Література:

1. Конвенція про кіберзлочинність (Будапештська конвенція). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
2. Присяжнюк М.М. Організаційно-правові основи забезпечення кібербезпеки. Київ : Видавництво Ліра-К, 2023. С. 194–195.
3. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. УДК 341.01. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf
4. Criminal Code of Germany. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

DOI https://doi.org/10.30525/978-9934-26-409-2-25

CURRENT ISSUES OF CRIMINAL AND LEGAL MEASURES FOR COMBATING CYBERCRIME

АКТУАЛЬНІ ПИТАННЯ КРИМІНАЛЬНО-ПРАВОВИХ ЗАСОБІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Zakharchenko A. Y.
master's student
Educational and Scientific Institute of Information Security and Strategic Communications
of the National Academy of the Security Service of Ukraine
Kyiv, Ukraine

Захарченко А. Є.
студентка магістратури
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій
Національної академії Служби безпеки України
м. Київ, Україна

Kamenskyi D. V.
Doctor of Law,
Professor at the Department of Criminal Law
National Academy of the Security Service of Ukraine
Kyiv, Ukraine

Каменський Д. В.
доктор юридичних наук,
професор кафедри кримінального права
Національна академія Служби безпеки України
м. Київ, Україна

Кіберзлочинність – це одна з основних проблем XXI ст., вирішення якої потребує розробки та застосування кримінально-правових засобів ефективної протидії цьому явищу [1, с. 129]. Додатково актуалізує

проблематику дослідження кіберзлочинності також те, що у зв'язку із веденням військових дій на території нашої держави, створюються передумови для зміни свідомості людей у бік протиправної поведінки. Загальновідомим також є те, що війна проти України ведеться не лише військовими методами, а й із застосуванням кіберпростору. Отож, дослідження кримінально-правових засобів протидії кіберзлочинності в сучасних суспільно-політичних умовах є дійсно важливим, оскільки такий вид злочинності, по-перше, набув значного поширення у період збройного вторгнення, а по-друге, становить суттєву загрозу для основ національної безпеки нашої держави.

Дослідження кримінально-правових засобів протидії кіберзлочинності першочергово базується на аналізі положень кримінального закону нашої держави, які встановлюють кримінальну відповідальність за кіберзлочини (виходячи із науково-теоретичних розробок поняття «кримінально-правові засоби»). Разом із тим, при дослідженні кримінально-правових заходів протидії будь-якому виду злочинності варто враховувати і стан розробленості термінологічного апарату у відповідній сфері.

З цього приводу, науковець Думчиков М.О. зауважує, що вперше на міжнародному рівні згадування про кіберзлочин було використано в Конвенції про кіберзлочинність 2001 року, разом із тим визначення цього поняття в ній не надається [2, с. 65]. Основним актом, який оперує термінологією у сфері кіберзлочинності та надає визначення багатьох термінів є Закон України «Про основні засади забезпечення кібербезпеки України». Серед іншого, закон надає визначення «кіберзлочинності» як сукупності кіберзлочинів.

Саме ж поняття кіберзлочину трактується як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. При цьому, кіберзлочин фактично ототожнюється з комп'ютерним злочином, про що свідчить п. 8 ч. 1 ст. 1 закону – «кіберзлочин (комп'ютерний злочин)…» [3].

У цьому контексті, цілком погоджуємося із думкою, яку висловлює О. О. Загуменний. У своєму дослідженні він підкреслює, що поняття «кіберзлочин» та «комп'ютерний злочин» часто вживаються як синоніми, однак, на його переконання, ці терміни дуже близькі, але не синонімічні: поняття «кіберзлочину» ширше, ніж «комп'ютерний злочин», і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Кіберзлочини – це злочини,

що пов'язані як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «комп'ютерний злочин» в основному відноситься до злочинів, направлених проти комп'ютерів або комп'ютерних даних [4, с. 69]. Отож, вважаємо, що на законодавчому рівні терміни «кіберзлочин» та «комп'ютерний злочин» помилково ототожнені, що у подальшому ускладнює розробку кримінально-правових засобів протидії кіберзлочинності та їх застосування під час здійснення кримінально-правової кваліфікації. Схожа ситуація спостерігається і на міжнародному рівні: частина держав закріплює у законодавстві поняття «комп'ютерний злочин», а інша – «злочини щодо інформаційних мереж» [9, с. 9–10].

Дається взнаки також те, що у положеннях Кримінального кодексу України (далі – КК України) не міститься навіть згадки про таке поняття як «кіберзлочин», а в назві Розділу XVI цього ж акту міститься вказівка на комп'ютери, системи та комп'ютерні мережі і мережі електрозв'язку як основні об'єкти кіберзлочинів, що значно звужує сферу дії кримінально-правових норм, що у ньому містяться [5]. На противагу цьому, хочемо звернути увагу на назву Розділу 7.7. проєкту КК України – «Кримінальні правопорушення проти безпеки інформаційних систем». Як бачимо, у ньому законодавець оперує більш загальним поняттям «інформаційна система» і навіть надає його визначення [6].

Повертаючись до питання кримінально-правових засобів протидії кіберзлочинності, то по-перше, у період воєнного стану підлягають застосуванню положення КК України, які встановлюють відповідальність за кіберзлочини, зокрема, статті Розділ XVI КК України. Разом із тим чимало різновидів кіберзлочинності залишаються поза межами національно-правового регулювання. Для прикладу, наразі КК України закріплює дії, що схожі на фішинг – шахрайство, однак для того, щоб закріпити дієву норму, яка передбачатиме кримінальну відповідальність за цей вид кіберзлочину, необхідно внести відповідні зміни до КК України [5].

У зв'язку із цим, задля вдосконалення кримінально-правових засобів протидії кіберзлочинності перед нашої державою постає виклик належної імплементації міжнародних нормативно-правових актів. При цьому, складність такої імплементації полягає у тому, що замало формального перекладу українською мовою міжнародних нормативно-правових актів, оскільки він породжуватиме юридичний хаос, а з цього – невизначеність рефлексії у поведінці суб'єктів [7, с. 1303].

Варто також звернути увагу на те, що в умовах повномасштабного вторгнення на територію нашої держави, країна-агресор вдається до численних кібератак. У зв'язку із цим, законодавцем вже було внесено окремі зміни до КК України, серед яких: 1) посилення альтернативної санкції ч. 1 ст. 361-1 КК; 2) зміна формулювання предмету кримінального правопорушення ст. 361-1 КК України; 3) внесення змін до примітки до ст. 361 КК України щодо збільшення розміру значної шкоди, передбаченої в якості кваліфікуючої ознаки у ч. 2 ст. 361-1 КК України [5]. Ці зміни вже спричинили жваві наукові дискусії. Більшість науковців запевняють, що такі зміни не є доцільними та виваженими, а тому й очікування їх позитивного впливу на подолання проявів кіберзлочинності є марними [8, с. 413]. Для прикладу, внесення змін до примітки до ст. 361 КК України щодо збільшення розміру значної шкоди суттєво ускладнює кваліфікацію окремих кіберзлочинів, які за своєю правовою природою є матеріальними злочинами [10, с. 35].

Таким чином, з урахуванням вищевикладеного, варто зазначити про те, що на сьогодні кримінально-правові засоби протидії кіберзлочинності нашою державою розроблені не в повній мірі, а ті, що існують не характеризуються ефективністю та доцільністю. Окрім цього, дається взнаки недосконаліть термінологічного апарату у сфері кіберзлочинності на законодавчому рівні, що також ускладнює застосування кримінально-правових засобів протидії кіберзлочинності.

Література:

1. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право*. 2021. № 4(39). С. 129–134. URL: https://orcid.org/0000-0002-2059-2045

2. Думчиков М. О. Кримінально-правова характеристика поняття та видів кіберзлочинів. *Науковий вісник Міжнародного гуманітарного університету. Сер. : Юриспруденція*. 2022. № 55. С. 65–68. DOI: https://doi.org/10.32841/2307-1745.2022.55.14

3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. № 2163-VIII. Дата оновлення: 01.01.2024. URI: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Загуменний О. О. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини». *Процесуальне та техніко-криміналістичне забезпечення досудового розслідування: тези доп. всеукр. наук.-практ. конф. (м. Харків, 28 листоп. 2019 р.) / МВС України, Харків. нац. ун-т*

внутр. справ. Харків, 2019. С. 67–70. URI: http://dspace.univd.edu.ua/xmlui/handle/123456789/13566

5. Кримінальний кодекс України: Закон України від 5 квітня 2001 року. № 2341-III. Дата оновлення: 01.01.2024. URI: https://zakon.rada.gov.ua/laws/show/2341-14#Text

6. Текст проєкту КК України (редакція від 10.01.2024). URI: https://newcriminalcode.org.ua/criminal-code

7. Цимбалюк В. С. Кіберпростір як компонент національної безпеки: політико-правовий аспект : Scientific monograph. Riga. Latvia. Baltija Publishing. 2022. P. 1298–1305. DOI: https://doi.org/10.30525/978-9934-26-223-4-163

8. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал.* 2022. № 12. С. 409–414. URI: http://lsej.org.ua/12_2022/96.pdf

9. Катеринчук І. П. Кримінальна відповідальність за злочини у сфері комп'ютерних технологій: досвід зарубіжних країн. *Південно-український правничий часопис.* 2016. № 1. С. 7–10.

10. Васильєв А. А., Пашнєв Д. В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України.* 2013. № 5. С. 34–42.