Bulletin of Taras Shevchenko National University of Kyiv. Economics, 2022; 1(218): 39-44
УДК 336.368
JEL classification: G22
DOI: https://doi.org/10.17721/1728-2667.2022/218-1/6

N. Prykaziuk, Doctor of Economics, Prof.
ORCID ID 0000-0002-7813-8590,
L. Gumenyuk, PhD Student
ORCID ID 0000-0002-2803-913X
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

PANDEMIC COVID-19 AS A KEY FACTOR IN THE DEVELOPMENT OF DDOS-ATTACKS INSURANCE

The COVID-19 pandemic was a turning point for all participants in economic relations. The insurance market has faced new challenges related to the format of cooperation with clients changing, as well as the transformation of clients' business. Remote work has identified threats that can not only stop the industry but also destroy it. One of the examples of such threats is DDoS-attacks, targeted at stopping the computer systems of the victims of the attack. In 2021, the share of organizations that suffered losses after DDoS-attack increased to 86.2 %, 9 pp more than before the COVID-19 pandemic. IT administrators sometimes don't notice the consequences of attacks, so they can't assess the state of their business entirely. Cybersecurity experts should be involved in this monitoring, but often they only restore IT systems, without compensation. The set of services in cyber-insurance policy consists of: monitoring the client's IT systems, providing recommendations for its improvement, assistance in case of DDOS-attack, payment of compensation, and restoration of reputation. Therefore, DDoS-attacks insurance has become more popular during the COVID-19 pandemic. The volume of the cyber-insurance market grew by 39 % in 2020 and reached $7 billion vs 2018. The primary insurers in this area are media and publications, as all their activities are built on Internet-based systems.

The article examines the transformation of the cyber insurance market in the world before and after the beginning of the COVID-19 pandemic. The state and prospects of DDoS-attacks insurance are considered, and the necessity of developing of this type of insurance in Ukraine is proved. Recommendations are provided for the introduction of cyber DDoS-attacks insurance products in the portfolio of Ukrainian insurance companies in the context of the Digital Strategy of Ukraine 2030.

Keywords: insurance; cyber insurance; cyber risk; DDoS-attack; digital transformation.

Introduction. The digital transformation of developed countries has accelerated globalization processes around the world. Along with the positive effects of innovation, some problems cannot be solved in the usual ways. The issue of low levels of cyber security became particularly acute with the onset of the global COVID-19 pandemic, and most business entities were forced to switch to a remote work format and automate much of their processes.

The international community has repeatedly covered cases of discrediting and shutting down reputable services through DDoS attacks carried out by interested groups of attackers. Despite the well-known devastating effects of such cyber-attacks, there is still no single tool to block them completely. It is a widespread practice of organizations to create cyber security departments, conduct briefings and staff training, and cooperate with relevant experts, but even such a set of measures does not provide zero risk. An effective mechanism in this case is the DDoS-attacks insurance, as it combines and prior monitoring of the insured in the field of cyber security, and providing recommendations for improving its IT-systems, and support the proposed software, and compensation in case the onset of a cyber incident, and the resumption of its activities after the attack. Therefore, the development of cyber insurance in the world needs research, as specific patterns will help start this type of insurance in Ukraine.

The purpose of the article is to determine the role and impact of the COVID-19 pandemic on the development of DDoS-attacks insurance and to outline the key features of its occurrence for use in the insurance market of Ukraine.

Methodology. The article is based on the following methods of research and analysis of insurance market development in the world and Ukraine: methods of induction and deduction in analyzing the cyber insurance market in the world; observation in identifying key features of the development of DDoS-attacks insurance in the world; synthesis in establishing relationships between the pace of market development and the challenges of the environment arising from the impact of COVID-19; comparison method to create a ranking of DDoS-attacks insurance types of policies, system analysis in the process of considering the prospects for the development of DDoS-attacks insurance in Ukraine.

Literature review. Cyber security has become an especially critical after the transition of business processes to digital structure. At the current stage of economic development, companies need to use digital technical devices and ensure their integrity and safety. Theoretical cyber insurance issues are reflected in many prominent economists' works. Thus, among the scientists who study and research the process of assessment and insurance of cyber risks, we can single out S. Romanosky, L. Ablon, A. Kuehn, T. Jones [1], who investigated approaches to cyber risk assessment risks from a practical perspective in their research. N. Kshetri conducted an institutional analysis and studied the evolution of the cyber insurance market [2], as well as considered the economic nature of cyber insurance with the justification of the profitability of its various types [3]. D. Woods and R. Bohme considered the mechanisms of response to cyber incidents in the context of globalization processes, as well as options for partnership with expert organizations [4]. D. Markopoulou compared the place of cyber insurance in EU and US policy and suggested regulatory options for various possible challenges [5]. M. Liu described the theoretical and practical aspects of cyber insurance as a key element in promoting the cyber security of enterprises and states [6]. At the same time, the issue of cyber insurance in Ukraine remains insufficiently disclosed, as there is a need to identify current global trends in cyber insurance and the position of domestic insurers on the readiness to present cyber insurance products in the Ukraine insurance market.

Results. Cyber insurance market overview in 2018–2021. The global COVID-19 pandemic has become the basis for the transformation of the insurance market. Optimization of insurance companies' business processes was based on the virtual jobs creation, data collection automation and transmission, branching out channels of communication with

customers and simplification of formalized procedures at the stage of insurers' acquisition process.

Global trends that have affected change include external and internal factors. The key factors that became the basis for the transformation of the cyber insurance market were:

- reduction in work efficiency due to illness (temporary absence from work) or death (loss of a skilled worker) from COVID-19,
- attempts to maintain business activity during the crisis with the maintenance of contacts with both external and internal customers,
- the transition of most enterprises to a remote format of work with the concomitant need to train staff in new technologies and programs,
- establishing continuous supply chains of organizations and their customers,
- organizations depend on the latest technologies and programs, as well as the level of their security and safety of data channels [7].

Obviously, the primary indicator that distinguishes the format of business organizations before and after the COVID-19 pandemic is the quality of digitalization of companies' processes. The transition adaptation period to new conditions has been crucial for many companies, as the share of companies that have suffered at least once from a successful cyber-attack has increased by 1 percent in 2019 vs 2018, by 3 percents in 2020 vs 2018 and by 9 percents in 2021 vs 2018 (see Figure 1). Such galloping growth is evidence of the cyber-attacks development, as well as the lack of enterprise IT-systems security.

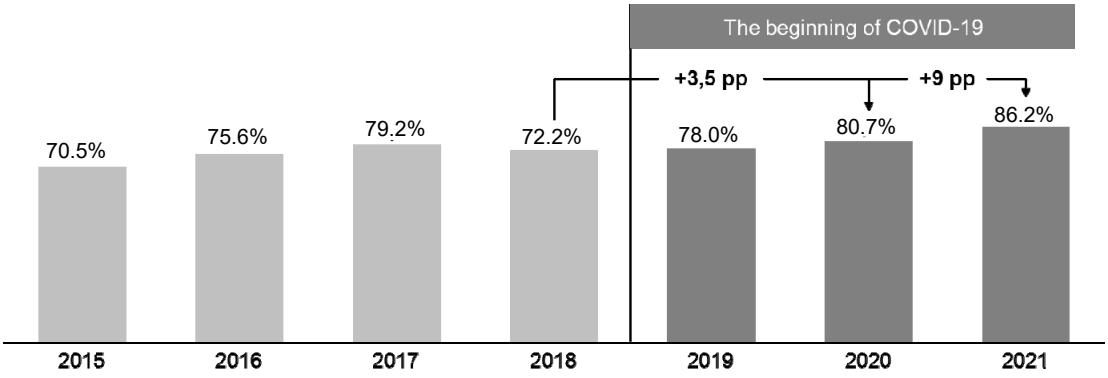

Figure 1. The share of organizations that suffered from at least one successful cyber-attack in 2015–2021

Source: Compiled by the authors based on [8].

At the end of 2021, about 86.2 % of companies have been attacked by cybercriminals with further consequences: financial and reputational losses. In order to reduce cyber-attacks negative impact, business owners have made decisions to secure information structures. However, today the pace of development of cybercrime tools is growing rapidly, so it is impossible to fully secure IT systems. A practical solution, in this case, is cyber insurance product usage, which on the one hand, help to monitor the current status of policyholders, and on the other hand provides financial support in case of losses due to the cyber incident.

Cyber insurance became more popular in 2019–2021 compared to 2017–2018, due to a higher growth rate of gross insurance premiums. The volume of the cyber insurance market shows an average growth rate of 28 % during 2015–2021 due to the increase in threats caused by cyber incidents (see Figure 2).

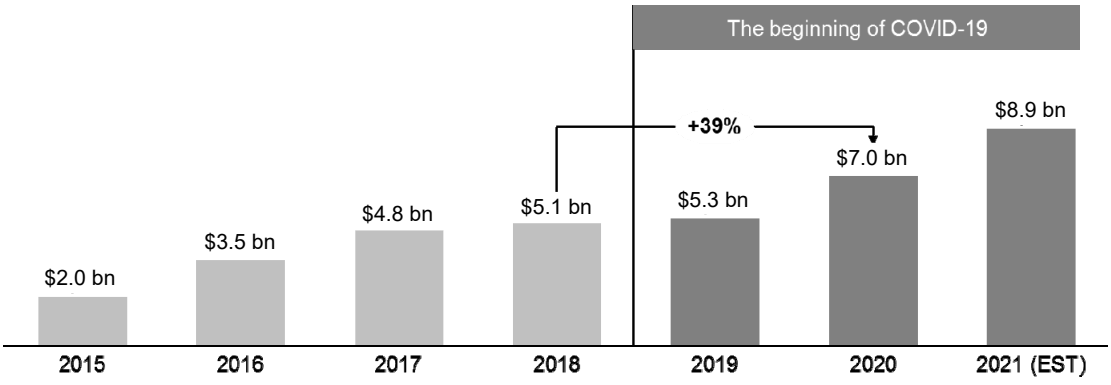

Figure 2. The volume of the cyber insurance market in 2015–2021

Source: Compiled by the authors based on [9].

ISSN 1728-3817

Every year, the diversity of cyber insurance products expands under the influence of challenges that arise at the global and local levels. It was found that the reason for the significant increase of 39 % of gross premiums in 2020 vs 2018 were an improvements of cyber insurance policies, which covered more types of risks than in the period before the COVID-19 pandemic. Scientists identified many approaches to the classification of the kinds of cyber insurance. However, in the framework of building a model for the development of this type of insurance, we consider the most appropriate classification by sources of risk. According to Alliant Cybersecurity, the most common sources of risk are cyber-attacks, such as:

- malicious software,
- denial of service due to DDoS-attack,
- employee attack (MITM),
- SQL injection into program code [10].

It is worth noting that this classification is currently a generalized state, as over time the variety of options for cyber threats will increase. In our opinion, one of the most promising areas of development of cyber insurance, which already exists, is the promotion of policies to cover the risk of denial of service through a DDoS attack.

DDoS-attack is implemented by attackers according to the following procedure: the site is attacked from a large number of devices, not one. The more devices, the more load on the server and the more chances to make the site inaccessible. The complexity of the attack is measured by time, the longer attack duration, the more dangerous it is. The attack can involve any device that connects to the Internet and can send requests: smartphones, smart watches, appliances, hosting servers [11].

After the start of the COVID-19 pandemic in 2019, the number of DDoS attacks increased by 20 % vs. 2018, and in 2020 by 37 % vs. 2018. As of the end of 2021, the daily number of DDoS attacks exceeded 33,000, as this type of cyber-attack is one of the cheapest and most accessible in the world (see Figure 3).

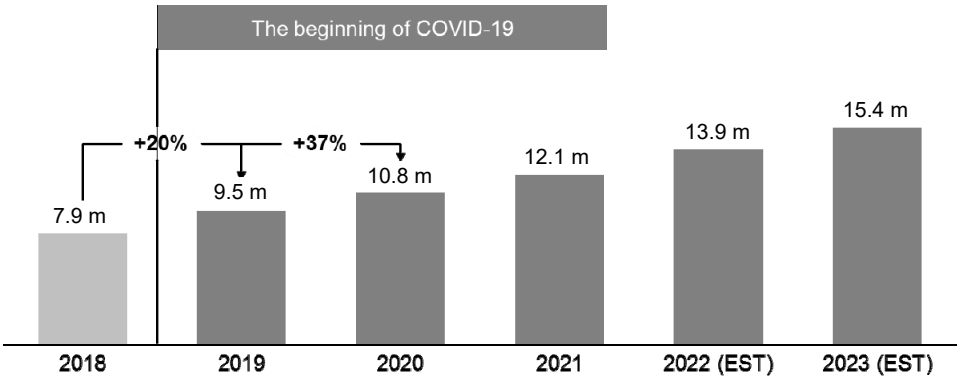

Figure 3. The dynamics of DDoS attacks in the world in 2018–2021

Source: Compiled by the authors based on [12].

Given the growth rate of DDoS attacks, in 2023, their number is expected to ~15 million. As the number of attacks increases and their success and effectiveness, we consider cyber insurance a promising option for securing organizations and their customers.

The state of DDoS-attacks insurance in the world. Despite their ease of implementation and relative cheapness, DDoS attacks are an effective instrument of discrediting government websites, official websites of global and local organizations or public figures; "freezing" the sites of competitors of online platforms for dating or sales; to stop the provision of certain administrative or entertainment services. For local organizations that do not have adequate protection against cyber-attacks, such interventions can be catastrophic, as DDoS attacks can completely stop their service or sales. The traditional consequences of DDoS attacks are:

- loss of income due to unavailability of service,
- inability to monetize content,
- reduction of labor productivity,
- costs for restoring IT systems,
- damage to the brand reputation,
- reduction of market share,
- redemption costs for blocked files/applications [13].

Given the possible consequences, most organizations create preventive sets of measures that increase the reliability of their IT systems. But it is impossible to altogether avoid this type of risk, as attackers, in turn, are constantly improving their tools, thereby increasing the opportunities for cybercrime. An effective way out of such conditions was to create a new type of cyber insurance – DDoS attacks insurance. Nowadays, the Financial Services Roundtable [13] has identified four types of cyber insurance policies aimed at protecting against the effects of DDoS attacks:

- covering losses caused by breaches of the integrity and confidentiality of the insured's data, as well as the costs of the process of restoring data warehouses (in some cases, the policy covers the costs of legal services and legal investigations),
- reputational costs associated with restoring the insured's multimedia profile (websites, media and intellectual property rights) that may have been harmed or blocked by cybercriminals,
- losses due to cyber extortion (for the return of rights to manage the systems or websites of the insured),
- covering the costs of security development of the insured's IT systems.

The world practice of using DDoS-attacks insurance has qualitatively changed under external conditions. Thus, the current procedure is the use of affiliate programs, which are based on the cooperation of insurance companies and expert

organizations in the field of cyber security. In this case, when concluding an insurance contract, the policyholder undertakes to monitor the current state of security of its IT structures and provide experts with access to internal control systems for storage, publication and transmission of data.

DDoS-attacks insurance services are already available in the USA, China, Japan and Europe. Insurers in these countries are guided by the position that buying an insurance policy does not replace the need to invest in improving cyber security systems. At the same time, the popularity of different types of policies differs in these countries, as the state policy on information support is different (see Table 1).

***Table* 1. Rating of DDoS-attacks insurance policies types**

Policy type	USA	China	Japan	EU
Cover the risks associated with data integrity and confidentiality	1	2	1	2
Cover the risks associated with the reputation of the insured	2	1	2	3
Cover the risks associated with cyber-extortion	4	3	3	1
Cover the risks arising from the insufficient level of security development of the insured's IT systems	3	4	4	4

Source: Compiled by the authors based on [14, 15, 16, 17].

The assessment of the popularity of insurance types is based on the availability of these policies in different regions, the number of cyber-attacks with the corresponding consequences and the features of regional cyber security policies. According to the analysis, we noticed that the most popular are the purchase of DDoS-attacks insurance policies, which are related to the integrity and confidentiality of data, as well as the insured's reputation. This is also confirmed by the expansion of international policies that control relations in data storage and confidentiality.

Prospects for the development of DDoS-attacks insurance in Ukraine. The modern Ukrainian insurance market is increasingly adapting to global requirements. Nowadays, about 5 % of insurance companies in Ukraine already provide cyber insurance services, but no one company offers standard policies that cover only the risks associated with DDoS-attacks. In addition, the confidentiality of data in the face of Russia's aggression is becoming one of the main tasks of the Ukrainian digital sector.

It is important to understand which countries carry out DDoS-attacks on Ukraine, as their features and consequences may differ. In the first quarter 2022, the most significant number of DDoS-attacks was committed by the USA – 17 %, indicating the presence of a large number of criminal centers that commit cybercrime; in second place was Russia – 9 %; in third Germany – 9 % (see Figure 4).

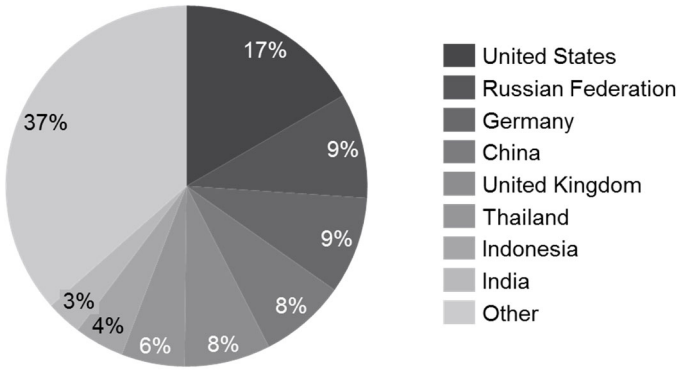

Figure 4. DDoS attacks on Ukraine in Q1 2022 by source countries

Source: Compiled by the authors based on [18].

Traditionally, the majour centers of DDoS-attacks are USA, Russia, and China. These countries are among the TOP-5 countries that attacked Ukraine during the first quarter of 2022.

Another approach to clustering DDoS-attacks is by object or industry. As each industry has its characteristics, the proposals for improving its IT structures may differ. Most cybersecurity experts have ready-made platforms and software suitable for a particular sector. During the first quarter of 2022, the following industries suffered the most from DDoS-attacks, %:

- Broadcast Media (41),
- Media and Publishing (17),
- Internet (11),
- Online Media (11),
- Media Production (7) [18].

Obviously, the most vulnerable industries related to media, advertising, and publication, due to the extensive information campaign to discredit Ukrainian information resources. An option to maintain their stable operation may be insurance against DDoS-attacks, as its implementation will check the current state of all organizations, create specialized mechanisms to protect and prevent blocking attacks and finance possible reputational and material losses.

DDoS attacks insurance is particularly important in the context of the Digital Strategy of Ukraine 2030. The national strategy includes digital transformation or the integration of the latest digital technologies in all areas of

business, supporting infrastructure changes including some provisions, one of which is the creation of cybersecurity infrastructure and computer systems (cloud and virtualized) [19]. These changes should be considered comprehensively and highlight both advantages and disadvantages. The advantages are the upgrading of infrastructure, its compliance with global trends, and a more comprehensive range of opportunities. We consider the need to train personnel who will work with the new systems, the lack of a unified legal framework in the field of cybersecurity and the difficulty of detecting cyber-attacks as possible obstacles to implementing the national strategy.

In this context, the frequency of DDoS-attacks may increase as business process virtualization expands opportunities for criminals. Therefore, the development of this type of insurance will take place simultaneously with the digital transformation to preserve the integrity and confidentiality of data.

Ukrainian insurance companies can use the European experience of introducing DDoS-attacks insurance in their portfolio. The priority is to find partner companies that will assess the condition of policyholders and support their IT systems. This format of cooperation will be mutually beneficial for both parties, as the permanent format of cooperation involves the availability of contracts and discounts, as well as joint, and therefore more effective, customer search. Discussion of their format of cooperation should be based on transparent conditions and in the presence of appropriate certificates confirming the qualifications of cyber security experts. Then the insurer must approve a clear list of risks associated with DDoS-attacks. Thanks to this, the client can choose the policy that will cover the required set of risks, thereby adjusting the cost of the policy itself.

Conclusions. The COVID-19 pandemic was a difficult period for all participants in economic relations. Due to the transition to remote format of doing business and increasing the share of automated processes, organizations were forced to create new departments dealing with cybersecurity. Even though the innovations have helped to increase the level of companies' protection, it was impossible to completely block the threats of attackers, as the share of companies that have suffered at least once from cyber-attacks has increased. Simultaneously with the development of cyber defense systems, the active spread of cyber insurance began, which served as an effective mechanism for checking the current status of the insured and compensation in the event of a cyber incident.

One area of cyber insurance actively developing in the world is DDoS-attacks insurance. The research identified four main types of policies to protect against the effects of DDoS attacks: coverage for damages caused by breaches of the integrity and confidentiality of policyholder data, scope of reputational costs, coverage of losses due to cyber claims, coverage of cost recovery security of IT systems. These types of insurance already exist in the USA, China, Japan, EU countries, but each of the regions has their own distinctive features. In 2022, this type of insurance became especially relevant in Ukraine. During the first quarter, attackers launched an information campaign to disrupt the stable operation of websites, servers, and public accounts of government, media, and television. Most of the attacks were carried out from the so-called global hubs of cybercriminals who carry out mass DDoS attacks: the United States, Russia, China, and others. Therefore, DDoS attacks insurance is a promising segment that needs investment and support at the state level, as the Digital Strategy of Ukraine 2030 includes provisions such as developing cyber security and building a cloud computing infrastructure. Broadcast Media, Media and Publishing, Internet, Online Media, and Media Production are areas for which the creation of appropriate mechanisms is particularly relevant. These industries have become the main target of aggression by cybercriminals, as today they have a special social and educational importance in the conditions of information war.

Discussion. Further research may address the mechanism of launching a product of DDoS-attacks insurance in Ukraine and creating government programs to support this innovation area. As cyber insurance products are built on the cooperation of insurance companies and specialized organizations in cyber security, it is worth considering options for mutually beneficial partnerships that will help minimize the risk of cyber incidents and accurately calculate the amount of losses.

References

1. Romanosky, S., Ablon, L., Kuehn, A. and Jones, T., 2019. Content analysis of cyber insurance policies: how do carriers price cyber risk? [online] Available at: <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419?login=true> [Accessed 3 April 2022].

2. Kshetri, N., 2020. The evolution of cyber-insurance industry and market: An institutional analysis [online] Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0308596120300999> [Accessed 3 April 2022].

3. Kshetri, N., 2018. The Economics of Cyber-Insurance [online] Available at: <https://ieeexplore.ieee.org/abstract/document/8617758> [Accessed 4 April 2022].

4. Woods, D. W. and Bohme, R., 2021. How Cyber Insurance Shapes Incident Response: A Mixed Methods Study [online] Available at: <https://informationsecurity.uibk.ac.at/pdfs/DW2021_HowInsuranceShapes_WEIS.pdf> [Accessed 3 April 2022].

5. Markopoulou, D., 2021. Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the US example [online] Available at: <https://www.sciencedirect.com/science/article/abs/pii/S026736492100100Xpdf> [Accessed 8 April 2022].

6. Liu, M., 2021. Embracing Risk: Cyber Insurance as an Incentive Mechanism for Cybersecurity [online] Available at: <https://www.morganclaypool.com/doi/abs/10.2200/S01093ED1V01Y202104LNA026> [Accessed 9 April 2022].

7. PWC, 2020. The PWC 2020 Report. Managing the impact of COVID-19 on cyber security [online] Available at: <https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/covid-19-impact-mar2020.pdf> [Accessed 9 April 2022].

8. Comparitech, 2020. Cybercrime and Cybersecurity Statistics 2022 Edition [online] Available at: <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends> [Accessed 9 April 2022].

9. GlobalData, 2022. Cyber insurance industry [online] Available at: <https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025-says-globaldata> [Accessed 9 April 2022].

10. Alliant, 2021. Types of Cyberattacks by Alliant cybersecurity [online] Available at: <https://www.alliantcybersecurity.com/our-services/respond/incident-response/types-of-cyber-attacks> [Accessed 13 April 2022].

11. Infocom, 2020. What are DDoS attacks and what is their purpose? [online] Available at: <https://infocom.ua/ %D1 %89 %D0 %BE- %D1 %82 %D0 %B0 %D0 %BA %D0 %B5-ddos- %D0 %B0 %D1 %82 %D0 %B0 %D0 %BA %D0 %B8> [Accessed 17 April 2022].

12. Cisco, 2021. Cisco Annual Internet Report (2018–2023) [online] Available at: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html#_Toc529314172> [Accessed 17 April 2022].

13. Corero, 2021. The Damaging Impacts of DDoS Attacks [online] Available at: <https://www.corero.com/blog/the-damaging-impacts-of-ddos-attacks> [Accessed 18 April 2022].

14. NAIC, 2021. Report on the Cybersecurity Insurance Market 2021 [online] Available at: <https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf> [Accessed 16 April 2022].

15. Marsh, 2021. Cyber Insurance Market Overview: Fourth Quarter 2021 [online] Available at: <https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html> [Accessed 16 April 2022].

16. Mordor Intelligence, 2022. China cyber (liability) insurance market – trends, industry competitiveness & forecasts to 2022 [online] Available at: <https://www.mordorintelligence.com/industry-reports/china-cyber-liability-insurance-market> [Accessed 16 April 2022].

17. Mordor Intelligence, 2022. Japan cyber (liability) insurance market – trends, industry competitiveness & forecasts to 2022 [online] Available at: <https://www.mordorintelligence.com/industry-reports/japan-cyber-liability-insurance-market> [Accessed 16 April 2022].

18. Radar, 2022. Cloudfare Radar DDoS Attack Trends for Q1 2022 [online] Available at: <https://radar.cloudflare.com/notebooks/ddos-2022-q1> [Accessed 15 April 2022].

19. Ukrainian Institute of the Future, 2021. Digital Strategy of Ukraine 2030 [online] Available at: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html> [Accessed 15 April 2022].

Received: 19/04/2022
1st Revision: 12/05/2022
Accepted: 30/05/2022

Author's declaration on the sources of funding of research presented in the scientific article or of the preparation of the scientific article: budget of university's scientific project

Н. Приказюк, д-р екон. наук, проф.,
Л. Гуменюк, асп.
Київський національний університет імені Тараса Шевченка, Київ, Україна

ПАНДЕМІЯ COVID-19 ЯК КЛЮЧОВИЙ ФАКТОР РОЗВИТКУ СТРАХУВАННЯ ВІД DDOS-АТАК

Досліджено трансформацію ринку кіберстрахування у світі до та після початку пандемії COVID-19, оскільки пандемія стала переломним моментом для усіх учасників економічних відносин. Страховий ринок зіштовхнувся з новими викликами, що пов'язані зі зміною формату співпраці з клієнтами, а також із трансформацією бізнесу самих клієнтів. Дистанційний формат співпраці відкрив багато загроз, що можуть не тільки зупинити бізнес, а й повністю його знищити. Одним із прикладів таких загроз є DDoS-атаки, що націлені на зупинку комп'ютерних систем жертв атаки. Також у статті розглянуто стан і перспективи страхування від DDoS-атак та доведено необхідність розвитку зазначеного виду страхування в Україні. Надано рекомендації з уведення продуктів кіберстрахування від DDoS-атак у портфель українських страхових компаній у контексті Цифрової стратегії України 2030.

Ключові слова: страхування, кіберстрахування, кіберризик, DDoS-атака, цифрова трансформація.