УДК 343.9.02:004.056.55
DOI https://doi.org/10.24144/2788-6018.2025.03.2.63

ЕВОЛЮЦІЯ КІБЕРЗЛОЧИННОСТІ: ЯК КРИМІНАЛЬНЕ ПРАВО АДАПТУЄТЬСЯ ДО ЦИФРОВОЇ ЕРИ?

Красько М.І.,
старший викладач кафедри правоохоронної діяльності та спеціальних юридичних дисциплін, Навчально-науковий інститут права Національного університету водного господарства та природокористування

Цевух А.І.,
здобувач другого (магістерського) рівня вищої освіти спеціальності 081 – Право, Навчально-науковий інститут права Національного університету водного господарства та природокористування
ORCID: 0000-0001-9696-5971

Красько М.І., Цевух А.І. Еволюція кіберзлочинності: як кримінальне право адаптується до цифрової ери?

У науковій статті здійснено ґрунтовне, міждисциплінарне дослідження процесів, що відбуваються у сфері кримінального права внаслідок стрімкої цифровізації суспільства. Автори аналізують кіберзлочинність не лише як новий вид злочинної діяльності, а як комплексне соціальне та правове явище, що постійно змінюється, вдосконалюється та створює виклики для правозастосовних органів, законодавців і міжнародної спільноти. Наголошується, що кіберзлочини сьогодні охоплюють надзвичайно широкий спектр правопорушень – від банального шахрайства до складних схем міжнародного відмивання грошей та фінансування тероризму.

У статті висвітлено основні інструменти та технології, які використовуються у кіберпросторі для вчинення злочинів: криптовалюти (зокрема біткоїн та монеро), технології блокчейн, даркнет, шифрувальні програми, фішингові кампанії, а також використання штучного інтелекту для генерації фальшивих особистостей або підробки документів. Розглянуто також явище етичного хакінгу та роль так званих «білих» хакерів, які, діючи в межах закону, сприяють підвищенню рівня кібербезпеки. Проаналізовано низку реальних кейсів, зокрема як в Україні, так і за кордоном, що дозволяє розкрити масштаби, способи реалізації та наслідки сучасних кіберзлочинів. Автори підкреслюють, що кіберзлочинність має транснаціональний характер, що ускладнює її виявлення, розслідування та притягнення винних до відповідальності в умовах, коли правова юрисдикція однієї держави не завжди достатня.

Особливий акцент зроблено на необхідності системного оновлення кримінального законодавства. Автори переконливо доводять, що традиційні інструменти кримінального права часто виявляються недостатніми або неефективними в умовах цифрової епохи. Розглянуто питання цифрових доказів, проблем їх належного документування, зберігання та використання в процесі доказування. Також піднято важливу проблему – відсутність єдиних міжнародних стандартів у сфері протидії кіберзлочинності, що суттєво гальмує взаємодію між країнами. У цьому контексті проаналізовано міжнародні конвенції, зокрема Будапештську конвенцію про кіберзлочинність, та окреслено напрями, в яких Україна має активізувати свою участь у глобальних ініціативах.

У статті представлено порівняльний аналіз підходів до протидії кіберзлочинності в різних країнах світу – США, Німеччині, Великій Британії, Естонії – та окреслено ті інструменти, які можна адаптувати до українських реалій. Наведено низку практичних рекомендацій щодо вдосконалення кримінального законодавства: запровадження нових складів злочинів, адаптація процедур збору цифрових доказів, розробка нормативної бази для співпраці правоохоронних органів з приватними кібербезпековими компаніями тощо.

Таким чином, дана стаття є важливим внеском у розвиток сучасної юридичної науки, адже вона не лише ідентифікує актуальні проблеми, але й пропонує реалістичні шляхи їх вирішення. Матеріал буде корисний не лише для теоретиків і практиків права, а й для IT-спеціалістів, розробників політик у сфері цифрової безпеки, міжнародних експертів та всіх зацікавлених у створенні безпечного цифрового середовища.

Ключові слова: цифрова ера, кримінальне право, кіберзлочинність, даркнет, хакери, білі хакери, криптовалюта, блокчейн, кібератаки, юрисдикція, транскордонність, цифрові докази.

Krasko M.I., Tsevukh A.I. Evolution of cybercrime: how criminal law adapting to the digital era?

In the scholarly article a thorough and interdisciplinary analysis is conducted on the transformations taking place within criminal law under the influence of rapid digitalization. The authors examine cybercrime not merely as a new form of criminal activity, but as a complex social and legal phenomenon that constantly evolves, becomes more sophisticated, and poses increasing challenges for law enforcement, legislators, and the international community. It is emphasized that cybercrimes today encompass an extremely wide range of offenses – from simple fraud to complex international money laundering schemes and the financing of terrorism.

The article explores the main tools and technologies used in cyberspace to commit crimes, including cryptocurrencies (particularly Bitcoin and Monero), blockchain technology, the darknet, encryption software, phishing campaigns, and the use of artificial intelligence to create fake identities or falsify documents. The concept of ethical hacking is also considered, along with the role of so-called "white hat" hackers, who work within legal frameworks to improve cybersecurity. The authors analyze a series of real-life cases, both in Ukraine and abroad, which illustrate the scale, methods, and consequences of modern cybercrime. They highlight the transnational nature of cybercrime, which significantly complicates its detection, investigation, and prosecution – especially when national legal jurisdictions prove insufficient.

Special emphasis is placed on the urgent need for a systemic update of criminal legislation. The authors convincingly argue that traditional legal tools are often inadequate or ineffective in the digital age. The paper addresses issues related to digital evidence, including the challenges of proper documentation, preservation, and admissibility in court. It also raises the important issue of the lack of unified international standards in the fight against cybercrime, which hinders intergovernmental cooperation. In this context, international legal instruments – particularly the Budapest Convention on Cybercrime – are reviewed, and the authors outline key areas where Ukraine must strengthen its participation in global initiatives.

A comparative analysis of national approaches to combating cybercrime is also provided, focusing on countries such as the United States, Germany, the United Kingdom, and Estonia. The study identifies best practices and legal mechanisms that could be adapted to the Ukrainian legal system. Practical recommendations are presented, including the introduction of new criminal offenses, the adaptation of procedures for handling digital evidence, and the development of a regulatory framework to facilitate cooperation between law enforcement and private cybersecurity firms.

Overall, this article represents a significant contribution to the development of modern legal scholarship. It not only identifies the most pressing problems related to cybercrime and criminal law but also proposes realistic and actionable solutions. The material is of particular interest not only to legal scholars and practitioners but also to IT specialists, cybersecurity policymakers, international legal experts, and all those engaged in building a secure and legally sound digital environment.

Key words: digital era, criminal law, cybercrime, darknet, hackers, white hat hackers, cryptocurrency, blockchain, cyberattacks, jurisdiction, cross-border issues, digital evidence.

Постановка проблеми: Розвиток технологій, що охоплює XXI століття, це безумовно стрімкий період, який веде людську цивілізацію до покращення якості нашого життя, проте швидкість цього розвитку також має і негативні моменти, одним з яких є кіберзлочинність. Кіберзлочинність є серйозним викликом для кримінального права в силу своєї постійної і швидкої трансформації від простих комп'ютерних вірусів до використання даркнету і криптовалют. За даними статистики, обсяг збитків внаслідок кіберзлочинності сягає трільйонів доларів на рік. Кібератаки, які здійснюються на персональні комп'ютери, великі компанії і криптовалютні біржі, демонструють вразливість існуючої правової системи і методів боротьби з таким видом правопорушенн.

Юрисдикція ускладнюється невизначеністю компетенції і транскордонністю злочинів, що вимагає міжнародної координації у боротьбі з кіберзлочинами. Як демонструють певні випадки, анонімність, яку забезпечують певні криптовалюти і технологія блокчейну, ускладнює збір цифрових доказів, що заважає притягненню до кримінальної відповідальності. Проблеми чинної правової міжнародної бази, доводять, що для ефективної протидії явищу кіберзлочинності, необхідно провести вдосконалення чинних правових норм, що в свою чергу має супроводжуватися міжнродною кооріднацією.

Дослідження проблеми: беручи до уваги шалений розвиток цифрових технологій, в різний час, багато вітчизняних вчених досліджувало явище кіберзлочинності у різних форматах: І.І. Ва-

сильковський у свої праці аналізував поняття «кіберзлочинність та «кіберзлочини», з'ясовуючи співвідношення цих понять. М.О. Кравцова досліджувала кіберзлочинність в рамках кримінологічної характеристики та запобігання таким злочинам з боку органів внутрішніх справ. В.В. Шевчук у своїй праці розкрив сутність кіберзлочинності, як перешкоди розвитку українського інформаційного суспільства, а О.С. Бондаренко та Д.А. Рєпін, у своїй науковій статті разом вивчали причини, ознаки та заходи протидії кіберзлочинності в Україні. Загалом, увага до даного питання з боку наукового суспільства є досить помітною, зважаючи на тисячі статей на подібну тему, що наявні у таких наукових системах, як Google академія.

Мета статті полягає в аналізі та дослідженні процесу еволюції кіберзлочинності і з'ясуванні, яким чином до цифрової ери пристосовується українське і міжнародне кримінальне право.

Виклад основного матеріалу: історія кіберзлочинності розпочала свій розвиток у 70-х роках минулого століття, коли 1971-го року було створено перший комп'ютерний вірус «Creeper» Бобом Томасом для ARPANET. В сучасному розумінні, цей експеримент не можна назвати «вірусом», адже в рамках тестування, його єдина функція полягала у виведенні на екран повідомлення: «I'm the Creeper, catch me if you can! (Я. Крипер, спіймай мене, якщо зможеш!)» [7, с. 211].

1986 року потенціал кіберзлочинності розпочав демонструвати свої можливості. Цього року було створено перше відоме шкідливе програмне забезпечення братами Амджадом і Басітом Фаруками з Пакістану. Вірус отримав назву «Brain» і заражав дискети IBM для захисту авторських прав, проте своїми діями він більше завдав хаосу користувачам, ніж допоміг [12, с. 9].

1989 рік – Джозеф Попп створив «AIDS Trojan», який зашифровував дані і за відновлення доступу до них вимагав грошову виплату у розмірі 189 доларів через поштову скриньку у Панамі. Автора вірусу було заарештовано в США, проте саме його «творіння» стало основою для майбутніх програм вимагачів по типу LockBit і WannaCry.

З початком XXI століття, цифрова ера і її розвиток набирає все більших обертів і тому, кіберзлочинність набуває комерційного характеру. Філіпінцем Онелом де Гузманом у 2000-му році створюється вірус-хробак «ILOVEYOU», який через фішингові листи заразив 50 мільйонів комп'ютерів і завдав збитків на 15 мільярдів (надалі - млрд) доларів. Але, не дивлячись на такі наслідки, автор вірусу уникнув покарання через відсутність відповідного законодавства на Філіппінах. 2004 року «Mydoom» створює ботнет для спаму, завдавши збитків обсягом 38 млрд доларів.

2010-ті роки – знаковий період у кіберзлочинності. Саме в цей час з'являється даркнет. Даркнет – або як його ще називають «чорна частина інтернету», це сегмент інтернету, що доступний через I2P (Invisible Internet Project) або Tor (The Onion Router), завдяки чому забезпечується анонімність через шифрування і маршрутизацію внаслідок застосування численних вузлів. Tor було розроблено у 2002 році Військово-морськими силами США для захисту комунікацій і який став основною для створення спеціальних прихованих сервісів із закінченням «.onion», які не можуть відобразити традиційні системи пошуку, як Google [15]. Згідно звіту Recorded Future за 2024 рік, близько 60 тисяч активний сайтів функціонує у даркнеті. 2011 року Россом Ульбріхтом запускається платформа «Silk Road» – одна з самих відомих платформ у світі, яка відома, як перший онлайн великий ринок торгівлі викраденими даними, хакерськими інструментами, зброєю та наркотиками, приймаючи у формі оплати криптовалюту біткойн (надалі – BTC). 2013 року ФБР закрило платформу, при цьому конфіскувавши 26 тисяч BTC (3,6 мільйона доларів за курсом 2013 року). Як основна форма оплати, BTC активно застосовувався у даркнеті до 2017 року, доки він не здобув велику популярність і з'явилась змога відслідковувати транзакції пов'язані з ним. Після цього на зміну йому прийшли більш анонімні криптоактиви, такі як Monero (XMR – створена 2014 року і використовує кільцеві підписи і приховані адреси для унеможливлення відстеження відправника і отримувача) і Zcash (ZEC - технологія дозволяє приховувати транзакції). В загальному, даркнет надає широкий спектр послуг: купівля викрадених даних, продаж зброї, наркотиків, шкідливого хакерського забезпечення, тощо. За свою діяльність з Silk Road, Ульбріхт отримав покарання у вигляді двох пожиттєвих термінів позбавлення волі, плюс 40 років за наркоторівлю і відмивання коштів, проте 21 січня 2025 року був помилуваний президентом США Дональдом Трампом, що визвало, як схвалення такого вчинку, так і обурення з боку певної частини суспільства [10].

Станом на сьогодні, кіберзлочинність охоплює як індивідуальні, так і ті атаки, що спонсоруються державою. Наприклад WannnaCry (2017), яка приписується групі хакерів «Lazarus» з Північної Кореї, вразила своєю кібератакою 200 тисяч комп'ютерів у 150-ти країнах світу, що також і зачепило Україну, де під атаку потрапили банки. У підсумку, ця атака задала збитків на 4 млрд доларів [6, с. 129]. Ще один вірус – «NotPetya» (2017), який пов'язаний з державним замовленням, оскільки його створення за підозрами, це справа рук російських спецслужб. Цей вірус у 2017 році завдав збитків на 10 млрд доларів, вразивши різноманітні міжнародні компанії серед яких Merck і Maersk, а також під вплив цього віруси потрапили «Укрпошта» та аеропорт «Бориспіль», що паралізовало їхню роботу [2, с. 187].

Як ми вже згадували раніше, криптовалюта має в собі як головну перевагу – анонімність. Внаслідок цього, вона як інструмент і технологія цікава хакерам.

У лютому 2025 хакери вже вище згадної північно-корейської групи «Lazarus», здійснили кібератаку на одну із найбільших світових криптобірж «Bybit», через що було викрадено 1,5 млрд доларів у криптовалюті ефіріум (надалі – ETH). Щоб досягти успіху, хакери застосували соціальну інженерію для обману підписантів електронних транзакцій шляхом підміну інтерфейсу транзакції [11]. Як стало відомо, за два дні через 50 новостворених електронних гаманців було відмито 160 млн доларів через децентралізовані біржі і інші інструменти технології блокчейн. Фактично причетність цієї організації до кібератаки і уряду Північної Кореї, підтвердила сама Північна Корея через декілька днів після кібератаки, шляхом оголошення створення країною власного криптовалютного державного резерву у криптовалюті ETH в еквівалентній сумі викрадних активів – 1,5 млрд доларів.

На жаль, через війну, яка триває в Україні, наша держава стала своєрідним випробувальним майданчиком для ефективності кібератак. У грудні 2023 року групою «Solntsepyok», яка як відомо, керується ГРУ РФ (Головне Розвідувальне Управління Російської Федерації), здійснила кібератаку на українську компанію зв'язку «Київстар», внаслідок якої 24 млн громадян залишились без зв'язку. 20 грудня 2024 року внаслідок чергової кібератаки, було завдано удар по державним реєстрам, що, як заявляють, стало однією із найпотужніших кібератак на нашу країну. Відомо, що від кібератаки постраждали портал «Дія», Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Єдиний державний реєстр прав на нерухоме майно, а також Супутні інформаційні системи державного управління [9].

Ключовою проблемою притягнення до кримінальної відповідальності за кіберзлочини є транскордонність цих злочинів, а також юридикція, де саме конкретно розпочалося кримінальне правопорушення. За приклад такої проблеми, можемо взяти ситуації, які доводять цю наявну проблему. Якщо, наприклад, згадати атаку на Bybit групою «Lazarus», то проблема полягає у тому, що КНДР (Корейська Народна Демократична Республіка) взагалі відмовляється співпрацювати з міжнародними правоохоронними органами, а сервери, якими могли для цієї атаки користуватися хакери, імовірно були розміщені в Сінгапурі або Нідерландах, а сама біржа Bybit базується в Дубаї, операційні центри якої знаходяться у Гонконгу. Тобто, на практиці виникає ситуція хаосу в питанні повноцінного контролю справи, який через такі обставини, не може забезпечити жодна країна.

Аналогічні випадки трапилися з розслідуванням кібератаки WannaCry у 2017 році, зломом соціальної мережі «Twitter» у 2020 році і операцією «Bayonet» проти діяльності даркнету 2017 року. У першому випадку 2017 року, США звинуватили групу хакерів «Lazarus», але зважаючи на відсутність з КНДР екстрадиційних угод, будь-яке притягнення до відповідальності, не вдалося. 2020 року відбулася кібератака на соціальну мережу Twitter, де головний підозрюваний діяв з штату Флорида (США), а його спільники працювали з Нідерландів та Великобританії, що вимагає співпраці національних правоохоронних органів і Інтерполу. В операції «Bayonet» 2017 року проти даркнету, ефективне слідство вимагало співпраці між такими країнами як США, Канада, Нідерланди та Тайланд, оскільки виникла наступна ситуація: засновник AlphaBay (платформа анонімного продажу нелегальних товарів і послуг) Олександр Казес (громадянин Канади) був заарештований у Бангкоку (Тайланд), сервери платформи конфісковані у Європі (Нідерланди), активи було заморожено в США. Через це правопорушення розслідувалося два роки через бюрократичні перепони [17]. Ці всі приклади, нам демонструють, що необхідно створити глобальну систему швидкого реагування на кіберзлочинність, яка надасть можливість у поєднанні з верховенством права, обходити національні бар'єри.

У таких видах правопорушень, як кіберзлочинність, докази або як їх ще можна назвати «цифрові докази», відіграють ключову роль у притягненні до кримінальної відповідальності за вчинення такого діяння. Як ми вже з'ясували, правопорушення у кіберпросторі, це справжній виклик для системи кримінального права, а це в свою чергу означає, що процес збору доказів є надзвичайно складним через крихкість, мінливість і вразливість до маніпуляцій.

Наприклад, у розслідування проти «Silk Road» 2013 року, захист стверджував, що докази, які були знайдені на ноутбуці Ульбрхта були підроблені ФБР шляхом використання спеціального програмного забезпечення, проте суд відхилив такі аргументи. Коли СБУ розслідувало атаку на «Київстар» у грудні 2023 року, були зібрані IP-адреси та знайдено зашифровані канали у месенджері «Telegram», проте через використання VPN сервісів і проксі-серверів у кількох країнах, зібрати усі докази було неможливо.

Якщо ж взяти до уваги криптовалютні кібератаки, наприклад ситуацією зі взломом біржі Bybit, то блокчейн-аналітики такі як Elliptic та ZachBit змогли надати детальні звіти про рух викрадених монет 401 тисячі ETH, але враховуючи, що хакери групи Lazarus, користувалися децентралізо-

ваними біржами (DEX) і мікшерами такими як Tornado Cash, що забезпечують повну анонімність, внаслідок чого збір доказів був неможливий. Також проблеми збору цифрових доказів включають в себе: проблеми з неналежним документуванням вилучення серверів, фізичне знищення серверів хакерами, використання зашифрованих протоколів, до яких не можливо отримати доступ без спеціального електронного ключа [14].

Ще однією проблемою у боротьбі з кіберзлочинністю варто окреслити застарілість законодавства, яке було сформовано в епоху фізичних злочинів. На жаль, традиційне кримінальне право не встигає за шаленими темпами розвитку кіберзлочинності і її технологічних методів. В Україні у Кримінальному Кодексі існує стаття 361 (Незаконне втручання в роботу комп'ютерів), яка була введена у дію 2001-го року, проте досі вона не охоплює поняття «блокчейн», соціальну інженерію і криптовалютні кібератаки на криптобіржі, що суттєво гальмує ефективність протидії кіберзлочинності і, наприклад, призводить до того, що не можливо до кінця довести кримінальну справу в силу відстуності у законодавстві такого визначення як «комп'ютерне шахрайство». Закон США Computer Fraud and Abuse Act (CFAA) 1986 року також зазнає критики через недостатню детальність норм. Наприклад, у розгляді справи «Van Buren v. United States» у 2021 році, Верховний Суд США дійшов висновку, що перевищення доступу до комп'ютеру не завжди є злочином, що перешкоджує переслідуванню хакерів, що використовують легальні облікові дані. 2024 року Конгрес США запропонував «H.R.7156 – Combating Money Laundering in Cyber Crime Act of 2024», направлений на посилену боротьбу з фінансовими злочинами у кіберпросторі. Станом на зараз він знаходиться на стадії розгляду у Конгресі [16].

Закон Великобританії «Computer Misuse Act» 1990-го року, був доповнений поправками 2015-го року стосовно визначень про «DDoS-атаки», але поки на жаль, не охоплює криптозлочини. Японський закон про кіберзахист 2016 року досі не враховує даркнет-ринки, а китайський закон не бере до уваги боротьбу з зовнішніми хакерами за типу як группа Lazarus, а концентрується на контролі даних. У Німеччині в рамках IT-Sicherheitsgesetz 2.0 було посилено захист кіберінфраструктури, проте як і в Україні не охоплюється соціальна інженерія у кібератаках.

Держави активно вживають заходів для боротьби з кіберзлочинністю. Наприклад, Україна 7 вересня 2005 року ратифікувала Будапешську конвенцію або як вона ще відома Конвенцію Ради Європи про кіберзлочинність [4]. 2017 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України». 30 грудня 2021 року було опубліковано рішення «Про План реалізації Стратегії кібербезпеки України» Ради Національної безпеки і оборони України (РНБО) і введено в дію Указом Президента України від 1 лютого 2022 року [8]. 24.03.2022 року було прийнято Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» [3]. Після прийняття закону було доповнено статті Кримінально Кодексу Україні (ККУ): 361 стаття ККУ (Несанкціоноване втручання в роботу автоматизованих систем) – додано частину п'яту про посилення відповідальності за втручання в роботу інформаційних систем у період воєнного стану [13, с. 411]. Стаття 361-1 ККУ (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів) у новій редакції, передбачає посилення санкцій за створення шкідливих програм для несанкціонованого втручання в роботу інформаційних систем [13, с. 410].

США розпочало адаптацію кримінального права до боротьби із кіберзлочинністю, що як раніше згадувалось, у 1986 році з прийняттям закону про комп'ютерне шахрайство та зловживання (CFAA), який став основою для криміналізації несанкціонованого доступу до комп'ютерних систем [1, с. 22]. 2001 року після серії терактів 11 вересня, було прийнято USA PATRIOT Act (Патріотичний Акт), який розширив повноваження правоохоронних органів у сфері кібербезпеки. 2015 року прийнято закон про модернізацію кібербезпеки для посилення захисту критичної інфраструктури і покращеної координації дій між державним і приватним сектором. У 2023 році було представлено нову стратегію кібербезпеки «National Cybersecurity Strategy» для боротьби з хакерськими кібератаками та цифровими злочинами. Згідно цієї стратегії, такі великі компанії як Google та Microsoft, зобов'язуються впроваджувати більш надійні системи кіберзахисту задля зменшення ризиків для користувачів. Як держава, США є активним учасником Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція) і підтримує тісний зв'язок зі своїми союзниками з Європейського Союзу в питанні протидіям кіберзагрозам.

Естонія – країна лідер цифрових технологій у Європі. Країна має достатньо чітке законодавство у сфері протидії кіберзлочинності, що базується на Кримінальному Кодексі країни від 2001-го року (Karistusseadustik) і Законі про запобігання відмиванню грошей і фінансуванню тероризму (надалі – AML Act). Внаслідок кібератак, що регулярно проводилися над урядовими і банківськими сайтами країни, найбільша відбулася у 2007 році з боку Росії, країна ратифікувала Будапештську конвенцію з метою покращення правової бази [5, с. 699]. У відповідних статтях КК Естонії зазначено: стат-

тя 206 (Незаконне проникнення до комп'ютерної системи) – передбачає до 3 років ув'язнення за таке діяння. Стаття 208 (Поширення комп'ютерного вірусу) – передбачає до 1 року ув'язнення за створення або розповсюдження шкідливого програмного забезпечення. Стаття 209 (Шахрайство) - застосовується також і до криптошахрайства з покаранням позбавленні волі до 7 років.

AML ACT 2017 року передбачає, що криптовалюти – це цифрова цінність і тому, вимагає від постачальників віртуальних активів ліцензії від Фінансової розвідки країни (FIU). Відмивання криптоактивів через різні мікшери і децентралізовані біржі, підпадають під статтю 394 КК (Легалізація доходів, одержаних злочинним шляхом). Країна активно співпрацює з білими хакерами, Інтерполом, США та рештою Європейського Союзу в рамках протидії кіберзлочинності. У місті Таллін міститься Центр кібероборони НАТО (CCDCOE).

Білі хакери - спеціалісти з кібербезпеки, що використовують свої знання у законних цілях і на відміну від «чорних хакерів», діють з дозволу власників систем для виявлення недоліків. Наприклад, білий хакер ZachXBT у лютому 2025 році допоміг ФБР ідентифікувати криптогаманці хакерів з групи Lazarus, за що отримав винагороду 50 тисяч доларів США. Білі хакери легалізовані і мають свій правовий статус, що захищає від переслідування, у таких країнах, як Естонія, Нідерланди, США та Великобританія.

На основі всього вищевикладеного матеріалу пропонуємо: доповнити Будапештську конвенцію шляхом додання до неї положення блокчейн-транзакцій, механізм естрадиції та економічні санкції для країн, що підтримують хакерів, як це робить Північна Корея. Необхідно розробити правила автоматичного заморожування криптоактивів на біржах після кібератак. Для успішності протидії кіберзлочинності потрібно застосовувати штучний інтелект, шляхом створення глобальної платформи відстеження криптотранзакцій і прогнозування кіберзагроз. Далі необхідно створити міжнародні кіберсили під егідою ООН для швидкого реагування на кібератаки з правом блокувати криптоактиви на біржах і координувати дії країн. Локально пропонуємо створити в Україні кіберцентри для звітів про кіберзлочини з цілодобовою підтримкою, а також легалізувати діяльність «білих хакерів» з чітким визнанням правового статусу та чіткими критеріями їхньої роботи, задля підвищення якості безпеки у кіберпросторі. Також, на нашу думку, в рамках мотивації можливо запровадити глобальну програму винагород за виявлення вразливостей у різних системах, що буде підтримувати загальносвітовий рівень кібербезпеки.

Висновок: Цифрова ера, яка характеризується стрімким розвитком інформаційних технологій, радикально трансформує як структуру суспільних відносин, так і природу злочинності. У ході дослідження було з'ясовано, що кіберзлочинність стала не лише окремим видом протиправної діяльності, а й глобальним викликом, що ставить під сумнів ефективність традиційних підходів до кримінального правозастосування.

По-перше, кіберзлочинність як соціально-правове явище має гібридну природу: вона водночас функціонує в межах технічних, економічних, юридичних та навіть політичних систем. Її основними рисами є анонімність, транскордонність, динамічність і висока технічна складність. Ці характеристики унеможливлюють ефективне реагування виключно засобами національного кримінального права.

По-друге, аналіз законодавства України та провідних зарубіжних країн свідчить про фрагментарність правового регулювання у сфері боротьби з кіберзлочинністю. Досі не вироблено уніфікованих підходів до кваліфікації цифрових злочинів, що, у свою чергу, перешкоджає правозастосуванню, обміну доказами, міжнародному розшуку осіб та притягненню їх до відповідальності.

По-третє, сучасні технології, зокрема даркнет, криптовалюти, блокчейн, а також розвиток технологій штучного інтелекту, відкривають не тільки нові можливості для бізнесу та комунікацій, але й слугують ефективним інструментом для організованої кіберзлочинності. Кримінальне право має відповідати не лише на вже відомі загрози, але й проактивно передбачати потенційні вектори розвитку цифрової злочинності.

По-четверте, ефективна протидія кіберзлочинності можлива лише за умови синхронного розвитку кількох компонентів:

- адаптації кримінального та кримінально-процесуального законодавства до цифрових викликів;
- технічного переозброєння правоохоронних і судових органів;
- зміцнення міжнародно-правової співпраці;
- підвищення рівня цифрової обізнаності суспільства.

Наведений прогноз Cybersecurity Ventures про щорічні збитки від кіберзлочинності у розмірі 10,5 трильйона доларів США вже у 2025 році свідчить не просто про масштаб проблеми – це сигнал до переосмислення стратегій національної та глобальної безпеки. Ігнорування необхідності глибинного реформування кримінального права означає втрату здатності держав адекватно реагувати на нові типи загроз.

Таким чином, лише поєднання правових, технологічних і міжнародно-кооперaційних зусиль може забезпечити адекватну відповідь на виклики цифрової епохи. Кримінальне право має трансформуватися з реактивного інструменту в гнучку систему, здатну адаптуватися до умов постійних технологічних змін, не втрачаючи при цьому основоположних принципів законності, справедливості та прав людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2024. № 3 (83). С. 19–23.
2. Артеменко, А.В. Масові кібератаки: навчання з найбільших випадків в історії. In: The 5 th International scientific and practical conference "Global science: prospects and innovations"(December 28-30, 2023) Cognum Publishing House, Liverpool, United Kingdom. 2023. С. 186–190.
3. Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 11.04.2025).
4. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 07.04.2025).
5. Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. Україна дипломатична. 2024. С. 696–708.
6. Насатов, О.І., Плєхова, Г.А. Хмарні технології та кібербезпека. 2024. С. 127–129.
7. Паржин, А.Ю. Комп'ютерні віруси та антивірусний захист: основні аспекти. 2023. С. 210–214.
8. Рішення Ради Національної безпеки і оборони України від 30 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 08.04.2025).
9. Суперкібератака росіян на Україну: що відбулося, що з реєстрами зараз і як це позначиться на громадянах. URL: https://news.telegraf.com.ua/ukr/ukraina/2024-12-20/5891087-superkiberataka-rosiyan-na-ukrainu-shcho-vidbulosya-shcho-z-reestrami-zaraz-i-yak-tse-poznachitsya-na-gromadyanakh (дата звернення: 09.04.2025).
10. Трамп помилував засновника даркнет платформи Silk Road: хто це та за що йому дали довічне. URL: https://24tv.ua/ross-ulbriht-silkroad-film-hto-tse-shho-take-darknet-chomu-tramp_n2735167.
11. Хакери могли викрасти у біржі Bybit $1,5 млрд у криптовалюті. URL: https://forbes.ua/news/u-birzhi-bybit-mogli-vikrasti-11-mlrd-u-kriptovalyuti-21022025-27418 (дата звернення: 10.04.2025).
12. Черненко Д.В. Інтелектуальна технологія детектування шкідливого програмного забезпечення : магістерська робота. Суми: Сумський державний університет. 2022. 44 с.
13. Юртаєва, К.В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. 2022. С. 409–414.
14. Bybit Hack Explained: Analyzing The Biggest Attack In Crypto History. URL: https://cryptomaniaks.com/bybit-lazarus-crypto-hack-explained (дата звернення: 11.04.2025).
15. Deep web vs. dark web: What's the difference? URL: http://surl.li/khfequ (Дата звернення: 08.04.2025).
16. H.R.7156 - Combating Money Laundering in Cyber Crime Act of 2024. URL: https://www.congress.gov/bill/118th-congress/house-bill/7156 (дата звернення: 05.04.2025).
17. Operation Bayonet (darknet). URL: https://en.wikipedia.org/wiki/Operation_Bayonet_%28darknet%29 (дата звернення: 06.04.2025).