УДК 343.31
DOI https://doi.org/10.32782/2524-0374/2022-12/96

# КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ, ВЧИНЕНІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ: МІЖНАРОДНІ ТЕНДЕНЦІЇ ТА УКРАЇНСЬКІ РЕАЛІЇ

# CRIMINAL LIABILITY FOR CYBERCRIMES COMMITTED AT THE TIME OF THE ARMED CONFLICT: INTERNATIONAL TENDENCIES AND UKRAINIAN REALITIES

**Юртаєва К.В., к.ю.н., доцент,**
**доцент кафедри кримінального права і кримінології факультету № 1**
*Харківський національний університет внутрішніх справ*
**Запрошений науковий співробітник Центру дипломатії Вайзера**
*Школа державної політики Дж. Форда Університету Мічигану*

У статті здійснено аналіз кримінальної відповідальності за кіберзлочини, вчинені під час збройного конфлікту, з врахуванням змін до КК України, внесених після 24 лютого 2022 року, та релевантних міжнародно-правових положень. Актуальність такого дослідження обумовлена зміною характеру й інтенсивності кіберзагроз під час збройної агресії Російської Федерації проти України. Здійснено детальний аналіз змін, внесених до ст. 361-1 КК України, та нової редакції ст. 361 КК України. Зроблено висновок про невиваженість змін, внесених до ст. 361 КК України: деякі положення в новій редакції значно ускладнили застосування цієї статті, інші – взагалі унеможливили дію її окремих частин. Переважна більшість зауважень стосується порушення правил законодавчої техніки, принципу юридичної визначеності та системності закону України про кримінальну відповідальність. Зроблено висновок, що внесення більшості змін до ст. 361 КК України не сприятиме підвищенню ефективності протидії кіберзлочинності в умовах дії воєнного стану та поліпшенню регулювання кримінальної відповідальності за акти кібераґресії, вчинені в умовах збройного конфлікту. З метою напрацювання позитивної правозастосовної практики щодо протидії кіберзлочинам, вчинених під час збройного конфлікту, пропонується здійснювати їх кваліфікацію статтями 113, 437 або 438 КК України в залежності від характеру та спрямованості вказаних протиправних посягань. Зазначені пропозиції здійснено з врахуванням передового світового досвіду в питанні кваліфікації кібероперацій, здійснюваних під час збройного конфлікту. Проаналізовано застосування норм міжнародного гуманітарного права до кібератак, спрямованих проти цивільних осіб і цивільних об'єктів. Наголошується, що безпрецедентні виклики в умовах розгортання гібридної війни проти України вимагають застосування проактивних підходів у забезпеченні кібербезпеки та врахування сучасного міжнародного досвіду в питаннях регулювання кримінальної відповідальності за кіберзлочини, вчинені під час збройних конфліктів. Робиться висновок про перспективність подальшого дослідження цього питання в межах вітчизняної доктрини кримінального права.

**Ключові слова:** кіберзлочини, кібераґресія, кримінальна відповідальність, збройний конфлікт, кібероперація, міжнародне гуманітарне право, гібридна війна.

The article analyses the issue of criminal liability for cybercrimes committed at the time of armed conflict considering amendments to the Criminal Code of Ukraine introduced after February, 24th 2022 and relevant international legal provisions. The relevance of the study is substantiated by the change of the character and severity of cyberthreats in the course of the Russian Federation aggression against Ukraine. The article provides detailed analyses of the amendments introduced to the Article 361-1 of the Criminal Code of Ukraine and a new version of the Article 361 of the Criminal Code of Ukraine. The conclusion is made about rashness of amendments introduced to the Article 361 of the Criminal Code of Ukraine: some of the newly introduced provisions render complexity to its application, some of its parts became completely inapplicable. Vast majority of the expressed criticisms concerns violation of the rules of legislative technique, the principle of legal certainty and consistency of the Ukrainian criminal law. The conclusion is made that majority of the amendments to the Article 361 of the Criminal Code of Ukraine will not increase efficiency in counteracting cybercrimes committed at the time of the armed conflict. To elaborate prospective law enforcement practice in counteracting cybercrimes committed at the time of the armed conflict the author suggests to qualify such actions under the Articles 113, 437 and 438 of the Criminal Code of Ukraine considering character and determination of the committed cybercrimes. The suggestions are supported by advanced international expertise in qualification of cyberoperations committed at the time of the armed conflict. The article analyses application of international humanitarian law to cyberattacks against civilians and civil objects. The article emphasizes unprecedented challenges posted to Ukraine by hybrid war that require proactive approaches to strengthening cybersecurity and considering relevant international experience in regulating criminal liability for cybercrimes committed at the time of the armed conflict. The conclusion is made about prospectiveness of further research of this issue within Ukrainian criminal law doctrine.

**Key words:** cybercrimes, cyberaggression, criminal liability, armed conflict, cyberoperation, international humanitarian law, hybrid law.

**Постановка проблеми.** Розпочату в лютому 2022 року збройну агресію Російської Федерації проти України все частіше називають війною нового типу. Цілком очевидно, що широкомасштабний наступ на незалежність України не обмежується посяганням лише на територіальну цілісність нашої держави. Агресія здійснюється одночасно на різних фронтах – політичному, дипломатичному, економічному, інформаційному тощо. Міжнародні експерти вже нарекли подібне цілеспрямоване поєднання різних військових форм, методів і тактик та стирання кордонів між ними на одному полі бою гібридної війною [1, p. 35–36]. Одним з вагомих компонентів гібридної війни проти України стала кібераґресія, розпочата за декілька років до повномасштабного вторгнення на територію України. Особливостями цілої серії кібератак проти України, починаючи з середини 2010-х років, можна назвати прицільне таргетування українських інформаційний ресурсів, широкий масштаб вказаних атак та їх спрямованість на державний сектор і державну інфраструктуру, застосування специфічних форм посягання, позбавлених корисливої мотивації, характерної для переважної більшості кіберзлочинів, атрибуція зазначених атак хакерським угрупуванням, асоційованих з владними структурами Російської Федерації, зокрема Головним розвідувальним управлянням [2, p. 7–8]. Вищевикладене свідчить про застосування Російською Федерацією цілеспрямованих кібератак як частини реалізації гібридних форм агресії проти України.

Український уряд, свідомий посилення кіберзагроз з боку країни-агресора, своєчасно врахував зазначені тенденції у протидії кіберпосяганням. Зокрема, у Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», прийнятій 26 серпня 2021 р., безпосередньо зазначено, що «Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосову-

ються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури» [3]. Відповідно до Плану реалізації Стратегії кібербезпеки, введеного в дію Указом Президента України від 1 лютого 2022 р. [4], вчасно вжиті заходи значною мірою забезпечили посилення кіберстійкості нашої держави, що дозволило загалом ефективно протидіяти кібератакам на державні інформаційно-комунікаційні ресурси. Іншою необхідною складовою протидії кіберзлочинам проти національної безпеки держави слід визначати належне регулювання кримінальної відповідальності за вказані посягання та напрацювання позитивної практики застосування відповідних кримінально-правових норм.

**Метою цієї статті** є аналіз кримінальної відповідальності за кіберзлочини, вчинені під час збройного конфлікту, з врахуванням змін до Кримінального кодексу України (далі – КК України), внесених після 24 лютого 2022 року, та актуальних міжнародно-правових положень щодо цього питання.

**Аналіз останніх досліджень і публікацій.** В Україні питання кримінальної відповідальності за кіберзлочини розглядаються в роботах цілої низки науковців. Серед них слід відзначити праці Д. С. Азарова, А. А. Васильєва, П. А. Воробея, О. О. Дудорова, О. О. Загуменного, М. В. Карчевського, О. О. Книженко, О. Г. Колба, В. К. Колпакова, Є. В. Лащука, М. І. Мельника, Р. О. Мовчана, А. А. Музики, С. О. Орлова, Д. В. Пашнєва, Н. А. Савінової, А. В. Савченка, М. І. Хавронюка, В. Г. Хахановского. Зміна характеру й інтенсивності кіберзагроз під час збройної агресії Російської Федерації проти України, а також внесення змін до відповідних статей КК України викликає необхідність проведення їх аналізу з врахуванням міжнародних тенденцій у кваліфікації кіберзлочинів, вчинених під час збройних конфліктів.

**Виклад основного матеріалу.** 24 березня 2022 року з метою посилення спроможності захисту нашої країни від постійних кібератак Верховною Радою України було внесено зміни до статей 361 і 361-1 КК України. Згідно Пояснювальної записки до проекту Закону України № 7182 від 20.03.2022 р. мотивуючим для його прийняття став той факт, що «формулювання окремих диспозицій статей Розділу XVI Кримінального кодексу України щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, зокрема статей 361, 361-1, не узгоджується з нормами Закону України від 16 грудня 2020 року № 1089-IX «Про електронні комунікації» й іншого законодавства України у сфері кібербезпеки, а також не забезпечує повноту і всебічність розслідування правоохоронними органами кримінальних правопорушень у відповідній сфері, а передбачені у статтях 361, 361-1 КК України санкції не є співмірними з тими наслідками, що завдаються державі та суспільству у результаті вчинення відповідних кримінальних правопорушень» [5]. Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 р. було запропоновано нову редакцію ст. 361 КК України та внесено зміни й доповнення до ст. 361-1 КК України [6]. Так, до ст. 361-1 КК України було внесено наступні зміни:

- було змінено формулювання предмету відповідного кримінального правопорушення (словосполучення «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку» було замінено на «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі»),

- при характеристиці мети відповідного правопорушення було додано вказівку на протиправність зазначених дій, що фактично звужує застосування цієї норми та легалізує непротиправне (передбачене законом) застосування шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;

- була дещо посилена альтернативна санкція ч. 1 ст. 361-1 КК (максимальний строк позбавлення волі було збільшено з двох до трьох років);

- шляхом внесення змін до примітки до ст. 361 КК України було збільшено розмір значної шкоди, передбаченої в якості кваліфікуючої ознаки у ч. 2 ст. 361-1 КК України.

Вищевказані зміни до ст. 361-1 КК України не викликають значних заперечень, а їх ефективність ще має бути перевірна часом і правозастосовною практикою. Порівняно зі ст. 361-1 КК України, стаття ст. 361 КК України зазнала кардинальних змін, які вже викликали жваву дискусію в науковому та експертному середовищі. У зв'язку з цим докладно зупинимся саме на аналізі цієї норми.

Так, по-перше, у багатьох експертів викликає занепокоєння надмірне посилення відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що не потягло за собою суспільно небезпечних наслідків (ч. 1 ст. 361 КК України в новій редакції). Наприклад, М. І. Хавронюк зазначає, що саме по собі несанкціоноване втручання в роботу згаданих систем чи мереж не є кримінальним правопорушенням, оскільки не створює жодних наслідків, які можна було б охопити поняттям істотної шкоди. При цьому науковець наводить приклад, в якому колега по роботі бажає подивитися новини з використанням персонального комп'ютера іншого працівника, поки свій в ремонті, включає його і робить пошук на сайтах [7]. Про недоцільність криміналізації безнаслідкового доступу до комп'ютерної системи раніше висловлювалися й інші науковці [8, с. 72]. Частково погоджуючись з аргументами М. І. Хавронюка, Р. О. Мовчан, на нашу думку, цілком слушно вказує на міжнародні зобов'язання України щодо криміналізації побідних діянь та позитивний досвід іноземних в цьому питанні [9, с. 160-161]. Так, у ст. 2 Конвенції про кіберзлочинність 2001 р., ратифікованій Україною ще у 2005 р., передбачається зобов'язання країн встановити кримінальну відповідальність за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. При цьому, як зазначається у ст. 2 Конвенції про кіберзлочинність, сторони можуть вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою [10]. При ратифікації Конвенції про кіберзлочинність Україна не зробила жодних застережень з приводу вказаного положення (хоча застереження щодо інших положень й були висловлені законодавцем [11]), тому криміналізацію несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж у чинній редакції ч. 1 ст. 361 КК України вважаємо запізнілим виконанням Україною своїх міжнародних зобов'язань. Також необхідно звернути увагу, що ст. 361 КК України криміналізує не доступ до комп'ютерної інформації, а несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Зазначене втручання має деструктивний характер і полягає у зміні режиму роботи вищевказаних систем і мереж. Вбачається, що ознайомлення з інформацією, яка зберігається,

обробляється чи передається в інформаційних (автоматизованих) системах, шляхом здійснення незаконного доступу до неї має у відповідних випадках бути кваліфіковано за ст. 212-6 Кодексу України про адміністративні правопорушення «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем», що є не кримінальним правопорушенням і, відповідно, не має суспільної небезпечності. Якщо щодо інформації, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, було встановлено передбачену чинним законодавством комплексну систему захисту і щодо такої інформації здійснено несанкціоновані дії у виді її збуту чи розповсюдження, то лише за таких умов вказані діяння набувають суспільної небезпечності і тягнуть за собою кримінальну відповідальність за ст. 361-2 КК України.

Аналіз наступних частин ст. 361 КК України справедливо викликає критику та обурення значної кількості дослідників. Переважна більшість зауважень стосується порушення правил законодавчої техніки, принципу юридичної визначеності та системності закону України про кримінальну відповідальність, на що справедливо звертають увагу науковці [7; 9]. Зокрема, у ч. 4 ст. 361 КК України встановлена відповідальність за дії, передбачені ч. 1 або ч. 2 цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, хоча склади, передбачені в ч. 1 і ч. 2 сформульовані як формальні, і, відповідно, не можуть заподіяти значної шкоди або навість створити реальну, а не потенційну небезпеку заподіяння тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Очевидно, що законодавець у ч. 4 ст. 361 КК України мав зробити посилання на ч. 4 цієї статті, яка передбачає настання суспільно небезпечних наслідків у виді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Зазначена законодавча помилка фактично робить неможливим застосування ч. 4 ст. 361 КК України і може бути усунена лише шляхом внесення наступних змін до цієї статті.

Як показує практика, побідні законодавчі помилки можуть «жити» у КК України роками, створюючи непереборні перешкоди для правозастосувачів і нові приводи для наукових дискусій. На жаль, законодавець прагне не помічати вже зроблені відверті промахи та взагалі не квапитися з їх виправленням, залишаючи їх на відкуп судовій інстанції. Так, наприклад, скоріш за все через суто технічну помилку при внесенні доповнень до ч. 2 ст. 49 КК України щодо підстав зупинення перебігу давності за кримінальні проступки [12] законодавець значно ускладнив розуміння та застосування вказаної норми, що через декілька років змусило Верховний Суд вирішити вказану виключну правову проблему шляхом судового тлумачення [13]. У цьому зв'язку пропозиція авторів Нового Кримінального кодексу України щодо внесення змін до нього не частіше одного разу протягом однієї сесії Верховної Ради України, крім випадків скасування кримінальної відповідальності за діяння або поліпшення правового статусу особи, яка вчинила кримінальне правопорушення (ст. 1.1.3) [14], виглядає цілком логічною з точки зору забезпечення стабільності кримінального закону, проте з іншого боку, враховуючи низький рівень української законотворчості, може взагалі заблокувати можливість виправлення подібних прикрих законодавчих помилок у найкоротший строк.

Продовжуючи аналіз ст. 361 КК України, не можна не звернути увагу на встановлення нової особливо кваліфікуючої ознаки в ч. 5 ст. 361 КК України у виді вчинення дії, передбаченої ч. 3 або ч. 4 цієї статті під час дії воєнного стану. Внесення подібних доповнень до інших статей КК України, зокрема злочинів проти національної безпеки України та кримінальних правопорушень проти власності, прискорило напрацювання певних наукових та правозастосовних підходів щодо вказаних норм. Як вказують фахівці, суди активно застосовують норми, що передбачають кваліфікуючу ознаку «вчинення під час дії воєнного стану» абсолютно недиференційовано до змісту відповідних кримінальних правопорушень, тобто без врахування факту їх зв'язку з воєнним станом або військовою агресією проти нашої держави [15, с. 313]. Буквальне тлумачення ч. 5 ст. 361 КК України призводить до аналогічних висновків, що формує абсурдну ситуацію, коли за будь-яке втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, яке потягло, передбачені в ч. 3 ст. 361 КК України наслідки, вчинене поза всяким зв'язком зі збройним конфліктом, передбачено безпідставно суворе покарання у виді позбавленням волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. Зазначимо, що в попередній редакції аналізованої статті (ч. 1 ст. 361 КК України в редакції до 24.03.2022 р.) аналогічні дії вважалися нетяжким злочином. Вбачається, що відсутність можливості диференціації відповідальності за вказані діяння підриває фундамент засад правосуддя: надвисока латентність кіберзлочинів з великою вірогідністю призведе до застосування суворих покарань до «рядових» правопорушників, залишаючи більш небезпечних та професійних кіберзлочинців, яких значно важче виявити і на яких фактично й спрямоване посилення відповідальності в ч. 5 ст. 361 КК України, без справедливого покарання.

Аналізуючи аналогічні зміни до кримінальних правопорушень проти власності, Р. О. Мовчан пропонує замінити формулювання відповідної кваліфікуючої обставини зі вчинення «в умовах воєнного або надзвичайного стану» на «використання умов воєнного або надзвичайного стану» [16, с. 285]. Слід зазначити, що подібний підхід використовується і під час формулювання військових злочинів на міжнародному рівні. Так, зокрема, в Елементах злочинів, які доповнюють Статут Міжнародного Кримінального Суду та встановлюють орієнтири щодо інтерпретації та застосування статей 6-8 Статуту, зазначається, що у всіх військових злочинах, передбачених ст. 8 Статуту має бути доведено, що діяння відбувалося в контексті або було асоційовано з міжнародним збройним конфліктом [17]. Враховуючи вищевикладене, вбачається, що застосування особливо кваліфікуючої ознаки, передбаченої ч. 5 ст. 361 КК України, без зв'язку кіберзлочину з військовим конфліктом є недоречним.

У цьому зв'язку слушною вбачається пропозиція Р. О. Мовчана, який пропонує кваліфікувати кібератаки Російської Федерації як одну з форм диверсії. Учений зазначає, що згадані у ч. 4 ст. 361 КК України потенційні наслідки у вигляді «тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків» фактично повністю охоплюються тими наслідками, з метою спричинення яких і вчиняється диверсія, передбачена ст. 113 КК України. Р. О. Мовчан пропонує за умови відсутності обставин воєнного стану подібні кібератаки кваліфікувати за сукупністю ч. 1, ч. 2 або ч. 3 ст. 361 та ч. 1 ст. 113 КК України, а за умов вчинення в умовах воєнного стану – за сукупністю ч. 5 ст. 361 КК України та ч. 2 ст. 113 КК України [18, с. 206]. У цілому підтримуючи позицію автора, хотілося зазначити, що нами ще до початку широкомасш-

табної збройної агресії Російської Федерації проти України також висловлювалася думка про доцільність кваліфікації «кібердиверсій» і «кібертероризму» за статтями 113 і 258 КК України відповідно. Указані кримінальні правопорушення в запропонованій класифікації кіберзлочинів, передбачених у КК України, було віднесено до спеціальних норм, які виділяються за наявністю спеціальної цілі посягання [19, с. 188]. При цьому, на наше переконання, кваліфікації випадків «кібердиверсій» за сукупністю зі ст. 361 КК України є зайвою, оскільки диспозиції ст. 113 КК України не встановлюють вичерпного переліку діянь, спрямованих на ослаблення держави. Окрім того, нагадаємо, що відповідно до п. 11 Постанови Пленуму Верховного Суду України «Про практику застосування судами кримінального законодавства про повторність, сукупність і рецидив злочинів та їх правові наслідки» від 04.06.2010 р. №7, якщо у складі злочину передбачене діяння, яке у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання про його кримінально-правову оцінку необхідно вирішувати з урахуванням того, наскільки охоплюється складом цього злочину таке діяння, а також з урахуванням змісту санкцій відповідних статей (частин статей) Особливої частини КК [20]. Оскільки, як зазначалося вище, формулювання поняття диверсії фактично охоплює випадки несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення або на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій, та той факт, що покарання за діяння передбачене ч. 2 ст. 113 КК України є більш суворим, ніж санкція ч. 5 ст. 361 КК України, кваліфікацію за сукупністю з останньою статтею вважаємо зайвою. Застосовуючи аналогічну аргументацію та враховуючи посилення відповідальності за ст. 361 КК України, вважаємо, що випадки «кібертероризму», вчинені в умовах воєнного стану, вимагають кваліфікації за сукупністю відповідної частини ст. 258 та ч. 5 ст. 361 КК України. Якщо випадки «кібертероризму» вчинені поза дією воєнного стану, останні, за загальним правилом, охоплюються ст. 258 КК України.

Іншою важливою тенденцією кваліфікації кібератак в умовах збройних конфліктів є віднесення їх до однієї з форм порушення законів та звичаїв війни. Як відомо, диспозиція ст. 438 КК України є частково бланкетною та не містить вичерпного переліку порушень законів та звичаїв війни. Для з'ясування змісту цього поняття необхідно звертатися до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. До них, зокрема, відносять Женевські конвенції, які на міжнародному рівні закріпили норми щодо гуманного поводження з військовополоненими, захисту цивільного населення та цивільних об'єктів під час війни та захисту жертв міжнародних збройних конфліктів. Залежність критичної інфраструктури від сучасних інформаційно-телекомунікаційних технологій роблять подібні об'єкти бажаною мішенню кібератак. Наслідки кібератак виходять за межі кіберпростору і можуть полягати у фізичному руйнуванні певних об'єктів, заподіянні тілесних ушкоджень або навіть смерті людей. На жаль, ми стаємо свідками того, що тактика цілеспрямованих атак на цивільні об'єкти стає невід'ємним компонентом сучасних збройних конфліктів. Порушення такими діями норм Женевських конвенцій піднімає питання про можливість застосування норм міжнародного гуманітарного права до актів кіберагресії.

Сьогодні міжнародні експерти загалом підтримують позицію, що норми міжнародного права можуть і навіть мають бути застосовані до військових операцій у кіберпросторі, в тому числі й в ситуаціях збройних конфліктів [21; 22]. При чому застосування норм міжнародного гуманітарного права можливе не лише за умови реального настання відповідних наслідків, а й у випадку спрямування кібератаки на заподіяння тяжкої шкоди цивільним об'єктам. Так, Міжнародний комітет Червоного Хреста зазначає, що кібероперація, спрямована на припинення функціонування комп'ютеру або комп'ютерної мережі під час збройного конфлікту підпадає під поняття атаки в розумінні міжнародного гуманітарного права, незалежно від того, чи було припинено функціонування об'єкту шляхом його руйнування чи будь-яким іншим шляхом [23]. Враховуючи значний розвиток інформаційно-комунікаційних технологій та у відповідь на кібератаки Російської Федерації проти України, керівництво НАТО також висловило позицію, що у випадку особливо тяжких наслідків кібератака може прирівнюватися до збройної атаки і викликати право на самооборону відповідно до ст. 5 Статуту НАТО [24]. Враховуючи вищезазначені міжнародні тенденції щодо правової оцінки кібератак, вчинених під час збройних конфліктів, вважаємо, на часі розглянути можливість кваліфікації відповідних діянь як порушення законів та звичаїв війни або за наявністю відповідних ознак як акту збройної агресії. Відповідальність за вказані діяння передбачена у статтях 438 і 437 КК України відповідно. Застосування такого підходу дозволить відмежувати загальнокримінальні кіберзлочини, не пов'язані зі збройним конфліктом, від кіберпосягань як компоненту збройної агресії проти України та її цивільного населення та врахувати більш високу суспільну безпечність останніх. Наразі зазначені тенденції правої оцінки кібератак поки що не закріплені у нормах «міжнародного твердого права», а викристалізовуються шляхом тлумачення загальновизнаних норм міжнародного гуманітарного права, у резолюціях Генеральної Асамблеї ООН та асоційованих з нею організацій. Проте, як відомо, «м'яке» право здатне скоротити шляхи і готує сприятливий ґрунт для успішного розвитку загальновизнаних норм міжнародного права.

Закінчуючи аналіз змін, внесених до ст. 361 КК України, слід звернути увагу на закріплення нової спеціальної обставини, що виключає кримінальну відповідальність, у ч. 6 ст. 361 КК України. При цьому падає в очі чергова законодавча помилка, яка полягає у невключенні до підстав застосування ч. 6 ст. 361 КК України вчинення відповідних дій під час дії воєнного стану (ч. 5 ст. 361 КК України). На цей недолік нової редакції ст. 361 КК України вже звертали увагу вітчизняні науковці [18, с. 200]. Слід зазначити, що таке формулювання ч. 6 ст. 361 КК України формально не позбавляє можливості її застосовування щодо діянь, вчинених в умовах збройного конфлікту. Водночас виникає інше питання про наявність самого порядку пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, на який посилається вказана норма, а також щодо порядку і можливості його застосування стосовно приватних комп'ютерних мереж. Необхідність розробити та забезпечити введення в дію зазначеного Порядку у місячний строк після внесення відповідних змін до ст. 361 КК України, було передбачено у Перехідних положеннях Закону України № 2149-IX від 24.03.2022 р. [6] Також слід зауважити, що в іноземних юрисдикціях діяльність «білих» хакерів здійснюється за пропозицією та в порядку процедури баг-баунті, яку встановлюють самі компанії, зокрема, такі цифрові гіганти, як Apple, Android, Goldman Sachs [25]. В Україні відповідно до Проекту Плану відновлення України, розробленого Національною радою з відновлення України від наслідків війни, Кабінет Міністрів України мав ухвалити Постанову «Про затвердження Порядку пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих),

електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж на підставі публічної пропозиції (оферти)». Проте оскільки вказаний Порядок й досі не було затверджено, проаналізувати його зміст та особливості застосування немає можливості. Відсутність затвердженого нормативного Порядку наразі унеможливлює застосування ч. 6 ст. 361 КК України.

Останнє, на що хотілося б звернути увагу під час аналізу нової редакції ст. 361 КК України, це зміна формулювання поняття значної шкоди у примітці до цієї статті. З одного боку можна погодитися з позицію авторів, які наголошують на невиправдане виключення наслідків нематеріального характеру з формулювання значної шкоди в примітці до ст. 361 КК України [9, с. 165]. З іншого, вбачається, доцільним взяти до уваги системне виключення законодавцем наслідків нематеріального характеру при визначенні змісту значної шкоди у нормах КК України та прив'язка оцінки значної шкоди до певної суми, обчислювальної зазвичай у неоподаткованих мінімумах доходів громадян. Тому зміни у формулюванні поняття значної шкоди в примітці до ст. 361 КК України у цілому слід визнати слушними. Що стосується збільшення розміру значної шкоди у три рази до трьохсот неоподатковуваних мінімумів доходів громадян, то таке занадто надмірне підняття порогу кримінальної відповідальності вбачається невиваженим. Окрім того, як слушно зазначає М. І. Хавронюк, внесення вказаних змін призведе до необхідності перегляду значної кількості вже винесених судами вироків відповідно до ч. 3 ст. 74 КК України [7]. У цьому зв'язку також слід підтримати пропозицію Р. О. Мовчана щодо необхідності передбачити кваліфікуючі ознаки у виді заподіяння значної шкоди та у виді створення небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків у різних частинах ст. 361 КК України, що дозволить диференціювати кримінальну відповідальність за їх вчинення [9, с. 164–165].

**Висновки та перспективи подальших досліджень.** Аналіз змін, внесених до КК України Законом України № 2149-IX від 24.03.2022 р. з метою підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану, у цілому призводить до висновку про їх невиваженість. Доведено, що деякі положення ст. 361 КК України в новій редакції значно ускладнили її застосування, інші – взагалі унеможливили дію її окремих частин. У цілому внесення більшості змін до ст. 361 КК України не сприятиме підвищенню ефективності протидії кіберзлочинності в умовах дії воєнного стану та поліпшенню регулювання кримінальної відповідальності за акти кібераґресії, вчинені в умовах збройного конфлікту. З метою належного регулювання кримінальної відповідальності за кібератаки, вчинені під час і у зв'язку зі збройним конфліктом, та вжиття кримінально-правових заходів, що відповідають їх суспільній небезпечності, пропонується здійснювати кваліфікацію подібних діянь за статтями 113, 437 або 438 КК України в залежності від характеру та спрямованості вказаних протиправних посягань. Зазначені пропозиції здійснено з врахуванням передового світового досвіду в цьому питанні та релевантних міжнародно-правових положень. При напрацюванні відповідної правозастосовної практики на національному рівні слід враховувати, що сьогодні наша країна зіштовхується з безпрецедентними викликами у сфері кібербезпеки. Їх подолання безпосередньо залежить від застосування проактивних підходів та врахування сучасного міжнародного досвіду, в тому числі й щодо питань регулювання кримінальної відповідальності за кіберзлочини, вчинені під час збройних конфліктів. Саме тому подальше дослідження цього питання в межах вітчизняної доктрини кримінального права вважаємо вельми перспективним.

**ЛІТЕРАТУРА**


1. Frank G. H. Hybrid Warfare and Challenges. *Joint Forces*. 2009. Quarterly 52. P. 34–39.
2. Yurtayeva K. V. Cyberaggression as a Component of Hybrid War Against Ukraine. *Humanitarian Aspects of Digital Society: PPSS RI (Dec. 8, 2022, Kharkiv, Ukraine)*, P. 6-9. https://doi.org/10.5281/zenodo.7437734
3. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 01.12.2022).
4. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30.12.2021 р. Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 01.12.2022).
5. Пояснювальна записка до проекту Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану». URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1247132 (дата звернення: 01.12.2022).
6. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: закон України № 2149-IX від 24.03.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2149-IX#Text (дата звернення: 01.12.2022).
7. Хавронюк М. Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1247132 (дата звернення: 01.12.2022).
8. Карчевський М. В. Питання опимізації зобов'язань, зумовлених ратифікацією Конвенції про кіберзлочинність. *Бюлетень Міністерства юстиції України*. 2012. № 3. С. 70–80.
9. Мовчан Р. О. Проблеми кваліфікації та розслідування кримінальних правопорушень в умовах воєнного стану : матеріали наук.-теорет. конф. (Київ, 26 трав. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 159–165.
10. Конвенція про кіберзлочинність 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 01.12.2022).
11. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/card/2824-15 (дата звернення: 01.12.2022).
12. Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень: Закон України від 22.11.2018 р. № 2617-VIII. URL: https://zakon.rada.gov.ua/laws/show/2617-19#n141 (дата звернення: 01.12.2022).
13. Щодо обчислення строків давності притягнення особи до кримінальної відповідальності: ч. 2 ст. 49 КК. URL: https://advokatpost.com/shchodo-obchyslennia-strokiv-davnosti-prytiahnennia-osoby-do-kryminalnoi-vidpovidalnosti-ch-2-st-49-kk/ (дата звернення: 01.12.2022).
14. Текст проєкту нового Кримінального кодексу України станом на 29.09.2022 р. URL: https://newcriminalcode.org.ua/upload/media/2022/09/29/1-kontrolnyj-tekst-proektu-kk-29-09-2022.pdf (дата звернення: 01.12.2022).
15. Вознюк А. А. Воєнний та надзвичайний стан як обставини, що впливають на кваліфікацію кримінального правопорушення або призначення покарання. *Юридичний науковий електронний журнал*. 2022, № 6. С. 308–317.
16. Мовчан Р. О. Аналіз законодавчого рішення про посилення кримінальної відповідальності за мародерство. *Аналітично-порівняльне правознавство. Електронне наукове видання*. 2022. № 1. С. 281–285.
17. Elements of Crimes. URL: https://www.icc-cpi.int/sites/default/files/ Publications/Elements-of-Crimes.pdf (дата звернення: 01.12.2022).
18. Новели кримінального законодавства України, прийняті в умовах воєнного стану : наук.-практ. комент. / А. А. Вознюк, О. О. Дудоров, Р. О. Мовчан, С. С. Чернявський та ін. ; за ред. А. А. Вознюка, Р. О. Мовчана, В. В. Чернєя. Київ : Норма права. 2022. 278 с.

19. Юртаева К. В. Киберпреступления в Уголовном кодексе Украины: виды и проблемы квалификации. *Предупреждение современной преступности (киберпреступность)* : материалы Международной научно-практической конференции, посвященной 30-летию Независимости Республики Казахстан. Караганда, Карагандинская академія МВД РК имени Б. Бейсенова. С. 185–191.

20. Про практику застосування судами кримінального законодавства про повторність, сукупність і рецидив злочинів та їх правові наслідки : Постанова Пленуму Верховного Суду України від 04.06.2010 № 7. URL: https://www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf (дата звернення: 01.12.2022).

21. Schmitt M. N. Tallin Manual 2.0 on the International Law Applicable to Cyber Operation. Cambridge. 2017. 648 p.

22. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly on 23 December 2015. A/RES/70/237. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement (дата звернення: 01.12.2022).

23. Gisel L., Rodenhäuser T., Dörmann K. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*. 2020. №102 (913). P. 287-334.

24. Banks W. Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation. *Georgetown Journal of International Affairs*. URL: https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%ef%bf%bc/ (дата звернення: 01.12.2022).

25. Секрети кібербезпеки: важливість баг баунті програм для бізнесу. Секрети кібербезпеки: важливість баг баунті програм для бізнесу. *Європейська Бізнес Асоціація* : веб-сайт. URL: https://eba.com.ua/sekrety-kiberbezpeky-vazhlyvist-bag-baunti-program-dlya-biznesu/ (дата звернення: 01.12.2022).