УДК 343.3/.7
DOI 10.36919/ELJ.1.2023.37

**В. Г. Хахановський,**
*доктор юридичних наук,професор,*
*професор кафедри інформаційних технологій*
*та кібербезпеки ННІ № 1,*
*Національна академія внутрішніх справ*
**ORCID ID 0000-0001-5676-5641;**

**В. Д. Гавловський,**
*кандидат юридичних наук,старший науковий співробітник,*
*головний науковий співробітник,*
*Міжвідомчий науково-дослідний центр*
*з проблем боротьби з організованою*
*злочинністю при РНБО України*
**ORCID ID 0000-0001-7496-9904**

# КРИМІНАЛЬНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ, ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ В УКРАЇНІ

*У науковій статті порушено питання законодавчої невизначеності кіберзлочину, що негативно позначається на ефективності протидії кіберзлочинності в Украйні. Наголошено, що на часі розроблення підстав віднесення кримінальних правопорушень, вчинюваних у кіберпросторі, до кіберзлочинів, започаткування змін до офіційної державної звітності для системного аналізу статистичних даних, об'єктивного оцінювання структури і змісту таких даних, можливостей їх використання для запобігання та протидії кіберзлочинності, а також для розв'язання окремих проблем щодо кримінально-правової кваліфікації кримінальних правопорушень, вчинюваних у кіберпросторі. Надано рекомендації щодо кваліфікації окремих кіберзлочинів. Зокрема, що стосуються випадків вчинення таких їх видів, які посягають на декілька об'єктів, що охороняються законодавством України про кримінальну відповідальність. Проаналізовано ряд судових рішень у контексті предмета дослідження.*

***Ключові слова:*** *кіберзлочин, класифікація кіберзлочинів, статистичні показники, кіберпростір, блокчейн, організована кіберзлочинність.*

**Постановка проблеми та її актуальність.** Сьогодні стан протидії кіберзлочинності у світі характеризується сталою тенденцією до погіршення. Кіберзлочинність набула якісно нових рис, представники злочинного середовища дедалі ширше використовують новітні комунікаційні технології під час вчинення як «традиційних», так і нових видів кримінальних правопорушень, пов'язаних із функціонуванням кіберпростору.

Наразі у національному та міжнародному законодавстві бракує загальновизнаного визначення киберзлочинів, тому немає і єдиного підходу до розроблення підстав віднесення протиправних діянь до таких кримінальних правопорушень, що негативно позначається на можливості отримання об'єктивних статистичних даних про кіберзлочини. Водночас постають певні проблеми їх кваліфікації.

**Аналіз останніх досліджень і публікацій.** Різні аспекти досліджуваного питання вивчали О. В. Амелін, В. В. Василевич, Б. М. Головкін, В. В. Голіна, М. В. Гуцалюк, О. М. Джужа, А. П. Закалюк, А. Ю. Ковальчук, О. Г Кулик, О. М. Литвинов, В. В. Марков, Д. М. Прокоф'єва-Янчиленко, А. В. Савченко, О. В. Таран, В. І. Трапезніков, В. О. Туляков та ін.

Сьогодні в цьому напрямі плідно працюють вітчизняний науковий загал і практики, порушуючи різні питання, серед яких: особливості правового регулювання протидії кіберзлочинності в Україні [20], розслідування кіберзлочинів в Україні під час воєнного стану [6], актуальні проблеми протидії кіберзлочинності в Україні [13], основні аспекти державної політики забезпечення протидії кіберзлочинності в Україні [5]. Наукові розвідки зарубіжних колег спрямовані на висвітлення різних аспектів цього феномена, зокрема таких як: кіберзлочинність і кримінальна відповідальність юридичних осіб [1], удосконалення норм

національного законодавства щодо кіберзлочинності, способів збирання, зберігання й управління даними та його гармонізація з міжнародним правом [3; 7], аналізують практику кримінальних розслідувань для всебічного розуміння кіберзлочинності [11; 14], етичний складник протидії кіберзлочинності в інтернеті [15], вивчають глобальну географію кіберзлочинності та її рушійні сили [2], аналізують теорії вчинення кіберзлочинів [4], організовану кіберзлочинність [21].

Водночас проблемам віднесення кримінальних правопорушень до кіберзлочинів, їхньої кваліфікації та аналізу кіберзлочинності, зокрема в частині офіційної статистики, приділяється недостатньо уваги, що й зумовлює актуальність обраної тематики.

**Мета статті** полягає у формуванні теоретичних положень і надання практичних рекомендацій щодо віднесення кримінальних правопорушень, вчинюваних у кіберпросторі, до кіберзлочинів, започаткування змін до офіційної державної звітності для системного аналізу статистичних даних, розв'язання окремих проблем кримінально-правової кваліфікації правопорушень, вчинюваних у кіберпросторі.

**Виклад основного матеріалу дослідження.** Поняття «кіберзлочинність» і «комп'ютерна злочинність» нерідко використовуються як синоніми. Однак саме термін «кіберзлочинність» найбільшою мірою відображає сутність цього явища.

У Законі України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність визначається як сукупність кіберзлочинів. А кіберзлочин – як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачено законом України про кримінальну відповідальність та/або визнано злочином міжнародними договорами України [19]. Отже, сьогодні в законодавстві України не існує чіткого визначення поняття «кіберзлочин».

Конвенція Ради Європи про кіберзлочинність містить набір основних засад для будь-якої країни, яка розробляє національне законодавство з протидії кіберзлочинності. Водночас наведена в Конвенції класифікація, на думку ряду західних і вітчизняних дослідників, не є всеосяжною.

У звіті Комітету внутрішніх справ Парламенту Великобританії з кіберзлочинності 2013 року кіберзлочини поділяють на три категорії:

– виключно мережеві злочини, де цифрові системи є основною метою, одночасно виступають і засобами посягання. Ця категорія включає посягання на комп'ютерні системи для знищення інфраструктури інтернет-технологій і незаконне заволодіння даними;

– традиційні злочини, які були переведені в площину кіберзлочинів через використання інтернету;

– використання інтернету з метою торгівлі наркотиками та як допоміжний інструмент для вчинення інших видів злочинів [8].

У спільному повідомленні Європейської комісії 2013 р. до Європейського парламенту, Ради Європейського економіко-соціального комітету та комітету регіонів кіберзлочинність також розкривається через три основні категорії: традиційні види злочинів (шахрайство, підроблення документів), що вчиняються із використанням електронних комунікаційних мереж та інформаційних систем; розміщення незаконного контенту в електронних медіа; атаки на інформаційні системи, блокування програмного забезпечення сайтів і хакерство [12].

Більшість дослідників пропонують розділяти кіберзлочини на види залежно від об'єкта та предмета посягання. Найпоширеніший поділ – це комп'ютерні злочини та злочини, вчинені за допомогою комп'ютерів, мереж та інших пристроїв для доступу до кіберпростору. Ця позиція була підтримана на Десятому Конгресі ООН, де поняття «кіберзлочин» розглядалося у двох аспектах: у «вузькому» та «широкому» сенсі.

1. Кіберзлочин у вузькому значенні (комп'ютерний злочин): будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є порушення безпеки комп'ютерних систем та оброблюваних ними даних.

2. Кіберзлочин у широкому розумінні (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою комп'ютерів або яке пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння та пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж.

Водночас у доповіді цього самого Конгресу вказується, що термін «комп'ютерні злочини» був розроблений для охоплення як абсолютно нових форм злочинності, орієнтованої на комп'ютери, мережі та їх користувачів, так і традиційних злочинів, які сьогодні вчиняються з використанням або за допомогою комп'ютерного устаткування [16].

До того ж у виступі Генерального секретаря ООН на X Конгресі було висловлено, що «використання нових технологій у злочинних цілях призвело до виникнення абсолютно нових форм злочинності. З іншого боку, більш традиційні злочини нині вчиняються новими методами, які дозволяють збільшити вигоди чи знизити ризики злочинців».

Зарубіжні вчені, зокрема Майк Макгуайр і Саманта Даулінг (Англія), також вважають, що кіберзлочинність є загальним терміном, який використовується для опису двох різних, але тісно пов'язаних між собою злочинних діянь: кіберзалежні та кіберутворюючі (злочини, пов'язані з кіберпростором).

Злочини, вчинені за допомогою комп'ютерів, комп'ютерних мереж чи інших комунікаційних форм ІКТ, наприклад поширення шкідливих програм, DDoS-атаки, зламування серверів для захоплення мережевої інфраструктури або вебсторінок, спрямовані на пошкодження комп'ютерів і мережевих джерел.

Злочини, пов'язані з кіберпростором, – це традиційні злочини, масштаби яких збільшуються чи досягаються за допомогою комп'ютерів, комп'ютерних мереж чи інших ІКТ. Вони досі можуть бути скоєні без використання ІКТ. Можна стверджувати, що доктринальні підходи до розуміння поняття кіберзлочинів є різними. Проте варто зазначити, що, попри наявні альтернативні дефініції, саме термін кіберзлочинності найбільше відбиває сутність цього явища.

За класифікацією кіберзлочинів можна дійти висновку, що більшість дослідників пропонують розділяти кіберзлочини на види залежно від об'єкта і предмета зазіхання: нові злочини стали можливими завдяки новітнім комп'ютерним технологіям (злочини, передбачені розділом XVI КК України); традиційні злочини вчиняються за допомогою комп'ютерних технологій та інтернету.

Проте сьогодні рекомендації, інструкції щодо віднесення кримінальних правопорушень, які вчиняються у кіберпросторі, до кіберзлочинів відсутні. Серед науковців і практиків немає єдиної думки з цього приводу, а тому й єдиного підходу до окреслення підстав віднесення протиправних діянь до таких злочинів. Отже, неможливо отримати об'єктивні статистичні дані про кіберзлочини.

Наразі офіційна державна статистика містить лише відомості про вчинені кримінальні правопорушення, передбачені розд. XVI КК України, що відображаються у звітах Генеральної прокуратури України (Єдиний звіт про кримінальні правопорушення; Єдиний звіт про осіб, які вчинили кримінальні правопорушення).

У Державній судовій адміністрації України готуються звіти судів першої інстанції про розгляд матеріалів кримінального провадження (форма № 1-к), про осіб, притягнутих до кримінальної відповідальності, види кримінального покарання (форма № 6) та про склад засуджених (форма № 7).

В Україні найбільш повно статистичні дані про кіберзлочини відображаються у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції, де, крім злочинів, передбачених розділом XVI КК України, позначені й інші, вчинені з використанням електронно-обчислювальної техніки: ст. 176 «Порушення авторського права та суміжних прав»; ст. 185 «Крадіжка»; чч. 3 та 4 ст. 190 «Шахрайство». До цієї категорії належать також злочини, передбачені стст. 200, 229, 231, чч. 3, 4 та 5 ст. 301 КК України.

Нещодавно цей перелік злочинів був доповнений такими статтями: ст. 120 «Доведення до самогубства», ст. 149 «Торгівля людьми», ст. 156 «Розбещення неповнолітніх», ст. $156^1$ «Домагання дитини для сексуальних цілей», ч. 1, 2 ст. 190 «Шахрайство», ст. 191 «Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем», ст. $203^2$ «Незаконна діяльність з організації або проведення азартних ігор, лотерей», ст. $301^1$ «Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження», ст. $301^2$ «Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи», ст. 307 «Незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів», ст. 321 «Незаконне виробництво, виготовлення, придбання, перевезення, пересилання, зберігання з метою збуту або збут отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів», ст. $321^1$ «Фальсифікація лікарських засобів або обіг фальсифікованих лікарських засобів», ст. 357 «Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або

їх пошкодження», ст. 358 «Підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів».

Крім того, окремі показники про кіберзлочини, передбачені іншими статтями КК України, відображено в інших статистичних звітах, зокрема злочини, передбачені ст. 376[1] «Незаконне втручання у роботу автоматизованої системи документообігу суду» – у Єдиному звіті про кримінальні правопорушення (готується Офісом Генерального прокурора України).

Частина українських учених до кіберзлочинів відносять злочини, передбачені статтями гл. XVI КК України, та злочини, показники про які відображаються у звіті Національної поліції України.

Водночас деякі вчені, зокрема О. В. Савченко, вважають, що, крім правопорушень, наведених у звіті, під категорію кіберзлочинів можуть підпадати й інші, передбачені КК України, за умови, що знаряддям їх вчинення були мережеві технології та/або їх наслідки відображатимуться в кіберпросторі.

До кіберзлочинів можуть належати такі: діяння, вчинені задля насильницької зміни чи повалення конституційного ладу чи захоплення структури державної влади (ст. 109); посягання на територіальну цілісність та недоторканність України (ст. 110); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114). Сюди можуть бути віднесені дії, передбачені такими статтям КК України: 132; 145; ч. 1 ст. 158; 159; 161; 163; 168; 182; 232; 259; 263; 295; 300; 303; 307; 312; 313; 328; 330; 345; 345[1]; ч. 1 ст. 346 та ін.

Варто також зазначити певні проблеми кваліфікації кіберзлочинів. Як зазначають фахівці, основним критерієм відмежування злочинів, передбачених стст. 361–363[1] КК України від інших, пов'язаних із використанням комп'ютерної техніки як знаряддя чи засоби вчинення злочину, є об'єкт зазіхання. Так, особливістю кримінально-правової кваліфікації злочинів проти власності, які вчиняються з використанням комп'ютерної техніки, визнається потреба у вирішенні питання про доцільність додаткової кваліфікації дій винної особи за статтями, які передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. У такому разі варто керуватися тим, що використання комп'ютерної техніки під час вчинення злочинів проти власності утворює самостійний склад злочину лише тоді, коли завдано певної шкоди відповідному об'єкту, – відносин власності на комп'ютерну інформацію, коли певну інформацію було незаконно знищено, блоковано, модифіковано. А у випадках коли певні інформаційні системи використовуються за призначенням, додаткова кваліфікація не потрібна [9].

Також нині існує проблема кримінально-правової кваліфікації дій, які користувачі комп'ютерів здійснюють у сфері обігу криптовалют і застосування штучного інтелекту.

*Так, 2018 р. дослідники з університету RWTH Aachen University (Німеччина) виявили, що блокчейн Bitcoin містить близько 1 600 файлів, де є сцени жорстокого поводження з дітьми, водночас не менше 8 файлів – з порнографічним контентом. Блокчейн містить зовнішні посилання на 274 відеофайли, присвячені жорстокому поводженню з дітьми, і близько 142 посилань на darkweb. За словами вчених, знахідка може поставити блокчейн поза законом, проте сьогодні не існує жодних судових ухвал із цього приводу, очевидно, через складність кримінально-правової кваліфікації. Усі, хто бере участь у процедурі Майнінг або має біткоїни, можуть бути причетні до появи порнографічного контенту в мережі* [18].

На практиці у працівників правоохоронних і судових органів виникає багато проблем щодо кваліфікації кіберзлочинів. Особливо це стосується випадків вчинення таких їх видів, які посягають на декілька об'єктів, які охороняються кримінальним законом. Найчастіше помилки зустрічаються у процесі кваліфікації одного діяння, яке, здавалося б, містить ознаки декількох складів. Так, основною проблемою тут є визначення наявності чи відсутності у вчиненому ідеальної сукупності злочинів.

Під час вчинення кіберзлочину шкода може завдаватися: 1) суспільним відносинам, що виникають у ході забезпечення (за допомогою ІТС) життєдіяльності людини, суспільства, держави; 2) традиційним суспільним відносинам (за допомогою ІТС); 3) традиційним суспільним відносинам, які охороняються законом, для заподіяння шкоди використовуються ІТС, яким не завдано шкоди.

Перша група відносин охороняється розд. XVI Особливої частини КК України. Ці відносини є частиною другої та третьої групи відносин, але у другій групі їм завдається шкоди разом із традиційними відносинами кримінально-правової охорони, а в третій – ні.

Ідеальною сукупністю злочинів вважається два чи більше злочинів, вчинених однією дією. Згідно із зазначеними групами відносин, яким завдано шкоди під час вчинення такого діяння у разі скоєння кіберзлочину, можна виділити три групи цих злочинів: 1) злочини

у сфері використання ЕОМ, їх систем, комп'ютерних мереж, мереж електрозв'язку; 2) злочини, що кваліфікуються за статтями КК України, відповідно до об'єкта зазіхання, з додатковим посиланням на статті глави XVI КК України; 3) злочини, що кваліфікуються за статтями КК України, відповідно до об'єкта посягання, без додаткового посилання на статті розд. XVI КК України.

Тобто дії з першої та третьої групи є одиничними злочинами, а з іншого – ідеальною сукупністю злочинів. Однак у практиці застосування норм КК України протидії кіберзлочинності діяння, які стосуються різних із зазначених груп, нерідко плутаються. Найчастіше злочини другої групи кваліфікуються лише за однією статтею, і навпаки, злочини першої чи третьої групи кваліфікуються за кількома статтями, хоча потребують додаткової кваліфікації. Водночас стаття застосовується у процесі кваліфікації другої групи злочинів або розділу XVI КК України, або інша – відповідно до безпосереднього об'єкта посягання. Очевидно, що в обох випадках частина злочину кваліфікації не охоплюється, що порушує принципи повноти і точності кваліфікації, а у разі кваліфікації одного діяння, що містить один склад злочину, за двома статтями порушується ще й принцип заборони подвійного інкримінування.

Узагальнення судової практики свідчить, що значна частина кіберзлочинів припадає на випадки, коли зазіхання у сфері використання ІТС здійснюється з корисливих спонукань з метою викрадення чи заволодіння чужим майном із заподіянням матеріальних збитків і є способом скоєння таких злочинів проти власності, як шахрайство (ст. 190 КК України) чи присвоєння чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК України). У більшості випадків суди кваліфікують такі дії щодо сукупності злочинів: за статтею глави XVI КК України та тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було використання ІТС.

*Наприклад, Печерський районний суд м. Києва визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток комерційного банку, як посадова особа, зловживаючи службовим становищем, маючи доступ до бази даних про клієнтів та їх рахунки, що містилася в його робочому комп'ютері, діючи з метою заволодіння грошима, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дубліката та банкоматів М. зняв і привласнив готівкою з рахунку клієнта кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч. 4 ст. 191 КК України як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах. Крім того, суд кваліфікував дії М. ще й за сукупністю ч. 3 ст. 362 КК України, оскільки М., будучи особою, яка мала право доступу до інформації, що обробляється на комп'ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації та завдало значної шкоди.*

Однак у деяких випадках суди кваліфікують зазначені дії лише за статтями глави XVI Особливої частини КК України. Так, Червоногвардійський районний суд м. Дніпра визнав Є. винним за ч. 1 ст. 361 КК України та призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих спонукань, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із ЗАТ КБ «ПриватБанк» надавала послуги з прискореного перерахування платежів за комунальні послуги та мобільний зв'язок через інтернет. У результаті такої діяльності Є. впродовж певного часу викрадав кошти з рахунків клієнтів ЗАТ КБ «ПриватБанк».

В останньому випадку, оскільки Є. шляхом обману неодноразово опановував грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання у роботу ЕОМ є способом скоєння злочину проти власності, то такі дії потребують додаткової кваліфікації ще й за ст. 190 КК України. Вважаємо, що тут дійсно є сукупність злочинів, але вона вже врахована до КК України у ч. 3 ст. 190, отже, потрібна кваліфікація за цією нормою без додаткових посилань на норми КК України [10].

Однією із загальних проблем кримінально-правової кваліфікації є питання кваліфікації ідеальної сукупності злочинів, а саме поглинання одного злочину іншим, яке було його частиною. Ця проблема досі потребує вирішення вченими. Зокрема, Т. І. Созанський формулює правило щодо злочинів, які мають додаткові об'єкти зазіхання: «Якщо ці об'єкти співвідносяться як основний та додатковий, то діяння кваліфікується як одиничний злочин, якщо ж обидва (або більше) об'єкти є основними, то діяння утворює ідеальну сукупність злочинів» [17].

У п. 11 Постанови Пленуму Верховного Суду зазначено, що «якщо у складі злочину передбачено діяння, у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання щодо його кримінально-правової оцінки необхідно вирішувати з урахуван-

ням того, наскільки охоплюється складом цього злочину таке діяння, а також з урахуванням змісту санкцій відповідних статей КК України. У випадках коли складом певного злочину охоплюється вчинене одночасно з цим злочином відповідне діяння та санкцією статті (частини статті) КК України встановлено за цей злочин більш строге максимальне основне покарання, ніж за відповідне діяння, таке діяння не утворює сукупності злочинів та окремої кваліфікації».

**Висновки.** Сьогодні офіційного, закріпленого в міжнародних документах визначення кіберзлочинності досі не існує. У вітчизняному законодавстві нині також не існує чіткого визначення поняття кіберзлочину. Дискутуються різні позиції щодо класифікації кіберзлочинів. Тому є нагальна потреба визначитися з переліком «традиційних» злочинів, які можуть належати до категорії кіберзлочинів, внести зміни до статистичної звітності Офісу Генерального прокурора України.

Отже, кримінально-правове забезпечення боротьби із кіберзлочинністю потребує подальшого вдосконалення, імплантації у національні правові норми міжнародних стандартів. Крім того, кваліфікація кіберзлочинів має свої особливості, на які потрібно зважати. Ці та інші проблеми боротьби із кіберзлочинністю далеко не вичерпані, вони можуть розглядатися на наукових міжнародних конференціях, а також виступати предметом подальших наукових досліджень, зокрема й на дисертаційному рівні.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Abel Souto M. Money Laundering, Cybercrime and Criminal Responsibility of Legal Persons. *Cybercrimes and Financial Crimes in the Global Era* / Eds. Liu, Y., Tian, M., Shao, Y. Singapore : Springer, 2022, 145–164. URL : https://doi.org/10.1007/978-981-19-3189-5_16

2. Chen S., Hao M., Ding F., Jiang D., Dong J., Zhang S., Guo Q., Gao, C. Exploring the global geography of cybercrime and its driving forces. *Humanities & social sciences communications*. 2023. No 10(1). P. 71. URL : https://doi.org/10.1057/s41599-023-01560-x

3. Creemers R. China's emerging data protection framework. *Journal of Cybersecurity*. 2022. No 8(1), tyac011. URL : https://doi.org/10.1093/cybsec/tyac011

4. Curry T. Cybercrime Perpetration Theories. *Oxford Research Encyclopedia of Criminology and Criminal Justice*. 2023. URL : https://doi.org/10.1093/acrefore/9780190264079.013.787

5. Довгань В., Коцман І. Основні аспекти державної політики забезпечення протидії кіберзлочинності в Україні. *Актуальні питання у сучасній науці*. 2023. № 3(9). С. 220–229. URL : https://doi.org/10.52058/2786-6300-2023-3(9)-220-229

6. Дунаєва Т. Є. Деякі особливості розслідування кіберзлочинів в Україні під час воєнного стану. *Становлення та розвиток правової держави: проблеми теорії та практики* : матеріали XV Міжнародної наук.-практ. конф., що присвячена 102-річчю Національного університету кораблебудування імені адмірала Макарова, м. Миколаїв, 28–29 груд. 2022 р. Львів – Торунь : Liha-Pres, 2022. С. 400–402. URL : https://doi.org/10.36059/978-966-397-287-9-109

7. Eboibi F. E. Cybercriminals and Nigerian cybercrimes act 2015: conceptualising computers for cybercrime justice. *Journal of Anti-Corruption Law*. 2023. No 3(1). URL : https://doi.org/10.14426/jacl.v4i.1310

8. Home Affairs Committee E-crime Fifth Report of Session 2013–2014. URL : https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf

9. Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України» / за ред. М. В. Гребенюка. Київ : Національна академія прокуратури України, 2019. 220 с.

10. Гриців М. І., Антощук В. В. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку / Верховний Суд України. [н.д.]. URL : http://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02

11. Jerome B. Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks*. 2020. No 8(3), 99. URL : https://doi.org/10.3390/risks8030099

12. Joint communication to the European parliament, the Council, the European economic and social committee and the committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 02.2013. URL : http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013JC0001

13. Козій А., Марченко Т., Шевченко В. Актуальні проблеми протидії кіберзлочинності в Україні. *Theoretical Foundations of State and Law*. 2022. С. 59–65. URL : https://doi.org/10.46299/isg.2022.mono.legal.1.2.3

14. Leukfeldt E. R., Kleemans E. R. Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime. *Researching Cybercrimes: Methodologies, Ethics, and Critical*

*Approaches* / Eds. A. Lavorgna, T. J. Holt. Springer, 2021. Pp. 127–144. Advance online publication. URL : https://doi.org/10.1007/978-3-030-74837-1_7

15. Martin, J. (2021). Ethics and Internet-Based Cybercrime Research in Australia. *Researching Cybercrimes* / Eds. Lavorgna A., Holt T. J. Palgrave Macmillan, Cham, P. 401–417. URL : https://doi.org/10.1007/978-3-030-74837-1_20

16. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Вена, 10–17 апреля 2000 г. URL : https://digitallibrary.un.org/record/432663/files/ A_CONF.187_15-RU.pdf; https://digitallibrary.un.org/record/432653/files/A_CONF.187_10-RU.pdf?version=1

17. Созанський Т. І. Кваліфікація сукупності злочинів : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.08 ; Львів. держ. ун-т внутр. справ. Львів, 2009. 18 с.

18. У блоках Bitcoin виявили сліди дитячої порнографії. *Інформаційне агентство Волинські Новини.* 2018. 22 берез. URL : https://www.volynnews.com/news/all/u-blokakh- Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi-/

19. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19

20. Якимчук М. Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. *New Ukrainian Law.* 2021. № 4. С. 182–186. URL : https://doi.org/10.51989/nul.2021.4.27

21. Zeng Y., Buil-Gil D. Organizational and Organized Cybercrime. *Oxford Research Encyclopedia of Criminology and Criminal Justice.* 2023. URL : https://doi.org/10.1093/acrefore/9780190264079.013.798

## REFERENCES

1. Abel Souto, M. (2022). Money Laundering, Cybercrime and Criminal Responsibility of Legal Persons. In: Liu, Y., Tian, M., Shao, Y. (Eds.) *Cybercrimes and Financial Crimes in the Global Era.* Springer, Singapore, 145–164. URL : https://doi.org/10.1007/978-981-19-3189-5_16

2. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities & social sciences communications*, 10(1), 71. URL : https://doi.org/10.1057/s41599-023-01560-x

3. Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, 8(1), tyac011. URL : https://doi.org/10.1093/cybsec/tyac011

4. Curry, T. (2023). Cybercrime Perpetration Theories. *Oxford Research Encyclopedia of Criminology and Criminal Justice.* URL : https://doi.org/10.1093/acrefore/9780190264079.013.787

5. Dovhan, V., & Kotsman, I. (2023). Osnovni aspekty derzhavnoi polityky zabezpechennia protydii kiberzlochynnosti v Ukraini [Main aspects of the state policy of combating cybercrime in Ukraine]. *Aktualni Pytannia u Suchasnii Nautsi,* 3(9), 220–229. URL : https://doi.org/10.52058/2786-6300-2023-3(9)-220-229 [in Ukrainian].

6. Dunaieva, T. Ye. (2022). Deiaki osoblyvosti rozsliduvannia kiberzlochyniv v Ukraini pid chas voiennoho stanu. *Stanovlennia ta rozvytok pravovoi derzhavy: problemy teorii ta praktyky* : materialy XV Mizhnarodnoi nauk.-prakt. konf., shcho prysviachena 102-richchiu Natsionalnoho universytetu korablebuduvannia imeni admirala Makarova, m. Mykolaiv, 28–29 hrud. 2022 r. Lviv – Torun : Liha-Pres. S. 400–402. URL : https://doi.org/10.36059/978-966-397-287-9-109 [in Ukrainian].

7. Eboibi, F. E. (2023). Cybercriminals and Nigerian cybercrimes act 2015: conceptualising computers for cybercrime justice. *Journal of Anti-Corruption Law,* 3(1). URL : https://doi.org/10.14426/jacl.v4i.1310

8. Home Affairs Committee E-crime Fifth Report of Session 2013–14. URL : https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf

9. Hrebeniuk, M. V. (Red.). (2019). Naukovo-praktychnyi komentar Zakonu Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy». Kyiv : Natsionalna akademiia prokuratury Ukrainy. 220 c.

10. Hrytsiv, M. I., & Antoshchuk, V. V. (n.d.). Sudova praktyka rozghliadu sprav pro zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), avtomatyzovanykh system ta kompiuternykh merezh i merezh elektrozviazku / Verkhovnyi Sud Ukrainy. URL : http://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/ AFB1E90622E4446FC2257B7C00499C02

11. Jerome, B. (2020). Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks,* 8(3), 99. URL : https://doi.org/10.3390/risks8030099

12. Joint communication to the European parliament, the Council, the European economic and social committee and the committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 02.2013. URL : http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013JC0001

13. Kozii, A., Marchenko, T., & Shevchenko, V. (2022). Aktualni problemy protydii kiberzlochynnosti v Ukraini. Theoretical Foundations of State and Law, 59–65. URL : https://doi.org/10.46299/isg.2022.mono.legal.1.2.3 [in Ukrainian].

14. Leukfeldt, E. R., & Kleemans, E. R. (2021). Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime. In A. Lavorgna, & T. J. Holt (Eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, pp. 127–144. Springer. Advance online publication. URL : https://doi.org/10.1007/978-3-030-74837-1_7

15. Martin, J. (2021). Ethics and Internet-Based Cybercrime Research in Australia. In: Lavorgna, A., Holt, T. J. (Eds.). *Researching Cybercrimes.* Palgrave Macmillan, Cham, 401–417. URL : https://doi.org/10.1007/978-3-030-74837-1_20

16. Organizatciia Obedinennykh natcii. (2000, Aprel 10–17). Desiatyi Kongress Organizatcii Obedinennykh Natcii po preduprezhdeniiu prestupnosti i obrashcheniiu s pravonarushiteliami. Vena. URL : https://digitallibrary.un.org/ record/432663/files/A_CONF.187_15-RU.pdf; https://digitallibrary.un.org/record/432653/files/A_CONF.187_10-RU.pdf?version=1 [in Russian].

17. Sozanskyi, T. I. (2009). Kvalifikatsiia sukupnosti zlochyniv (avtoref. dys. kand. yuryd. nauk, Lviv. derzh. un-t vnutr. sprav). Lviv. 18 s. [in Ukrainian].

18. U blokakh Bitcoin vyiavyly slidy dytiachoi pornohrafii. (2018, Berezen 22). *Informatsiine ahentstvo Volynski Novyny.* URL : https://www.volynnews.com/news/all/u-blokakh- Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi-/ [in Ukrainian].

19. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 2017, Zhovten 05 No 2163-VIII / Verkhovna Rada Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

20. Yakymchuk, M. Yu. (2021). Osoblyvosti pravovoho rehuliuvannia protydii kiberzlochynnosti v Ukraini: porivnialno-pravovyi aspekt [Special aspects of the legal regulation of combating cybercrime in Ukraine: comparative and legal aspect]. *New Ukrainian Law,* 4, 182–186. URL : https://doi.org/10.51989/nul.2021.4.27 [in Ukrainian].

21. Zeng, Y., & Buil-Gil, D. (2023). Organizational and Organized Cybercrime. *Oxford Research Encyclopedia of Criminology and Criminal Justice.* URL : https://doi.org/10.1093/acrefore/9780190264079.013.798

## V. Khakhanovskyi, V. Havlovskyi. CRIMINAL-LEGAL PROVISION OF CYBERCRIME PREVENTION, PECULIARITIES OF THE QUALIFICATION OF CYBERCRIMES IN UKRAINE

*The scientific article raised the issue of legislative uncertainty of cybercrime, which negatively affects the effectiveness of countering cybercrime in Ukraine. It was emphasized that it is time to develop the grounds for classifying criminal offenses committed in cyberspace as cybercrimes, to initiate changes to official state reporting for the systematic analysis of statistical data, objective assessment of the structure and content of such data, the possibilities of their use to prevent and counter cybercrime, and also to solve certain problems regarding the criminal-legal qualification of criminal offenses committed in cyberspace. Recommendations are provided on the qualification of certain cybercrimes. In particular, concerning the cases of committing such types of crimes, which encroach on several objects protected by the legislation of Ukraine on criminal liability. A number of court decisions were analyzed in the context of the subject of the study.*

***Key words:*** *cybercrime, classification of cybercrimes, statistical indicators, cyberspace, blockchain, organized cybercrime.*