UDC 339.564
DOI: https://doi.org/10.32782/2224-6282/186-2

Myronchenko Dmytro
Postgraduate Student,
National Aviation University
ORCID: https://orcid.org/0000-0002-9422-961X

Sydorenko Kateryna
PhD in Economics, Associate Professor,
Vice-Dean of the International Relations Faculty,
National Aviation University
ORCID: https://orcid.org/0000-0003-3231-2247

Мирончeнко Д.В., Сидоренко К.В.
Національний авіаційний університет

ROLE OF THE IT-SECTOR OF UKRAINE IN THE GLOBAL CYBER SECURITY SYSTEM

The purpose of the study is to develop mechanisms and tools for strengthening cybersecurity and maintaining the growth of the IT sector of Ukraine based on the study of global experience in preventing cyberthreats and post-shock recovery of economic systems, determining the contribution and potential of Ukraine in the field of ensuring global information security. The methodological basis of the work includes fundamental provisions of theories and concepts of the development of digital economy, conceptual approaches to ensuring global cybersecurity. The article establishes that Ukraine is a promising player in the world market of information technologies due to the availability of highly qualified personnel. It's emphasized that the Ukrainian IT sector remains the most profitable and is one of the few that can continue to support the national economy; however, the development of critical information infrastructure becomes a special priority for Ukraine in war conditions. Research results can be used for scientific substantiation and further creation of appropriate conditions for the development of the digital economy.

Keywords: *international business, digital economy, economic security, cyber threats, global cyber security, information infrastructure.*

JEL classification: *E24, F21, F22, F23, F52*

РОЛЬ ІТ-СЕКТОРУ УКРАЇНИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ГЛОБАЛЬНОЇ КІБЕРБЕЗПЕКИ

Метою дослідження є розроблення механізмів та інструментів зміцнення кібербезпеки та підтримання зростання ІТ-сектору України на основі вивчення світового досвіду попередження кіберзагроз та післяшокового відновлення економічних систем, визначення внеску та потенціалу України у сфері забезпечення глобальної інформаційної безпеки. Методологічна база роботи включає фундаментальні положення теорій та концепцій розвитку цифрової економіки, концептуальних підходів до забезпечення світової кібербезпеки. В статті визначено сутнісну природу кібербезпеки. Проаналізовано світовий досвід та наслідки хакерських атак на міжнародний бізнес, як от компанії Acer, Kaseya, Facebook, American Airlines тощо. Встановлено, що порушення цифрової безпеки як правило має фінансову мотивацію. Визначено роль, внесок та потенціал України у сфері кібербезпеки на глобальній арені. Зазначено, що завдяки наявності висококваліфікованого кадрового забезпечення Україна є перспективним гравцем на світовому ринку інформаційних технологій. Підкреслено, що вітчизняний ІТ-сектор залишається найприбутковішим та є одним з небагатьох, які можуть і надалі підтримувати національну економіку, однак для України в умовах війни набуває особливої пріоритетності розвиток критичної інформаційної інфраструктури. В межах проведеного дослідження запропоновано механізми та інструменти зміцнення кібербезпеки та підтримки зростання ІТ-сектору країни, зокрема акцентовано увагу, що попередження кіберзагроз та формування безпечного цифрового простору в Україні має відбуватися комплексно і системно (на рівні надання освітніх послуг та формування кадрового потенціалу країни, партнерство освітньо-наукових інституцій і міжнародного ІТ-бізнесу з метою передачі передового світового досвіду, підтримка вітчизняних стартапів в ІТ-сфері, реалізація стратегії кібербезпеки країни, проведення інформаційних кампаній та підвищення рівня обізнаності про кібербезпеку широкої громадськості тощо). Результати досліджень можуть бути використані для наукового обґрунтування та подальшого створення належних умов для розвитку цифрової економіки.

Ключові слова: *міжнародний бізнес, цифрова економіка, економічна безпека, кіберзагрози, світова кібербезпека, інформаційна інфраструктура.*

Statement of the problem. In the conditions of globalization changes in an increasingly interconnected and digitized world, the importance of cyber security reaches new heights. Cyberthreats and attacks continue to affect the global economy, changing the trajectory of socio-economic development. In this context, Ukraine is becoming a prominent provider in the global cybersecurity arena, making contributions to the fight against cyber threats and improving the security of the digital business environment. The country boasts a growing IT industry with a large number of cybersecurity experts, ethical hackers, and information security specialists. A highly qualified personnel reserve provides Ukraine with the necessary experience to identify, prevent and respond to various cyber threats. Their knowledge and capabilities contribute not only to the provision of national digital infrastructure,

but are also a valuable resource for the international community in the fight against cyber challenges.

By cooperating with neighbouring countries and international partners, Ukraine supports a common policy of countering cyber threats, effectively mitigating risks that may extend beyond state borders. Ukraine's demonstrated resilience to cyberattacks further underscores its potential as a main cybersecurity provider. Ukraine's ability to recover and respond to attacks underscores the value of its information to other countries dealing with similar threats. Learning from this experience can significantly increase global economic sustainability.

In addition to the technical contribution, it is necessary to note Ukraine's involvement in global cyberdiplomacy initiatives. Ukraine takes an active part in the formation of international norms, rules and policies regarding cybersecurity. By advocating for a safe and stable cyberspace, Ukraine can play a main role in building consensus among nations, promoting responsible behaviour in cyberspace, and deterring criminals. The Ukrainian cybersecurity services sector has the potential to increase the share of exports, cost-effective solutions and skilled specialists make it an attractive partner for countries seeking to improve their cybersecurity capabilities. By spreading its experience beyond its borders, Ukraine can contribute to the development of global cyber resilience, which will benefit the whole world in the face of new cyberthreats. Protecting critical infrastructure from cyber threats is a top priority. As more sectors of the economy rely on the digitization of operations, the protection of essential services such as energy, finance, healthcare and transport become increasingly critical.

Analysis of recent research and publications. The problem of the stability of the world economic system in the context of information security has received the attention of many domestic and foreign scientists. Thus, Garstka J., Libicki M., Nye J., Cebrovski A., Hoffman F. offer the latest theories of information wars, cyberthreat tools and institutional foundations of the international security system, explore international cooperation on information security at the level of international organizations and leading countries of the world [3; 10; 14; 22]. Professor Dorothy E. Denning made a significant contribution to the study of cybersecurity and information warfare in the context of international conflicts [4]. Scientists Bjelousova N.B., Frolova O.M., Makarenko Je.A., Ozhevan M.A., Ryzhkov M.M. highlight theoretical and applied studies of international information and cybersecurity as a component of the international system of maintaining peace and stability [16; 17; 26]. Scientist Ghoncharenko I.H. notes that the spread of cybercrime is facilitated by such factors as hyperdemand for various types of information services in the developed countries of the world, processes of globalization of the world economy, development of modern information technologies, etc. [7]. Skoroboghatova N.Je. examines the extent of the spread of cyberthreats in the global economy and proposes the implementation of a comprehensive information security policy to minimize losses from them [33]. Peculiarities of cybersecurity regulation in the system of international economic relations are studied by the following scientists: Onyshhenko S.V. and Ghlushko A.D. – analyze the dynamics of cyberattacks and the level of financial losses of the world economy from the realization of cyberthreats, prove that cyberattacks on critical infrastructure objects of Ukraine and government information resources are a threat to national interests [23]; Pipchenko N.O. – examines the practice of the EU's regional information and communication activities and the specifics of the association's positioning in Ukraine [24]; Ghrynchuk M.S. – defines the specifics of the implementation of external communications of the EU in the field of fighting cyberthreats [8]; Lykhova S.Ja. and Bilenchuk P.D. – analyze the phenomenon of space and ground cyber threats in the modern electronic world [15]. The specifics of ensuring cyber security of international business are studied by such scientists as: Zolotukhyn D. – focuses on cybersecurity policy and international relations, made a significant contribution to understanding the consequences of cyber security for the international business environment [35]; Anderson R. – studies various aspects of cybersecurity, including its implications for companies and governments [1]; Baskerville R. and Spafford E. – explore the features of risk management and ensuring cybersecurity in the context of global business operations [2; 30]; Piper F. – conducts research on cybersecurity issues faced by multinational corporations [25]; Thomas W. Shinder – studies network security and security issues of international business networks [28]. At the same time, taking into account a significant amount of thorough and meaningful scientific work, the manifestations and consequences of cyberthreats in the global economy remain insufficiently researched, tools and mechanisms for their prevention and post-shock recovery of economic systems need improvement.

The purpose of the article is the development of mechanisms and tools for strengthening cybersecurity and maintaining the growth of the IT sector of Ukraine based on the study of global experience in preventing cyberthreats and post-shock recovery of economic systems, determining the contribution and potential of Ukraine in the field of global information security.

Summary of the main results of the study. Cybersecurity is the practice of protecting digital devices, networks, and sensitive information from unauthorized access, theft, or damage. It involves the implementation of tools, processes and technologies to protect computers, networks, electronic devices, systems and data from cyber attacks [11]. Cybersecurity ensures confidentiality, integrity and availability of data throughout the entire life cycle [10]. Cybersecurity is important because it helps protect personal information like bank accounts, social media accounts, and other sensitive data from digital attacks. Helps protect businesses and organizations from cyberattacks that can cause financial loss or damage their reputation.

A digital security breach is a type of security breach that involves the theft of sensitive or protected data from a computer system or network. The economic consequences of a digital security breach can be costly for both companies and individuals. According to a report by the Foundation for the Defense of Democracies (FDD), ransomware causes economic and financial harm because it affects things that directly affect the balance sheet, such as productivity and cost-effectiveness [21]. The economic consequences of data security breaches can be costly to companies both financially and in terms of their reputation

[9]. Cybersecurity and data security are aimed at preserving the confidentiality, integrity and availability of information assets. Most cyber attacks are financially motivated. Typically, an attacker infiltrates a target system and then uses malware to extort information assets, withdraw funds, demand ransom, or commit other crimes.

An example of the importance of cyber protection can be a series of hacker attacks in the recent period on large global companies, which cost their owners dearly:

– Acer: In March 2021, electronics manufacturer Acer was hit by ransomware, leading to the largest ransom in history: $50 million;

– Kaseya: In July 2021, Kaseya was hit by a ransomware attack that affected hundreds of companies around the world [18];

– Facebook: In April 2021, Facebook was hit by a data breach that exposed the personal information of over 533 million users;

– Reddit data leak: Hackers allegedly belonging to the BlackCat ransomware gang threatened Reddit to leak 80GB of sensitive data they stole from its servers in February 2023. The gang is demanding $4.5 million and wants Reddit to abandon its controversial new pricing policy;

– American Airlines: Hackers reportedly stole the personal information of thousands of pilots applying for positions at American Airlines and Southwest Airlines [5].

For Ukraine, cyber defense is a priority due to the escalation of the Russian-Ukrainian conflict. Given the escalation of the conflict in Ukraine, businesses around the world must prepare now. Corporate security and intelligence groups have said they are seeing an increase in cyber investigations, and the US Cybersecurity and Infrastructure Security Agency and the European Central Bank have warned of possible Russian cyberattacks [13]. Ukraine was not the first «cyberwar» zone, but this is the first major conflict involving large-scale cyber operations. Cybersecurity is important because it protects all categories of data from theft and damage. This includes confidential data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and government and industry information systems.

In the period from 2020 to 2023, several cyber attacks were committed against Ukraine. In February 2022, Ukraine was under new attacks, which, according to the government, were «on a completely different level» [27]. In May 2023, an unknown group hacked surveillance and data collection systems in both Russia and Ukraine. In June 2023, Ukrainian hackers claimed responsibility for an attack on a Russian telecommunications company that provides critical infrastructure for the Russian banking system. Microsoft's threat intelligence teams have been tracking a wave of cyberattacks from the so-called Cadet Blizzard, which is linked to Russia's GRU. These attacks, which began in February 2023, targeted government agencies and IT service providers in Ukraine. Google's Threat Analysis Group said it is «highly confident» that Moscow will «increase disruptive and disruptive attacks» in 2023 if the war shifts «fundamentally» in Ukraine's favour [27].

The cyber security strategy of Ukraine for 2021–2025 is aimed at creating conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. The strategy defines three priorities: safe cyberspace, protection of citizens' rights in the digital space, and European and Euro-Atlantic integration [12]. The goals of the strategy include strengthening the capabilities of the national cyber security system, creating effective cyber defenses, and developing communication, coordination and partnership between cyber security participant at the national level. In recent years, hackers have penetrated poorly secured networks using methods as simple as guessing passwords or intercepting their use on unprotected computers. More sophisticated cyberattacks in Ukraine used social engineering techniques, including phishing emails that tricked netizens into revealing their IDs and passwords. Starting in 2020, USAID launched an ambitious $38 million cybersecurity reform program, which over the next few years will work to strengthen the legal and regulatory environment in the field of cybersecurity in Ukraine, build Ukraine's cyber workforce, and expand course offerings at leading Ukrainian universities, and as well as developing links between critical infrastructure operators and private sector solution providers. The White House declares that it will provide Ukraine with all the necessary support to recover from cyber attacks [34].

Changes are being made to the education system of Ukraine to integrate cyber security into the core curriculum. In order to overcome the growing challenges associated with cyber threats and to ensure a safe digital environment, initiatives were implemented to improve programs in educational institutions. Implementation of courses, programs related to cyber security, which should cover both theoretical and practical applications. Students have the opportunity to learn about network security, cryptography, ethical hacking, digital forensics, and more.

To bridge the gap between education and industry, partnerships with companies and cybersecurity experts have been established. IT industry leaders are interested in and actively contribute to the development of educational programs, ensuring a focus on the latest cybersecurity trends and labour market requirements. Cybersecurity competitions, hackathons and conferences are regularly organized in Ukraine to increase interest and develop skills. At such events, students get the opportunity to exchange experience, demonstrate their talents, communicate with experts, etc. This makes it possible to select valuable personnel for companies and focus their development in a relevant direction depending on global needs. Due to this, ready–made resources that can contribute to global cyber security are being integrated into the world market.

The government is taking measures to support cybersecurity education. Scholarships and grants were offered to students pursuing cybersecurity-related degrees. Certifications and specialized training programs have gained popularity, allowing for cybersecurity credentials such as: Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH). These certifications increase the employability of cybersecurity professionals and validate their experience.

Beyond academic institutions, cybersecurity awareness is being actively promoted among the general public. Awareness campaigns educate people about safe online practices and potential cyber risks, helping to create a more vigilant and secure digital community. Ukraine also participates in international cooperation and partnership in the field of cyber security. This opens up opportunities for

knowledge sharing, joint research projects and exposure to best practices from around the world.

In general, the integration of cyber security into the Ukrainian education system demonstrates the country's commitment to ensuring the security of its cyber space and the formation of a skilled workforce capable of protecting against cyber threats. As technology continues to evolve, continued efforts are needed to ensure that the education system remains relevant and proactive in addressing cybersecurity issues.

Also, Ukrainian startups play a dynamic role in the field of cyber security. As the cybersecurity industry continues to evolve, these startups bring innovation, expertise, and other perspectives to combat ever-evolving cyber threats. One of the main roles of Ukrainian startups is to stimulate innovation and technological progress. Startups often use emerging technologies such as artificial intelligence, machine learning, big data analytics, and blockchain to develop advanced cybersecurity solutions. Work is underway to develop new approaches to detect, prevent, and respond to cyberattacks, helping individuals, businesses, and organizations stay ahead of cybercriminals. Some Ukrainian cybersecurity startups specialize in incident response and data recovery services (Spin.AI, Hacken).

Another important role of Ukrainian startups, given their own experience, is the protection of critical infrastructure sectors, such as energy, health care, finance and transport. These startups aim to strengthen the protection and stability of these sectors. However, protection of organizations and critical infrastructure is not the only protection provided by Ukrainian companies. Priority is also given to data privacy and compliance with relevant regulations such as GDPR. The development of such solutions allows to strengthen trust in the digital sphere. Quite often, such startups meet the needs of small and medium-sized enterprises, pushing cost–effective and individual solutions in the field of cyber security. This helps improve the security of smaller companies that may not have the resources to invest in comprehensive cybersecurity measures.

Ukrainian cyber security startups actively participate in international cooperation and partnership, where knowledge is exchanged at global cyber security events, contributing to a wider exchange of ideas and experience.

A positive factor that should contribute to the support of initiatives for the development of the cyber security sector in Ukraine is the impact on the economy. The growing number of startups that are focused on the main global problem of data protection in cyberspace leads to the creation of new jobs and attracting more investments.

However, it should be noted that at the moment this industry in Ukraine has reduced the pace of development due to the full-scale invasion of Russia on the territory of Ukraine. Due to the invasion, there was an outflow of resources from Ukraine, as companies are afraid of losing Research and Development (RND) sectors that were concentrated in one place. In order to prevent losses of production, or reduce its volumes in view of the military invasion and energy terror on the part of the Russian Federation, companies distribute their RND network outside of Ukraine whenever possible. As a result, the money does not reach Ukraine, since taxes and wages are paid in the country where RND is established. In order to help representatives of the IT business in Ukraine who are currently abroad, the «Dija City» platform was launched in 2022. One of the advantages of «Dija City» is the opportunity to remain a resident of Ukraine and work for the economy of Ukraine while abroad [29].

Conclusions. The Ukrainian government should take several key next steps to strengthen cybersecurity and support the growth of the country's cybersecurity sector. First of all, strengthening cyberdefense capabilities. In connection with Ukraine's ongoing war with Russia, it is imperative to invest in advanced technologies and tools to effectively detect and respond to cyber threats, promote cooperation with international cyber security experts to share knowledge and apply industry best practices.

The cybersecurity strategy of Ukraine for 2021–2025 needs constant updating and revision. The government should actively engage relevant stakeholders, including industry experts and academic institutions, to ensure the strategy remains relevant and adapt to changes as needed. It is necessary to continue the integration of the basics of cyber security into the basic curriculum of educational institutions. Improving and expanding cybersecurity-related programs will equip students with both theoretical knowledge and practical skills, and collaboration with industry leaders will help align educational programs with the latest cybersecurity trends and industry requirements.

Supporting and developing cybersecurity startups is essential to drive innovation and growth in the sector. The government should provide financial assistance, grants and tax incentives to stimulate the creation and development of startups in the field of cyber security in Ukraine. Encouraging partnerships between start-ups and the critical infrastructure sector can strengthen protection and stability in vital industries.

Public awareness of cybersecurity is critical to building a vigilant and secure digital community. The government should continue to promote cyber security awareness campaigns that educate the general public about safe online practices and potential cyber risks. Finally, the government should work to create recognized cybersecurity certifications and standards. This will increase employment opportunities and confidence in cybersecurity professionals in Ukraine, ensuring compliance with international cybersecurity standards.

By taking these comprehensive next steps, the Ukrainian government can build a robust cybersecurity ecosystem, protecting critical infrastructure, fostering innovation, and increasing the nation's cybersecurity resilience to emerging cyber threats.

References:

1. Anderson R. (2020) *Security Engineering: A Guide to Building Dependable Distributed Systems.* New York: Wiley.

2. Baskerville R., Capriglione F., Nunzio C. (2023) Impacts, Challenges and Trends of Digital Transformation in the Banking Sector. *Law and Economics Yearly Review Journal*, vol. 9, part 2, pp. 341–362.

3. Cebrovski A., Garstka J. (1998) Network-Centric Warfare: Its Origin and Future. *Proceedings*, vol. 124. Available at: https://www.usni.org/magazines/proceedings/1998/january (accessed 18 July 2023).

4. Denning D. (1999) *Information Warfare and Security*. Canada: ACM Press, 522 p.

5. Drapkin A. (2023) Data Breaches That Have Happened in 2022 and 2023 So Far. *Tech.Co*. Available at: https://tech.co/news/data-breaches-updated-list (accessed 24 July 2023).

6. Frankenfield J. (2022) Cybersecurity: Meaning, Types of Cyber Attacks, Common Targets. *Investopedia*. Available at: https://www.investopedia.com/terms/c/cybersecurity.asp (accessed 3 July 2023).

7. Ghoncharenko I. (2023) Kiberzaghrozy finansovogho sektora v umovakh vijny [Cyber threats of the financial sector in the conditions of war]. *Economy and society*, no 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-82 (accessed 1 July 2023). (in Ukrainian)

8. Ghrynchuk M.S. (2021) Osoblyvosti zdijsnennja zovnishnikh komunikacij JeS u sferi borotjby z kiberzaghrozamy [Peculiarities of the implementation of EU external communications in the field of combating cyber threats]. Proceedings of the *Pryncypovyj praghmatyzm JeS – naslidky dlja Skhidnoji ta Pivdenno-Skhidnoji Jevropy: politychni, ekonomichni, pravovi ta komunikacijni aspekty (Ukraine, Kyiv, May 21–22, 2021)*, Kyiv: Taras Shevchenko national university of Kyiv, pp. 123–125. Available at: https://e-learning.iir.edu.ua/pluginfile.php/5230/mod_book/chapter/881/PROCEEDINGS_EU_PRINCIPLED_PRAGMATISM_2021.pdf#page=123 (accessed 22 July 2023). (in Ukrainian)

9. Hightower S.S. (2023) The economic impact of data security breaches in e-commerce. *Verzion*. Available at: https://www.verizon.com/business/resources/articles/s/economic-impact-of-data-security-breaches-in-ecommerce/ (accessed 10 July 2023).

10. Hoffman F. (2009) Hybrid vs Compound. *Small Wars Journal*. Available at:http://armedforcesjournal.com/hybrid-vs-compound-war/ (accessed 15 July 2023).

11. IBM (2022) *What is cybersecurity?* Available at: https://www.ibm.com/topics/cybersecurity (accessed 22 July 2023).

12. Jermak A. (2021) Pro Strateghiju kiberbezpeky Ukrajiny [About Cyber Security Strategy of Ukraine]. *Verkhovna Rada Ukrajiny.* Available at: https://zakon.rada.gov.ua/laws/show/447/2021 (accessed 29 July 2023). (in Ukrainian)

13. Kolbe P.R., Morrow M.R., Zabierek L. (2022) *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict.* Harvard: Harvard Business Review. Available at: https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict (accessed 18 July 2023).

14. Libicki M.C. (2007) *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

15. Lykhova S.Ja., Bilenchuk P.D. (2021) Kosmichni i nazemni kiberzahrozy tretoho tysiacholittia: zasoby piznannia, dokazuvannia, rozsliduvannia [Space and ground cyber threats of the third millennium: means of knowledge, proof, investigation]. *Naukovi praci Nacionaljnogho aviacijnogho universytetu*, vol. 2, № 59, pp. 9–17. DOI: 10.18372/2307-9061.59.15585. (in Ukrainian)

16. Makarenko Je.A., Ryzhkov M.M., Kuchmij O.P., Frolova O.M. (2022) *Mizhnarodna informacija: terminy i komentari* [International information: terms and comments]. Kyiv: Vadeks. (in Ukrainian)

17. Makarenko Je.A., Ryzhkov M.M., Ozhevan M.A. and others (2006) *Mizhnarodna informacijna bezpeka: suchasni vyklyky ta zaghrozy* [International information security: modern challenges and threats]. Kyiv: Centr viljnoji presy. (in Ukrainian)

18. Morrow S. (2021) 7 worst security breaches of 2021 (so far). *InfoSec*. Available at: https://resources.infosecinstitute.com/topic/7-worst-security-breaches-of-2021-so-far/ (accessed 12 July 2023).

19. Myronchenko D. (2023) Cybersecurity as a Factor of Stabilization of the Global Economy. Proceedings of the *Fundamental shifts in geo-economic systems of the world: collection of international scientific works (Ukraine, Kyiv, December 20-21, 2022)* (ed. by Dr. (Econ.), Prof. O. Borzenko), Kyiv: National Academy of Sciences of Ukraine, pp. 191–195. Available at: http://ief.org.ua/wp-content/uploads/2023/06/Fundamental-shifts_.pdf (accessed 14 July 2023).

20. Myronchenko D. (2023) Ensuring national and economic security through effective cybersecurity measures. Proceedings of the *XIV Mizhnarodna naukovo-praktychna konferencija «Nacionaljni ekonomichni strateghiji rozvytku v ghlobaljnomu seredovyshhi» (Ukraine, Kyiv, May 11, 2023),* Kyiv: National aviation university, pp. 27–30. Available at: https://drive.google.com/file/d/18gwyby-PV5UPbae1rcWR-PDiZwne8bbxe/view (accessed 18 July 2023).

21. Nolan C., Fixler A. (2019) The Economic Costs of Cyber Risk. *FDD*. Available at: https://securityintelligence.com/series/2019-cost-of-a-data-breach-report/ (accessed 28 July 2023).

22. Nye J.S. (2010) *Cyber Power*. Cambridge: Pub. by Belfer Center for Science and International Affairs.

23. Onyshhenko S.V., Ghlushko A.D. (2022) Analitychnyj vymir kiberbezpeky Ukrajiny v umovakh zrostannja vyklykiv ta zaghroz [Analytical measurement of cyber security of Ukraine in the conditions of growing challenges and threats]. *Ekonomika i region*, vol. 84, pp. 13–20. DOI: https://doi.org/10.26906/EiR.2022.1(84).2540 (accessed 18 July 2023). (in Ukrainian)

24. Pipchenko N.O. (2021) *Jevropejsjki komunikaciji* [European communications]. Kyiv: VADEKS. (in Ukrainian)

25. Piper F., Murphy S. (2002) *Cryptography: A Very Short Introduction*. Oxford: Oxford University Press.

26. Ryzhkov M.M., Bjelousova N.B. (2009) *Informacijne zabezpechennja proghnozno-analitychnoji dijaljnosti v mizhnarodnykh vidnosynakh* [Information provision of predictive and analytical activities in international relations]. Kyiv: Centr viljnoji presy. (in Ukrainian)

27. Sakellariadis J., Miller M. (2023) Ukraine gears up for new phase of cyber war with Russia. *Politico*. Available at: https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429 (accessed 26 July 2023).

28. Shinder T. (2011) *The Best Damn Firewall Book Period*. New York: Syngress.

29. Sigtax (2023) *Everything you need to know about Ukraine's special regime for IT companies.* Available at: https://sigtax.com/en/diia-city (accessed 27 July 2023).

30. Skoroboghatova N.Je. (2018) *Analiz poshyrennja kiberzaghroz u ghlobaljnij ekonomici ta minimizaciji zbytkiv vid nykh* [Analysis of the spread of cyber threats in the global economy and the minimization of losses from them]. Available at: http://sb-keip.kpi.ua/article/view/144604 (accessed 12 July 2023). (in Ukrainian)

31. Spafford G., Garfinkel S. (1997) *Web Security & Commerce*. Newton: O'Reilly & Associates.

32. Sydorenko K., Bugayko D., Gurina G., Korzh M., Zablotska R. (2023) National economic interests of Ukraine in the field of international economic relations. *Internauka,* vol. 1(69). DOI: https://doi.org/10.25313/2520-2294-2023-1-8510 (accessed 18 July 2023). (in Ukrainian)

33. Sydorenko K.V., Bughajko D.O., Ghurina Gh.S., Zablocjka R.O., Korzh M.V. (2022) Svitovyj rynok tekhnologhij u sferi aviaciji jak forma realizaciji mizhnarodnykh naukovo-tekhnologhichnykh vidnosyn [The global technology market in the field of aviation as a form of implementation of international scientific and technological relations]. *Internauka*, vol. 12. DOI: https://doi.org/10.25313/2520-2294-2022-12-8491 (accessed 18 July 2023). (in Ukrainian)

34. Tidy J. (2022) Ukraine cyber-attack: Russia to blame for hack, says Kyiv. *BBC*. Available at: https://www.bbc.com/news/world-europe-59992531 (accessed 18 July 2023).

35. Zolotukhyn D. (2018) *Ukraine Needs Systemic Management Decisions in Cybersecurity Field*. Available at: https://mkip.gov.ua/en/news/2426.html (accessed 15 July 2023).