi.

org/10.15587/2312-8372.2020.210376.

5. Buriak A.A., Makhovka V.M. & Storozhuk L.M. (2023). Stratehiia i mekhanizmy zaprovadzhennia tsyfrovoi ekonomiky v krainakh YeS ta Ukraini yak umova podolannia kryzovykh yavyshch. Ekonomika i rehion, vol. 2(89), pp. 53–59.

6. Buriak A.A., Kudriashova D.O., Storozhuk L.M. (2023) Stratehiia rozvytku digital-ekonomiky v Ukraini: natsionalna viziia ta vyklyky hlobalizatsii. Systema upravlinnia vidkhodamy v tsyrkuliarnii ekonomitsi: finansovi, sotsialni, ekolohichni ta enerhetychni determinanty: monohrafiia. Sumy: Sumskyi derzhavnyi universytet. (in Ukrainian).

7. Buriak A., Levchenko I., Herashchenko V., Shevchenko O. (2023). Impact of full-scale war on changes in the format of Ukraine's cooperation with the European Union. The EU Cohesion policy and healthy national development: Management and promotion in Ukraine: monograph. In: Letunovska N., Saher L. & Rosokhata A. Szczecin: Centre of Sociological Research. DOI: https://doi.org/10.14254/978-83-968258-5-8/2023.

8. Puhach O. (2015). Modeliuvannia zahroz systemi ekonomichnoi bezpeky natsionalnoi ekonomiky z pozytsii yikh svoiechasnoho vyiavlennia ta peredbachennia. Ekonomika i rehion, vol. 3(52), pp. 103–109.

9. Buriak A., Bachykalo K. (2023). The role of chambers of commerce and industry in ensuring the external economic security of the state. Ekonomika i rehion, vol. 4(91), pp. 249–254. DOI: https://doi.org/10.26906/EiR.2023.4(91).3220.

10. Masliy O.A., Buriak A.A. (2023). Transformation of threats for the economic security and security of the information environment of Ukraine in the conditions of a full-scale war. State and regions. Series: Economics and Business, vol. 3(129), pp. 28–32.

11. Levchenko I.V., Buriak A.A. (2023). Derzhavna pidtrymka rozvytku APK dlia zabezpechennia ekolohichnoi bezpeky y podolannia ekozahroz: svitovyi dosvid ta realii Ukrainy. Ahrosvi, vol. 18, pp. 96–105. DOI: https://doi.org/10.32702/2306-6792.2023.18.96.

Література

1. Danylyshyn B.M., Onyshchenko S.V., Maslii O.A. Socio-economic security: modern approach to ensuring the socio-economic development of the region. Економіка і регіон. 2019. № 4 (75). С. 6–13.

2. Onyshchenko, V., Onyshchenko, S., Verhal, K., Buriak, A. The Energy Efficiency of the Digital Economy. In: Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (eds) Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering, vol 299. Springer, Cham. URL: https://doi.org/10.1007/978-3-031-17385-1_64 (дата звернення: 13.03.2024).

3. Onyshchenko S.V., Masliy O.A., Buriak A.A. Threats and risks of ecological and economic security of Ukraine in the conditions of war. XVII International Scientific Conference «Monitoring of Geological Processes and Ecological Condition of the Environment», 7-10 November 2023, Kyiv, Ukraine. Mon23-072. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/13700/1/2023_11_Mon23-072.pdf (дата звернення: 13.03.2024).

4. Holik Yu., Maksiuta N. Establishment of a network for the public atmospheric air monitoring and informing the population. Technology audit and production reserves. 2020. № 4/3 (54). Pp. 36–40. DOI: https://doi.org/10.15587/2312-8372.2020.210376.

5. Буряк А.А., Маховка В.М., Сторожук Л.М. Стратегія і механізми запровадження цифрової економіки в країнах ЄС та Україні як умова подолання кризових явищ. Економіка і регіон. 2023. № 2(89). С. 53–59.

6. Буряк А.А., Кудряшова Д.О., Сторожук Л.М. Стратегія розвитку digital-економіки в Україні: національна візія та виклики глобалізації. Система управління відходами в циркулярній економіці: фінансові, соціальні, екологічні та енергетичні детермінанти: монографія. Суми: Сумський державний університет, 2023. С. 239–248.

7. Buriak A., Levchenko I., Herashchenko V., Shevchenko O. Impact of full-scale war on changes in the format of Ukraine's cooperation with the European Union. The EU Cohesion policy and healthy national development: Management and promotion in Ukraine: monograph. In: Letunovska N., Saher L. & Rosokhata A. Szczecin: Centre of Sociological Research, 2023. P. 369–378. DOI: https://doi.org/10.14254/978-83-968258-5-8/2023.

8. Пугач О. Моделювання загроз системі економічної безпеки національної економіки з позицій їх своєчасного виявлення та передбачення. Економіка і регіон. 2015. № 3 (52). С. 103–109.

9. Buriak A., Bachykalo K. The role of chambers of commerce and industry in ensuring the external economic security of the state. Економіка і регіон. 2023. №4 (91). С. 249–254. DOI: https://doi.org/10.26906/EiR.2023.4(91).3220.

10. Маслій О.А., Буряк А.А. Трансформація загроз економічній безпеці та безпеці інформаційного середовища України в умовах повномасштабної війни. Держава та регіони. Серія: Економіка та підприємництво. 2023. № 3 (129). С. 28–32.

11. Левченко І.В., Буряк А.А. Державна підтримка розвитку АПК для забезпечення екологічної безпеки й подолання екозагроз: світовий досвід та реалії України. Агросвіт. 2023. № 18. С. 96–105. DOI: https://doi.org/10.32702/2306-6792.2023.18.96.