

DOI: [https://doi.org/10.18371/fp.1\(33\).2019.177102](https://doi.org/10.18371/fp.1(33).2019.177102)

JEL Classification D74, K32, K42, L86, O30

## **INSURANCE IN THE BUSINESS CYBER RISK MANAGEMENT SYSTEM IN THE DIGITAL ECONOMIC CONDITIONS**

**NAHAICHUK Nelya**

*Ph.D in Economics, Associate Professor  
Dean of the Management and Law Faculty  
Banking University, Cherkasy Institute*

**TRETIK Natalia**

*Ph.D in Economics, Associate Professor  
Department of the Banking and Finance  
Banking University, Cherkasy Institute*

**TKALENKO Oksana**

*Bachelor of Higher Education Master's Degree  
specialty 073 Management  
Banking University, Cherkasy Institute*

**Annotation.** *The concept of cyber risk is explored in the article, the processes of organization of insurance protection against cyber risk are theoretically described. The methodical and practical aspects of the participation of insurance companies in the development and implementation of the program of insurance protection of enterprises against cyber risks are revealed. The directions of strengthening the role of insurance companies in securing the insurance interests of citizens, business and the state from the effects of cyber risks have been identified.*

**Keywords.** *Cyber Risk, Cyber Threat, Cyber Risk Insurance, Cyber Insurance Risk Management System, Utility Function.*

The development of a modern economy based on the use of the latest digital technologies, the creation of new materials, the analysis of large data sets, the development of new management systems leads to a change in the principles of competitive relations.

Despite the unconditional benefits of digitizing the economy - the emergence of Dig Data, artificial intelligence, blockchain technology, cloud computing, the latest risks are appeared, generated by

their use, which can negatively influence on economic entities and their performance.

Taking into consideration the insufficient insurance activity of potential victims of cyber risk (consumers of insurance services), due to ignorance or lack of awareness, consideration of the current state and determinants of the development of cyber risk insurance is a relevant area of research.

The purpose of this article is to identify ways to enhance the role of insurance companies in securing the insurance interests of citizens, businesses and the state from the effects of cyber risks.

The conducted research allows tracking the transformation of insurance risks in the Internet of Things (IoT), to identify existing approaches to the classification of cyber risks and to clarify the vision of the content of cyber insurance, to reveal its purpose, objectives, and principles of organization of insurance protection against cyber risks.

The processes of organization of insurance protection against cyber risks are theoretically described. The methodical and practical aspects of the participation of insurance companies in the development and implementation of the program of insurance protection of enterprises against cyber risks are revealed.

The main results of the research are formed, which are to clarify the content of "cyber risk" (through the identification of its specificity) as a risk, the emergence of which is caused by the activity in the electronic market and the use of IT technologies, algorithmic approach to deciding on the expediency of cyber risk insurance taking into account utility

functions for both the policyholder and the insurer.

The conducted research of scientific achievements of Ukrainian and foreign scientists made it possible to interpret "cyber insurance" as a component of enterprise risk management, which is a financial mechanism of recovery after significant losses, the purpose of which is to help insurers to get back to normal functioning, maintain stability, solvency and lower cost, related to interruptions in production caused by cyber risks.

Nowadays, a situation arises in which domestic insurance companies are not yet able to develop their approach to cyber risk assessment, which is holding back the growing popularity of this service in Ukraine. Domestic insurance companies, preparing a proposal for a client, evaluate the risks of the company with the help of indirect signs and characteristics, such as: methods of risk management in the company; ways of storing data; conducting or testing information security and auditing systems, and assessing the number of employees employed in IT. It is to be expected that more detailed techniques will be formed in the nearest future, which will nevertheless answer the direct question of cyber insurance risk assessment.

### *References*

1. A.V. Keshelava V.H. Budanov, V.Iu. Rumiantsev (2017). Vvedenye v «Tsyfrovuiu» ekonomyku [Introduction to the Digital Economy]. VNYYHeosystem, 28. [in Russian].
2. Tynkova A.A., Zamotaikyna A.A. Osobennosty y preymushchestva platformu Watson IoT dlia Ynterneta veshchei [Features and Benefits of the Watson IoT Form

- Board for the Internet of Things]. Retrieved from <http://nauka-rastudent.ru/39/4148/> [in Russian].
3. Ynternet Veshchei: ynnovatsyonnyye y perspektivnyye tekhnolohyy – IoT Russia 2015 [Internet of Things: Innovative and Advanced Technologies - IoT Russia 2015]. Retrieved from <http://www.tmtconferences.ru/iot2015.html> [in Russian].
4. Karachev O. Ynternet veshchei: chto eto takoe y s chem eho ediat? [Internet of Things: What is It and what is It Eaten with?]. Retrieved from <http://chezasite.com/news/chto-takoe-internet-veshei-82180.html>. [in Russian].
5. Ways to make global e-commerce easier for everyone (December, 2017). Retrieved from <https://www.weforum.org/agenda/2017/12/e-commerce-trade-wto-growth-opportunity>.
6. 2018.iforum.ua/ru/speakers/alexandra-gladyshevskaya. [in English].
6. Calderon C., Marta E. (2007). A taxonomy of software security requirements. *Avances en Sistemas e Informatica*, 4 (3), 47-56. [in English].
7. Cebula J., Young L. (2010). A taxonomy of operational cyber security risks. Software Engineering Institute, Carnegie Mellon University. Retrieved from <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395> [Accessed 12/04/16]. [in English] .
9. Firesmith D. (2004) Specifying reusable security requirements. *Journal of object technology*, 3 (1), 61-75. [in English] .
10. Donnelly C., Englund M., Nielsen J.P., Tangaard C. (2014). Asymmetric information, self-selection and pricing of insurance contracts: the simple no-claims case. *Journal of risk and insurance*, 81 (4), 757-780. [in English].
11. Gerasimenko V.A. (1994). *Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh* [Data protection in data processing systems]. Moscow: Energoatomizdat Publ. [in Russian].
12. Mirsanova, O.A. (2016). The Bonus-Malus System as the policyholders classification method in cyber-insurance / *Economics: Yesterday, Today and Tomorrow*, 6. [in English]
13. Biener C., Eling M., Wirfs J.H. (2015). Insurability of cyber risk: an empirical analysis. *Working papers on risk management and insurance*, 151. Retrieved from <http://www.ivw.unisg.ch/~media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf> [Accessed 15/04/16]. [in English].

14. Voronova T. Bezopasnoi ynternet [Safe Internet]. Calaméo. Retrieved from <http://ru.calameo.com/books/002793881c6046eb0d2fb>[in Russian].
15. Zavorodnyi V.Y. Paradyhma ynformatsyonnykh ryskov [The Paradigm of Information Risks]. Fynansovui Unyversytet pry Pravytelstve RF. Retrieved from [http://www.fa-kit.ru/main\\_dsp.php?top\\_id=591](http://www.fa-kit.ru/main_dsp.php?top_id=591) [in Russian].
16. Zaitseva O.N. (2013). O neobkhodymosti vvedeniya poniatiya «rysky adekvatnosti ynformatsyy» [On the Need to Introduce the Concept of "Information Adequacy Risks"]. Fundamentalnye yssledovaniya. Vol 1–3, 807–811. [in Russian].
17. Myshel M. (2003). Upravleniye ynformatsyonnyu ryskamy [Information Risk Management]. Fynansovui dyrektor, 9, 64–68. [in Russian].
18. Data scarce for insurers covering cyber risks. Business Insurance. Retrieved from <http://www.businessinsurance.com/article/20150610/NEWS06/150619981/1251>. [in English].
19. Vinnikova I.I., (2018). Kiber-ryzyky yak odyin iz vydiv suchasnykh ryzykiv u diialnosti maloho ta serednoho biznesu ta upravlinnia nymy [Cyber Risks as a Type of Modern Risks in the Management and Management of Small and Medium Business]. Skhidna Yevropa: ekonomika, biznes ta upravlinnia. Vol. 5 (16) 2018. [in Ukrainian].
20. Böhme R., Schwartz G. (2010). Modeling cyber-insurance: towards a unifying framework. WEIS. Retrieved from [http://econinfosec.org/archive/weis2010/papers/session5/weis2010\\_boehme.pdf](http://econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf) [Accessed 12/04/16]. [in English].
21. Tsena ynformatsyonnoi bezopasnosti y strakhovaia zashchyta otkyber – ryskov [The Price of Information Security and Insurance Protection Against Cyber risks]. Retrieved from <http://strahovkunado.ru/insur/strakhovan>. [in Russian].
22. Strakhovanye kyber-ryskov [Cyber Risk Insurance]. Retrieved from <https://www.arsenalins.ru>. [in Russian].
23. Ponomarëv A. N. (2009). Razrabotka modely protsessa korporativnoho strakhovaniya [Development of a Model of the Process of Corporate Insurance]. Ymushchestvennoe korporativnoe strakhovanye Vestnyk VHU. Seryia: Ekonomyka y upravleniye, 2, 61-68. [in Russian].
24. Bratiuk V.P. (2015). Sutnist kiber-zlochyniv ta strakhovyi zakhyst vid kiber-ryzykiv v Ukraini [The Essence of Cybercrime and Insurance Protection Against Cyber Risks in Ukraine], Aktualni problemy ekonomiky, 9, 421-427. [in Ukrainian].

25. Siedov Ye. S. (2016). Deiaki aspekty strakhuvannia kiber-ryzykiv [Some Aspects of Cyber Risk Insurance]. Kyiv: KT «Zabelina-Filkovska T. S. i kompaniia Kyivska notna fabryka», 288–291. [in Ukrainian].
26. Marotta A. A. (2015). Survey on Cyber-Insurance. Bologna, Italy: Unipol Gruppo Finanziario S.p.A., 52 [in English].
27. Kurbanova O.Э., Laryonov V.Y. (2017). Kyberstrakhovanye kak sposob obespecheniya ynformatsyonnoi bezopasnosti [Cyber Insurance as a Way of Providing Information Security], 55-58. [in Russian].
28. CRO Forum. The Cyber Risk Challenge and the Role of Insurance. December 2014. Retrieved from <http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance>. [in English].
29. Yvashchenko A.N., Sharko Y.A (2016). Myrovoi runok strakhovanyia kyber-ryskov: perspektyvu y prepiatstvyia dlia razvytyia v Respublyke Belarus [The world Market for Cyber Risk Insurance: Prospects and Obstacles for Development in the Republic of Belarus], 196–202. [in Russian].
30. Kropotyna O.E. (2009). Strakhovanye kak metod upravleniya ryskamy promushlennukh predpriiatyi [Insurance as a Risk Management Method for Industrial Enterprises]. Экономыка y upravlenye narodnum khaziaistvom, 11/12, 12–14. [in Russian].