УДК: 343.9:004.738.5
DOI https://doi.org/10.24144/2788-6018.2025.04.3.26

ЦИФРОВА КРИМІНАЛІСТИКА ТА МІЖНАРОДНА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ (НА ПРИКЛАДІ ЕЛЕКТРОННОЇ ТОРГІВЛІ)

Діденко О.В.
аспірант Державного податкового університету
ORCID: 0009-0005-1273-7514

Діденко О.В. Цифрова криміналістика та міжнародна протидія кіберзлочинності (на прикладі електронної торгівлі).

Стаття присвячена проблемі міжнародної кримінально-правової протидії кібершахрайству в електронній торгівлі, яке розглядається як особливий прояв високотехнологічної злочинності у сфері підприємництва. Увагу акцентовано на тому, що традиційні інструменти виявлення та розслідування шахрайства не відповідають сучасним викликам цифрового середовища, зокрема транснаціональному характеру таких злочинів, використанню шкідливого програмного забезпечення, цифрових платформ, інструментів анонімізації та високому рівню латентності.

Особливу увагу приділено необхідності посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю, створення узгоджених правових механізмів та спільних баз даних, а також налагодженню ефективного та оперативного обміну інформацією між правоохоронними органами різних держав. У цьому контексті розкрито значення Будапештської конвенції про кіберзлочинність як універсального інструмента для гармонізації кримінального законодавства держав-учасниць і забезпечення спільного реагування на цифрові загрози.

У роботі проаналізовано значення цифрової криміналістики та електронних доказів у процесі документування та доведення фактів кібершахрайства. Підкреслено, що для забезпечення належної доказової сили таких матеріалів необхідно дотримуватись міжнародних стандартів допустимості, достовірності, автентичності й відтворюваності. Автор звертає увагу на наявні прогалини в національному правовому регулюванні, які ускладнюють ефективне використання цифрових доказів у кримінальному провадженні.

Цифрова криміналістика є напрямом криміналістичної науки, що спеціалізується на виявленні, збиранні, збереженні, аналізі та презентації цифрових доказів, вилучених із електронних пристроїв, комп'ютерних мереж чи цифрових середовищ. Її основне призначення – сприяння розслідуванню злочинів, зокрема тих, що мають кібернетичну природу. Цей напрям охоплює методи і засоби ідентифікації, вилучення та тлумачення даних із комп'ютерів, мобільних пристроїв, серверів, хмарних технологій та інших джерел, із забезпеченням їх правової валідності для подальшого використання у судових процесах. Усі процеси при цьому здійснюються з дотриманням вимог захисту персональних даних і поваги до прав людини.

Зроблено висновок, що ефективна протидія шахрайству в електронній торгівлі потребує оновлення підходів на національному рівні, а також активної участі України в міжнародних ініціативах, спрямованих на боротьбу з кіберзлочинністю, з одночасним удосконаленням кримінально-процесуальних механізмів роботи з цифровими доказами.

Ключові слова: шахрайство в електронній торгівлі, Будапештська конвенція про кіберзлочинність, цифрова криміналістика.

Didenko O.V. Digital forensics and international counteraction to cybercrime (based on the example of e-commerce).

The article is devoted to the pressing issue of international criminal law counteraction to cyber fraud in electronic commerce, which is considered a specific manifestation of high-tech crime in the field of entrepreneurship. The author emphasizes that traditional tools for detecting, qualifying, and investigating fraud do not meet the modern challenges of the digital environment, particularly its transnational nature, the use of malicious software, digital platforms, anonymization tools, and the high level of latency. The need to develop a specialized criminal law approach to such acts is substantiated, taking into account new forms of criminal behavior in the online space.

Special attention is paid to the necessity of strengthening international cooperation in combating cybercrime, creating harmonized legal mechanisms and joint databases, as well as establishing effective and rapid information exchange between law enforcement agencies of different countries. In

this context, the importance of the Budapest Convention on Cybercrime is highlighted as a universal instrument for harmonizing the criminal laws of participating states and ensuring a coordinated response to digital threats.

The paper provides a detailed analysis of the significance of digital forensics and electronic evidence in documenting and proving acts of cyber fraud. It is emphasized that in order to ensure the proper evidentiary value of such materials, it is necessary to comply with international standards of admissibility, reliability, authenticity, and reproducibility. The author draws attention to existing gaps in national legal regulation that hinder the effective use of digital evidence in criminal proceedings.

Digital forensics is a branch of forensic science focused on the identification, collection, preservation, analysis, and presentation of digital evidence obtained from electronic devices, computer networks, or digital environments. Its primary purpose is to support the investigation of crimes, particularly cybercrimes. This field encompasses methods and techniques for identifying, extracting, and interpreting data from computers, mobile devices, servers, cloud storage, and other sources, ensuring their legal validity for use in judicial proceedings. All procedures are carried out in compliance with data protection standards and the principles of respect for human rights and privacy.

The conclusion is drawn that effective counteraction to fraud in electronic commerce requires the modernization of national approaches, as well as Ukraine's active participation in international initiatives aimed at combating cybercrime, accompanied by the improvement of criminal procedural mechanisms for handling digital evidence.

Key words: E-commerce fraud, Budapest Convention on Cybercrime, digital forensics.

Постановка проблеми. Активна цифровізація підприємницької діяльності, зростання обсягів електронної торгівлі та трансформація способів надання товарів і послуг спричинили появу нових викликів у сфері боротьби зі злочинністю. Одним із найбільш динамічних і водночас складних для виявлення явищ став стрімкий розвиток кібершахрайства в онлайн-торгівлі. Цей вид високотехнологічного злочину відзначається транснаціональним характером, анонімністю правопорушників, складністю ідентифікації джерел та напрямів фінансових транзакцій, використанням шкідливого програмного забезпечення. Наявна правозастосовна практика виявляє істотні прогалини у національному та міжнародному законодавстві, зокрема щодо кваліфікації таких злочинів, збору доказів, а також взаємодії між державами в умовах кіберпростору.

Попри наявність міжнародних інструментів, таких як Будапештська конвенція про кіберзлочинність, процес інтеграції уніфікованих стандартів міжнародного співробітництва залишається неповним і потребує суттєвого посилення. Водночас розвиток цифрової криміналістики відкриває нові можливості для виявлення й доведення кібершахрайства, однак вимагає дотримання високих стандартів достовірності, допустимості й відтворюваності електронних доказів. У таких умовах виникає потреба у комплексному міждисциплінарному дослідженні, спрямованому на удосконалення кримінально-правового механізму протидії кіберзлочинності у сфері підприємництва, з урахуванням цифрової специфіки, міжнародного досвіду та практики доказування.

Стан опрацювання проблематики. Питання міжнародного співробітництва у кримінальному провадженні розглядали Д. Грицишен, В. Зуєв, М. Смирнов, В. Волошина, А. Підгородинська, В. Яремчук. Проблеми кіберзлочинності та кібершахрайства досліджували О. Бодунова, М. Думчиков, Н. Сметаніна, Т. Діброва, Д. Пісенко, С. Харитонов та інші.

Мета статті – дослідити особливості кібершахрайства в електронній торгівлі як окремого різновиду кіберзлочинності у сфері підприємництва та обґрунтувати сучасні підходи до міжнародної кримінально-правової протидії цим злочинам із урахуванням можливостей цифрової криміналістики, міжнародного співробітництва та уніфікації стандартів електронних доказів.

Цілі статті: з'ясувати кримінально-правову природу шахрайства в електронній торгівлі, визначити його особливості; проаналізувати нормативно-правові засади міжнародної співпраці у сфері протидії кіберзлочинності, зокрема роль Будапештської конвенції та її додаткових протоколів у створенні єдиної системи кримінального переслідування у цифровому просторі; розкрити значення цифрової криміналістики в процесі виявлення та аналізу цифрових доказів, визначити її місце в структурі криміналістичної науки та основні методологічні засади застосування; визначити умови ефективного використання цифрової криміналістика та електронних доказів.

Методологія. У процесі написання статті було використано комплекс методів наукового пізнання, які забезпечили міждисциплінарний характер дослідження та дозволили досягти поставленої мети. Філософсько-діалектичний метод сприяв аналізу розвитку цифрових технологій і трансформації форм злочинності у цифровому середовищі, зокрема кібершахрайства в електронній торгівлі, в контексті глобалізації та цифровізації суспільства. Формально-логічний метод був застосований для з'ясування ознак і правової природи кібершахрайства, визначення структурних елементів

цифрової криміналістики та електронних доказів. Спеціально-юридичний метод дозволив здійснити системний аналіз міжнародно-правових актів, зокрема положень Будапештської конвенції та її додаткових протоколів, а також норм національного законодавства, що регулюють питання доказування у сфері кіберзлочинності. Порівняльно-правовий метод дав змогу зіставити підходи до розслідування кіберзлочинів у різних юрисдикціях, що стало основою для формування рекомендацій щодо уніфікації стандартів доказування. Емпіричний метод був використаний для аналізу актуальної практики застосування цифрової криміналістики та міжнародного співробітництва у сфері протидії кіберзлочинності. Сукупне застосування вказаних методів забезпечило глибоке наукове осмислення теми дослідження й обґрунтування висновків, що мають як теоретичне, так і прикладне значення.

Виклад основного матеріалу. У сфері кримінально-правової науки та практики правоохоронної діяльності дедалі більшої актуальності набуває проблема кваліфікації та протидії злочинам, що вчиняються у кіберпросторі. З огляду на способи їх реалізації, такі кримінальні правопорушення можуть бути типологізовані за характерними механізмами вчинення на кілька ключових категорій:

– неправомірний доступ до інформаційно-телекомунікаційних систем і мереж – полягає у несанкціонованому проникненні в комп'ютерні системи чи мережі з метою отримання, зміни, блокування або знищення інформації;

– розроблення, використання, поширення та збут шкідливого програмного забезпечення – охоплює створення та обіг шкідливих програмних засобів (вірусів, троянських програм, шпигунського ПЗ), призначених для ураження інформаційних систем, викрадення даних або порушення їхньої цілісності та функціонування;

– протиправне створення, використання, розповсюдження або збут матеріалів, заборонених до публічного обігу – включає поширення через цифрові платформи інформації, що містить дитячу порнографію, пропаганду насильства, терористичних актів, заклики до ворожнечі або іншого контенту, забороненого чинним законодавством;

– порушення авторських і суміжних прав у мережі Інтернет – полягає в незаконному відтворенні, поширенні або іншим несанкціонованим використанні об'єктів інтелектуальної власності (творів, музики, фільмів, програмного забезпечення) без згоди правовласників;

- шахрайство з використанням цифрових пристроїв – охоплює різноманітні форми обману, які реалізуються через Інтернет або інші цифрові засоби, зокрема фішинг, створення фіктивних онлайн-магазинів, шахрайські інвестиційні платформи тощо;

– крадіжка в кіберпросторі – включає незаконне заволодіння грошовими коштами, криптовалютою або персональними даними користувачів через використання кіберзасобів, у тому числі шляхом злому систем, зараження вірусами чи маніпуляцій з даними;

– здійснення комерційної діяльності без державної реєстрації фізичної особи-підприємця – передбачає надання товарів або послуг через мережу Інтернет без належної юридичної реєстрації, що є порушенням податкового та господарського законодавства [1, с. 288].

В умовах цифровізації суспільства злочинність все більше зміщується в онлайн-сферу. Той факт, що Інтернет не має кордонів, дозволяє надавати електронні послуги з будь-якої точки світу без фізичної присутності постачальника в країні, де ці послуги споживаються. Однак Інтернет також може бути використаний як засіб вчинення або сприяння вчиненню злочинів. Зі зростанням комп'ютеризації з'являється нове явище – вчинення злочинів за допомогою комп'ютерних технологій. Це явище часто називається «комп'ютерною злочинністю», «кіберзлочинністю», «інформаційно-технологічною злочинністю» або «високотехнологічною злочинністю» [10, с. 701].

Узагальнення зазначених категорій дозволяє сформувати цілісне уявлення про найбільш поширені моделі кіберзлочинної діяльності та, відповідно, створити передумови для більш ефективної протидії цим загрозам у межах кримінального права. Оскільки за результатами опитування українських респондентів у рамках Всесвітнього дослідження економічних злочинів та шахрайства 2020 року, звертається увага на зростання обсягу шахрайства [16], є необхідність дослідити зазначену проблему.

Шахрайство, що полягає у заволодінні чужим майном або отриманні права на нього через обман чи зловживання довірою, є злочином, який швидко адаптується до соціально-економічних змін в Україні. З огляду на розвиток ринкових відносин і впровадження сучасних технологій у різні сфери суспільного життя, такі кримінальні правопорушення проявляються у різноманітних формах [4, с. 213-214]. Зокрема, треба констатувати настання нового етапу розвитку злочинності у сфері інформаційних технологій, що відзначається активним застосуванням засобів масової інформації для спотворення достовірної інформації, а також значним поширенням кібершахрайства [2, с. 444]. У таких умовах активно розвивається шахрайство у сфері електронної торгівлі, передбачене частиною 3 статті 190 Кримінального кодексу України [7]. Цей вид злочинів характеризується

низкою особливостей: недостатнім рівнем контролю з боку суспільства та правоохоронних органів, що ускладнює їх виявлення; високим інтелектуальним рівнем виконання, оскільки злочинці використовують складні технічні схеми; значною латентністю, адже багато жертв не повідомляють про такі випадки через сором чи недовіру до системи правосуддя; мінімальним ризиком для правопорушників через анонімність у цифровому просторі; а також порівняно легким досягненням злочинного результату. Ці фактори створюють сприятливе середовище для поширення кіберзлочинності, що потребує вдосконалення правових і технічних механізмів протидії [8, с. 503].

Кібершахрайство являє собою окремий вид кримінального правопорушення, який відрізняється від традиційного шахрайства і виник у процесі еволюції злочинної діяльності під впливом розвитку інформаційних технологій. Цей вид злочину характеризується застосуванням нових, раніше не досліджених методів, що стали можливими завдяки цифровим технологіям, хоча за своєю структурою та складом кібершахрайство має схожість із класичним шахрайством [15, с. 547], адже також передбачає обман чи зловживання довірою з метою заволодіння чужим майном або майновими правами. Такі методи включають, зокрема, фішинг, створення фальшивих вебсайтів, використання шкідливого програмного забезпечення чи соціальну інженерію, що дозволяє зловмисникам діяти анонімно та на відстані, ускладнюючи їх виявлення та притягнення до відповідальності.

З огляду на те, що шахрайство у сфері електронної торгівлі відбувається в кіберпросторі, необхідно проаналізувати особливості правового регулювання відповідної сфери життєдіяльності суспільства. Згідно з ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», національна система кібербезпеки визначається як комплексна сукупність суб'єктів, які відповідають за кібербезпеку, та взаємопов'язаних заходів різного спрямування. Ці заходи охоплюють політичні, науково-технічні, інформаційні та освітні ініціативи, а також організаційні, правові, оперативно-розшукові, розвідувальні, контррозвідувальні, оборонні й інженерно-технічні дії. Крім того, система включає заходи криптографічного й технічного захисту національних інформаційних ресурсів, а також кіберзахист об'єктів критичної інформаційної інфраструктури, таких як державні інформаційні системи, фінансові платформи та енергетичні мережі, що є ключовими для функціонування держави та економічної безпеки [13]. А відповідно до п. 11 с. 1 ст. 1 зазначеного Закону, кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та / або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та / або інших глобальних мереж передачі даних [13].

Оскільки кіберпростір є віртуальним середовищем, що забезпечує комунікації та суспільні відносини через глобальні мережі, а національна система кібербезпеки охоплює широкий спектр заходів для захисту інформаційних ресурсів і критичної інфраструктури, логічним є створення необхідної основи для протидії кіберзлочинам. Такий багатогранний підхід спрямований на запобігання кіберзлочинам, зокрема шахрайству в електронній торгівлі, та забезпечення стабільності цифрового середовища [17, с. 502-503]. Це є важливим, оскільки електронна комерція в Інтернеті майже повністю покладається на фінансові установи, які виступають у ролі довірених третіх сторін при обробці електронних платежів. Хоча така система працює достатньо добре для більшості транзакцій, вона все ж має вади, притаманні моделі, що базується на довірі. Цілковито незворотні транзакції неможливі, оскільки фінансові установи змушені виступати посередниками у вирішенні спорів. Це підвищує вартість обробки транзакцій, обмежуючи мінімально доцільну суму переказу та унеможливлюючи дрібні повсякденні платежі. Крім того, втрачається можливість здійснення незворотних платежів за незворотні послуги. Через ризик скасування транзакцій зростає потреба у взаємній довірі. Продавці змушені бути обережними щодо покупців, вимагаючи від них більше інформації, ніж це було б потрібно в іншому випадку. Певний відсоток шахрайства визнається неминучим [21].

У численних випадках після вчинення протиправного діяння на місці події зберігаються матеріальні сліди, так само і інформація в електронно-обчислювальній техніці, яка була задіяна для здійснення злочину. Такі сліди можуть включати фізичні докази, наприклад, відбитки пальців, документи чи предмети, а також цифрові дані, як-от записи в комп'ютерних системах, історія транзакцій, листування чи логи доступу, що дозволяють правоохоронним органам ідентифікувати злочинця та реконструювати обставини правопорушення [9, с. 158].

У контексті дослідження протидії злочинності у сфері підприємництва, зокрема шахрайства в онлайн-торгівлі, важливе значення має використання цифрових доказів та методів цифрової криміналістики. Наукова робоча група з цифрових доказів (SWGDE), до складу якої входять представники правоохоронних органів, науковці та комерційні організації у сфері цифрової криміналістики, визначає цифрові докази як інформацію з доказовим значенням, що зберігається або передається у бінарній формі, розробляючи міждисциплінарні стандарти для їх виявлення, збереження та ана-

лізу [Див.: 10, с. 700]. Цифрова криміналістика розглядається як процес отримання, збереження, аналізу та документування електронно збереженої інформації з використанням науково обґрунтованих методів, що характеризуються надійністю, верифікованістю та відтворюваністю, для забезпечення їх застосування у судових провадженнях, зокрема у справах, пов'язаних із шахрайством в онлайн-торгівлі. У цьому процесі ключовими є принципи, які застосовуються на всіх етапах дослідження – від збору даних до їх аналізу та підготовки звітів. Однак у розслідуванні шахрайських схем в онлайн-торгівлі, де методи цифрової криміналістики використовуються як інструмент, основний акцент робиться на ідентифікації та вилученні інформації, що може бути отримана з різноманітних цифрових джерел, таких як комп'ютери, мобільні пристрої, платформи електронної торгівлі, соціальні мережі чи інші цифрові платформи, які часто використовуються зловмисниками для вчинення шахрайських дій. Такий підхід стимулює розвиток інноваційних методів пошуку релевантної інформації, що є критично важливою для виявлення схем шахрайства, таких як фіктивні продажі, підробка платіжних даних чи маніпуляції з відгуками. Інформація, отримана в процесі цифрового розслідування, може бути передана для подальшого аналізу в рамках цифрової криміналістики, але для цього вона повинна відповідати суворим вимогам наукового методу та правилам допустимості доказів у суді. Водночас результати, отримані за допомогою цифрової криміналістики, можуть слугувати основою для цифрових розслідувань, сприяючи ефективній протидії шахрайству в онлайн-торгівлі та підвищенню якості доказової бази у кримінальних провадженнях [23]. Але це можливо тільки за умови ефективного міжнародного співробітництва, зокрема, можливості здійснення оперативного обміну інформацією: зростаючий рівень транскордонної злочинності зумовлює необхідність оперативної та ефективної взаємодії між компетентними органами різних держав. У відповідь на ці виклики міжнародна правова спільнота дедалі частіше вдається до укладення міжвідомчих угод і формування гнучких механізмів інформаційного обміну, що дозволяє пришвидшити отримання процесуально значущих даних та забезпечити реальний доступ до правосуддя в умовах, коли традиційні канали співпраці не завжди відповідають сучасним потребам [5, с. 611]. Таким чином, цифрова криміналістика – це галузь криміналістичної науки, що займається збором, аналізом, збереженням і представленням цифрових доказів, отриманих з електронних пристроїв, мереж або цифрових середовищ, з метою розслідування злочинів, зокрема кіберзлочинів. Вона включає методики ідентифікації, вилучення та інтерпретації даних з комп'ютерів, смартфонів, серверів, хмарних сховищ тощо, забезпечуючи їх юридичну достовірність для використання в судових процесах, при цьому дотримуючись принципів захисту прав людини та конфіденційності.

Організована злочинність за своєю сутністю долає національні кордони, набуваючи транснаціонального характеру. Унаслідок цього жодна держава не здатна самостійно ефективно розслідувати та притягувати до відповідальності за злочинні дії без підтримки інших країн, які або зазнають впливу цих діянь, або через які вони поширюються. Для дієвої протидії необхідні спільні зусилля та співпраця як на двосторонньому, так і на міжнародному рівні. Щоб досягти значних результатів і запобігти розробці та реалізації злочинних планів, така співпраця повинна бути активною й багатосторонньою [12, с. 6]. Міжнародне співробітництво у кримінальному судочинстві є комплексним правовим інститутом і включає як норми кримінального процесуального законодавства, що регламентують власні кримінальні провадження у зв'язку із таким співробітництвом, та і норми міжнародного права [11, с. 17].

Міжнародне співробітництво у сфері запобігання та протидії злочинам організується за такими критеріями: за напрямами (презентаційна, навчально-освітня, технічна допомога, інші види підтримки, пряма взаємодія); за формами реалізації (через встановлення інформаційно-комунікаційних каналів, договірні відносини, спільні правоохоронні заходи); за суб'єктами (шляхом утворення міжнародних правоохоронних організацій (глобального та регіонального рівня), міжвідомча співпраця (на рівні відомств або через міжнародні організації); за участю окремих осіб (офіцери зв'язку, особисті контакти). У практичній діяльності розрізняють два способи обміну інформацією: формальний і неформальний. Перший відбувається через офіційні документальні канали, які використовуються для отримання або надсилання офіційних документів, пов'язаних із економічною злочинністю чи особами, які її вчинили. Натомість неформальний обмін інформацією здійснюється за допомогою недокументальних засобів зв'язку, таких як телефонні розмови, електронні листи або інші способи передачі даних через мережу Інтернет [3, с. 47-48]. Міжнародна співпраця країн Європи та України у галузі криміналістики завжди була плідною та ефективною: іноземні спеціалісти надавали великий спектр різноманітної допомоги як у проведенні окремих видів судових експертиз так і ділилися досвідом щодо використання криміналістичних знань при розслідуванні кримінальних правопорушень [18, с. 214].

Ключову роль у виявленні злочинних схем, ідентифікації суб'єктів правопорушень та попередженні протиправних дій відіграє обмін інформацією, що вимагає налагодження чітких механізмів

взаємодії на національному та міжнародному рівнях. Саме тому виникає потреба в уніфікованих міжнародних стандартах, які б регулювали обмін інформацією у сфері боротьби зі злочинами, особливо в цифровому просторі.

Будапештська конвенція про кіберзлочинність, також відома як Конвенція Ради Європи про кіберзлочинність (Convention on Cybercrime, Council of Europe), є першим міжнародним договором, який було відкрито для підписання 23 листопада 2001 року з метою протидії злочинам у сфері Інтернету та комп'ютерних мереж (кіберзлочинності). Цей документ розробили у відповідь на зростання кіберзлочинів наприкінці 1990-х років, спричинене широким поширенням використання Інтернету. На квітень 2023 року до Конвенції приєдналися 68 держав (ратифікована Україною 07.09.2005) [14]. Конвенція, сприяючи уніфікації стандартів розслідування та переслідування кіберзлочинів, має на меті: забезпечити баланс між ефективною роботою правоохоронних органів і захистом основних прав людини; створити основу для взаємодопомоги між державами у питаннях кібербезпеки; надати можливість країнам обмінюватися даними та ресурсами під час розслідування кіберзлочинів; узгодити національні законодавства та зміцнити співпрацю у транснаціональних відносинах у сфері кібербезпеки [6].

Зазначена конвенція виходить за рамки звичайного юридичного документа, який встановлює кримінальну відповідальність за кіберзлочини, визначає процесуальні механізми для збору електронних доказів і створює правові засади для міжнародної взаємодії. Завдяки діяльності Комітету з питань Конвенції про кіберзлочинність (T-CY) та Офісу програми з кіберзлочинності Ради Європи (C-PROC), вона слугує універсальною платформою, що сприяє обміну досвідом і налагодженню контактів, спрощуючи співпрацю в конкретних ситуаціях, зокрема в екстрених випадках, навіть якщо це виходить за межі її прямих положень. Хоча будь-яка країна може застосовувати Конвенцію як основу для розробки національного законодавства, статус сторони відкриває додаткові можливості: використання її як правової бази для міжнародної співпраці, участь у розробці нових настанов чи протоколів, доступ до мережі контактних пунктів в режимі 24/7, посилення взаємодії з приватним сектором, а також пріоритетність для країн-учасниць і тих, що прагнуть приєднатися. Відкрита для підписання в Будапешті в листопаді 2001 року, Конвенція про кіберзлочинність вважається ключовим міжнародним договором у сфері боротьби з кіберзлочинами та роботи з електронними доказами. Вона охоплює: (i) криміналізацію діянь, таких як незаконний доступ, втручання в дані чи системи, комп'ютерне шахрайство та дитяча порнографія; (ii) процесуальні інструменти для розслідування кіберзлочинів і збору електронних доказів у кримінальних провадженнях; (iii) ефективні механізми міжнародної співпраці. Конвенція балансує між ідеєю вільного Інтернету, де інформація поширюється без перешкод, та необхідністю дієвої кримінально-правової реакції на зловживання цифровими технологіями. При цьому обмеження чітко визначені: розслідуються лише конкретні злочини, а доступ до даних відбувається з урахуванням прав людини та верховенства права. Розроблена країнами Ради Європи спільно з Канадою, Японією, ПАР і США, Конвенція відкрита для приєднання будь-якої держави, і дедалі більше країн з Африки, Америки та Азійсько-Тихоокеанського регіону долучаються до неї для посилення своєї кримінальної юстиції в справах, пов'язаних із кіберзлочинами. Держави, які є сторонами, підписали документ або отримали запрошення приєднатися, беруть участь у роботі Комітету T-CY як члени чи спостерігачі. T-CY, зокрема, аналізує виконання Конвенції, розробляє роз'яснення та створює додаткові правові інструменти. Конвенцію також підтримують проєкти з розбудови потенціалу, які координує Офіс C-PROC у Румунії, допомагаючи країнам по всьому світу розвивати спроможності для розслідування, переслідування та судового розгляду кіберзлочинів відповідно до стандартів Конвенції та рекомендацій T-CY. Таким чином, Будапештська конвенція є не лише юридичним документом, а й ефективним інструментом глобальної взаємодії [24].

Оскільки кіберзлочинність поширюється, а отримання доказів, які можуть зберігатися в іноземних або невідомих юрисдикціях, ускладнюється транскордонними обмеженнями [22] і з метою удосконалення дії зазначеного міжнародного договору, в ЄС був розроблений Другий Додатковий Протокол до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів (CETS № 224), який відповідає на цей виклик і надає інструменти для посиленої співпраці та розкриття електронних доказів, такі як пряма співпраця з постачальниками послуг та реєстраторами, ефективні засоби отримання інформації про абонентів та даних про трафік, негайна співпраця в надзвичайних ситуаціях або спільні розслідування, які підпадають під систему прав людини та верховенства права, включаючи гарантії захисту даних [20].

Конвенція про кіберзлочинність (ETS № 185) є першим міжнародним договором про злочини, скоєні через Інтернет та інші комп'ютерні мережі, що стосується, зокрема, порушень авторських прав, комп'ютерного шахрайства, дитячої порнографії та порушень мережевої безпеки. Вона також містить низку повноважень та процедур, таких як пошук у комп'ютерних мережах та перехоплення.

Його головна мета, викладена у преамбулі, полягає у проведенні спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, зокрема шляхом прийняття відповідного законодавства та сприяння міжнародній співпраці [19].

27 червня 2016 року Україна уклала Угоду про співпрацю з Європейською організацією з питань юстиції (Євроюстом), створеною у березні 2002 року для підвищення ефективності роботи правоохоронних органів країн ЄС у розслідуванні та судовому переслідуванні особливо небезпечних кримінальних правопорушень. Проблемним є те, що положення Угоди не включають норм, які б повністю та вичерпно регулювали права й обов'язки сторін. У кількох статтях Угоди (ст. 1, 3, 4, 5, 6, 18) є посилання на положення Рішення Ради Європейського Союзу від 28 лютого 2002 року – документа, прийнятого третьою стороною без участі України. При цьому в Угоді відсутнє застереження, що для її цілей положення цього Рішення застосовуватимуться виключно в редакції, чинній на момент укладення Угоди. Таким чином, будь-які зміни до цих положень, що відбуватимуться без участі, згоди чи волі України, призводитимуть до зміни обсягу прав та обов'язків України за цією Угодою без її відома. Як бачимо, інтереси України в контексті цієї Угоди суттєво вразливі через її правову невизначеність та залежність від зовнішніх нормативних актів. Угода не забезпечує повного і вичерпного регулювання прав та обов'язків сторін, а відсилки до Рішення Ради Європейського Союзу від 28 лютого 2002 року створюють ризик односторонньої зміни умов без участі України, внаслідок чого вона втрачає контроль над обсягом своїх зобов'язань, що може негативно вплинути на її правову та економічну стабільність.

Таким чином, міжнародна протидія кіберзлочинності, зокрема у сфері електронної торгівлі, полягає у формуванні комплексної системи співпраці між державами, спрямованої на уніфікацію правових стандартів, оперативний обмін інформацією та забезпечення доступу до електронних доказів. Ключовим інструментом виступає Будапештська конвенція про кіберзлочинність, яка встановлює юридичні та процесуальні засади для транснаціональної взаємодії. Її положення доповнюються Другим Додатковим Протоколом, що передбачає механізми прямої співпраці з постачальниками цифрових послуг і спрощений доступ до даних. Міжнародне співробітництво також реалізується через договірні відносини, такі як Угода України з Євроюстом, яка, попри недоліки, розширює можливості обміну релевантною інформацією. Таким чином, ефективна протидія кібершахрайству в електронній торгівлі можлива лише за умов інтеграції цифрової криміналістики, належної правової регламентації та скоординованої взаємодії міждержавних структур.

Висновки:

1. Кібершахрайство в електронній торгівлі є окремим видом високотехнологічного злочину, що потребує окремого кримінально-правового підходу через особливості його здійснення – транснаціональний характер, анонімність правопорушників, використання шкідливого ПЗ та цифрових платформ, високу латентність і мінімальні ризики викриття. Це зумовлює потребу в оновленні інструментів кримінально-правової кваліфікації та засобів виявлення таких злочинів.

2. Міжнародна протидія кіберзлочинності в електронній торгівлі базується на уніфікації правових стандартів, швидкому обміні інформацією та доступі до цифрових доказів. Ключову роль у цьому відіграє Будапештська конвенція та її додаткові протоколи, які формують правову основу для транснаціональної взаємодії й кримінального переслідування кібершахрайства.

3. Цифрова криміналістика – це галузь криміналістичної науки, що займається збором, аналізом, збереженням і представленням цифрових доказів, отриманих з електронних пристроїв, мереж або цифрових середовищ, з метою розслідування злочинів, зокрема кіберзлочинів. Вона включає методики ідентифікації, вилучення та інтерпретації даних з комп'ютерів, смартфонів, серверів, хмарних сховищ тощо, забезпечуючи їх юридичну достовірність для використання в судових процесах, при цьому дотримуючись принципів захисту прав людини та конфіденційності.

4. Цифрова криміналістика та електронні докази є ключовими засобами виявлення й доведення кіберзлочинів, зокрема шахрайства в онлайн-торгівлі. Проте їх ефективне використання можливе лише за умови дотримання стандартів достовірності, допустимості та відтворюваності доказової інформації, що потребує подальшої розробки національних нормативних актів і узгодження з міжнародними підходами до доказування у сфері цифрових злочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Думчиков М.О. Криміналістична типологізація кримінальних правопорушень у кіберпросторі. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. № 2. С. 287–290. DOI: https://doi.org/10.24144/2788-6018.2023.02.49.
2. Бодунова О.М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. № 1. С. 441–445. DOI: https://doi.org/10.24144/2788-6018.2023.01.76.

3. Грицишен Д.О. Міжнародна співпраця в сфері запобігання та протидії економічній злочинності: державно-управлінський аспект. *Економічний вісник*. 2020. № 4. С. 36–50. DOI: https://doi.org/10.33271/ebdut/72.036.
4. Заяць К.Д., Заяць Д.Д. Особливості розслідування шахрайств, що маскуються під оболонкою цивільних правовідносин. Вісник Харківського національного університету внутрішніх справ. 2023. № 101(2) Part 1. С. 213-224. DOI: https://doi.org/10.32631/v.2023.2.20.
5. Зуєв В.В. Тенденції міжнародного співробітництва України у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2024. № 4. С. 608–612. DOI: https://doi.org/10.32782/2524-0374/2024-4/144.
6. Карвацька С. Будапештська конвенція про кіберзлочинність як основний міжнародно – правовий стандарт щодо кіберзлочинності. Юридичний факультет Чернівецького національного університету ім. Ю. Федьковича. 27.02.2025. URL: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist (дата звернення: 06.06.2025).
7. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 06.06.2025).
8. Кулик О.І. Поняття і елементи господарської правосуб'єктності постачальників послуг, пов'язаних з оборотом віртуальних активів. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 5. С. 282–287. DOI: https://doi.org/10.24144/2788-6018.2024.05.45.
9. Лепей М.В. Наукові дискусії щодо проведення різних видів огляду під час розслідування шахрайства у сфері використання банківських електронних платежів. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 105(2) (Part 1). С. 158–166. DOI: https://doi.org/10.32631/v.2024.2.15.
10. Матіс Я. Деякі аспекти кримінальних доказів та цифрових доказів. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2024. № 2. С. 699–704. DOI: https://doi.org/10.24144/2788-6018.2024.02.116.
11. Міжнародне співробітництво у кримінальному судочинстві: навч.-метод. посіб. [Електронне видання] / уклад.: М.І. Смирнов, В.К. Волошина, А.В. Підгородинська; Нац. ун-т «Одеська юрид. академія». Одеса: Фенікс, 2024. 165 с. URL: https://document.kdu.edu.ua/info_zab/081_2048.pdf (дата звернення: 06.06.2025).
12. Посібник з міжнародного співробітництва та інформаційного обміну. Керівництво для співробітників регулятивних, судових та правоохоронних органів. Комісія Британських Віргінських островів. 2013. 43 с. URL: https://star.worldbank.org/sites/star/files/ bvi_international_cooperation_handbook_2013_ukraine_version.pdf (дата звернення: 06.06.2025).
13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 06.06.2025).
14. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.
15. Сметаніна Н.В., Діброва Т.А., Пісенко Д.О. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*, 2022. С. 546–549.
16. Третяк А., Рябова Д. Результати опитування українських респондентів у рамках Всесвітнього дослідження економічних злочинів та шахрайства 2020 року: основні тенденції – зростання обсягу шахрайства та економічних злочинів. Європейська Бізнес Асоціація. 01.12.2020. URL: https://eba.com.ua/ader-haber-yurydychnyj-radnyk-svitovogo-banku-z-reformuvannya-pensijnoyi-systemy-ukrayiny/ (дата звернення: 06.06.2025).
17. Харитонов С.О. Суб'єкти запобігання шахрайству у сфері електронної торгівлі. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2023. № 5. С. 502–505. DOI: https://doi.org/10.24144/2788-6018.2023.05.90.
18. Яремчук В.О. Міжнародна співпраця у галузі криміналістики та судової експертизи в умовах війни. *Теорія та практика протидії злочинності у сучасних умовах*: збірник тез Міжнародної науково-практичної конференції (3 листопада 2023 року) / упор. Р.М. Шехавцов. Львів: Львівський державний університет внутрішніх справ, 2023. С. 214-215.
19. Details of Treaty No.185. Convention on Cybercrime (ETS No. 185). An official website of the European Union. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (дата звернення: 06.06.2025).
20. Details of Treaty No.224. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). An official website of the European Union. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (дата звернення: 06.06.2025).

21. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin Project. *Investopedia*. URL: https://www.investopedia.com/terms/c/cryptocurrency.asp#citation-8 (дата звернення: 06.06.2025).
22. Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). An official website of the European Union. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol (дата звернення: 06.06.2025).
23. SWGDE: Digital and Multimedia Evidence (Digital Forensics) as a Forensic Science Discipline. 05.09.2014. URL: https://www.swgde.org/14-f-001/ (дата звернення: 06.06.2025).
24. The Budapest Convention on Cybercrime: benefits and impact in practice. Cybercrime Convention Committee (T-CY). Strasbourg, 13 July 2020. URL: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (дата звернення: 06.06.2025).