УДК 343.9:004.056
DOI https://doi.org/10.32782/klj/2026.3.42

Тарнаруцька А. В.,
здобувач вищої освіти
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького
ORCID: 0009-0003-8246-2128

Ніколаєнко Т. Б.,
доктор юридичних наук, професор,
професор кафедри теорії права та кримінально-процесуальної діяльності
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького
ORCID: 0000-0002-4587-2561

КІБЕРЗЛОЧИНИ: СУЧАСНІ ВИКЛИКИ КРИМІНАЛЬНОМУ ПРАВУ

Анотація. У статті проведено дослідження сучасних викликів, які у зв'язку із цифровізацією державного сектору, впровадження кіберфізичних систем у промисловість та енергетику створили, з однієї сторони безпрецедентні можливості для загальносвітового прогресу, з іншої сторони, відкриті питання, які потребують системного підходу щодо зміни усталених постулатів щодо об'єкта, суб'єкта, предмета та місця вчинення кіберзлочинів.

Висвітлено, що в умовах розвитку технологій є потреба у перегляді правових положень у чинному КК щодо територіалізації вчинення кіберзлочинів з можливістю притягнення винних до відповідальності.

Проаналізовано, що нові форми посягань (маніпуляції ШІ, крадіжки віртуальних активів, атаки на інтернет речей) потребують перегляду об'єктів правової охорони в контексті захисту кіберпростору.

Окреслено, що з розвитком децентралізованих фінансів, технології блокчейн та віртуальних активів необхідно розширити предмети кіберзлочинів, унормувати заходи для забезпечення притягнення до відповідальності, на кшталт «крипто-арешту» в мережі, правового врегулювання статусу смарт-контрактів, а також впровадження спеціальної кримінальної відповідальності для розробників та власників ШІ за неналежний нагляд за автономними системами.

Встановлено, що сучасне кримінальне законодавство повинно враховувати при визначенні суті шкоди, які заподіюється від вчинення кіберзлочинів в розрізі системного аналізу деструктивного їх впливу на інформаційні та управлінські процеси на рівні державі.

Сучасні кібератаки, які в умовах воєнного стану впливають на забезпечення критичної інфраструктури, критичної інформаційної інфраструктури та за своїми наслідками є загрозою національній та громадській безпеці, доцільно розглянути такі кіберзлочини в системі воєнних злочинів.

Ключові слова: *кіберзлочини, об'єкт злочину, суб'єкт злочину, предмет злочину, територіалізація злочину, штучний інтелект, воєнні злочини.*

Tarnautska A. V., Nikolaienko T. B. Cybercrime: current challenges for criminal law

Abstract. This article examines the current challenges that, due to the digitization of the public sector and the introduction of cyber-physical systems in industry and the energy sector, have, on the one hand, created unprecedented opportunities for global progress, and, on the other hand, have raised unresolved issues that require a systematic approach to revising established assumptions regarding the object, subject, subject matter, and location of cybercrimes. The article highlights that, in light of technological advancements, there is a need to revise the legal provisions in the current Criminal Code regarding the territorial jurisdiction of cybercrimes, with a view to holding perpetrators accountable. The analysis shows that new forms of cybercrimes (AI manipulation, theft of virtual assets, and attacks on the Internet of Things) require a review of the objects of legal protection

© Тарнаруцька А. В., Ніколаєнко Т. Б., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

in the context of cybersecurity. It is noted that with the development of decentralized finance, blockchain technology, and virtual assets, it is necessary to expand the scope of cybercrimes, standardize measures to ensure accountability–such as “crypto-seizure” online–legal regulation of the status of smart contracts, and the introduction of specific criminal liability for AI developers and owners for failing to properly supervise autonomous systems. It has been established that modern criminal legislation must take into account, when determining the nature of the harm caused by cybercrimes, a systematic analysis of their destructive impact on information and management processes at the national level. Given that modern cyberattacks, under conditions of martial law, affect the security of critical infrastructure and critical information infrastructure and, due to their consequences, pose a threat to national and public security, it is appropriate to classify such cybercrimes as war crimes.

Key words: *cybercrimes, object of the crime, subject of the crime, subject matter of the crime, territorialization of the crime, artificial intelligence, war crimes.*

Постановка проблеми. На межі першої та другої чверті XXI століття стрімка та незворотна конвергенція цифрових технологій стала визначальним фактором радикальної трансформації всієї системи соціальних, економічних, політичних та правових відносин. Інформаційно-комунікаційні системи, мобільні мережі нового покоління (5G/6G), глобальний інтернет речей (IoT), нейромережі та розподілені хмарні обчислення сформували нову багатошарову реальність – кіберпростір. Відповідно до Закону «Про основні засади забезпечення кібербезпеки України» цей простір фактично позбавлений будь-яких фізичних кордонів, він функціонує в режимі «24/7» і характеризується надвисокою швидкістю обміну інформаційними потоками, що остаточно нівелює традиційні геополітичні та юридичні уявлення про простір, час і державні межі. [16, стаття 1].

Масштабна цифровізація державного сектору (зокрема, успішна реалізація концепції «держави у смартфоні» в Україні), бурхливий розвиток децентралізованих фінансів (DeFi), впровадження кіберфізичних систем у промисловість та енергетику створили безпрецедентні можливості для загальносвітового прогресу. Водночас ці процеси породили глибокі системні вразливості, які стали фундаментом для появи та стрімкого поширення якісно нових, так би мовити «інтелектуальних» злочинів. Кіберзлочини сьогодні – це не поодинокі акти аматорського хакерства, а потужна, високотехнологічна, анонімна та ієрархічно структурована транснаціональна індустрія, яка починає функціонувати за бізнес-моделлю «злочин як послуга» (Crime-as-a-Service). За рівнем своєї прибутковості, масштабами охоплення аудиторії та ступенем руйнівного впливу на фінансову і політичну стабільність провідних держав вона сьогодні впевнено конкурує з найбільш небезпечними видами транснаціональної організованої злочинності. Для класичної доктрини кримінального права, як зазначають провідні вчені у цій галузі О.О. Дудоров, М.І. Хавронюк, це явище стало фундаментальним екзистенційним викликом, оскільки поставило під сумнів базові, усталені століттями постулати, зокрема, про місце вчинення кримінального правопорушення/злочину, державний суверенітет у віртуальному полі, правову природу об’єкта посягання та психологічні й юридичні характеристики суб’єкта вчинюваного правопорушення [9, с. 745-764].

Аналіз останніх досліджень і публікацій. Фундаментальні питання щодо протидії комп’ютерним кримінальним правопорушенням/злочинам (надалі будемо зазначати лише як злочини), формування засад так званого «цифрового кримінального права» та правової охорони інформаційних відносин перебували у колі наукових інтересів таких вчених, як: В.М. Бутузов [7], О.О. Дудоров, М.І. Хавронюк [9]. Процесуальні аспекти роботи із цифровими слідами, особливості використання електронних доказів та цифрова криміналістика ґрунтовно висвітлені у працях М.А. Погорецького [14], Ю.Ю. Орлова [12], Е. Кейсі [1], Б. Шнайєра [18]. Попри значний науковий вклад у цьому напрямку, стрімка еволюція технологій потребує оновлення правового реагування та унормування з урахуванням викликів суачсності. Так, невирішеними залишаються питання кваліфікації діянь, які вчиняються автономними агентами штучного інтелекту без прямого втручання людини, правового статусу смарт-контрактів як інструментів автоматичного вчинення таких злочинів.

У звязку з цим **метою нашого дослідження** є проведення системного аналізу трансформації ключових інститутів кримінального права

в контексті кваліфікації кіберзлочинів, дослідження природи новітніх технологічних загроз та наукове обґрунтування концептуальних засад переходу до нової правової парадигми як «цифрового кримінального права».

Виклад основного матеріалу. Сучасна кримінально-правова наука розглядає кіберзлочини не як окремий вид злочину, а як складну, динамічну сукупність суспільно небезпечних діянь, де комп'ютерні системи, мережі або цифрові дані виступають або як безпосередній об'єкт злочинного посягання, або як головний інструмент його підготовки та реалізації [7, с. 67-81]. Особливість цього явища полягає у його здатності до миттєвої зміни та адаптації будь-яких технологічних інновацій. У кримінально-правовому аспекті кіберзлочинів можна виокремити у певні групи. Це: а) кіберзалежні злочини (cyber-dependent), які технічно неможливі без існування комп'ютерних мереж та цифрових систем (до них можна віднести наприклад, «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» (ст. 361 Кримінального кодексу України (далі – КК), «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» (ст. 361^1 КК); «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» (ст. 363^1 КК)) та б) кіберопосередковані злочини (cyber-enabled). До останньої групи злочинів можна віднести ті злочини, де цифрові технології масштабують та модифікують так би мовити загально кримінальні протиправні діяння, на кшталт, шахрайства, крадіжки, вимагання, надаючи їм ознак анонімності та масовості. Для прикладу крадіжка цифрових активів або розповсюдження забороненого контенту [8, 142]. Проведення такої диференціації є фундаментом для удосконалення як самої кваліфікації нових видів злочинів у кіберпросторі, так й підвищенням ефективності методики їх розслідування.

В умовах шаленого розвитку технологій територіалізація вчинення злочину є одним із правових аспектів, які потребують уваги їх правового вирішення. Сучасне кримінальне право у традиційному його розумінні вибудоване за територіальним принципом щодо вчинення кримінального правопорушення (ст. 10 КК) [19, ст. 10]. У кіберпросторі «місце вчинення злочину» має дещо інший зміст. Правопорушник для вчинення кіберзлочинів може використовувати різні схеми щодо так званого «заплутування» ідентифікації місця його вчинення. Вчиняючи злочин, наприклад, щодо певної інформації, яка перебуває в певному місці (місто, країна, континент), сам порушник може перебувати у зовсім іншому місці і це місце може бути кардинально інше від предмету вчиненого злочину (інший континент, чи безпосередньо країна, яка взагалі не має кримінальної відповідальності за подібні дії або не підтримує договори про екстрадицію). У такому разі складається ситуація «позитивного конфлікту юрисдикцій», коли декілька держав одночасно мають формальне право на розслідування, проте жодна з них не володіє повним доступом до серверів та цифрової доказової бази [4, с. 59-71]. Порушники при цьому можуть уникати відповідальності використовуючи «юрисдикційний арбітраж», де свідомо переносячи свої технічні потужності в країни з низьким рівнем регулювання IT-сфери та відсутністю міжнародної правової кооперації [10, ст. 22].

Також у сучасних цифрових реаліях ми змушені говорити про появу абсолютно нових об'єктів правової охорони, як, наприклад: віртуальні активи, персональні дані (цінні економічні ресурси, цілісні алгоритми штучного інтелекту), стабільність функціонування об'єктів критичної інформаційної інфраструктури (енергомережі, транспортні системи, реєстри виборців тощо), посягання на які може призвести не лише до заподіяння матеріальної шкоди, до соціального колапсу цілих регіонів та потребують належного правового захисту. Тому сучасне кримінальне право має враховувати ці виклики сучасності та поступово відходити від вузького розуміння заподіяння матеріальної шкоди, а розглядати системність аналізу деструктивного впливу на інформаційні та управлінські процеси на рівні державі.

Потребує також нового підходу і розуміння суб'єкту кіберзлочину. Відповідно до умов чинного законодавства (ст. 18 КК) «суб'єктом кримінального правопорушення може бути лише фізична осудна особа, яка вчинила кримінальне правопорушення» [19] Проте, як ми вже зазначали вище, вчинення кіберзлочинів можливо у симбіозі людини та технологій, де ідентифікація виконавця вчиненюваного діяння ускладнюється сучасними технологічними винаходами (шифруванням, «цибулевою маршрутизацією» (Tor), використанням анонімних проксі-серверів та VPN тощо). Крім того в контексті професіоналізації кіберкриміналу, сьогодні вчиняють такі злочини не поодинокі «хакери», а високоорганізовані угруповання з чітким розподілом ролей та функцій щодо виконання того чи іншого процесу/складової об'єктивної сторони злочину (кодери, тестувальники вразливостей, психологи-маніпулятори, «мувери» криптовалют тощо). Слід враховувати також і те, що учасники (співучасники) кіберзлочинів, здебільшого можуть не знати один про одного, доведення наявності у них «єдиного умислу» щодо вчинення кіберзлочину у їх співучасті є надзвичайно складним завданням. Як правильно зазначив В.П. Шеломенцев: «Криміналізація суспільства обумовлює поширення організованої злочинності у середовищі глобальних інформаційних мереж, які давно вже перетворилися в електронний аналог суспільного життя.» [17, с. 314]. Доволі небезпечними у цьому разі виступають APT-групи (Advanced Persistent Threats), які мають пряму або опосередковану державну підтримку, якафактично перетворює кіберзлочини на інструмент гібридної війни.

Окремим викликом для сучасного суспільства є розвиток децентралізованих фінансів, технології блокчейн та віртуальних активів, які не лише позитивно впливають на суспільство в цілому, але й сприяють трансформації методів легалізації (відмиванню) доходів, одержаних злочинним шляхом. Так, на зміну класичним офшорам прийшли так звані «міксери», анонімні криптогаманці та децентралізовані протоколи обміну, які дозволяють миттєво конвертувати викрадені активи, оминаючи будь-який централізований банківський контроль. Особливістю блокчейну (децентралізована цифрова база даних, що функціонує як ланцюжок блоків, де кожен блок містить інформацію, захищену криптографією.) є його незмінність та децентралізація, що створює унікальну правову дилему: з однієї сторони, всі транзакції є публічними, з іншої, – встановлення реального власника гаманця без спеціалізованих інструментів аналітики є фактично неможливим [4, с. 60]. В контексті кримінального права, така ситуація вимагає чіткого визначення та унормування, з однієї сторони, віртуальних активів, як предметів кіберзлочинів, з іншої сторони, з дотриманням вимог Конвенції про кіберзлочинність, унормуванні заходів для забезпечення відповідальності, на кшталт «крипто-арешту» в мережі, а також правового врегулювання статусу смарт-контрактів [10, заголовок 4, ст.19]. Якщо смарт-контракт автоматично виконує розподіл вкрадених коштів, то як наголошує В.П. Шеломенцев, є потреба у кваліфікації такої діяльності не просто як шахрайства, а як високотехнологічного відмивання грошей із використанням автономного програмного коду [17, с. 316].

Особливої гостроти в умовах сучасних глобальних конфліктів набувають і питання захисту критичної інформаційної інфраструктури та протидії кібертероризму. Сьогоднені кібератаки, які відбуваються в умовах воєнного стану на енергосистему України, системи водопостачання, транспортні вузли за своїми негативними наслідками можна прирівняти до застосування зброї масового ураження. Крім того втручання в систему керування зокрема АЕС чи роботу залізничного сполучення можна однозначно визначити як вчинення терористичного акту (ст. 258 КК). І знову ж таки у цьому аспекті залишається проблемним питання суб'єкта вчинюваного злочину, адже, як показують реалії сьогодення, він може діяти від імені іншої особи чи іншої держави з використанням сучасних технологій. Тому доцільно унормувати у КК кіберзлочини як одними із видів воєнних злочинів. Я переконана, що кібератаки в умовах воєнного стану доцільно розглядати і як злочини проти миру та безпеки людства з посиленням кримінальної відповідальності за створення «бот-нетів», призначених для масштабних деструктивних операцій.

Наступним викликом у системі вчинюваних кіберзлочинів для кримінального права є розвиток штучного інтелекту (далі – ШІ). Як показав аналіз вчинюваних правопорушень у період 2024-2026 рр., технології генеративного ШІ постали одним із основних інструментів створення надреалістичного маніпулятивного контенту. Це призвело до появи нових видів злочинів, пов'язаних із маніпуляцією на світових фінансових ринках шляхом генерування фальшивих заяв політиків чи бізнесменів, використанням автономних шкідливих програм, які здатні самостійно, без вказівок людини, досліджувати систему захисту жертви, обирати оптимальну стратегію атаки та змінювати свій код для обходу антивірусних систем [6, с. 1-19]. Така ситуація породила концептуальну проблему встановлення вини вчинюваного діяння, де вибір дій покладається на автономні системи (алгоритми). У зв'язку з цим виникає питання: а хто б є суб'єктом злочину? Оскільки за чинним КК ним може бути лише фізична особа, то у разі, коли діяння вчиняється автономною системою (алгоритмом), питання притягнення винних до відповідальності залишається відкритим. Особа може бути притягнути до кримінальної відповідальності у разі створення, розповсюдження або збуту шкідливих програмних чи технічних засобів (ст. 361^1 КК), втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК), проте якщо злочин вчиняє автономна шкідлива програма, які здатна самостійно, без вказівки людини обирати оптимальну стратегію атаки, а змінювати свій код для обходу антивірусних систем, обирати «жерству», притягнути до відповідальності ШІ є неможливим. Тому, зрозумілою є позиція науковців, які обговорюють питання впровадження спеціальної кримінальної відповідальності для розробників та власників ШІ за неналежний нагляд за автономними системами, або ж введення поняття «технологічної необережності» [2].

Висновки. Проведене дослідження дозволяє дійти висновку, що у сучасних умовах розвитку технологій кіберзлочини набувають нових форм, що потребує перегляду базових юридичних інститутів щодо суб'єкта та об'єкта кіберзлочинів, особливостей місця їх вчинення та визначення кіберзлочинів у системі воєнних злочинів.

Доцільно у чинному КК сформулювати нові форми посягань (маніпуляції ШІ, крадіжки віртуальних активів, атаки на інтернет речей) як види кіберзлочинів; розширити види предметів кіберзлочинів та розуміння матеріальної шкоди від їх вчинення в контексті деструктивного впливу на інформаційні та управлінські процеси на рівні державі; запровадити нові види відповідальність за використання автономних бот-мереж та технологій синтетичного медіаконтенту у формі крипто-арешту та запровадити кримінальну відповідальність для розробників та власників ШІ за неналежний нагляд за автономними системами.

Конфлікт інтересів: один із авторів є членом редакційної колегії журналу. Для забезпечення незалежності редакційного процесу рукопис розглядався редактором, який не мав конфлікту інтересів з автором. Автор не брав участі у відборі рецензентів, процесі рецензування та прийнятті рішення щодо публікації статті. Рукопис пройшов стандартну процедуру подвійного сліпого рецензування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Burlington : Academic Press, 2011. 840 p. URL: https://shop.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-08-092148-8.

2. Cumbhadrika C., Herman K. Utilization of Artificial Intelligence in Cybercrime Investigation Process and Protection of Suspects' Human Rights. Global International Journal of Law and Social Sciences. 2025. Vol. 3, № 3. URL: https://www.researchgate.net/publication/397881735.

3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

4. Mordvyntsev M. V., Pashniev D. V., Khliestkov O. V. International Models of Legal Regulation for Combating Cybercrime: Recommendations for Ukraine. Проблеми законності. 2025. № 1. URL: https://pb.univd.edu.ua/index.php/PB/article/view/894.

5. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence : international treaty of 12 May 2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol.

6. Varela Enríquez C., Toasa R., Urdaneta M. The Use of Artificial Intelligence in Cybercrime: Impact Analysis in Ecuador and Mitigation Strategies. Journal of Cybersecurity and Privacy. 2025. Vol. 5, № 4. DOI: https://doi.org/10.3390/jcp5040100.

7. Бутузов, В. (2011). Системно-структурний аналіз як метод дослідження протидії комп'ютерній злочинності. *Правова інформатика*, (1), 67-71.

8. Демедюк С. В., Користін О. Є. Тенденції та характерні особливості online-шахрайства в Україні. Наука і правоохорона. 2024. № 3–4 (142–154). DOI: https://doi.org/10.36486/np.2024.3(65).12

9. Дудоров О. О., Хавронюк М. І. Кримінальне право України : навчальний посібник. Київ : Ваіте, 2014. 944 с.

10. Конвенція про кіберзлочинність : міжнародний документ від 23.11.2001 (Budapest Convention). URL: https://zakon.rada.gov.ua/laws/show/994_575.

11. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

12. Кудінов В. А., Орлов Ю. Ю. Підготовка фахівців з протидії кіберзлочинності. Бюлетень з обміну досвідом роботи. 2011. № 138. С. 23–34.

13. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

14. Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. Аналітично-порівняльне правознавство. 2025. Т. 3, № 5. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.37.

15. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

16. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

17. Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2009. Вип. 21. С. 314–322.

18. Schneier, B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W.W., 2021.

19. Кримінальний кодекс України : Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 06.07.2026)

Дата першого надходження статті до видання: 07.07.2026
Дата прийняття статті до друку після рецензування: 04.08.2026
Дата публікації (оприлюднення) статті: 16.11.2026