DOI: https://doi.org/10.18371/fp.1(33).2019.177107

JEL M15, O32, F52

CYBERTHREATS IN THE DIGITAL ECONOMY

PANTIELIEIEVA Nataliia
Dr.Sc. in Economics, PhD in Technical sciences, Assoc. Prof.,
Banking University, Cherkasy Institute
ORCID ID: 0000-0001-6457-6912
e-mail: nnpanteleeva2017@gmail.com

ROMANOVSKA Liudmyla
researcher of Banking University
e-mail: ludmila08romanovska@gmail.com

ROMANOVSKA Mariia
cadet of Military institute of
telecommunications and informatization
named after Herois of Kruty

Abstract. *The theoretical assumptions of the debatable interpretation of the concept of "cybersecurity" by systematic and subject-object approaches are generalized; examined the position of the international professional society and governments of the world on strategic management of cybersecurity; generalized characteristics of typology of cyberthreats, objects, spheres and tendencies of their spread and destructive influence are defined; revealed the multidimensional nature of digital technologies in terms of vulnerability, resilience and ability to counter cyberthreats; institutional infrastructure was uncovered and a critical analysis of conceptual documents of the national cybersecurity system are carried out.*

Keywords: *digital economy, digital technologies, cyber security, cyberthreats, cryptocurrency, blockchain, artificial intelligence.*

The modern driver of socio-economic development, competitiveness and improving the quality of life for both the individual country and the world is the digital economy. Digitization processes are rapidly expanding and particular important in all areas of life, in the same time creating new threats and challenges, opening up previously unknown opportunities for improprieties and legal abuse. That is why development of the cyber security and implementation of effective measures to combat cybercrime have become a major issue on the world agenda. All this determines the relevance of the study. The research methodology involved the use of methods of analysis and synthesis, abstraction, generalization, systematic, subject-object and institutional approaches, empirical comparison.

The article shows that the concept of cybersecurity is complex, combining in its essence the substantive basis of cyberspace and the process functionality of the protection mechanism that relies

on systemic and institutional approaches, adheres to the principles of efficiency, reliability, optimality.

Adhering to the view that typologization of cyber threats is an open system, which is quite naturally connected with the progressive development of technologies, their most known types from the point of view of destructive properties, technical functionality and motive factors, trends of dissemination are considered and characterized by authors.

The article reveals the multidimensional nature of modern digital technologies, including blockchain, artificial intelligence, the Internet of Things, regarding cybersecurity vulnerability and / or resilience and cybersecurity capabilities.

A critical assessment of the institutional infrastructure and regulatory framework of Ukraine's cybersecurity system are given.

It is concluded that building a digital economy is impossible without understanding the technological and social nature of cyberthreats, requires initiatives and effective steps in developing and strengthening institutional and information infrastructure at the national and global levels, develop a sound and consistent digital legal framework, formulate the necessary digital and digital competencies literacy, including the cyber-threat models and cybercrime mechanisms and their consequences, compliance with cybersecurity principles in all areas of professional activities and building smart-oriented ecosystems and more.

References

1. Hutsaliuk, M.V. (2019). Otsinka realizatsii stratehii kiberbezpeky Ukrainy z urakhuvanniam dosvidu yevropeiskykh i svitovykh praktyk [Assessment of the implementation of the cybersecurity strategy of Ukraine, taking into account the experience of European and world practices]. *Informatsiia i pravo,* 2(29), 90-99. [in Ukrainian].

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cyber security of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19. [in Ukrainian].

3. National Military Strategy for Cyberspace Operations. Retrieved from //www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf. [in English].

4. Cyber Security Strategy of the United Kingdom. Retrieved from http://ccpic.mai.gov.ro/docs/UK_cyber_security.pdf. [in English].

5. Estrategia de Ciberseguridad Nacional. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ES_NCSS.pdf. [in English].

6. National Cyber Security Strategy for Norway New national strategy for cybersecurity published by Norway. Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf. [in English].

7. Rus, I. (2017) Study of cybersecurity issues. *Studia universitatis petru maior series oeconomica*, 1, 1-16. [in English].

8. Furashev, V.M. (2012) Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and the information space, cybersecurity and information security: the essence, definition, differences]. *Informatsiia i pravo*.. 2(5), 162-175. [in Ukrainian].

9. Baranov, O.A. (2014). Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» [On the interpretation and definition of the term “cybersecurity”]. *Pravova informatyka,* 2(42), 54-62. [in Ukrainian].

10. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. Retrieved from https://www.iso27001security.com/html/27032.html. [in English].

11. Recommendation X.1205 (04/08). Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I. [in English].

12. Kiberbezopasnost' [Cybersecurity]. Retrieved from http://digitalbusiness.by/napravleniya-sotrudnichestva/natsionalnyj-bank-respubliki-belarus/kiberbezopasnost. [in Russian].

13. Kiberataki [Cyberattacks]. Tadviser. Retrieved from http://www.tadviser.ru/index.php. [in Russian].

14. Aktual'nye kiberugrozy [Actual cyber threats.]. Retrieved from https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/#id2. [in Russian].

15. Kiberugrozy: statistika, praktika i prognoz [Cyberthreats: statistics, practice and forecast]. Retrieved from http://lib.itsec.ru/articles2/Oborandteh/kiberugrozy-statistika-praktika-i-prognoz. [in Russian].

16. Sovremennye kiberugrozy – techenie, razvitie, prognoz [Modern cyber threats - course, development, forecast]. Retrieved from http://www.cio-sibir.ru/files/Meet/2015/2015-10-09-03.pdf. [in Russian].

17. Zaporozhets, O.Yu. (2014) Kiberviina: kontseptualnyi vymir [Cyber war: a conceptual dimension]. *Aktualni problemy mizhnarodnykh vidnosyn,* 121(I), 80-86. [in Ukrainian].

18. Topchii V.V. Kiberteroryzm v Ukraini: poniattia ta zapobihannia kryminalno-pravovymy ta kryminolohichnymy zasobamy [Cyber terrorism in Ukraine: the concept and prevention of criminal law and criminology means]. Retrieved from http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf. [in Ukrainian].

19. Buryak, V.V. (2019). Tsifrovaya ekonomika, khaktivizm i kiberbezopasnost' [Digital economy, hacktivism and cybersecurity]. Simferopol': IP Zueva T.V. [in Russian].

20. Artamonova, A.A. (2018). Apparatnye zakladki kak komponent vredonosnogo apparatnogo obespecheniya: obzor, klassifikatsiya i analiz ugrozy [Hardware Bookmarks as a Component of Malicious Hardware: Overview, Classification, and Threat Analysis]. *ITportal,* 1(17). Retrieved from http://itportal.ru/science/tech/apparatnye-zakladki-kak-komponent-v/. [in Russian].

21. Microsoft Security Intelligence. Report. Retrieved from https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/. [in English].

22. 4 startapa, kotorye sozdayut iskusstvennyy intellekt dlya vedeniya kibervoyn [4 startups that create artificial intelligence for cyber warfare]. Retrieved from https://www.tsarev.biz/news/zapadnopartnerskij-kontrol-4-startapa-kotorye-sozdayut-iskusstvennyj-intellekt-dlya-vedeniya-kibervojn/. [in Russian].

23. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku. «Pro Doktrynu informatsiinoi bezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 “On the Doctrine of Information Security of Ukraine”]. Retrieved from https://www.president.gov.ua/documents/472017-21374. [in Ukrainian].

24. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 “On the Cyber

Security Strategy of Ukraine”]. Retrieved from https://zakon5.rada.gov.ua/laws/show/96/2016. [in Ukrainian].

25. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cyber security of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19. [in Ukrainian].

26. Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii [On approval of the Concept for the development of the digital economy and society of Ukraine for 2018-2020 and approval of an action plan for its implementation]. Retrieved from https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80. [in Ukrainian].

27. U MERT poiasnyly, shcho ye diievym instrumentom ekonomichnoho zrostannia [The Ministry of Economic Development and Trade explained that it is an effective tool for economic growth]. Retrieved from https://news.finance.ua/ua/news/-/444894/u-mert-poyasnyly-shho-ye-diyevym-instrumentom-ekonomichnogo-zrostannya. [in Ukrainian].