DOI https://doi.org/10.30525/978-9934-26-686-7-10

СУЧАСНІ ВИКЛИКИ КРИМІНАЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРЗЛОЧИННОСТІ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ ВИМІРИ

Ларченко М. О.

ВСТУП

Стрімкий розвиток цифрових технологій та глобалізація кіберпростору зумовили нові загрози безпеці держав, суспільства та окремих українських громадян. Кіберзлочинність набуває все більшої організованості, а її наслідки можуть мати критичний вплив на функціонування інформаційних систем, фінансового сектору, критичної інфраструктури та навіть національної безпеки. Кримінально-правове регулювання кіберзлочинності стикається з низкою викликів, серед яких: швидка еволюція способів вчинення кіберзлочинів, складність ідентифікації правопорушників, проблеми кваліфікації окремих діянь та їх відмежування від суміжних правопорушень, відсутність єдиних стандартів відповідальності на міжнародному рівні, а також неефективність деяких механізмів правозастосування. Зважаючи на глобальний характер кіберзлочинності, особливої уваги потребує питання міжнародного співробітництва у цій сфері. Незважаючи на існування таких міжнародних правових актів, як Будапештська конвенція про кіберзлочинність, проблема гармонізації законодавства та координації дій держав у боротьбі з кіберзлочинами залишається актуальною. У цьому контексті виникає необхідність комплексного аналізу кримінально-правового регулювання кіберзлочинності, визначення його сучасних викликів на національному та міжнародному рівнях, а також пошуку шляхів удосконалення законодавства та правозастосовної практики.

1. Виникнення передумов проблеми та формулювання проблеми

Дослідження проблеми кіберзлочинності останнім часом постійно проводиться на міжнародному та національному рівнях. Значний внесок у розвиток цієї тематики зробили такі науковці, як Аніщук В. В. та Зицик С. Г., які аналізують методи протидії кіберзлочинам через міжнародну співпрацю[1], а також Степаненко Н. В., Піддубний Д. Д., що досліджують проблематику кримінально-правової кваліфікації атак на критичну інфраструктуру. Зокрема, наголошується, що запобігання та боротьба з кіберзлочинністю вимагає комплексного підходу, що поєднує правове регулювання, технологічні рішення, міжнародне співробітництво та кіберграмотність, йдеться і про необхідність розвитку національного законодавства у сфері кібербезпеки та

[1] Аніщук В. В., Зицик С. Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського Національного Університету.* 2024. Серія ПРАВО. Випуск 83: частина 3, С. 19-23. DOI https://doi.org/10.24144/2307-3322.2024.83.3.2

кіберзлочинності відповідно до міжнародних стандартів[2]. Бараненко Р. В. аналізує особливості застосування спеціальної термінології, аналізуючи наукові праці вітчизняних та зарубіжних дослідників із питань протидії кіберзлочинності[3].

Ряд авторів, зокрема: Авдєєва Г. та Живуцька-Козловська Е., Романюк В. В. та Абламський С. Є., Гарасимів О. І., Марко С. І. та Ряшко О. В. аналізують проблеми використання цифрових доказів у кримінальному судочинстві України та критерії їх допустимості, що є досить серйозною проблемою для судової практики на сучасному етапі. Важливим є також міжнародний досвід у цій сфері, який ще потрібно вивчати та аналізувати[4].

У зарубіжній науці кіберзлочинність вивчають досить глибоко і вже тривалий час. Зокрема, варто згадати роботу Sergiu Cernomoreț та Andrei Nastas, які звертають увагу саме на порівняльний аналіз кіберзлочинності в системі кримінального права та необхідність уніфікації національних правових систем у зазначеній сфері[5]. Актуальним представляється дослідження Murshal Senjaya, де йдеться про кіберзлочинність і кримінальне право в епоху штучного інтелекту. Зокрема, проблеми в правоохоронних органах Індонезії та інших аналізованих автором країн, пов'язані з неправомірним використанням штучного інтелекту, є досить складними, особливо через відсутність конкретних норм, які б регулювали його використання в контексті кіберзлочинності. Існуючі норми часто не охоплюють нові ситуації, що знижує ефективність правозастосування[6]. У підсумку варто згадати Ajoy P. B., який критично аналізуючи ефективність кримінального права в боротьбі з кіберзлочинністю, зазначає, що існує багато факторів, які сприяють неспроможності кримінального права повністю контролювати кіберзлочинність. Ці фактори включають проблеми, пов'язані з анонімністю, юрисдикцією, екстрадицією, правоохоронним механізмом;

---

[2] Степаненко Н. В., Піддубний Д. Д. Сучасні проблеми запобігання і протидії злочинності у сфері інформаційних технологій. *Legal Bulletin.* 2024, 73-81. https://doi.org/10.31732/2708-339X-2024-14-A10

[3] Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ "КПІ" Політологія. Соціологія. Право.* № 1(49) (2021). DOI: https://doi.org/10.20535/2308-5053.2021.1(49).233023

[4] Авдєєва, Г., Живуцька-Козловська, Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*, Вип. 1 (30), 2023. 126-143. https://doi.org/10.32353/khrife.1.2023.07; Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека,* 2 (93), 2024. 140-150. https://doi.org/10.32631/pb.2024.2.13; Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО.* Вип. 75: ч. 2. 2023. 158-162. https://doi.org/10.24144/2307-3322.2022.75.2.25

[5] Sergiu Cernomoreț & Andrei Nastas. Comparative Analysis of Cybercrime in the Criminal Law System. International Academic Publisher. Bucharest, Paris, Calgary 2023. 82 p. URL: https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf

[6] Senjaya, Murshal. Cyber Crime And Criminal Law In The Era Of Artificial Intelligence. International Journal of Law and Society. 1, 2024. 268-276. DOI: https://doi.org/10.62951/ijls.v1i4.210

відсутність даних, що стосуються кіберзлочинності, включаючи неповідомлення про кіберзлочини, труднощі з ідентифікацією, визначенням місцезнаходження та арештом кіберзлочинців, відсутність експертів, проблеми, пов'язані з технологіями, міжнародним правом тощо[7].

Попри значну кількість сучасних українських та закордонних досліджень, ще більше питань залишаються невирішеними. Серед них: 1) недостатня уніфікація кримінально-правових норм щодо відповідальності за кіберзлочини на міжнародному рівні; 2) проблеми ідентифікації злочинців, які діють у цифровому просторі, та особливості збору доказів; 3) відсутність дієвих механізмів співпраці між державами у сфері екстрадиції та спільного розслідування кіберзлочинів; 4) використання криптовалют, анонімних мереж, Darknet(у), що ускладнює виявлення злочинців і відстеження фінансових потоків.

Метою дослідження є комплексний аналіз сучасних викликів кримінально-правового регулювання кіберзлочинності на національному та міжнародному рівнях, зокрема проблем правозастосування щодо кібератак на критичну інфраструктуру, кримінальної відповідальності за розповсюдження шкідливого програмного забезпечення, а також особливостей міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Дослідження спрямоване на виявлення прогалин у чинному законодавстві та правозастосовній практиці, визначення перспектив їх усунення, а також оцінку ефективності міжнародних механізмів протидії кіберзлочинам.

2. Проблеми правозастосування щодо кібератак на критичну інфраструктуру

Критична інфраструктура є однією з найважливіших сфер національної безпеки будь-якої держави, а її захист від кібератак набуває дедалі більшої актуальності. Атаки на енергетичні системи, транспортні мережі, фінансові установи та державні інформаційні ресурси можуть мати катастрофічні наслідки, включаючи порушення функціонування життєво важливих сервісів, економічні збитки та загрозу людським життям. Проте практика правозастосування у сфері боротьби з такими кіберзлочинами стикається з низкою викликів, пов'язаних із міжнародною юрисдикцією, проблемами ідентифікації зловмисників, доказуванням та адекватністю національного законодавства.

Однією з базових проблем є визначення правового статусу кібератак на критичну інфраструктуру. У різних країнах такі злочини можуть кваліфікуватися по-різному: як незаконне втручання в комп'ютерні системи, терористична діяльність або навіть акт кібервійни. В Україні кримінальна відповідальність за кібератаки передбачена Кримінальним кодексом України, зокрема статтями 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»), 361[1] («Створення з метою протиправного

[7] Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis (March 20, 2022). Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2), 2022. 74-79. http://dx.doi.org/10.2139/ssrn.4061947

використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), 361[2] («Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації») та 363[1] («Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»)[8]. Проте визначення «кібератаки» залишається нечітким, що створює труднощі для правозастосовних органів.

Оскільки більшість кібератак здійснюються з-за кордону, правозастосовні органи часто стикаються з труднощами у встановленні та притягненні винних до відповідальності. Ключовими міжнародними інструментами для боротьби з кіберзлочинністю є Будапештська конвенція про кіберзлочинність (2001) та директиви Європейського Союзу у сфері кібербезпеки. Однак ефективність міжнародного співробітництва залежить від рівня взаємної правової допомоги між державами, що може ускладнюватися політичними чинниками та відсутністю єдиних стандартів кримінально-правового переслідування кіберзлочинців. Докладніше в Таблиці 1.

Таблиця 1

Порівняння правових режимів у різних країнах щодо кваліфікації кібератак

Країна	Основні закони та кодекси	Кваліфікація кібератак	Максимальне покарання
Україна	Кримінальний кодекс України (ст. 361, 361-1, 361-2, 363-1)	Незаконне втручання в комп'ютерні системи, поширення шкідливого ПЗ, кібершахрайство	До 10 років позбавлення волі
США	Computer Fraud and Abuse Act (CFAA), Patriot Act	Кіберзлочини кваліфікуються як шахрайство, злом, тероризм або шпигунство	До довічного ув'язнення (якщо спричинені людські жертви)
ЄС (загальні правила)	Директива ЄС 2013/40/EU, GDPR	Несанкціонований доступ, порушення даних, кібершахрайство	Від штрафів до 10 років позбавлення волі
Велика Британія	Computer Misuse Act 1990	Несанкціонований доступ, модифікація даних, DDoS-атаки	До довічного ув'язнення (якщо є серйозні наслідки)

[8] Верховна Рада України. Розділ: Законодавство України. Кримінальний кодекс України. 5 квітня 2001 року, № 2341-III. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 13.03.2025).

Продовження таблиці 1

Німеччина	Strafgesetzbuch (StGB), Telemediengesetz (TMG)	Несанкціонований доступ, порушення конфіденційності, шкідливе ПЗ	До 10 років позбавлення волі
Франція	Code pénal, Loi pour la confiance dans l'économie numérique	Кіберзлочини як комп'ютерне шахрайство або порушення інформаційної безпеки	До 7 років та штрафи до 300 000 євро
Китай	Cybersecurity Law, Criminal Law of PRC	Кібератаки можуть вважатися шпигунством або загрозою держбезпеці	До смертної кари (у випадках державної зради)
Японія	Act on the Prohibition of Unauthorized Computer Access	Несанкціонований доступ, модифікація даних	До 3 років позбавлення волі та штрафи

Ще однією серйозною проблемою є збирання та використання доказів у справах про кібератаки. Виявлення джерела атаки часто є технічно складним завданням, оскільки злочинці використовують анонімізаційні технології, ботнети та викрадені облікові записи. У судовій практиці нерідко виникають питання щодо допустимості цифрових доказів, а також їхньої автентичності та цілісності. Законодавство України містить загальні положення про електронні докази (ст. 99 КПК України «Документи»), а саме: документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження[9], проте потребує подальшої деталізації щодо специфіки доказування кіберзлочинів.

Варто звернути увагу, що в КПК взагалі не йдеться про цифрові докази, бо вони зовсім не тотожні електронним. Якщо під електронними доказами Закон розуміє певним чином розміщену на матеріальному носії цифрову або аналогову інформацію (аудіо чи відео записи, скріншоти переписки тощо), то цифрові докази це зліпки (дампи) оперативної пам'яті комп'ютера, дані аналізу його файлової системи, історія браузера тощо. Аналіз цих об'єктів може виступати предметом технічної експертизи, однак, коли мова йде про кіберзлочини, а також про багато інших категорій кримінальних правопорушень, які вчиняються з використанням комп'ютерів та комп'ютерних

[9] Верховна Рада України. Розділ: Законодавство України. Кримінальний процесуальний кодекс України. 13 квітня 2012 року, № 4651-VI. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 13.03.2025).

мереж, то саме такі цифрові докази мають вирішальну силу, звісно при дотриманні технічних правил їх збирання, зберігання та аналізу. Отримання цифрових доказів здійснюється виключно із дотриманням стандартів цифрової криміналістики та відповідно до міжнародних практик, зокрема, NIST та ISO 27037:2012[10] – єдиний стандарт з цього питання, що офіційно визнаний в Україні (ДСТУ 27037:2012). Лише він нормативно регулює в Україні технічні аспекти збору, зберігання та аналізу цифрових доказів.

Враховуючи вищезазначене, захист критичної інфраструктури від кібератак безумовно вимагає комплексного підходу, що включає вдосконалення національного законодавства, посилення міжнародного співробітництва та розвиток технічних засобів і методів розслідування. Вирішення зазначених проблем можливе шляхом адаптації кримінального та кримінального процесуального законодавства до новітніх викликів у сфері кібербезпеки, а також через активну участь України в міжнародних ініціативах щодо боротьби з кіберзлочинністю.

Ще одним критично важливим аспектом правозастосування щодо кібератак на критичну інфраструктуру є питання відповідальності приватного сектору. У сучасних реаліях значна частина критичної інфраструктури належить або обслуговується приватними компаніями, які не завжди належним чином дотримуються стандартів кібербезпеки. Недостатній рівень захисту інформаційних систем комерційних суб'єктів, які взаємодіють із державними мережами або фінансовими установами, може суттєво посилювати ризики успішності кібератак. У зв'язку з цим деякі країни, зокрема Європейський Союз, запроваджують механізми жорсткішого регулювання кібербезпеки приватного сектору, як-от Директива NIS2, яка встановлює вимоги до суб'єктів критичної інфраструктури щодо управління ризиками кіберзагроз та обов'язкового обміну інформацією про інциденти[11].

Окрім правового аспекту, важливою проблемою залишається питання превентивних заходів та стратегій кіберзахисту. У багатьох випадках кібератаки на критичну інфраструктуру виявляються лише після їх здійснення, що вимагає кардинального перегляду підходів до кібербезпеки на державному рівні. Одним із перспективних напрямів є розбудова національних центрів реагування на кіберінциденти (CERT), які координують діяльність державних і приватних суб'єктів у випадку масштабних атак. Український уряд також активно працює над посиленням кіберзахисту критичної інфраструктури, що знайшло своє відображення у прийнятті Закону України «Про основні засади забезпечення кібербезпеки України»[12] та створенні Національного координаційного центру кібербезпеки.

---

[10] International Standard ISO/IEC 27037. Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

[11] H-X. Директива кібербезпеки NIS2. *Електронний ресурс.* URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua

[12] Верховна Рада України. Розділ: Законодавство України. Закон України «Про основні засади забезпечення кібербезпеки України». 5 жовтня 2017 року № 2163-VIII. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 13.03.2025).

Водночас розвиток міжнародного співробітництва залишається ключовим елементом ефективної боротьби з кібератаками на критичну інфраструктуру. Участь у таких ініціативах, як Глобальний форум із кіберекспертизи (GFCE) чи діяльність у межах партнерства з НАТО (наприклад, у рамках Програми розширених можливостей), дає Україні можливість отримувати оперативну допомогу, обмінюватися розвідданими про нові загрози та вдосконалювати свої методи кіберзахисту.

З огляду на зростаючу кількість кібератак на критичну інфраструктуру, подальший розвиток правозастосування у цій сфері має орієнтуватися на такі ключові напрями: удосконалення кримінального законодавства щодо кіберзлочинів, створення ефективних механізмів притягнення до відповідальності суб'єктів, що нехтують вимогами кібербезпеки, а також активну участь у міжнародних ініціативах з метою посилення глобальної кіберстійкості. Докладніше: рисунок 1.

Рис. 1. Ланцюг кібератак на критичну інфраструктуру

3. Відповідальність за розповсюдження шкідливого програмного забезпечення

Розповсюдження шкідливого програмного забезпечення (ШПЗ) є одним із найбільш небезпечних кіберзлочинів, що завдає значної шкоди як приватним особам, так і державним установам та бізнесу. ШПЗ може використовуватися для крадіжки даних, несанкціонованого доступу до інформаційних систем,

вимагання та навіть для здійснення атак на критичну інфраструктуру. В Україні кримінальна відповідальність за такі дії регламентується статтею 361-1 Кримінального кодексу України, яка передбачає покарання за створення, розповсюдження або збут шкідливих програм.

Однією з основних проблем у боротьбі з розповсюдженням ШПЗ є необхідність доведення умислу правопорушника. Наприклад, розробка програмного забезпечення, яке може бути використане в злочинних цілях, сама по собі не є злочином, якщо особа не мала наміру завдати шкоди. Це створює значні труднощі для правоохоронних органів, особливо з огляду на те, що багато хакерських інструментів мають подвійне використання.

Ще одним викликом є транскордонний характер цього виду кримінальних правопорушень. Шкідливе програмне забезпечення часто поширюється через міжнародні сервери або анонімні платформи, що ускладнює встановлення особи злочинця та його притягнення до відповідальності. Важливу роль у цьому відіграє міжнародна співпраця, зокрема в рамках Будапештської конвенції та діяльності Європолу й Інтерполу.

Правоохоронні органи та кібербезпекові структури використовують різні підходи для боротьби з розповсюдженням ШПЗ, серед яких:

1) використання аналітичних методів та штучного інтелекту для відстеження нових загроз;

2) створення законодавчих механізмів для блокування шкідливого контенту та платформ, що його поширюють;

3) посилення відповідальності за кіберзлочини та вдосконалення правозастосовних процедур.

Таким чином, боротьба з розповсюдженням шкідливого програмного забезпечення вимагає комплексного підходу, що включає як ефективне кримінальне переслідування винних осіб, так і запровадження превентивних заходів, спрямованих на зниження ризику використання ШПЗ. Важливу роль у цьому процесі відіграє міжнародна співпраця, оскільки більшість загроз у кіберпросторі мають глобальний характер.

Також важливо враховувати, що ефективність кримінально-правового регулювання відповідальності за розповсюдження ШПЗ значною мірою залежить від гармонізації національного законодавства з міжнародними стандартами. Зокрема, у межах Європейського Союзу директива 2013/40/ЄС «Про атаки на інформаційні системи» встановлює вимоги до криміналізації незаконного втручання в комп'ютерні системи, включаючи створення та розповсюдження шкідливого програмного забезпечення.

Водночас, практика кримінального переслідування кіберзлочинців свідчить про необхідність запровадження спеціальних слідчих методів, адаптованих до кіберпростору. Наприклад, у деяких країнах застосовуються так звані «контрольовані операції» (controlled delivery), які дозволяють правоохоронцям відстежувати розповсюдження шкідливого програмного забезпечення та виявляти ключових фігурантів кіберзлочинних угруповань.

Окрему проблему становить відповідальність за розповсюдження ШПЗ у випадках, коли його поширення здійснюється через децентралізовані платформи або у мережах даркнету. Через особливості анонімізації,

притягнення до відповідальності таких зловмисників стає надзвичайно складним. Одним із можливих рішень у цій сфері є застосування методів цифрового профілювання кіберзлочинців, що дозволяє ідентифікувати потенційних правопорушників на основі їхніх поведінкових шаблонів у мережі.

На міжнародному рівні варто також враховувати роль приватного сектору у боротьбі з розповсюдженням шкідливого програмного забезпечення. Такі технологічні гіганти, як Microsoft, Google та Amazon, активно співпрацюють із правоохоронними органами у справі блокування зловмисних серверів і видалення контенту, пов'язаного з кіберзлочинною діяльністю. Наприклад, у 2020 році корпорація Microsoft спільно з ФБР та Європолом здійснила успішну операцію з ліквідації ботнету TrickBot, який використовувався для поширення програм-вимагачів.

З огляду на ці виклики, удосконалення кримінально-правового регулювання у сфері розповсюдження ШПЗ потребує комплексного підходу, що включає:

1) удосконалення механізмів співпраці між державами у сфері екстрадиції та збору цифрових доказів;

2) розробку міжнародних стандартів кваліфікації кіберзлочинів для уніфікації підходів до кримінальної відповідальності;

3) використання новітніх технологій, включаючи штучний інтелект, для виявлення та нейтралізації шкідливих програм на ранніх етапах їх розповсюдження.

Таким чином, боротьба з розповсюдженням шкідливого програмного забезпечення виходить за межі традиційних підходів кримінального права і вимагає інтеграції технологічних, правозастосовних та міжнародних інструментів для забезпечення ефективного реагування на загрози у кіберпросторі.

4. Актуальні кейси міжнародного співробітництва у боротьбі з кіберзлочинністю

Злочинність у кіберпросторі давно перестала бути локальним явищем і набула глобального характеру, що вимагає від держав тісної співпраці у сфері розслідувань, обміну інформацією та екстрадиції правопорушників. З огляду на складність встановлення особи злочинця, транскордонний характер атак та анонімність цифрових технологій, боротьба з кіберзлочинністю є значним викликом для правоохоронних органів. Варто також проаналізувати найважливіші кейси міжнародного співробітництва у боротьбі з кіберзлочинами.

1. Операція "Bayonet": ліквідація найбільшого нелегального маркетплейсу AlphaBay

Одним із найбільш значущих прикладів міжнародного співробітництва стало закриття даркнет-маркетплейсу AlphaBay у 2017 році. Ця платформа діяла як глобальний чорний ринок для продажу наркотиків, викрадених даних, шкідливого програмного забезпечення та інших незаконних товарів і послуг. Розслідуванням займалися правоохоронні органи США, Європолу, Канади, Великої Британії, Нідерландів та Таїланду. Ключовим фактором успіху стало залучення технологій аналізу блокчейн-транзакцій та координація між країнами щодо арешту засновника сайту Олександра Казеса. Цей кейс

демонструє ефективність міжнародної співпраці у боротьбі з кіберзлочинами, що використовують криптовалютні платежі[13].

2. Операція "GHOST": затримання учасників кіберзлочинного угруповання REvil

Група REvil, відома атаками програм-вимагачів (ransomware), у 2020 – 2021 роках атакувала низку великих компаній та державних установ, включаючи постачальників критичної інфраструктури. Одним із найгучніших випадків стала атака на компанію Kaseya, яка вплинула на понад 1500 організацій по всьому світу. У відповідь на ці злочини було проведено міжнародну операцію "GHOST", організовану ФБР, Європолом та правоохоронними органами низки європейських держав. Унаслідок спільних дій у 2021 році було заарештовано кількох учасників угруповання, а сервери REvil були виведені з ладу. Операція стала показовою з точки зору координації дій спецслужб та обміну інформацією між різними юрисдикціями[14].

3. Ліквідація ботнету Emotet

Emotet вважався одним із найнебезпечніших ботнетів у світі, використовуваним для розповсюдження банківських троянів та програм-вимагачів. У 2021 році внаслідок міжнародної операції за участі правоохоронних органів США, Німеччини, Великої Британії, Нідерландів, Канади та України вдалося ліквідувати цей ботнет, а також заарештувати причетних осіб. Одним із ключових аспектів успіху операції стала розробка та впровадження механізму дезактивації шкідливого програмного забезпечення на заражених пристроях, що стало прецедентом у світовій практиці боротьби з кіберзлочинами[15].

Попри описані та деякі інші успішні кейси у боротьбі з кіберзлочинністю, міжнародне співробітництво стикається з низкою проблем серед яких:

1) юридичні бар'єри – відмінності у кримінальному законодавстві різних країн, що можуть ускладнювати екстрадицію та притягнення кіберзлочинців до відповідальності;

2) нестача оперативного обміну інформацією – не всі держави мають ефективні механізми взаємодії між правоохоронними органами;

3) використання юрисдикцій з низьким рівнем регулювання – багато хакерських угруповань базуються в країнах, де відсутні суворі закони щодо кіберзлочинності.

Ефективна боротьба з кіберзлочинністю вимагає подальшої інтеграції міжнародних зусиль, розширення повноважень інституцій, таких як Європол, Інтерпол та ФБР, а також вдосконалення механізмів спільного реагування. Приклад операцій "Bayonet", "GHOST" та ліквідації Emotet свідчить

[13] CybelAngel. Home. The Impact of Dark Web Marketplace Takedowns [AlphaBay and Hansa]. September 24, 2024. URL: https://cybelangel.com/alphabay-hansa-two-major-dark-web-marketplaces-shut/

[14] CSO. Home. Security REvil ransomware explained: A widespread extortion operation. 12 Nov 2021. URL: https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html

[15] EUROPOL. Home. Media & Press. World's most dangerous malware EMOTET disrupted through global action. 27 Jan 2021. URL: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

про необхідність комплексного підходу до протидії кіберзлочинам, який включає правозастосовні, технічні та дипломатичні інструменти.

Одним із перспективних напрямів міжнародного співробітництва у боротьбі з кіберзлочинністю є створення єдиних стандартів доказування у кіберсправах, що дозволило б уникнути проблем, пов'язаних із різними підходами до кваліфікації цифрових злочинів у національних правових системах. На сьогодні в рамках Європейського Союзу та ООН активно обговорюється питання розробки глобального механізму збору та визнання цифрових доказів, що стане вагомим кроком до гармонізації слідчих процесів у сфері кібербезпеки.

Крім того, сучасні тенденції міжнародної співпраці свідчать про посилення приватно-державного партнерства у боротьбі з кіберзлочинністю. Такі компанії, як Microsoft, Google, Amazon та інші технологічні гіганти, все частіше беруть участь у розслідуванні глобальних кіберзагроз, зокрема через надання інформації про підозрілі активності, підтримку ініціатив із блокування шкідливих серверів та спільні проєкти з правоохоронними органами.

Окремим викликом залишається регулювання криптовалютних транзакцій, які є основним фінансовим інструментом кіберзлочинців. Незважаючи на розвиток технологій відстеження цифрових активів, таких як Chainalysis або TRM Labs, існує потреба у створенні єдиних міжнародних стандартів контролю за нелегальними криптоопераціями. Деякі держави вже ухвалили відповідні нормативні акти, зокрема у США запроваджені нові вимоги до реєстрації криптовалютних бірж, що допомагають запобігати фінансуванню кіберзлочинності.

Ще одним напрямом міжнародної боротьби з кіберзлочинністю є розробка спільних механізмів реагування на атаки на критичну інфраструктуру. Зокрема, у 2022 році НАТО започаткувало ініціативу Cyber Rapid Reaction Teams, що передбачає можливість швидкого розгортання експертних груп для допомоги країнам-членам у разі масштабних кібератак[16]. Такий підхід може стати зразком для інших міжнародних об'єднань у сфері безпеки, адже він дозволяє не лише оперативно реагувати на загрози, а й напрацьовувати спільні практики цифрової форензіки.

Попри значний прогрес у міжнародному співробітництві, все ще залишаються невирішеними проблеми політичного та юридичного характеру. Багато країн неохоче діляться інформацією про кібератаки, побоюючись, що це може зашкодити їхній національній безпеці або репутації. До того ж, деякі держави використовують кіберзлочинність як інструмент гібридної війни, що ускладнює глобальну координацію у боротьбі з такими загрозами.

З огляду на зазначене, подальша ефективність міжнародного співробітництва у сфері кіберзлочинності залежатиме від удосконалення нормативно-правової бази, зміцнення партнерства між державами та приватним сектором, а також активного впровадження інноваційних технологій для ідентифікації та нейтралізації кіберзлочинних угруповань.

[16] North Atlantic Treaty Organization (NATO). NATO Rapid Reaction Team to fight cyber attack. 13 Mar. 2012. URL: https://www.nato.int/cps/en/natolive/news_85161.htm

ВИСНОВКИ

У сучасних умовах глобальної цифровізації та зростання залежності суспільства від інформаційно-комунікаційних технологій кіберзлочинність стала однією з найбільш актуальних загроз національній та міжнародній безпеці. Кібератаки на критичну інфраструктуру, поширення шкідливого програмного забезпечення та необхідність міжнародного співробітництва у боротьбі з кіберзлочинністю є ключовими викликами, що потребують невідкладної реакції з боку державних органів, правоохоронних структур та міжнародних організацій.

Насамперед, розгляд проблем правозастосування у сфері кібератак на критичну інфраструктуру засвідчив, що чинне законодавство України та міжнародні нормативні акти не завжди відповідають динаміці розвитку кіберзагроз. Наявні правові механізми часто виявляються недостатньо ефективними для забезпечення належного рівня захисту об'єктів критичної інфраструктури, що стають мішенню зловмисників. Аналіз сучасної практики правозастосування демонструє необхідність удосконалення кримінального законодавства, зокрема чіткішого визначення складів злочинів, пов'язаних із кібератаками, розширення повноважень правоохоронних органів у сфері розслідування кіберзлочинів, а також розробки єдиних стандартів кібербезпеки для критичних об'єктів.

Другим важливим аспектом дослідження є кримінально-правова відповідальність за розповсюдження шкідливого програмного забезпечення, яка передбачена Кримінальним кодексом України. Проте аналіз законодавчих норм показав, що існує низка проблем, пов'язаних із доказуванням умислу правопорушників, класифікацією програмного забезпечення як шкідливого та встановленням його реального впливу на інформаційні системи. Крім того, в умовах анонімності та транснаціонального характеру кіберзлочинності існує складність у притягненні винних осіб до відповідальності, особливо якщо вони перебувають поза межами юрисдикції України. У зв'язку з цим актуальним є посилення міжнародної співпраці у сфері кібербезпеки, гармонізація національного законодавства з міжнародними стандартами та створення ефективних механізмів екстрадиції кіберзлочинців.

Окремо було розглянуто актуальні кейси міжнародного співробітництва у боротьбі з кіберзлочинністю, що підтвердило ключову роль спільних зусиль держав у протидії кіберзагрозам. Практика діяльності таких організацій, як Інтерпол, Європол, НАТО та ООН, свідчить про ефективність міжнародних ініціатив, спрямованих на обмін інформацією, проведення спільних розслідувань та розробку глобальних стандартів кібербезпеки. Зокрема, успішні операції з викриття кіберзлочинних угруповань, таких як «Emotet» та «REvil», продемонстрували важливість міжнародної взаємодії та необхідність розширення договірної бази для боротьби з транснаціональною кіберзлочинністю.

Таким чином, дослідження засвідчило, що боротьба з кіберзлочинністю вимагає комплексного підходу, що включає вдосконалення кримінального законодавства, посилення правоохоронних механізмів, забезпечення надійного захисту критичної інфраструктури, а також активну міжнародну співпрацю. Вирішення зазначених проблем потребує не лише законодавчих змін, а й

запровадження інноваційних технічних рішень, підвищення рівня цифрової грамотності населення та створення єдиної глобальної стратегії кібербезпеки. Подальший розвиток цієї сфери має ґрунтуватися на принципах правової визначеності, міжнародної солідарності та технологічної адаптивності, що дозволить ефективно протидіяти кіберзлочинам в Україні.

АНОТАЦІЯ

У статті здійснено комплексний аналіз сучасних викликів кримінально-правового регулювання кіберзлочинності в національному та міжнародному вимірах. Досліджено проблеми правозастосування щодо кібератак на об'єкти критичної інфраструктури, зокрема труднощі кваліфікації таких діянь, особливості збору й використання цифрових доказів, а також недосконаліть окремих положень кримінального та кримінального процесуального законодавства України. Проаналізовано питання кримінальної відповідальності за створення та розповсюдження шкідливого програмного забезпечення, акцентовано увагу на проблемі доведення умислу та подвійного призначення окремих програмних засобів. Окремо розглянуто актуальні кейси міжнародного співробітництва у боротьбі з кіберзлочинністю (ліквідація AlphaBay, REvil, Emotet), які демонструють ефективність координації між державами, міжнародними організаціями та приватним сектором.

Обґрунтовано необхідність удосконалення національного законодавства з урахуванням міжнародних стандартів, гармонізації підходів до криміналізації кіберзлочинів, розширення механізмів міжнародної правової допомоги та впровадження сучасних технологій цифрової форензіки. Зроблено висновок про потребу формування комплексної моделі протидії кіберзлочинності, що поєднує кримінально-правові, процесуальні, організаційні та технологічні інструменти в умовах глобальної цифровізації.

Література

1. Аніщук В. В., Зицик С. Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського Національного Університету. 2024. Серія ПРАВО.* Випуск 83: частина 3, С. 19-23. DOI https://doi.org/10.24144/2307-3322.2024.83.3.2

2. Степаненко Н. В., Піддубний Д. Д. Сучасні проблеми запобігання і протидії злочинності у сфері інформаційних технологій. *Legal Bulletin.* 2024, 73-81. https://doi.org/10.31732/2708-339X-2024-14-A10

3. Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ "КПІ" Політологія. Соціологія. Право.* № 1(49) (2021). DOI: https://doi.org/10.20535/2308-5053.2021.1(49).233023

4. Авдєєва, Г., Живуцька-Козловська, Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*, Вип. 1 (30), 2023. 126-143. https://doi.org/10.32353/khrife.1.2023.07

5. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека,* 2 (93), 2024. 140-150. https://doi.org/10.32631/pb.2024.2.13

6. Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО.* Вип. 75: ч. 2. 2023. 158-162. https://doi.org/10.24144/2307-3322.2022.75.2.25

7. Sergiu Cernomoreț & Andrei Nastas. Comparative Analysis of Cybercrime in the Criminal Law System. International Academic Publisher. Bucharest, Paris, Calgary 2023. 82 p. URL: https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf

8. Senjaya, Murshal. Cyber Crime And Criminal Law In The Era Of Artificial Intelligence. *International Journal of Law and Society.* 1, 2024. 268-276. DOI: https://doi.org/10.62951/ijls.v1i4.210

9. Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis (March 20, 2022). Ajoy P. B. Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2), 2022. 74-79. http://dx.doi.org/10.2139/ssrn.4061947

10. Верховна Рада України. Розділ: Законодавство України. Кримінальний кодекс України. 5 квітня 2001 року, № 2341-III. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 13.03.2025).

11. Верховна Рада України. Розділ: Законодавство України. Кримінальний процесуальний кодекс України. 13 квітня 2012 року, № 4651-VI. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 13.03.2025).

12. International Standard ISO/IEC 27037. Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. URL: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf

13. H-X. Директива кібербезпеки NIS2. *Електронний ресурс.* URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua

14. Верховна Рада України. Розділ: Законодавство України. Закон України «Про основні засади забезпечення кібербезпеки України». 5 жовтня 2017 року № 2163-VIII. *Електронний ресурс.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 13.03.2025).

15. CybelAngel. Home. The Impact of Dark Web Marketplace Takedowns [AlphaBay and Hansa]. September 24, 2024. URL: https://cybelangel.com/alphabay-hansa-two-major-dark-web-marketplaces-shut/

16. CSO. Home. Security REvil ransomware explained: A widespread extortion operation. 12 Nov 2021. URL: https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html

17. EUROPOL. Home. Media & Press. World's most dangerous malware EMOTET disrupted through global action. 27 Jan 2021. URL: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

18. North Atlantic Treaty Organization (NATO). NATO Rapid Reaction Team to fight cyber attack. 13 Mar. 2012. URL: https://www.nato.int/cps/en/natolive/news_85161.htm

Information about the author:
Larchenko Maryna Oleksandrivna,
Candidate of Juridical Sciences (Ph. D.), Associate Professor,
Associate Professor at the Department of Cyber Security
and Mathematical Modeling,
Educational and Scientific Institute of Electronics
and Information Technologies,
Chernihiv Polytechnic National University
95, Shevchenko Str., Chernihiv, 14030, Ukraine,
Associate Professor at the Department of
Law and Social and Philosophical Sciences
Faculty of Philology, History and Political and Legal Sciences,
Mykola Gogol Nizhyn State University
2 Grafska Str., Nizhyn, 16600, Ukraine
https://orcid.org/0000-0002-2643-980X