DOI (Issue): https: //doi.org/10.36486/np.2022.3(57) Issue 3(57) 2022

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Єрема М.* Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 02.10.2022).

2. *Шиян Д.Г.* Актуальні питання забезпечення кібербезпеки України. *Актуальні проблеми кібербезпеки*: Всеукраїнська наукова конференція. 2019. Київ: Державний університет телекомунікацій. С. 42–44. URL: http://www.dut.edu.ua/uploads/p_1895_91824930.pdf (дата звернення: 02.10.2022).

3. *Веселова Л.Ю.* Адміністративно-правові основи кібербезпеки в умовах гібридної війни: автореф. дис. ... д-ра юрид. наук. Одеса, 2021. 35 с.

4. *Дем'янчук М.А.* Процесний підхід до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів. *Інтелект XXI*. 2020. № 1. С. 36–43. URL: http://www.intellect21.nuft.org.ua/journal/2020/2020_1/6.pdf (дата звернення: 03.10.2022).

5. *Кулешов М.В.* Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України. Інформація і право. 2019. № 2(29). С. 115–122. URL: http://ippi.org.ua/sites/default/files/15_10.pdf (дата звернення: 02.10.2022).

6. *Трофименко О., Прокоп Ю., Логінова Н., Задерейко О.* Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21. № 3. С. 150–157.

7. *Трофименко О.* Моніторинг стану кібербезпеки в Україні. *Правове життя сучасної України*: матер. Міжнар. наук.-практ. конф., 17 травня 2019 р. Одеса: Видавничий дім "Гельветика", 2019. Т. 1. С. 642–646.

8. *Черней В.В.* Роль відомчої освіти та науки в забезпеченні протидії кіберзлочинності в Україні. *Науковий вісник Національної академії внутрішніх справ*. 2014. № 3. С. 3–15.

9. *Чинник П.А.* Світовий досвід боротьби з кіберзлочинністю. *Протидія кіберзлочинності та торгівлі людьми*: зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків), МВС України, Харків. нац. ун-т внутр. справ; Координатор проєктів ОБСЄ в Україні. Харків: ХНУВС, 2020. С. 221–223.

10. *Самойленко О.А.* Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія; за заг. ред. А.Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

11. *Яцишин М.Ю.* Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. № 5. С. 92–99.

12. *Білобров Т.В.* Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України: дис. ... канд. юрид. наук. Київ, 2020. 209 с.

13. *Шемчук В.В.* Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Юридичні науки. 2018. Т. 29. № 6. С. 119–124.

14. *Довженко О.Ю.* Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 19–22.

REFERENCES

1. *Yerema M.* Borotba z kiberzlochynnistyu v umovakh dii voiennoho stanu. "Fighting cybercrime under martial law: Law 2149-IX". URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix. (Date of Application: 02.10.2022) [In Ukrainian].

2. *Shyian D.H.* (2019). Aktualni pytannia zabezpechennia kiberbezpeky Ukrainy. "Current issues of ensuring cyber security of Ukraine". Actual problems of cyber security: All-Ukrainian scientific conference. Kyiv: State University of Telecommunications. P. 42–44. URL: http://www.dut.edu.ua/uploads/p_1895_91824930.pdf (Date of Application: 02.10.2022) [In Ukrainian].

3. *Veselova L.Yu.* (2021). Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoi viiny. "Administrative and legal foundations of cyber security in conditions of hybrid warfare". Extended abstract of Doctor's thesis. Odesa. 35 p. [In Ukrainian].

4. *Demianchuk M.A.* (2020). Protsesnyi pidkhid do vyznachennia zasobiv zakhystu aktyviv telekomunikatsiinoho pidpryiemstva vnaslidok vynyknennia kiberintsydentiv. "A process approach to determining the means of protecting the assets of a telecommunications enterprise due to the occurrence

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).9

of cyber incidents". Intelligence XXI, 1, 36–43. URL: http://www.intellect21.nuft.org.ua/journal/2020/2020_1/6.pdf (Date of Application: 03.10.2022) [In Ukrainian].

5. *Kuleshov M.V.* (2019). Sutnist ta zmist rozsliduvannia kiberintsydentiv ta kiberatak pidrozdilamy SB Ukrainy. "The essence and content of the investigation of cyberincidents and cyberattack units of the Security Service of Ukraine". Information and law. No 2(29). P. 115–122. URL: http://ippi.org.ua/sites/default/files/15_10.pdf (Date of Application: 02.10.2022) [In Ukrainian].

6. *Trofymenko O., Prokop Yu., Lohinova N., Zadereiko O.* (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu. "Cybersecurity of Ukraine: analysis of the current state". Protection of information. Vol. 21. No 3. P. 150–157. [In Ukrainian].

7. *Trofymenko O.* (2019). Monitorynh stanu kiberbezpeky v Ukraini. Pravove zhyttia suchasnoi Ukrainy. "Monitoring of cybersecurity in Ukraine". Proceedings from MIIM '19: International Scientific and Practical Conference "Legal life of modern Ukraine". Odesa: Helvetyka Publishing House. Vol. 1, P. 642–646. [In Ukrainian].

8. *Cherniei V.V.* (2014). Rol vidomchoi osvity ta nauky v zabezpechenni protydii kiberzlochynnosti v Ukraini. "The role of departmental education and science in ensuring the counteraction of cybercrime in Ukraine". Scientific Bulletin of the National Academy of Internal Affairs. No 3. P. 3–15. [In Ukrainian].

9. *Chynnyk P.A.* (2020). Svitovyi dosvid borotby z kiberzlochynnistiu. "World experience in combating cybercrime". Proceedings from MIIM '20: International Scientific and Practical Conference "Counteracting cybercrime and trafficking in human beings". (pp. 221–223). Kharkiv: KhNUVS. [In Ukrainian].

10. *Samoilenko O.A.* (2020). Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori: monohrafiia. "Fundamentals of the Crime Investigation Methodology committed in cyberspace" monograph; in general ed. A.F. Volobueva. Odesa: TES. 372 p. [In Ukrainian].

11. *Yatsyshyn M.Yu.* (2018). Kryminalizatsiia kiberzlochyniv u mizhnarodnomu pravi: porivnialnyi analiz. "Criminalization of cybercrime in international law: comparative analysis". Law forum. No 5. P. 92–99. [In Ukrainian].

12. *Bilobrov T.V.* (2020). Administratyvno-pravovyi status Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy. "Administrative and legal status of the Cyber Police Department of the National Police of Ukraine". Candidate's thesis. Kyiv. 209 p. [In Ukrainian].

13. *Shemchuk V.V.* (2018). Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini. "Cybercrime as an obstacle to the development of information society in Ukraine". Academic notes of V.I. Vernadskyi TNU. Series: Legal Sciences. Vol. 29. No 6. P. 119–124. [In Ukrainian].

14. *Dovzhenko O.Yu.* (2019). Klasyfikatsiia kiberzlochyniv u kryminalistytsi. "Classification of cybercrime in forensics". South Ukrainian legal journal. No 1. P. 19–22. [In Ukrainian].

UDC 343.973

Blyzniuk Ihor,
Candidate of Juridical Sciences, Senior Research Officer, Chief Scientist,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-3882-5790

CHARACTERISTICS OF TYPICAL METHODS OF COMMITTING CIBERCRIME UNDER MARTIAL LAW

This article presents a description of typical ways of committing cybercrime. Author reveals the peculiarities of the causal complex of cybercrime. Along with this, the article details the reasons why cyber threats are evolving at an accelerated pace, and cybercrimes are becoming more advanced, better organized and transnational.

At the same time, in the article, the author outlines the types of cybercrimes that pose the greatest threat today, i.e., under martial law. Changes in the criminal and

criminal procedural legislation that occurred during the war, with the improvement of the grounds and procedural mechanisms for bringing cybercriminals to justice, were not left without consideration.

The author pays special attention to the characteristics of the crimes provided for in Articles 361 ("Unauthorized interference with the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks"), 361-1 ("Creation for the purpose of illegal use, distribution or sale of malicious software or hardware, as well as their distribution or sale"), 361-2 ("Unauthorized sale or distribution of information with restricted access stored in electronic computers (computers), automated systems, computer networks or on carriers of such information") , 362 ("Unauthorized actions with information that is processed in electronic computers (computers), automated systems, computer networks or that is stored on the media of such information, committed by a person who has the right to access it", 363 ("Violation of the rules for the operation of electronic - computers (computers), automated systems, computer networks or telecommunication networks or the procedure or rules for protecting the information processed in them"), 363-1 ("Obstruction of the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks by mass dissemination of messages Telecommunications") of the Criminal Code of Ukraine contained in Section XVI "Criminal offenses in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks".

According to the classification of criminal offenses introduced by the Criminal Code of Ukraine, the author defines criminal offenses covering the concept of cybercrime. In conclusion, the author gives the most common types of cybercrime at the international level.

Keywords: cybercrime, cyberthreats, martial law, criminal law and criminal procedure, malware, cyberfraud, phishing, cyberterrorism, cyberespionage, DDoS or DoS attacks, deface, skimming, remote banking.

Отримано 06.10.2022