УДК 343.9:004:341.1/8
DOI 10.33244/2617-4154.2(23).2026.278-285

А. Г. Станецький,
здобувач ступеня доктора філософії,
ПВНЗ «Європейський університет»
A. H. Stanetskyi,
postgraduate student at the private educational institution «European University»
email: ianton3@gmail.com
ORCID 0009-0002-8489-3661

КІБЕРЗЛОЧИНИ ЯК СУЧАСНИЙ ВИД ТРАНСНАЦІОНАЛЬНОЇ ЗЛОЧИННОСТІ: ПРОБЛЕМИ РОЗСЛІДУВАННЯ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

CYBERCRIME AS A MODERN FORM OF TRANSNATIONAL CRIMINALITY: CHALLENGES IN INVESTIGATION AND INTERNATIONAL COOPERATION

У статті розглянуто кіберзлочини як сучасний вид транснаціональної злочинності, проаналізовано їхні характерні ознаки та особливості прояву в умовах цифровізації суспільних відносин. Визначено особливості розслідування кіберзлочинів, зокрема проблеми роботи із цифровими доказами, забезпечення їх допустимості та ідентифікації осіб, причетних до їхнього вчинення. Окрему увагу приділено нормативному регулюванню та формам міжнародного співробітництва у сфері протидії кіберзлочинності, а також визначено основні проблеми й напрями вдосконалення взаємодії держав у цій сфері.

У процесі дослідження використано загальнонаукові та спеціально-юридичні методи, зокрема: діалектичний – для аналізу розвитку кіберзлочинності; системно-структурний – для визначення її місця в системі транснаціональної злочинності; формально-юридичний – для дослідження норм національного та міжнародного законодавства; порівняльно-правовий – для аналізу міжнародних механізмів співробітництва; логіко-юридичний – для узагальнення отриманих результатів.

Встановлено, що кіберзлочини характеризуються транснаціональністю, високим рівнем латентності та складністю доказування, що зумовлює потребу у використанні спеціальних знань і сучасної криміналістичної методики. Обґрунтовано, що ефективне

розслідування таких злочинів неможливе без належної роботи із цифровими доказами й подолання проблем анонімності в кіберпросторі. Доведено, що міжнародне співробітництво є ключовим елементом протидії кіберзлочинності, однак потребує подальшого вдосконалення в частині спрощення процедур взаємодії, гармонізації законодавства та підвищення ефективності обміну інформацією між державами.

Ключові слова: *кіберзлочинність, транснаціональна злочинність, розслідування кіберзлочинів, цифрові докази, цифрова криміналістика, міжнародне співробітництво, Будапештська конвенція, кібербезпека, допустимість доказів, інтернет-технології.*

This article examines cybercrime as a modern form of transnational crime, analyzing its characteristic features and patterns of manifestation in the context of the digitalization of social relations. It identifies the specific challenges of investigating cybercrime, particularly issues related to handling digital evidence, ensuring its admissibility, and identifying individuals involved in its commission. Special attention is paid to regulatory frameworks and forms of international cooperation in the field of combating cybercrime, and the main challenges and directions for improving state cooperation in this area are identified.

The aim of the study is to analyze cybercrimes as a modern form of transnational crime, identify the specific features of their investigation, and examine regulatory frameworks and forms of international cooperation in this field.

The study employs general scientific and specialized legal methods, including: dialectical – to analyze the development of cybercrime; system-structural – to determine its place within the system of transnational crime; formal-legal – to examine the norms of national and international legislation; comparative-legal – to analyze international cooperation mechanisms; and logical-legal – to generalize the obtained results.

It has been established that cybercrimes are characterized by their transnational nature, high level of latency, and the complexity of proving them, which necessitates the use of specialized knowledge and modern forensic methods. It has been demonstrated that effective investigation of such crimes is impossible without proper handling of digital evidence and addressing the challenges of anonymity in cyberspace. It has been demonstrated that international cooperation is a key element in combating cybercrime, but it requires further improvement in terms of simplifying cooperation procedures, harmonizing legislation, and enhancing the effectiveness of information exchange between states.

Keywords: *cybercrime, transnational crime, cybercrime investigation, digital evidence, digital forensics, international cooperation, Budapest Convention, cybersecurity, admissibility of evidence, Internet technologies.*

Постановка проблеми. Актуальність дослідження зумовлена стрімким зростанням кіберзлочинності як одного із найбільш динамічних і небезпечних видів транснаціональної злочинності. Цифровізація суспільних відносин, розвиток інформаційно-комунікаційних технологій і глобалізаційні процеси сприяють розширенню можливостей для вчинення злочинів у кіберпросторі, що не обмежуються державними кордонами.

В умовах збройної агресії проти України кіберзлочини набувають додаткової загрози, поєднуючись із елементами гібридної війни та інформаційного впливу, що ускладнює їх виявлення, розслідування та притягнення винних до відповідальності. Водночас ефективна протидія кіберзлочинності неможлива без належного міжнародного співробітництва, оскільки більшість таких злочинів має транскордонний характер. Наявні механізми взаємодії держав не завжди відповідають сучасним викликам, що зумовлює потребу в їхньому вдосконаленні.

Отже, дослідження проблем розслідування кіберзлочинів і розвитку міжнародного співробітництва в цій сфері є досить актуальним як з теоретичного, так і з прикладного погляду.

Стан наукової розробленості проблеми. Проблематика кіберзлочинності як різновиду транснаціональної злочинності останніми роками стала предметом активного наукового дослідження у вітчизняній правовій доктрині.

Так, у дисертації М. Ю. Яцишин «Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю» здійснено комплексне дослідження міжнародно-правових механізмів протидії кіберзлочинності. Значну увагу приділено питанням гармонізації національного законодавства з міжнародними стандартами, проблемам юрисдикції та класифікації кіберзлочинів. У дисертаційному дослідженні С. А. Буяджи «Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект» проведено комплексний аналіз теоретико-правових засад формування та функціонування механізму протидії кіберзлочинності в умовах розвитку інформаційного суспільства та глобалізації цифрового простору. У дисертаційному дослідженні О. М. Бодунової «Кримінологічні засади запобігання злочинності у сфері інформаційних технологій» виконано комплексний кримінологічний аналіз злочинності у сфері інформаційних технологій як сучасного соціально-правового явища, що характеризується високим рівнем латентності, транснаціональним характером і динамічною трансформацією способів вчинення кримінальних правопорушень.

У дослідженні А. Гребенюка «Міжнародне співробітництво при розслідуванні кіберзлочинів» проаналізовано поняття кіберзлочинності та особливості міжнародно-правової допомоги під час розслідування відповідних кримінальних проваджень. Автор акцентує увагу на проблемах застосування міжнародних договорів і чинного законодавства України у сфері міжнародного співробітництва. У дисертаційному дослідженні В. П. Бєлєнького «Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України (порівняльно-правове дослідження)» здійснено комплексний порівняльно-правовий аналіз кримінальної відповідальності за кіберзлочини в правових системах США, Великої Британії та України. Автором досліджено особливості криміналізації кіберзлочинів у зазначених державах, проаналізовано структуру відповідних кримінально-правових норм, а також визначено спільні та відмінні підходи до правового регулювання відповідальності у сфері інформаційних технологій. У дисертаційному дослідженні О. В. Тихонова «Кримінально-правова характеристика кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» було проведено комплексний аналіз кримінально-правових аспектів протидії злочинам у сфері інформаційних технологій.

І. М. Леган у монографії «Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності» комплексно досліджує форми та напрями міжнародної взаємодії держав у сфері протидії транснаціональній злочинності, зокрема кіберзлочинності та кібертероризму.

Я. М. Костюченко в науковій статті «Співпраця України та ЄС у сфері кібербезпеки: механізми міжнародної взаємодії» аналізує нормативно-правові механізми співпраці України та Європейського Союзу у сфері кібербезпеки, акцентуючи увагу на гармонізації українського законодавства з європейськими стандартами та потребі в посиленні міжнародної координації. У статті В. Л. Гончарука «Правові механізми боротьби з кіберзлочинністю: світова практика та український контекст» досліджено сучасні міжнародні підходи до боротьби з кіберзлочинністю та можливості їхньої імплементації в Україні. М. В. Гуцалюк у дослідженні «Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності» акцентує увагу на потребі в стратегічному підході до кіберзахисту та важливості належного процесуального регулювання використання електронних доказів у кримінальному провадженні.

Аналіз дисертаційних досліджень свідчить про відмінність наукових підходів до вивчення кіберзлочинності. Одні автори зосереджуються переважно на міжнародно-правових і теоретико-правових аспектах протидії кіберзлочинам, інші – на кримінально-правових, порівняльно-правових або кримінологічних засадах їхнього дослідження. Водночас спільною рисою більшості праць є недостатня увага до комплексної методики розслідування та запобігання транснаціональних кіберзлочинів і практичних механізмів міжнародної взаємодії правоохоронних органів.

Виділення невирішених раніше частин загальної проблеми. Попри значну кількість наукових праць, присвячених кіберзлочинності, низка проблем залишається недостатньо дослідженою. Зокрема, потребують подальшого наукового опрацювання питання комплексної системи запобігання кіберзлочинів транснаціонального характеру, механізмів оперативного отримання електронних доказів у різних юрисдикціях, а також особливостей взаємодії правоохоронних органів із міжнародними цифровими платформами та провайдерами електронних сервісів. Недостатньо дослідженими залишаються також проблеми юрисдикційних конфліктів під час розслідування кіберзлочинів, використання штучного інтелекту у виявленні та документуванні кіберзлочинної діяльності, а також специфіка протидії кіберзлочинності в умовах воєнного стану й гібридних загроз. Крім того, потребують удосконалення наукові підходи до гармонізації кримінального законодавства різних держав у сфері кібербезпеки.

Метою статті є аналіз кіберзлочинів як сучасного виду транснаціональної злочинності, визначення особливостей їхнього розслідування, а також дослідження нормативного регулювання й форм міжнародного співробітництва в цій сфері.

Виклад основного матеріалу. Розслідування кіберзлочинів є складним і багаторівневим процесом, що зумовлено специфікою їхнього вчинення в кіберпросторі, використанням інформаційно-комунікаційних технологій і транснаціональним характером таких правопорушень. На відміну від традиційних кримінальних правопорушень кіберзлочини часто не мають чіткої територіальної прив’язки, що суттєво ускладнює визначення юрисдикції та організацію досудового розслідування [2, с. 262].

Однією із ключових особливостей розслідування кіберзлочинів є відповідність роботи із цифровими доказами, які суттєво відрізняються від традиційних джерел доказової інформації. Цифрові докази мають нематеріальний характер та існують у формі електронних даних, що зберігаються на різноманітних носіях: комп'ютерах, мобільних пристроях, серверах, у хмарних сховищах тощо. Їхня специфіка полягає у високій динамічності: такі дані можуть бути швидко змінені, скопійовані, переміщені або повністю знищені, часто без залишення очевидних слідів втручання.

Особливу складність становить те, що значна частина цифрових доказів є «леткими», тобто зберігається тимчасово, наприклад у оперативній пам'яті пристрою, кеші або мережевих сесіях. Такі дані можуть бути втрачені вже під час вимкнення пристрою або перезавантаження системи, що зумовлює потребу в їхній негайній фіксації із застосуванням спеціалізованих технічних засобів [3, с. 152].

Варто зазначити, що отримання цифрових доказів потребує використання спеціальних знань у сфері кібербезпеки та цифрової криміналістики. Зокрема, застосовуються методи комп'ютерно-технічної експертизи, цифрової форензіки, аналізу мережевого трафіку, відновлення видалених файлів, дослідження журналів подій тощо. Водночас потрібно дотримуватися принципу незмінності доказів, що передбачає створення точних копій носіїв інформації із використанням криптографічних хеш-функцій для підтвердження їхньої автентичності.

Не менш важливим є процесуальний аспект роботи із цифровими доказами. Відповідно до вимог кримінального процесуального законодавства їх збирання, фіксація, зберігання та дослідження мають здійснюватися з дотриманням встановлених процедур, що забезпечує допустимість таких доказів у суді. Згідно із вимогами КПК України порушення порядку вилучення або обробки електронної інформації може призвести до визнання доказів недопустимими [1].

Крім того, особливості цифрових доказів зумовлюють потребу в документуванні так званого «ланцюга збереження доказів», який забезпечує контроль за всіма етапами їх отримання, передачі та дослідження. Це дає змогу гарантувати, що докази не були змінені або підроблені.

На сьогодні суттєвою проблемою під час розслідування кіберзлочинів є забезпечення ідентифікації осіб, причетних до їхнього вчинення, що ускладнюється високим рівнем анонімності в мережі «Інтернет» і широким використанням засобів маскування. Зокрема, зловмисники активно застосовують VPN-сервіси, проксі-сервери, мережі типу Tor, технології шифрування трафіку, а також інструменти підміни IP-адрес і цифрових ідентифікаторів. Такі засоби дають змогу приховувати реальне місцезнаходження користувача, ускладнюють відстеження його дій і створюють додаткові бар'єри для встановлення зв'язку між особою та вчиненим правопорушенням. Крім того, активно використовуються криптовалюти, анонімні месенджери та тимчасові облікові записи, що значно ускладнює процес збору доказів і встановлення кола співучасників [3, с. 153]. У багатьох випадках зловмисники застосовують комплексні схеми багаторівневого маскування, що охоплюють використання серверів у різних юрисдикціях, що зі свого боку ускладнює отримання відповідної інформації в межах національного кримінального провадження.

У таких умовах ефективне розслідування кіберзлочинів потребує активного залучення спеціалізованих підрозділів, зокрема кіберполіції, а також використання сучасних криміналістичних методик і технологій цифрової розвідки. Важливого значення набуває застосування методів аналізу мережевого трафіку, цифрової ідентифікації користувачів, кореляції даних із різних джерел, а також співпраця з провайдерами телекомунікаційних послуг і міжнародними правоохоронними структурами.

Отже, проблема анонімності в кіберпросторі є однією із ключових перешкод у розслідуванні кіберзлочинів і потребує комплексного підходу, що поєднує технічні, правові та організаційні механізми протидії.

Варто звернути увагу на те, що отримання цифрових доказів потребує використання спеціальних знань у сфері кібербезпеки та цифрової криміналістики, оскільки така діяльність пов'язана з обробкою складних технічних систем і великих обсягів електронної інформації. З цією метою застосовуються спеціалізовані методи комп'ютерно-технічної експертизи, цифрової форензіки, аналізу мережевого трафіку, відновлення видалених даних, дослідження журналів подій, а також інструменти аналізу файлових систем і метаданих.

Особливу увагу приділяють процедурі вилучення інформації з електронних носіїв, яка має здійснюватися так, щоб не змінити первинний стан даних. Для цього використовуються спеціальні програмно-апаратні комплекси, що дають змогу створювати біт-копії носіїв інформації без внесення змін до оригіналу [2, с. 154]. Подальший аналіз здійснюється саме на копіях, що мінімізує ризик втрати або пошкодження доказової інформації.

Ключовим принципом роботи з цифровими доказами є забезпечення їхньої незмінності, що досягається через використання криптографічних хеш-функцій (наприклад, MD5, SHA-1, SHA-256). Формування хеш-значень дає нагоду підтвердити автентичність даних і довести, що вони не зазнали змін у процесі вилучення, зберігання та дослідження. Будь-яка зміна цифрового файлу призводить до зміни його хеш-значення, що дає змогу контролювати цілісність доказів на всіх етапах кримінального провадження. У контексті цього важливим є дотримання процедури документування процесу вилучення та обробки цифрових доказів, зокрема фіксація часу, способу доступу до інформації, технічних засобів, що використовувалися, а також осіб, які здійснювали відповідні дії, що забезпечує прозорість процесу й підтверджує достовірність отриманих результатів.

Отже, ефективне отримання та дослідження цифрових доказів вимагає поєднання високого рівня технічної підготовки, використання спеціалізованих інструментів і суворого дотримання кримінально-процесуальних вимог, що є вагомою умовою їх допустимості та доказового значення в кримінальному провадженні.

Варто звернути увагу також на процесуальний аспект роботи з цифровими доказами, який безпосередньо впливає на їх допустимість і доказове значення в кримінальному провадженні. Відповідно до вимог кримінального процесуального законодавства України збирання, фіксація, вилучення, зберігання та дослідження електронної інформації мають здійснюватися із чітким дотриманням встановлених процедур. Йдеться, зокрема, про проведення слідчих (розшукових) дій на підставі належних процесуальних рішень

(ухвал слідчого судді або постанов слідчого / прокурора), обов'язкове складання протоколів із детальним описом технічних дій, використаних засобів і отриманих результатів, а також забезпечення участі спеціалістів у випадках, коли це потребує спеціальних знань [1].

Порушення процесуального порядку роботи із цифровими доказами, зокрема недотримання вимог щодо фіксації, неповне документування технічних операцій, використання неналежних або несертифікованих засобів, може призвести до втрати доказової сили таких даних і визнання їх недопустимими судом. Так, процесуальні гарантії роботи із цифровими доказами є невід'ємною складовою ефективного розслідування кіберзлочинів і потребують комплексного поєднання правових норм, технічних стандартів і професійної підготовки суб'єктів досудового розслідування.

Відмітимо, що транснаціональний характер кіберзлочинності зумовлює потребу в ефективному міжнародному співробітництві, оскільки злочини в кіберпросторі часто охоплюють території кількох держав, а їхні суб'єкти, технічна інфраструктура та докази можуть перебувати в різних юрисдикціях. У таких умовах лише національні механізми протидії є недостатніми, що обумовлює потребу в скоординованій взаємодії держав.

Нормативне регулювання міжнародного співробітництва у сфері протидії кіберзлочинності базується на міжнародно-правових актах, ключовим серед яких є Конвенція Ради Європи про кіберзлочинність 2001 року (Будапештська конвенція) [5]. Вона встановлює уніфіковані підходи до криміналізації кіберзлочинів, визначає механізми міжнародної правової допомоги, охоплюючи збереження комп'ютерних даних, їхнє швидке розкриття, а також порядок взаємодії правоохоронних органів.

Національне законодавство України імплементує положення зазначених міжнародних актів, зокрема в Кримінальному процесуальному кодексі України, законах у сфері кібербезпеки та міжнародного співробітництва в кримінальних провадженнях. Форми міжнародного співробітництва у сфері протидії кіберзлочинності є різноманітними й охоплюють: надання міжнародної правової допомоги в кримінальних провадженнях; екстрадицію правопорушників; створення спільних слідчих груп; обмін оперативною та доказовою інформацією; проведення спільних операцій; навчання й підвищення кваліфікації фахівців; технічну допомогу та обмін кращими практиками [1]. Особливого значення набувають механізми оперативного збереження й передачі електронних даних, що є критично важливими для розслідування кіберзлочинів.

Водночас міжнародне співробітництво в цій сфері супроводжується низкою проблем. Серед них: відмінності в національних правових системах, зокрема у визначенні складів кіберзлочинів і процедур збору доказів; складність і тривалість процедур надання міжнародної правової допомоги; обмеження доступу до даних, що зберігаються в юрисдикціях інших держав або в провайдерів; питання захисту персональних даних і дотримання прав людини; недостатній рівень технічної сумісності та координації між правоохоронними органами різних країн [4, с. 483].

У результаті проведеного дослідження встановлено, що кіберзлочини є одним із найбільш динамічних і небезпечних проявів транснаціональної злочинності, що характеризується відсутністю територіальних меж, високим рівнем латентності та використанням сучасних інформаційно-комунікаційних технологій.

Висновки. Ефективність розслідування кіберзлочинів значною мірою залежить від належної роботи із цифровими доказами, які мають особливий характер, потребують спеціальних знань і технічних засобів, а також чіткого дотримання процесуальних вимог щодо їх отримання, фіксації та збереження. Водночас суттєвими перешкодами у встановленні осіб, причетних до вчинення таких злочинів, залишаються анонімність у мережі «Інтернет» і використання сучасних засобів маскування.

Отже, транснаціональний характер кіберзлочинності обумовлює ключову роль міжнародного співробітництва в протидії цим правопорушенням. Нормативну основу такої взаємодії становлять міжнародно-правові акти, насамперед Будапештська конвенція про кіберзлочинність, а також національне законодавство, що імплементує її положення. Наявні механізми міжнародної взаємодії не завжди є достатньо ефективними через складність процедур, відмінності правових систем та обмеження доступу до цифрових даних.

З урахуванням викладеного, перспективними напрямами вдосконалення протидії кіберзлочинності є підвищення ефективності розслідування за допомогою розвитку цифрової криміналістики, удосконалення механізмів роботи з електронними доказами, посилення координації між правоохоронними органами, а також міжнародного співробітництва, зокрема через спрощення процедур обміну інформацією та гармонізації законодавства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України.* URL : https://zakon.rada.gov.ua/laws/show/4651-17

2. Тєтєвін М. С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2024. Вип. 82, ч. 3. С. 263–266. DOI : https://doi.org/10.24144/2307-3322.2024.82.3.41

3. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації.* 2019. № 3, том 21. С. 150–157. DOI 10.18372/24107840/21/13951

4. Сливка М. М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний науковий електронний журнал*. 2022. № 10. С. 489–491. DOI : https://doi.org/10.32782/2524-0374/2022-10/121

5. Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. *Відомості Верховної Ради України.* URL : https://zakon.rada.gov.ua/laws/show/994_575

Дата надходження 24.02.2026
Дата прийняття 11.03.2026
Дата рекомендації 28.05.2026
Дата публікації 30.06.2026