DOI: https://doi.org/10.18371/fp.1(45).2022.113122

JEL Classification K14, K42, O39

COVID-19 AS AN ACTIVATOR OF THE CYBER CRIME PANDEMIC

BRAICHENKO Sergiy
PhD in Economics, Associate Professor
Cherkasy Institute of the Banking University
ORCID ID: https://orcid.org/0000-0002-8476-6622

PANTIELIEIEVA Nataliia
Doctor of Economics, Professor,
Cherkasy Institute of the Banking University
ORCID ID: https://orcid.org/0000-0001-6457-6912

VDOVICHENKO Ruslana
Student,
Cherkasy Institute of the Banking University

Abstract. *The conceptual essence of cybercrime and its typology are considered in the article, the modern legal regulation of fight against cybercrime is generalized. The criminal-legal assessment of the intensification of cybercrime under the influence of COVID-19 in Ukraine is given. A comparative analysis of the criminological practice of counteracting the cybercrime pandemic in the conditions of COVID-19 is conducted. Recommendations on criminalization of some types of crimes and threats in the field of digital transformation, introduction of the newest tools of fight against cybercrime on the basis of modern digital technologies are substantiated.*

Key words: *cybersecurity, cybercrime, digitalization, criminalization, COVID-19, criminal offenses in cyberspace, combating cybercrime.*

At the present stage of its development, humanity is facing not only the changes associated with globalization and scientific and technological progress, but also completely new challenges and threats posed by a dynamically developing society. These, of course, include the COVID-19 pandemic, which, among other things, led to an increase in criminal activity in cyberspace. Therefore, the issue of generalization of theoretical and legal principles and criminological aspects of cybercrime, development of recommendations for improving criminal law regulation and improving the effectiveness of the system of countermeasures to overcome the challenges of COVID-19 became relevant.

Generalization of scientific views and taking into account the current situation, allowed to formulate the author's interpretation of the concept of "cybercrime" in the subject-object and target approaches, highlighting its

substantive nature and organizational aspects.

The COVID-19 pandemic has been shown to activate cybercrime. The analysis of the dynamics of cybercrime in Ukraine during 2018-2021 showed a steady trend towards an increase in offenses related to unauthorized interference and unauthorized actions with information. This allowed authors to make recommendations on the criminalization of certain types of crimes and threats, strengthening the set of measures aimed at effectively combating cybercrime.

Particular attention is paid to digital technologies that can be an effective tool in the fight against cybercrime, including artificial intelligence, Blockchain, XDR, Secure Access Service Edge (border secure access services).

Thus, to overcome the impact and consequences of the COVID-19 pandemic crisis on cybercrime, the potential of modern digital technologies can be successfully used along with continuous monitoring and identification of objective patterns, determinants and characteristics of certain types of cybercrime, forecasting the behavioral profiles of cybercriminals to ensure cybersecurity in the period of post-war recovery.

Reference

1. Dashyan, M.S. (2007). *Pravo informatsionnykh magistraley[Law of Information Highways]*. M.: Norma. [in Russian]

2. Golubev, V.A. «Kiberterrorizm» - mif ili real'nost'? Tsentr issledovaniya komp'yuternnykh prestupleniy ["Cyberterrorism" - myth or reality? Computer Crime Research Center]. Retrieved from : http://www.crime-research.org. [in Russian]

3. Kravtsova, M. O. (2016). *Kiberzlochynnist: kryminolohichna kharakterystyka ta zapobihannia orhanamy vnutrishnikh sprav [Cybercrime: criminological characteristics and prevention by law enforcement agencies]*. Extended abstract of PhD thesis. Khark. nats. un-t vnutr. sprav: Kharkiv. [in Ukrainian]

4. Karpova, D.M. (2014). Kiberzlochynnist: hlobalna problema ta yii vyrishennia[Cybercrime: a global problem and its solution]. *Vlada - Power*, 8, 46-50. [in Ukrainian]

5. Sirenko, O.V. Poniattia kiberzlochyniv ta osoblyvosti metodyky yikh rozsliduvannia [The concept of cybercrime and features of the methodology of their investigation]. Retrieved from: http://dspace.oduvs.edu.ua/bitstream/123456789/486/1/ ilovepdf_com-48-49%5B1%5D.pdf [in Ukrainian]

6. Bielienkyi, V. P. (2016). *Vidpovidalnist za kiberzlochyny za kryminalnym pravom SShA, Velykobrytanii ta Ukrainy (porivnialno-pravove doslidzhennia) [Liability for cybercrime under the criminal law of the United States, Britain and Ukraine (comparative law study)]*. Extended abstract of PhD thesis. Akad. advokatury Ukrainy : Kyiv. [in Ukrainian]

7. Rusetskyi, A. A. (2017). Kutsolabskyi D. A. Teoretyko-pravovyi analiz poniat «kiberzlochyn» i «kiberzlochynnist»[Theoretical and legal analysis of the concepts

of "cybercrime" and "cybercrime"]. *Pravo i Bezpeka - Law and Security*. 1, 74-78. [in Ukrainian]

8. Convention on Cybercrime of the Council of Europe (2001 November 23) (the Convention was ratified with reservations and declarations by Law No. 2824-IV (2824-15). Retrieved from: https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian]

9. Nomokonov, V. A. (2003). Aktualni problemy borotby z kiberzlochynnistiu [Actual problems in the fight against cybercrime]. *Informatsiini tekhnolohii i bezpeka: zb. nauch. tr. mizhnar. konf. – Proceedings of the Internation Scientific and Practical Conference: Information Technology and Security.* (pp.104-108). Kyiv: Natsionalna akademiia nauk Ukrainy. [in Ukrainian]

10. On registered criminal offenses and the results of their pre-trial investigation. Reporting by the Office of the General Prosecutor. Retrieved from: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 [in Ukrainian]

11. Criminal Code of Ukraine (Vidomosti Verkhovnoi Rady Ukrainy (VVR) № 25-26, p.131. (2001) Retrieved from: https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian]

12. Kiberzlochynnist ne spyt – yak ne potrapyty u teneta aferystiv [Cybercrime does not sleep - how not to fall into the net of scammers]. Retrieved from: https://news.finance.ua/ua/news/-/395023/kiberzlochynnist-ne-spyt-yak-ne-potrapyty-v-siti-aferystiv [in Ukrainian]

13. Informatsiine protystoiannia yak faktor zahrozy natsionalnii bezpetsi Ukrainy [Information confrontation as a factor of threat to the national security of Ukraine]. *Osnovni tendentsii proiaviv orhanizovanoi zlochynnosti v suchasnykh umovakh (zb. nauk.- analit. materialiv) - The main trends in the manifestations of organized crime in modern conditions (collection of scientific and analytical materials).* K.: MNDTs. 2014, 1, 161-165. [in Ukrainian]

14. Synookyi, O.V. (2011). *Osnovy informatsiinoho prava ta zakonodavstva u haluzi vysokykh tekhnolohii ta IT – innovatsii [Fundamentals of information law and legislation in the field of high technologies and IT innovations]*. Kh.: Pravo. [in Ukrainian]

15. Kharchuk, V. (2010). Zaprovadzhennia pravovoho rehuliuvannia vidnosyn u hlobalnii merezhi Internet [Introduction of legal regulation of relations in the global Internet]. *Yurydychnyi zhurnal - Legal Journal*, 12, 80-82. [in Ukrainian]

16. Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. unodc.org. Retrieved from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf