**DOI: 10.33663/1563-3349-2022-33-488-497**
УДК 343.34:004.087

***В. Н. КУБАЛЬСЬКИЙ,***
*кандидат юридичних наук, доцент**
**ORCID: 0000-0001-6127-5786**

# ПРОБЛЕМИ КРИМІНАЛІЗАЦІЇ КІБЕРТЕРОРИСТИЧНИХ ПОСЯГАНЬ

*Стаття присвячена питанням криміналізації актів кібертероризму. Проаналізовано пропозиції вчених, а також законопроєкти, спрямовані на криміналізацію актів кібертероризму. Запропоновано шляхи удосконалення кримінально-правової протидії актам кібертероризму в Україні. Автор обґрунтовує та пропонує внести зміни до положень чинного Кримінального кодексу України та проєкту нового Кримінального кодексу України (у редакції станом на 24 грудня 2021 р.).*

***Ключові слова:*** *криміналізація, кібертероризм, акт кібертероризму, кіберпростір.*

***Kubalskiy Vladyslav.*** **Problems of criminalization of cyberterrorist encroachments**

*The article deals with the criminalization of acts of cyberterrorism. The proposals of scientists, as well as draft laws aimed at criminalizing acts of cyberterrorism are analyzed. Ways to improve the criminal law response to acts of cyberterrorism in Ukraine are proposed. The author substantiates and proposes amendments to the provisions of the current Criminal Code of Ukraine and the draft of the new Criminal Code of Ukraine (as amended on December 24, 2021).*

***Key words:*** *criminalization, cyberterrorism, act of cyberterrorism, cyberspace.*

**Вступ.** Розвиток інформаційних технологій і процес глобалізації зумовили появу нових загроз як міжнародній, так і національній безпеці, зокрема кібертероризму[1]. Аналізуючи проблеми світових загроз, колишній директор ЦРУ США Джордж Тенет свого часу наголошував, що кібертероризм у світі стрімко набуває неочікувано великих масштабів і зрештою стає реальною загрозою для національної безпеки будь-якої держави[2]. Досвід, який вже є у світової спільноти в цій сфері, з усією очевидністю свідчить про безперечну вразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів, кібертерорист здатний однаково загрожувати інформаційним системам, розташованим у будь-якому місці земної кулі[3].

Парадоксально, але успіх у «війні з терором», на думку Г. Веймана, змусить терористів частіше звертатися до нетрадиційних видів зброї, серед

* ***Kubalskiy Vladyslav****, Candidate of Juridical Sciences (Ph. D.), Docent*

яких – кібертероризм[4], який є привабливим для сучасних терористів з багатьох причин. У колективній монографії «Світова гібридна війна: український фронт», підготовленій фахівцями Національного інституту стратегічних досліджень, звертається увага на те, що терористичні організації широко використовують сучасні засоби зв'язку, Інтернет та інші новітні технології (криптозв'язок, системи глобального позиціонування тощо) для рекрутування, консолідації, координації дій, обміну інформацією, навчання, поширення пропагандистських матеріалів, безпосереднього вчинення терактів. У всьому світі зростає кібертероризм, відчутнішими стають його наслідки для національної і міжнародної безпеки. Дедалі частішими стають DDoS атаки на сайти урядів (у т. ч. США, Канади, Південної Кореї, Ізраїлю, Естонії та ін.), державних і приватних компаній (NASA, Delta Air, Dell, Yahoo, Amazon, E- bay, Sony та CNN), міжнародних організацій (ООН, МОК)[5].

Згідно з абзацом 2 п. 3 Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 р., до загроз кібербезпеці України належить, зокрема, використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності. В абзаці 5 п. 1 цієї Стратегії визначено, що РФ залишається одним з основних джерел загроз національній і міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури. Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо (абзаци 5 та 8 п. 1 Стратегії)[6].

**Стан дослідження.** Різноманітні аспекти кібертероризму як явища досліджувались українськими вченими-юристами, такими як Д. С. Азаров, Ю. Р. Акчурін, Р. О. Банк, О. В. Бойченко, С. А. Буяджи, Л. Ю. Веселова, С. Б. Гавриш, К. С. Герасименко, О. С. Геращенко, О. О. Грицун, М. В. Гуцалюк, В. О. Голубєв, О. Д. Довгань, І. М. Дронін, М. В. Карчевський, Ю. І. Когут, О. Є. Користін, Б. В. Кузьменко, С. Є. Кучерина, В. А. Ліпкан, Б. Д. Леонов, С. Я. Лихова, Д. О. Олєйніков, О. О. Ончурова, В. А. Трофименко, О. Г. Широкова-Мурараш та ін. Проте вчені не приділяли належної уваги у своїх працях питанням криміналізації кібертерористичних посягань.

**Постановка проблеми.** Терористична діяльність у кіберпросторі в умовах глобалізації та поширеного використання інформаційно-комунікаційних технологій становить серйозну загрозу для безпеки будь-якої держави та зумовлює необхідність протидії зазначеному явищу. Неможливо належно

протидіяти проявам кібертероризму (в науковій літературі його іноді називають «електронний», «інформаційний», «комп'ютерний» тероризм) як нового різновиду тероризму без розуміння його сутності, сучасних форм та тенденцій розвитку цього явища.

Метою дослідження є визначення основних шляхів удосконалення кримінального законодавства України у сфері протидії кібертероризму.

**Виклад основного матеріалу.** На сьогодні вектор правового регулювання боротьби із кіберзлочинністю пов'язується із протидією кібертероризму як найнебезпечнішого вияву кіберзлочинності[7]. Кібертероризм – це терористична діяльність, що здійснюється у кіберпросторі або з його використанням (п. 13 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р.).

Вчені звертають увагу на те, що на відміну від звичайного терориста, який для досягнення своїх цілей використовує вибухівку або стрілецьку зброю, кібертерорист використовує для досягнення своїх цілей сучасні інформаційні технології, комп'ютерні системи і мережі, спеціальне програмне забезпечення, призначене для несанкціонованого проникнення в комп'ютерні системи й організації дистанційної атаки на інформаційні ресурси об'єкта нападу[8].

На думку фахівців, метою державних і військових кібероперацій, спонсорованих Росією, є підтримка стратегічних політичних цілей Росії. Це може бути внесення хаосу в американську політичну систему, підрив суверенітету України, демонстрація України в негативному світлі для світу, як у 2017 р. з кібератакою NotPetya[9].

За наявною інформацією Служби безпеки України, хакерське угруповання «Armagedon» як спеціальний проєкт ФСБ Росії здійснило понад 5 тисяч кібератак і намагалося «заразити» понад півтори тисячі урядових комп'ютерних систем. Основними цілями зловмисників були:

– контроль над об'єктами критичної інфраструктури (електростанції, системи тепло- та водопостачання);

– викрадення та збір розвідувальних даних, у тому числі інформації з обмеженим доступом (сектор безпеки та оборони; державні установи);

– проведення акцій інформаційно-психологічного впливу;

– блокування інформаційних систем[10].

З повідомлень у ЗМІ відомо про наявну небезпеку терористичних кібератак на інформаційні мережі державних структур та приватних компаній, пов'язаних із керуванням об'єктами антикризової інфраструктури. При кваліфікації наведених діянь як терористичних необхідно враховувати положення ратифікованих Україною міжнародних антитерористичних угод, згідно з якими терористичні злочини – це суспільно небезпечні діяння, які вчиняються з метою досягнення терористичних цілей. Під останніми розуміються цілі залякування населення з метою здійснення впливу на прийняття рішень органами державної влади або міжнародними організаціями.

Однією з необхідних умов дієвості вжитих заходів у сфері протидії кібертероризму є криміналізація в усіх державах хоча б мінімального набору протиправних діянь, що вчиняються за допомогою ІТ-технологій[11]. Криміналізація суспільно небезпечних діянь у сфері кібертероризму сприятиме, на нашу думку, більш ефективній протидії цьому небезпечному явищу.

У кримінально-правовій літературі переважно наводяться дві групи принципів – критеріїв кримінально-правової заборони діяння. Перша: соціальні та соціально-психологічні, які виражають суспільну необхідність і політичну доцільність встановлення й існування кримінальної відповідальності за те чи інше посягання. До них відносять: суспільну небезпеку діяння як необхідну умову криміналізації; відносну його поширеність; співрозмірність позитивних і негативних наслідків криміналізації; неможливість подолання даного правопорушення без застосування кримінально-правових заходів[12]. Підтверджуючи позицію з приводу необхідності законодавчого врегулювання кримінальної відповідальності за кібертерористичний акт, зауважимо, що запропонована ідея відповідає підставам та критеріям криміналізації, які розроблені у кримінально-правовій науці.

У пояснювальній записці до проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» (реєстр. № 2439а від 24 липня 2015 р.) вказується, що у сьогоднішньому стані підвищеної зовнішньої небезпеки дуже важливо законодавчо визначити поняття кібертероризму й встановити сурову кримінальну відповідальність за вчинення актів кібертероризму, які можуть бути вчинені з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокацій військового конфлікту та спрямовані на підрив національних інтересів й національної безпеки[13].

Вчені в Україні доводять необхідність криміналізації дій, пов'язаних з вчиненням кібертерористичних атак[14]. На нашу думку, відповідальність у таких випадках повинна наставати за конкретні акти кібертероризму як прояви цього явища. У зв'язку з цим невдалою є назва ст. 2586 «Кібертероризм» проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» (реєстр. № 2439а від 24 липня 2015 р.), якою пропонувалось доповнити КК України. Частину першу цієї статті пропонувалось викласти у такій редакції: «Кібертероризм, тобто умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків, якщо такі дії були скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту, – карається…»[15].

В іншому проєкті Закону про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини) (реєстр. № 2328а від 10 липня 2015 р.) ч. 2 ст. 258 КК України пропону-

валось викласти у новій редакції: «Ті самі дії, вчинені повторно або за попередньою змовою групою осіб або якщо вони пов'язані з несанкціонованим втручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку об'єкта підвищеної небезпеки або якщо вони призвели до заподіяння значної майнової шкоди чи інших тяжких наслідків, – караються…»[16].

На думку вченого-юриста Р. О. Банка, доцільно доповнити КК України ст. 2586 «Інформаційний терористичний акт: інформаційний терористичний акт, тобто дії інформаційно-психологічного та інформаційно-технічного впливу, спрямовані на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктних ситуацій з метою маніпуляції та зомбіювання свідомості особи чи широкого кола осіб шляхом реалізації способів і методів інформаційного насильства, застосування інформаційної зброї, – караються…»[17].

Д. С. Азаров зазначає, що можливі ситуації, коли злочини у сфері комп'ютерної інформації необхідно кваліфікувати за сукупністю з іншими посяганнями. Саме таку кримінально-правову оцінку, на його думку, мають дістати втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж з метою вчинення терористичного акту[18]. У цьому контексті, на його думку, видаються недоцільними пропозиції окремих дослідників щодо створення кримінально-правової норми про відповідальність за кібернетичний тероризм – «руйнування комп'ютерних систем та дестабілізація кібернетичного простору, які спрямовані на підрив атмосфери спокою, на залякування чи пригнічення суспільства з метою вплинути на прийняття державою, міжнародною організацією, фізичною чи юридичною особою будь-якого рішення чи утримання від нього»[19]. Наведена дефініція, на думку Д. С. Азарова, має певні вади логічного та термінологічного характеру (діяння у вигляді «руйнування комп'ютерних систем» за змістом повністю охоплюється ст. 258 КК України «Терористичний акт»; термінологічний зворот «дестабілізація кібернетичного простору» є надто неконкретним; поняття «тероризм» швидше характеризує злочинність і тому належить до кримінологічних, а не до кримінально-правових понять). Окрім того, вона фактично враховує ідеальну сукупність злочинів, оскільки охоплює два діяння, кожне з яких при окремому аналізі має кваліфікуватися як злочинне, що, очевидно, є безпідставним. Таке врахування може бути доцільним лише у тому разі, коли зазначені діяння характеризуватимуться органічною єдністю, що зумовлює створення норм про так звані складені (складні) злочини. На думку Д. С. Азарова, злочини у сфері комп'ютерної інформації і терористичний акт не перебувають у названому зв'язку, а тому їх об'єднання одним складом злочину є штучним[20].

В окремих державах (Грузія, США) останнім часом з'явився такий склад злочину, як кібертероризм[21]. Особливу увагу серед наведених діянь привертає диспозиція ст. 324[1] «Кібертероризм» розділу 11 «Злочини проти держави» КК Грузії, яка викладена у такій редакції: «Кібертероризм, тобто проти-

правне заволодіння комп'ютерною інформацією, що охороняється законом, її використання або погроза використанням, які створюють небезпеку настання тяжких наслідків, вчинені з метою залякування населення чи (і) впливу на орган влади, – карається…»[22].

Як уже зазначалось, назва статті «кібертероризм» у КК видається невдалою, оскільки відповідальність у таких випадках повинна наставати за конкретні акти кібертероризму як прояви цього явища.

На нашу думку, вчинювані в нашій державі кібертерористичні акти необхідно кваліфікувати за ст. 258 «Терористичний акт» КК України. Враховуючи наведене, заслуговує на підтримку підхід М. А. Єфремової, яка пропонує диспозицію статті «Терористичний акт» КК викласти у такій редакції: «Вчинення вибуху, підпалу, протиправного впливу на інформаційно-телекомунікаційні системи або інших дій, що залякують населення та створюють небезпеку загибелі людини, заподіяння значної майнової шкоди чи настання інших тяжких наслідків з метою впливу на прийняття рішення органами влади або міжнародними організаціями, а також загроза вчинення зазначених дій у зазначених цілях»[23].

Підтримуваний нами підхід набув певного втілення у положеннях ст. 237 «Акти тероризму» розділу 3 «Кримінальні правопорушення проти державної влади» Кримінального кодексу Естонії, згідно з якою «… втручання в комп'ютерні дані, або перешкоджання функціонуванню комп'ютерних систем, а також погроза вчинення таких дій, якщо вони вчинені з метою примусу держави або міжнародної організації до дії або бездіяльності …, караються позбавленням волі терміном від п'яти до двадцяти років або довічним позбавленням волі»[24]. По суті, перераховані у диспозиції наведеної статті окремі діяння становлять акти кібертероризму.

Криміналізація усіх без винятку форм терористичної діяльності та кваліфікація їх як терористичних злочинів виступає необхідною передумовою для організації належної протидії тероризму. На користь такого вирішення проблем свідчить аналогічна тенденція, що простежується останнім часом в європейських державах[25]. Проєкт нового КК України (станом на 24 грудня 2021 р.) у Книзі 5 «Злочини та проступки проти суспільства» містить розділ 5.2 «Злочини проти безпеки суспільства від тероризму», в якому передбачені терористичні злочини. Зокрема, ст. 5.2.4 «Терористичне діяння» проєкту нового КК України (у редакції станом на 24 грудня 2021 р.) викладена у такій редакції: «особа, яка з метою залякати населення або дестабілізувати діяльність публічної влади чи міжнародної організації, або примусити їх вчинити яку-небудь дію чи утриматися від її вчинення: 1) захопила людину, 2) застосувала зброю чи інший предмет, яким може бути спричинена шкода життю чи тяжка шкода здоров'ю людини, 3) захопила, утримувала, знищила або пошкодила об'єкт критичної інфраструктури чи його устаткування, необхідне для діяльності цього об'єкта, або вивела його з ладу, 4) захопила повітряне, морське судно або інший засіб пасажирського чи вантажного транспорту,

5) влаштувала перешкоду для руху на вулиці, дорозі, іншому шляху сполучення, заблокувала транспортну комунікацію, роботу морського, річкового порту чи аеропорту, трубопровідного транспорту, 6) виготовила, придбала, перевезла, поставила, використала вогнепальну зброю, вибуховий пристрій, ядерний, біологічний чи хімічний боєприпас або заволоділа такою зброєю чи таким боєприпасом, 7) вивільнила у навколишнє середовище небезпечну речовину або здійснила небезпечну для життя людей пожежу, повінь чи вибух, або 8) припинила постачання води, електроенергії чи іншого природного ресурсу, що має життєво важливе значення для людей, – вчинила злочин 5 ступеня[26].

**Висновки.** Вважаємо доцільним диспозицію частини першої ст. 258 «Терористичний акт» чинного КК України після слів «терористичний акт, тобто застосування зброї, вчинення вибуху, підпалу» доповнити словами «протиправного впливу на інформаційно-телекомунікаційні системи» і далі за текстом. У проєкті нового КК України (у редакції станом на 24 грудня 2021 р.) вважаємо доцільним доповнити ст. 5.2.4 «Терористичне діяння» положенням, яке присвячене кібертерористичному акту. Таким чином, ст. 5.2.4 розглядуваного проєкту КК слід доповнити п. 9, який варто викласти в такій редакції: «особа, яка з метою залякати населення або дестабілізувати діяльність публічної влади чи міжнародної організації, або примусити їх вчинити яку-небудь дію чи утриматися від її вчинення: … 9) *вчинила кримінальне правопорушення з використанням інформаційно-комунікаційних технологій у кіберпросторі».* Реалізація зазначених пропозицій, на нашу думку, сприятиме більш ефективній протидії актам кібертероризму, матиме певний запобіжний потенціал, а також свідчитиме про належне розуміння законодавцем рівня суспільної небезпеки аналізованих діянь.

**1.** Бойченко О. В., Ончурова О. О. Кібертероризм у складі сучасних проблем національної безпеки. *Форум права*. 2010. № 2. С. 57. **2.** Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ, 2015. С. 58. **3.** Голубев В. А. Кибертерроризм как новая форма терроризма. URL: https://www.crime-research.org/library/Gol_tem3.htm (дата звернення: 12.01.2022). **4.** Gabriel Weimann. Cyberterrorism How Real Is the Threat? *Special report.* December 2004. P. 11. URL: https://www.usip.org/sites/default/files/sr119.pdf (дата звернення: 09.12.2021). **5.** Світова гібридна війна: український фронт / за заг. ред. В. П. Горбуліна. Національний інститут стратегічних досліджень. Київ: НІСД, 2017. С. 89. **6.** Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 09.12.2021). **7.** Буяджи С. А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект: дис. … канд. юрид. наук:12.00.01. Івано-Франківськ, 2018. С. 151. **8.** Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «АртЕк», 2017. С. 35–36. **9.** Наскільки надійна в Україні система захисту кіберпростору, які цілі російських хакерів, хто їх фінансує та в чому їх сильні

та слабкі сторони? URL: https://www.epravda.com.ua/publications/2021/11/3/679341/ (дата звернення: 25.12.2021). **10**. СБУ встановила хакерів ФСБ, які здійснили понад 5 тис. кібератак на державні органи України. URL: https://ssu.gov.ua/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy (дата звернення 01.11.2021). **11.** Когут Ю. І. Протидія кібертероризму як загрозі інформаційній безпеці України: дис. … канд. юрид. наук: 21.07.01. Київ, 2021. С. 211. **12.** Брич Л. П., Навроцький В. О. Кримінально-правова кваліфікація ухилення від оподаткування в Україні: монографія. Київ: Атіка, 2000. С. 14. **13.** Проєкт Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» (реєстр. № 2439а від 24 липня 2015 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183 (дата звернення: 19.11.2021). **14.** Когут Ю. І. Протидія кібертероризму як загрозі інформаційній безпеці України: дис. … канд. юрид. наук: 21.07.01. Київ, 2021. С. 24. **15.** Проєкт Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» (реєстр. № 2439а від 24 липня 2015 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183 (дата звернення: 19.11.2021). **16.** Проєкт Закону про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини) (реєстр. № 2328а від 10 липня 2015 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55972 (дата звернення: 19.11.2021). **17.** Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* 2016. № 1 (16). С. 115–116. **18.** Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. … канд. юрид. наук: 12.00.08. Київ, 2003. С. 104. **19.** Ліпкан В. А. Щодо поняття тероризму. *Право України.* 2000. № 7. С. 69. **20.** Азаров Д. С. Вказ. праця. С. 104–105. **21.** Сравнительное уголовное право. Особенная часть: монография / В. Н. Додонов, О. С. Капинус, С. П. Щерба; под общ. и науч. ред.: С. П. Щерба. Москва: Юрлитинформ, 2010. С. 391. **22.** Уголовный кодекс Грузии 1999 г. (с изменениями от 2020 г.). URL: https://www.legislationline.org/download/id/8847/file/Georgia_Criminal_Code_am2020_ru.pdf (дата звернення: 31.10.2021). **23.** Ефремова М. А. Уголовно-правовая охрана информационной безопасности: дис. … д-ра юрид. наук: 12.00.08. Москва, 2017. С. 328–329. **24.** Penal Code of the Republic of Estonia (2001, amended 2021). URL: https://www.legislationline.org/download/id/9098/file/EST_CC_as%20of%20May%202021.pdf (дата звернення: 02.01.2022) **25.** Кубальський В. Н. Кримінально-правові проблеми протидії тероризму в Україні: дис. … канд. юрид. наук: 12.00.08. Київ, 2007. С. 87. **26.** Кримінальний кодекс України (проєкт). Контрольний текст (станом на 24 грудня 2021 р.). URL: https://newcriminalcode.org.ua/upload/media/2021/12/28/kontrolnyj-proekt-kk-24-12-2021.pdf (дата звернення: 12.01.2022).

### *References*

**1.** Bojchenko O. V., Onchurova O. O. Kiberteroryzm u skladi suchasnykh problem natsional'noi bezpeky. *Forum prava.* 2010. № 2. S. 57 [ukr]. **2.** Buriachok V. L. Informatsijna ta kiberbezpeka: sotsiotekhnichnyj aspekt: pidruchnyk / [V. L. Buriachok, V. B. Tolubko, V. O. Khoroshko, S. V. Toliupa]; za zah. red. d-ra tekhn. nauk, profesora V. B. Tolubka. Kyiv: DUT, 2015. S. 58 [ukr]. **3.** Holubev V. A. Kyberterroryzm kak novaia forma terroryzma. URL: https://www.crime-research.org/library/Gol_tem3.htm (data zvernennia: 09.12.2021) [rus]. **4.** Gabriel Weimann. Cyberterrorism How Real Is the Threat? *Special report. December* 2004. P. 11. URL: https://www.usip.org/sites/default/files/sr119.

pdf (data zvernennia: 09.12.2021). **5.** Svitova hibrydna vijna: ukrains'kyj front / Za zah. red. V. P. Horbulina. Natsional'nyj instytut stratehichnykh doslidzhen'. Kyiv: NISD, 2017. S. 89 [ukr]. **6.** Stratehiia kiberbezpeky Ukrainy, zatverdzhena Ukazom Prezydenta Ukrainy vid 26 serpnia 2021 roku № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (data zvernennia: 09.12.2021) [ukr]. **7.** Buiadzhy S. A. Pravove rehuliuvannia borot'by iz kiberzlochynnistiu: teoretyko-pravovyj aspekt: dys. … kand. iuryd. nauk:12.00.01. Ivano-Frankivs'k, 2018. S. 151 [ukr]. **8.** Dovhan' O. D., Doronin I. M. Eskalatsiia kiberzahroz natsional'nym interesam Ukrainy ta pravovi aspekty kiberzakhystu: monohrafiia. Kyiv: Vydavnychyj dim «ArtEk», 2017. C. 35–36 [ukr]. **9.** Naskil'ky nadijna v Ukraini systema zakhystu kiberprostoru, iaki tsili rosijs'kykh khakeriv, khto ikh finansuie ta v chomu ikh syl'ni ta slabki storony? URL: https://www.epravda.com.ua/publications/2021/11/3/679341/ (data zvernennia: 25.12.2021) [ukr]. **10.** SBU vstanovyla khakeriv FSB, iaki zdijsnyly ponad 5 tys. kiberatak na derzhavni orhany Ukrainy. URL: https://ssu.gov.ua/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy (data zvernennia 01.11.2021) [ukr]. **11.** Kohut Yu. I. Protydiia kiberteroryzmu iak zahrozi informatsijnij bezpetsi Ukrainy: dys. … kand. iuryd. nauk: 21.07.01. Kyiv, 2021. S. 211 [ukr]. **12.** Brych L. P., Navrots'kyj V. O. Kryminal'no-pravova kvalifikatsiia ukhylennia vid opodatkuvannia v Ukraini: Monohrafiia. Kyiv: Atika, 2000. S. 14 [ukr]. **13.** Proiekt Zakonu Ukrainy «Pro vnesennia zmin do Kryminal'noho kodeksu Ukrainy schodo vstanovlennia vidpovidal'nosti za kiberteroryzm» (reiestr. № 2439a vid 24 lypnia 2015 r.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183 (data zvernennia: 19.11.2021) [ukr]. **14.** Kohut Yu. I. Protydiia kiberteroryzmu iak zahrozi informatsijnij bezpetsi Ukrainy: dys. … kand. iuryd. nauk: 21.07.01. Kyiv, 2021. S. 24 [ukr]. **15.** Proiekt Zakonu Ukrainy «Pro vnesennia zmin do Kryminal'noho kodeksu Ukrainy schodo vstanovlennia vidpovidal'nosti za kiberteroryzm» (reiestr. № 2439a vid 24 lypnia 2015 r.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183 (data zvernennia: 19.11.2021) [ukr]. **16.** Proiekt Zakonu pro vnesennia zmin do Kryminal'noho kodeksu Ukrainy (schodo posylennia vidpovidal'nosti za kiberteroryzm ta kiberzlochyny) (reiestr. № 2328a vid 10 lypnia 2015 r.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55972 (data zvernennia: 19.11.2021) [ukr]. **17.** Bank R. O. Informatsijnyj teroryzm iak zahroza natsional'nij bezpetsi Ukrainy: teoretyko-pravovyj aspekt. *Informatsiia i pravo.* 2016. № 1. (16). S. 115–116 [ukr]. **18.** Azarov D. S. Kryminal'na vidpovidal'nist' za zlochyny u sferi komp'iuternoi informatsii: dys… kand. iuryd. nauk: 12.00.08. Kyiv, 2003. S. 104 [ukr]. **19.** Lipkan V. A. Schodo poniattia teroryzmu. *Pravo Ukrainy.* 2000. № 7. S. 69 [ukr]. **20.** Azarov D. S. Vkaz. pratsia. S. 104–105 [ukr]. **21.** Sravnytel'noe uholovnoe pravo. Osobennaia chast': Monohrafyia / Dodonov V. N., Kapynus O. S., Scherba S. P.; Pod obsch. y nauch. red.: Scherba S. P. Moskva: Yurlytynform, 2010. C. 391 [rus]. **22.** Uholovnyj kodeks Hruzyy 1999 r. (s yzmenenyiamy ot 2020 r.). URL: https://www.legislationline.org/download/id/8847/file/Georgia_Criminal_Code_am2020_ru.pdf (data zvernennia: 31.10.2021) [rus]. **23.** Efremova M. A. Uholovno-pravovaia okhrana ynformatsyonnoj bezopasnosty: dys. … d-ra iuryd. nauk: 12.00.08. Moskva, 2017. S. 328–329 [rus]. **24.** Penal Code of the Republic of Estonia (2001, amended 2021). URL: https://www.legislationline.org/download/id/9098/file/EST_CC_as%20of%20May%202021.pdf (data zvernennia: 02.01.2022). **25.** Kubal's'kyj V. N. Kryminal'no-pravovi problemy protydii teroryzmu v Ukraini: dys. … kand. iuryd. nauk: 12.00.08. Kyiv, 2007. S. 87 [ukr]. **26.** Kryminal'nyj kodeks Ukrainy (proiekt). Kontrol'nyj tekst (stanom na 24 hrudnia

2021 r.). URL: https://newcriminalcode.org.ua/upload/media/2021/12/28/kontrolnyj-proekt-kk-24-12-2021.pdf (data zvernennia: 12.01.2022) [ukr].

***Kubalskiy Vladyslav.*** **Problems of criminalization of cyberterrorist encroachments**

*This research is aimed at identify the main ways to improve the criminal legislation of Ukraine in the field of counteracting cyberterrorism. The most precise attention is focused on considering of scientists' proposals, as well as bills dealing with the criminalization of acts of cyberterrorism. The research is based on results of the analysis of the norms of criminal codes of some foreign states in the field of counteracting acts of cyberterrorism.*

*Terrorist activities in cyberspace in the context of globalization and the widespread use of information and communication technologies pose a serious threat to the security of any state and necessitate countering this phenomenon. It is impossible to properly counteract the manifestations of cyberterrorism (in the scientific literature it is sometimes called «electronic», «information», «computer» terrorism) as a new type of terrorism without understanding its nature, modern forms and trends.*

*The author consider that confirming the position on the need for legislative regulation of criminal responsibility for cyberterrorist acts, we note that the proposed idea meets the grounds and criteria for criminalization, which are developed in the science of criminal law. The criminalization of all forms of terrorist activity without exception and their qualification as terrorist crimes is a necessary precondition for the organization of proper counter-terrorism. A similar recent trend in European countries is in favor of such a solution. The cyber-terrorist acts committed in our state must be qualified under Article 258 «Terrorist act» of the Criminal Code of Ukraine.*

*The study contains proposals to change the provisions of the current Criminal Code of Ukraine and its new draft, aimed at improving counteracting acts of cyberterrorism. The adoption of the rule in the proposed wording will contribute to a more effective response to acts of cyberterrorism, has a certain preventive potential, and also demonstrates the correct understanding by the legislator of the level of public danger of the analyzed acts.*

***Key words:*** *criminalization, cyberterrorism, act of cyberterrorism, cyberspace.*