

УДК 343.14:004.77:[343.9.024:336.7](477:4-6ЄС)
DOI <https://doi.org/10.32999/ksu2307-8049/2026-3-13>

ТРАНСКОРДОННЕ ОТРИМАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ПРОВАДЖЕННЯХ ЩОДО ЛЕГАЛІЗАЦІЇ ЗЛОЧИННИХ ДОХОДІВ: ДРУГИЙ ДОДАТКОВИЙ ПРОТОКОЛ ДО БУДАПЕШТСЬКОЇ КОНВЕНЦІЇ ТА ПАКЕТ ЄС E-EVIDENCE

Луцик Володимир Олександрович,
здобувач вищої освіти 2 року денної форми навчання
третього (освітньо-наукового) рівня вищої освіти
спеціальності 081 «Право»
Київського національного університету імені Тараса Шевченка
volodymyr.lutsyk@knu.ua
orcid.org/0009-0007-6308-4925

Метою статті є аналіз змісту та практичного значення Другого додаткового протоколу до Будапештської конвенції (надалі – «Другий додатковий протокол»), Регламенту (ЄС) 2023/1543 Європейського Парламенту і Ради (надалі – «Регламент (ЄС) 2023/1543»), та Директиви (ЄС) 2023/1544 Європейського Парламенту і Ради (надалі – «Директива (ЄС) 2023/1544») для вдосконалення механізму збирання електронних доказів у кримінальних провадженнях, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, а також обґрунтування необхідності їх урахування в національному законодавстві України. Крім того, у статті проаналізовано окремі новітні акти права Європейського Союзу, які передбачають використання електронних доказів у сфері протидії відмиванню доходів та регулювання криптоактивів.

Методи. Дослідження ґрунтується на застосуванні формально-юридичного методу для аналізу змісту міжнародно-правових актів, порівняльно-правового методу для зіставлення положень права Ради Європи та Європейського Союзу з чинним кримінальним процесуальним законодавством України, а також системного аналізу для визначення взаємозв'язку між розглянутими інструментами та їхнього сукупного значення для правозастосовної практики.

Результати. Встановлено, що Другий додатковий протокол запроваджує (за авторською узагальнювальною моделлю) три розмежовані за предметом і процедурою рівні співробітництва, з яких лише перший, безпосереднє звернення до постачальника послуг щодо даних про абонента, дозволяє повністю уникнути процедури взаємної правової допомоги, тоді як трафікові дані та дані про зміст комунікації залишаються предметом окремої, хоча й спрощеної, процедури. Визначено, що передбачений Регламентом (ЄС) 2023/1543 поріг у три роки позбавлення волі для доступу до трафікових даних і даних про зміст за загальним правилом застосовується для складу легалізації доходів з огляду на вимоги Директиви (ЄС) 2018/1673 Європейського Парламенту і Ради (надалі – «Директива (ЄС) 2018/1673») щодо мінімального покарання, хоча застосування Регламенту (ЄС) 2023/1543 додатково залежить від кваліфікації діяння, судового затвердження та пропорційності втручання. Виявлено юридичну невизначеність щодо застосування Регламенту (ЄС) 2023/1543 до постачальників послуг з обігу віртуальних активів, яка потребує окремого вирішення.

Висновки. Обґрунтовано необхідність прискорення ратифікації Другого додаткового протоколу Україною як найбільш застосовного інструмента, урахування процесуальних стандартів права Європейського Союзу під час удосконалення Кримінального процесуального кодексу України, а також вивчення можливості запровадження національного аналога інституту представника для цілей збору електронних доказів стосовно постачальників послуг, що діють на території України.

Ключові слова: транскордонний доступ до даних, представник для збору доказів, Регламент (ЄС) 2023/1543, Директива (ЄС) 2023/1544, взаємна правова допомога, Державна служба фінансового моніторингу, віртуальні активи, цифрові докази.



CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE IN MONEY LAUNDERING PROCEEDINGS: THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION AND THE EU E-EVIDENCE PACKAGE

Lutsyk Volodymyr Oleksandrovych,
2nd-year full-time PhD student,
third (educational and scientific) level of higher education,
specialty 081 «Law»
Taras Shevchenko National University of Kyiv
volodymyr.lutsyk@knu.ua
orcid.org/0009-0007-6308-4925

The purpose of the article is to analyse the content and practical significance of the Second Additional Protocol to the Budapest Convention (the «Second Additional Protocol»), Regulation (EU) 2023/1543 of the European Parliament and of the Council (the «Regulation (EU) 2023/1543») and Directive (EU) 2023/1544 of the European Parliament and of the Council (the «Directive (EU) 2023/1544») for improving the mechanism of collecting electronic evidence in criminal proceedings related to the legalisation (laundering) of proceeds of crime, and to substantiate the necessity of taking these acts into account in the national legislation of Ukraine. In addition, the article analyses selected recent European Union legal acts governing the use of electronic evidence in the fields of anti-money laundering and crypto-asset regulation.

Methods. The study is based on the formal-legal method for analysing the content of international legal acts, the comparative-legal method for correlating the provisions of Council of Europe and European Union law with the current criminal procedural legislation of Ukraine, and systemic analysis for determining the interrelation between the instruments examined and their cumulative significance for law-enforcement practice.

Results. It has been established that the Second Additional Protocol introduces (according to the author's generalised model) three subject and procedure-differentiated levels of cooperation, of which only the first, direct requests to service providers for subscriber data, allows the mutual legal assistance procedure to be avoided entirely, whereas traffic data and content data remain subject to a separate, albeit simplified, procedure. It has been determined that the three-year custodial threshold set by Regulation (EU) 2023/1543 for access to traffic and content data is, as a general rule, met for the offence of money laundering given the minimum penalty requirements of Directive (EU) 2018/1673 of the European Parliament and of the Council (the «Directive (EU) 2018/1673»), although the application of the Regulation additionally depends on the legal classification of the act, judicial authorisation, and the proportionality of the interference. Legal uncertainty has been identified regarding the application of the Regulation to virtual asset service providers, which requires a separate solution.

Conclusions. The necessity is substantiated of accelerating Ukraine's ratification of the Second Additional Protocol as the most directly applicable instrument, taking into account the procedural standards of European Union law when improving the Criminal Procedure Code of Ukraine, and examining the possibility of introducing a national analogue of the institution of a representative for the purpose of gathering electronic evidence in respect of service providers operating in Ukraine.

Keywords: cross-border data access, service provider representative, Regulation (EU) 2023/1543, Directive (EU) 2023/1544, mutual legal assistance, State Financial Monitoring Service, virtual assets, digital evidence.

Вступ. Транснаціональний характер легалізації доходів, одержаних злочинним шляхом, а також дедалі ширше використання цифрових фінансових інструментів і послуг іноземних постачальників зумовлюють нагальну потребу в оперативних та ефективних механізмах транскордонного отримання електронних доказів. Національне кримінальне процесуальне законодавство України, орієнтоване здебільшого на традиційні процедури міжнародної правової допомоги, не завжди здатне забезпечити швидкість, необхідну для збереження та отримання даних, що зберігаються на серверах постачальників послуг за межами України. У зв'язку з цим особливого значення набувають новітні інструменти Ради Європи та Європейського Союзу, які запроваджують спрощені та пришвидшені механізми взаємодії із постачальниками послуг. Новизна дослідження полягає в тому, що ці інструменти вперше аналізуються саме в контексті

проваджень про легалізацію злочинних доходів, а не як загальна проблематика кіберзлочинності.

Проблематика електронних доказів активно розробляється в українській юридичній науці. Серед українських дослідників увагу привертають праці Д. Б. Сергєєвої, М. А. Погорецького, Н. М. Ахтирської, О. В. Сіренка, В. М. Бутузова, В. В. Лисенка, В. О. Мещерякова, А.-М. Ю. Ангеленюк, С. Й. Гонгало та інших. Водночас проблематика застосування новітніх актів права Ради Європи та Європейського Союзу щодо електронних доказів саме у контексті кримінальних проваджень про легалізацію злочинних доходів досі не отримала комплексного висвітлення у вітчизняній науці, що і зумовлює актуальність цієї публікації. Окремо варто відзначити нещодавню публікацію М. А. Погорецького, у якій обґрунтовано, що цифрові (електронні) докази не утворюють самостійної онтологічної категорії доказів, а цифрова форма

є лише техніко-юридичним способом фіксації доказової інформації, який не змінює процесуальної природи показань, документів, речових доказів чи висновків експертів (Погорецький, 2026). Це методологічне уточнення враховано і в цій статті: термін «електронні докази» вживається далі не як окремий вид доказів, а як узагальнене позначення доказової інформації, зафіксованої у цифровій формі, безвідносно до її формальної процесуальної природи. Питання допустимості та ознак електронних доказів у кримінальному судочинстві України також розглянуто в новітньому дослідженні Л. В. Мілімко та Ю. В. Жидовцева, які встановили, що чинне кримінальне процесуальне законодавство регулює відносини щодо електронних доказів недостатньо чітко, що спричиняє відсутність єдиного підходу судів до їх розуміння (Мілімко, Жидовцев, 2025). Цей висновок повністю узгоджується з виявленою в цій статті потребою в удосконаленні норм Кримінального процесуального кодексу України з урахуванням трансграничного походження значної частини сучасних електронних доказів.

Метою статті є аналіз змісту та значення Другого додаткового протоколу, Регламенту (ЄС) 2023/1543 та Директиви (ЄС) 2023/1544 для вдосконалення механізму збирання електронних доказів у кримінальних провадженнях, пов'язаних із легалізацією доходів, одержаних злочинним шляхом в Україні, а також обґрунтування процесуальних гарантій їх допустимості та специфіки застосування у справах цієї категорії.

Для досягнення зазначеної мети визначено такі завдання дослідження: проаналізувати зміст та рівні співробітництва, запроваджені Другим додатковим протоколом; з'ясувати стан підписання та ратифікації його Україною; розкрити зміст категорій електронних доказів та процесуальних строків, встановлених Регламентом (ЄС) 2023/1543; визначити механізм призначення представників постачальників послуг за Директивою (ЄС) 2023/1544; обґрунтувати значення розглянутих актів для кримінальних проваджень про легалізацію доходів, одержаних злочинним шляхом, та сформулювати пропозиції щодо їх урахування в національному законодавстві, визначити процесуальні гарантії допустимості й автентичності трансгранично отриманих електронних доказів та стандарти захисту прав людини, застосовні до розглянутих механізмів; розкрити специфіку предмета доказування у справах про легалізацію доходів, одержаних злочинним шляхом, та роль електронних доказів у його встановленні.

Методологічну основу дослідження становлять формально-юридичний метод (аналіз змісту міжнародно-правових актів), порівняльно-правовий метод (зіставлення положень права Ради Європи та Європейського Союзу з чинним кримінальним процесуальним законодавством України) та системний аналіз (визначення взаємозв'язку між розглянутими інструментами). Логіка викладу матеріалу побудована таким чином: спочатку

розглянуто Другий додатковий протокол, Регламент (ЄС) 2023/1543 та Директиву (ЄС) 2023/1544, а потім проаналізовано їх значення для національної правозастосовної практики у провадженнях про легалізацію доходів, одержаних злочинним шляхом. Окремо розглянуто процесуальні гарантії допустимості таких доказів, специфіку доказування у справах про легалізацію доходів та відповідні стандарти захисту прав людини.

1. Другий додатковий протокол: зміст і ратифікація

Конвенція про кіберзлочинність (Будапештська конвенція) (надалі – «**Конвенція про кіберзлочинність**») була відкрита для підписання 23 листопада 2001 року та набула чинності 1 липня 2004 року, ставши першим міжнародним договором, спрямованим на протидію злочинам, що вчиняються з використанням комп'ютерних систем (Конвенція про кіберзлочинність, 2001). Україна ратифікувала Конвенцію про кіберзлочинність 7 вересня 2005 року (Про ратифікацію Конвенції про кіберзлочинність, 2005).

Однак закладений у Конвенції про кіберзлочинність механізм отримання електронних доказів спирався на класичну процедуру взаємної правової допомоги, яка не була розрахована на ситуацію, коли дані, що мають доказове значення, зберігаються на серверах постачальників послуг, розташованих у невизначеній або множинній юрисдикції, і можуть бути видалені чи змінені ще до завершення міждержавного запиту.

Другий додатковий протокол, відкритий для підписання 12 травня 2022 року, усуває цю прогалину не одним універсальним механізмом, а сукупністю послідовно ускладнюваних процесуальних інструментів. Стаття 6 Другого додаткового протоколу стосується звернення до реєстраторів доменних імен щодо інформації про реєстрацію домену, тоді як стаття 7 передбачає окреме звернення до постачальника послуг щодо даних про абонента. Стаття 8 (розділ 3) стосується вже не прямого звернення до приватного суб'єкта, а обов'язку виконання наказів іншої Сторони щодо прискореного надання даних про абонента і трафікових даних, тоді як стаття 9 передбачає окрему, вужчу за предметом процедуру невідкладного розкриття збережених комп'ютерних даних в надзвичайних ситуаціях через мережу цілодобових контактних пунктів. Стаття 10 (розділ 4) встановлює вже повноцінну, хоча й пришвидшену, взаємну правову допомогу у визначених Другим додатковим протоколом надзвичайних ситуаціях (Другий додатковий протокол, 2022). Окремо слід зазначити, що дані про зміст комунікації поза межами надзвичайних ситуацій (статті 9–10) отримуються в порядку взаємної правової допомоги: стаття 34 Конвенції про кіберзлочинність поширює зобов'язання надавати взаємну допомогу на перехоплення даних про зміст у межах, дозволених застосовними договорами та національним правом запитуваної



держави, а процедура такого звернення визначається загальними положеннями статті 27 (зокрема, шляхом направлення запиту центральному органу запитуваної Сторони) (Конвенція про кіберзлочинність, 2001). Застосування всіх зазначених механізмів обумовлене дотриманням визначених Другим додатковим протоколом гарантій захисту персональних даних (Другий додатковий протокол, 2022). Для зручності подальшого викладу в цій статті використовується авторська умовна модель, яка об'єднує розглянуті статті у три рівні за ступенем інтенсивності співробітництва: від прямого звернення до приватного суб'єкта (статті 6–7) через взаємодію компетентних органів (статті 8–9) до повноцінної взаємної правової допомоги (стаття 10), що є аналітичним спрощенням для цілей цієї статті, а не відтворенням формальної структури Другого додаткового протоколу.

Практичне значення такого розмежування є принциповим: якщо для встановлення особи власника облікового запису чи платіжного профілю (найпоширеніший перший крок у справах про легалізацію доходів) досі потрібно проходити повний цикл міжнародної правової допомоги, то після ратифікації Другого додаткового протоколу ця дія виконується без нього. Натомість трафікові дані та дані про зміст комунікації, які найчастіше містять доказову інформацію про сам механізм відмивання коштів (маршрути переказів, листування між учасниками схеми), залишаються предметом хоча й спрощеної, але окремої процедури співробітництва між органами, а не прямого звернення до приватного суб'єкта.

Україна підписала Другий додатковий протокол 30 листопада 2022 року одночасно з Хорватією, Республікою Молдова, Словенією, Шрі-Ланкою та Великою Британією (Таблиця з переліком країн, б.д.). Другий додатковий протокол набуває чинності після здачі на зберігання п'ятої ратифікаційної грамоти. Станом на 3 серпня 2026 року офіційні джерела Договірного бюро Ради Європи фіксують чотири завершені ратифікації: Сербією (9 лютого 2023 року), Японією (10 серпня 2023 року), Угорщиною (5 лютого 2026 року) та Коста-Рикою (15 квітня 2026 року). Таким чином, для набрання Другим додатковим протоколом чинності бракує лише однієї, п'ятої ратифікації (Таблиця з переліком країн, б.д.), а чинні стратегічні документи України у сфері кібербезпеки визначають імплементацію норм Другого додаткового протоколу як один із пріоритетних, але ще не виконаних напрямів (Огляд системи кібербезпеки України, 2026). Це означає, що станом на дату підготовки цієї статті Україна не може поспішити на жодне з описаних вище пришвидшених механізмів у відносинах з іншими Сторонами Другого додаткового протоколу, вона залишається в межах класичної, значно повільнішої моделі взаємної правової допомоги за Конвенцією про кіберзлочинність, і саме в цьому, а не в декларативній «євроінтеграційній

важливості», полягає конкретна ціна затримки з ратифікацією для розслідувань легалізації доходів, де швидкість отримання навіть базових ідентифікаційних даних про власника рахунку чи облікового запису часто визначає, чи вдасться взагалі зафіксувати ланцюг руху коштів до моменту, коли дані будуть видалені постачальником послуг.

2. Регламент (ЄС) 2023/1543 про електронні докази

12 липня 2023 року Європейський Парламент і Рада Європейського Союзу ухвалили Регламент (ЄС) 2023/1543, яким запроваджено європейський наказ про надання електронних доказів та європейський наказ про збереження електронних доказів. Регламент застосовуватиметься в усіх державах Європейського Союзу (окрім Данії) з 18 серпня 2026 року, тобто вже за кілька тижнів від дати підготовки цієї статті (Резюме про Регламент (ЄС) 2023/1543, 2023).

Регламент (ЄС) 2023/1543 розрізняє три категорії електронних доказів із різними пороговими значеннями застосування. Дані про абонента (встановлення особи користувача) можуть бути витребувані щодо будь-якого кримінального правопорушення, а наказ достатньо санкціонувати прокурором. Натомість трафікові дані та дані про зміст комунікації може витребувати лише суддя чи суд, і лише за умови, що правопорушення карається позбавленням волі на максимальний строк не менше трьох років або належить до окремого переліку тяжких злочинів, прямо визначених Регламентом (ЄС) 2023/1543 (Регламент (ЄС) 2023/1543, 2023). Це розмежування має значення для теми статті, адже Директива (ЄС) 2018/1673 зобов'язує держави Європейського Союзу встановлювати за легалізацію (відмивання) доходів покарання у вигляді позбавлення волі на максимальний строк не менше чотирьох років (Резюме Директиви (ЄС) 2018/1673, 2022). Тобто формальний поріг у три роки, встановлений Регламентом (ЄС) 2023/1543 для доступу саме до трафікових даних і даних про зміст, за загальним правилом виконується для складу легалізації доходів з огляду на вимоги Директиви (ЄС) 2018/1673 щодо мінімального покарання. Досягнення цього порогу не є достатньою умовою видачі наказу, оскільки застосування Регламенту (ЄС) 2023/1543 додатково залежить від конкретної правової кваліфікації діяння та передбаченої за нього санкції в державі, що видає наказ, від дотримання вимог щодо компетенції органу й судового затвердження наказу, а також від оцінки необхідності й пропорційності втручання в кожному конкретному випадку. Відтак у справах про легалізацію доходів послідовно доступні всі три категорії доказів, включно з найбільш змістовними трафіковими даними та даними про зміст, які здебільшого і розкривають саму механіку руху коштів.

Строки виконання наказу є визначальною відмінністю від традиційної моделі:

постачальник послуг зобов'язаний передати дані протягом 10 днів з моменту отримання наказу, а в невідкладних випадках протягом 8 годин; наказ про збереження даних діє 60 днів з можливістю одноразового продовження ще на 30 днів до моменту оформлення повноцінного запиту (Резюме про Регламент (ЄС) 2023/1543, 2023). За невиконання чи неналежне виконання наказу Регламент (ЄС) 2023/1543 передбачає штрафні санкції у розмірі до 2 % загального річного світового обороту постачальника послуг, тобто реально діючий, а не декларативний механізм примусу (Регламент (ЄС) 2023/1543, 2023).

Застосування Регламенту (ЄС) 2023/1543 має дві істотні межі, які варто враховувати під час оцінки його значення для українських провадженнь. По-перше, він є інструментом взаємного визнання виключно між державами Європейського Союзу, а оскільки Україна не входить у цей союз, національні органи не можуть видавати чи виконувати такі накази безпосередньо, а можуть розраховувати лише на орієнтир гармонізації процесуальних строків і категорій доказів під час приведення власного законодавства у відповідність до права Європейського Союзу в межах євроінтеграційного процесу. По-друге, зі сфери дії акта виключені постачальники фінансових послуг, зокрема банківських, кредитних, страхових, недержавного пенсійного забезпечення, послуг з цінними паперами, інвестиційними фондами, платіжних та інвестиційно-консультаційних (Резюме про Регламент (ЄС) 2023/1543, 2023). Постачальники послуг з обігу віртуальних активів у цьому переліку винятків окремо не згадані, так само, як і в переліку охоплених категорій послуг, таких як комунікаційні послуги, послуги інтернет-інфраструктури, інші інформаційні послуги, що уможливають комунікацію чи зберігання даних (Резюме про Регламент (ЄС) 2023/1543, 2023). Це створює реальну невизначеність застосування Регламенту (ЄС) 2023/1543 саме до постачальників послуг з обігу віртуальних активів, а отже, для найпоширенішої в сучасних схемах легалізації доходів категорії доказів, пов'язаних з рухом віртуальних активів, покладатися на однозначне охоплення цієї категорії постачальників послуг пакетом електронних доказів ЄС наразі не можна. Для точнішої кваліфікації цієї невизначеності доцільно співвіднести визначення «постачальника послуг» за Регламентом (ЄС) 2023/1543 і Директивою (ЄС) 2023/1544 із суміжним регулюванням обігу криптоактивів у праві Європейського Союзу. Регламент (ЄС) 2023/1114 Європейського Парламенту і Ради (надалі – «**Регламент (ЄС) 2023/1114**»), який застосовується з 30 грудня 2024 року, визначає постачальника послуг, пов'язаного із криптоактивами, як особу, що на професійній основі надає одну чи декілька послуг, пов'язаних із криптоактивами, клієнтам (Регламент (ЄС) 2023/1114, 2023). Значно важливішим для цілей цього дослідження є те, що Регламент (ЄС) 2023/1113

про інформацію, яка супроводжує перекази коштів та певні перекази криптоактивів, поширив визначення «фінансової установи» за Директивою (ЄС) 2015/849 про запобігання відмиванню коштів саме на постачальників послуг, пов'язаних із криптоактивами, врегульованих Регламентом (ЄС) 2023/1114 (Регламент (ЄС) 2023/1113, 2023). Це системне рішення права Європейського Союзу: прирівняти постачальника послуг з обігу криптоактивів до фінансової установи для цілей законодавства про запобігання відмиванню коштів, зокрема щодо обов'язкового супроводження кожного переказу криптоактивів верифікованими відомостями про особу відправника та отримувача. Це є вагомим системним аргументом на користь авторського висновку, що про абонента мають підпадати під той самий виняток фінансових послуг зі сфери дії Регламенту (ЄС) 2023/1543, попри відсутність прямої згадки категорії криптоактивів у самому переліку винятків цього акта. Застосування цього аргументу обмежується виключно тими даними, які постачальник послуг з обігу криптоактивів обробляє саме як прирівняні до фінансової установи (відомості про клієнта, дані про відправника й отримувача переказу). Категорії даних, не пов'язані з виконанням цієї функції, а охоплені загальними категоріями послуг, прямо переліченими в Регламенті (ЄС) 2023/1543, зокрема послуги електронних комунікацій, послуги реєстрації доменних імен та розподілу IP-адрес, а також інші інформаційні послуги, що уможливають комунікацію чи зберігання даних, під наведений вище аргумент про прирівняння до фінансової установи не підпадають. Отже, для практичних потреб кримінального провадження визначальне значення має не встановлення статусу постачальника послуг як такого, а функціональна кваліфікація конкретної категорії даних, яку намагається отримати орган досудового розслідування: дані фінансово-розвідувального характеру слід витребувати через канали, передбачені законодавством про запобігання відмиванню коштів, тоді як суто комунікаційні чи технічні дані тієї самої платформи можуть, за загальним правилом, бути предметом звернення в порядку Регламенту (ЄС) 2023/1543. Це питання потребує додаткового вирішення через профільне законодавство про запобігання відмиванню коштів.

3. Директива (ЄС) 2023/1544 про представників

Одночасно з Регламентом (ЄС) 2023/1543 було ухвалено Директиву (ЄС) 2023/1544 для цілей збору електронних доказів, якою встановлено уніфіковані правила щодо призначення визначених установ та юридичних представників постачальниками послуг для цілей отримання, дотримання та виконання рішень і наказів про збір електронних доказів (Директива (ЄС) 2023/1544, 2023). Директива (ЄС) 2023/1544 зобов'язує кожного постачальника послуг, що пропонує їх на території Європейського Союзу, незалежно від місця



його заснування, призначити визначену установу або юридичного представника в межах Європейського Союзу. Саме ця особа отримує, опрацьовує та виконує від імені постачальника послуг як накази за Регламентом (ЄС) 2023/1543, так і рішення, ухвалені на підставі Директиви 2014/41/ЄС про Європейський слідчий ордер та Конвенції про взаємну правову допомогу між державами Європейського Союзу (Директива (ЄС) 2023/1544, 2023).

До ухвалення цього акта постачальник послуг, зареєстрований у третій країні, але фактично орієнтований на європейський ринок, міг ефективно ухилитися від виконання процесуальних рішень європейських органів через відсутність в Європейському Союзі суб'єкта, якому такі рішення можна було б адресувати з юридичними наслідками для постачальника послуг. Директива (ЄС) 2023/1544 усуває цю прогалину не шляхом розширення екстериторіальної юрисдикції окремої держави, а через покладення на самого постачальника послуг обов'язку створити передбачуваний та юридично відповідальний адресат на території Європейського Союзу (Директива (ЄС) 2023/1544, 2023).

Для проваджень про легалізацію доходів, одержаних злочинним шляхом, це має конкретне прикладне значення: значна частина комунікаційних, хмарних і платіжних сервісів, що використовуються учасниками схем відмивання коштів, зареєстрована поза межами України, а нерідко й поза межами Європейського Союзу, але формально підпадає під дію Директиви (ЄС) 2023/1544, оскільки послуга фактично надається на території Європейського Союзу. Наявність визначеної установи або юридичного представника такого постачальника послуг в конкретній державі Європейського Союзу перетворює раніше практично недосяжного суб'єкта на суб'єкта, який принаймні теоретично досяжний, але не для органу України безпосередньо. Директива (ЄС) 2023/1544 не надає українському органу досудового розслідування права самостійно адресувати наказ чи звернення такому представнику: оскільки Україна не є державою Європейського Союзу і не є учасницею передбаченого Регламентом (ЄС) 2023/1543 механізму взаємного визнання, звернення України має проходити через компетентний орган відповідної держави Європейського Союзу в межах чинного договору про правову допомогу чи іншого наявного міжнародного механізму, і саме цей орган держави Європейського Союзу, а не український орган і не сам представник постачальника послуг вирішує, чи застосовувати для виконання запиту національне законодавство своєї держави, чи інструменти права Європейського Союзу. Цей додатковий ланцюг посередництва означає, що практична цінність Директиви (ЄС) 2023/1544 для України є не прямим каналом доступу, а лише підвищенням ймовірності того, що звернення України через компетентний орган держави Європейського Союзу буде

результативним, оскільки в такої держави з'являється конкретний, юридично зобов'язаний адресат, до якого вона сама може звернутися. Без такого представника Директива (ЄС) 2023/1544 не давала б жодного ефекту, оскільки в подібних справах перепорою є не відсутність правової підстави для звернення, а фізична неможливість встановити суб'єкта, якому таке звернення можна адресувати з реальними юридичними наслідками.

4. Значення розглянутих актів

Розглянуті акти утворюють не три окремі, а два взаємодоповнювальні рівні регулювання з різним ступенем обов'язковості для України. Другий додатковий протокол — це єдиний з трьох інструментів, дія якого не залежить від членства в Європейському Союзі, а обумовлена лише участю в Конвенції про кіберзлочинність (Другий додатковий протокол, 2022). Саме тому завершення його ратифікації є не одним із багатьох, а першочерговим і найдосяжнішим кроком, здатним дати відчутний ефект для розслідувань уже найближчим часом. Натомість акти права Європейського Союзу (Регламент (ЄС) 2023/1543 і Директива (ЄС) 2023/1544) прямо не зобов'язують Україну, проте виконують подвійну опосередковану функцію: задають конкретний, вимірюваний процесуальний стандарт у вигляді трьох категорій доказів, строків у 10 днів і 8 годин, порогу у три роки позбавлення волі для трафікових даних і даних про зміст, санкцій до 2 % обороту тощо. Цей стандарт може слугувати предметним орієнтиром під час перегляду власних процесуальних строків отримання електронних доказів. З іншого боку, значення обов'язкового призначення представників постачальників послуг у межах Європейського Союзу за Директивою (ЄС) 2023/1544 для України не слід переоцінювати: наявність такого представника чи визначеної установи в конкретній державі Європейського Союзу не надає українському органу права адресувати йому наказ чи запит. Юридичний ланцюг є довшим: український орган досудового розслідування звертається до компетентного органу відповідної держави на підставі чинного двостороннього чи багатостороннього договору про правову допомогу, і вже цей орган держави Європейського Союзу вирішує, застосовувати йому національний порядок виконання запиту чи звертатися до передбаченого правом Європейського Союзу механізму, зокрема шляхом видання власного європейського наказу до визначеного представника постачальника послуг. Отже, Директива (ЄС) 2023/1544 розширює коло практично досяжних джерел доказів не для України безпосередньо, а для органів держав Європейського Союзу, до співробітництва з якими Україна, своєю чергою, може вдатися в межах чинних міжнародних механізмів.

Водночас для проваджень про легалізацію доходів, одержаних злочинним шляхом, необхідно окремо враховувати виявлену межу цього регулювання: оскільки застосування

Регламенту (ЄС) 2023/1543 до постачальників послуг з обігу віртуальних активів залишається юридично невизначеним, бо вони не названі ні серед прямо виключених фінансових послуг, ні серед прямо охоплених категорій (Резюме про Регламент (ЄС) 2023/1543, 2023), то розглянутий пакет інструментів надійно вирішує проблему доступу до даних комунікаційних і хмарних тоді як дані традиційних платіжних установ, навпаки, прямо виключені з його сфери дії, а щодо доказів, пов'язаних із рухом віртуальних активів, однозначної відповіді немає. Відповідно, паралельно з імплементацією положень, розглянутих у цій статті, потребує вдосконалення взаємодія органів досудового розслідування з Державною службою фінансового моніторингу України, зокрема в частині віртуальних активів.

5. Допустимість електронних доказів та їх зв'язок із кримінальним процесуальним законодавством України

Транскордонне отримання електронних доказів за розглянутими вище механізмами не є самоціллю: отримана інформація набуває доказового значення для українського кримінального провадження лише за умови дотримання вимог Кримінального процесуального кодексу України щодо належності, допустимості та достовірності доказів. Відповідно до статті 85 Кримінального процесуального кодексу України належними є докази, які прямо чи непрямо підтверджують існування обставин, що підлягають доказуванню, а відповідно до статті 86 доказ визнається допустимим, якщо він отриманий у порядку, встановленому Кримінальним процесуальним кодексом України. Відповідно до частини першої статті 93, збирання доказів здійснюється сторонами кримінального провадження у порядку, передбаченому Кримінальним процесуальним кодексом України, а тому докази, отримані за кордоном у межах міжнародного співробітництва, повинні відповідати саме цьому порядку, а не лише вимогам іноземного чи міжнародного акта, на підставі якого їх було отримано; питання їх достовірності, своєю чергою, вирішується судом за правилами оцінки доказів, встановленими статтею 94 (Кримінальний процесуальний кодекс України, 2012). Недотримання встановленого Кримінальним процесуальним кодексом України порядку отримання доказів за кордоном тягне за собою визнання таких доказів недопустимими, незалежно від того, наскільки бездоганно вони були отримані з погляду законодавства запитуваної держави. Водночас стаття 90, яка визначає преюдиціальне значення рішень інших судів у питаннях допустимості доказів, створює додатну нормативну основу для судової перевірки саме тих електронних доказів, які отримано на підставі рішення іноземного судового чи іншого компетентного органу в порядку розглянутих у цій статті транскордонних механізмів.

Показово, що чинний Кримінальний процесуальний кодекс України уже містить процесуальний інструмент, придатний для роботи

з електронними доказами на національному рівні, а саме тимчасовий доступ до речей і документів (стаття 159 глави 15), який прямо передбачає можливість тимчасового доступу до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку шляхом зняття копії інформації без вилучення самої системи (Кримінальний процесуальний кодекс України, 2012). Цей механізм може слугувати орієнтиром для розробки національного порядку реалізації розглянутих у цій статті транскордонних інструментів: подібно до статті 159 Кримінального процесуального кодексу України, виконання європейського наказу про надання чи збереження електронних доказів також не передбачає фізичного вилучення обладнання постачальника послуг, а обмежується отриманням копії визначених даних, що концептуально зближує обидва механізми.

Порядок міжнародного співробітництва під час кримінального провадження регулюється розділом IX Кримінального процесуального кодексу України (статті 541–614): глава 42 визначає загальні засади такого співробітництва, зокрема, роз'яснення використувуваних термінів (стаття 541), вимоги до запиту про міжнародне співробітництво (стаття 548) та порядок його направлення до уповноваженого (центрального) органу України (стаття 551) (Кримінальний процесуальний кодекс України, 2012). Жодна з цих статей, однак, не враховує специфіки пришивдшених механізмів, запроваджених Другим додатковим протоколом та Регламентом (ЄС) 2023/1543, зокрема, можливості прямого звернення до постачальника послуг без посередництва центрального органу (статті 6–7 Другого додаткового протоколу) або строків виконання, обчислюваних годинами, а не місяцями. Це створює конкретний, а не абстрактний предмет для законодавчих пропозицій: доповнення розділу IX Кримінального процесуального кодексу України окремою главою, яка визначала б компетентний орган, уповноважений здійснювати звернення до постачальника послуг (наприклад, суд або прокурор), строк у 10 днів, форму відповідного процесуального рішення (за аналогією з ухвалою слідчого судді про тимчасовий доступ до речей і документів), а також порядок судового контролю за таким зверненням.

Окремого вирішення потребує й питання автентичності та цілісності електронних доказів, отриманих у транскордонному порядку. Оскільки постачальник послуг передає дані у відповідь на європейський наказ про надання електронних доказів без участі українського слідчого чи прокурора в процесі їх отримання, виникає питання про те, яким чином має підтверджуватися незмінність такої інформації з моменту її отримання постачальником послуг до моменту використання в українському суді. У межах національного регулювання це питання мало б вирішуватися через поєднання технічних засобів підтвердження



цілісності даних (зокрема, обчислення контрольних сум файлів) із процесуальним закріпленням ланцюга зберігання доказу, тобто послідовної фіксації кожної особи, яка мала доступ до електронного доказу з моменту його отримання, за аналогією з порядком, що вже застосовується судами до речових доказів. Так само потребує законодавчого закріплення порядок відкриття стороною обвинувачення отриманих у транскордонному порядку електронних доказів стороні захисту відповідно до статті 290 Кримінального процесуального кодексу України, оскільки специфіка обсягу й формату таких доказів (значні масиви метаданих, необхідність спеціального програмного забезпечення для їх перегляду) може ускладнювати виконання цього обов'язку в загальному порядку (Кримінальний процесуальний кодекс України, 2012).

6. Специфіка доказування легалізації доходів, одержаних злочинним шляхом

Значення розглянутих транскордонних механізмів розкривається повною мірою лише з урахуванням специфіки предмета доказування у справах про легалізацію (відмивання) доходів, одержаних злочинним шляхом. Об'єктивна сторона злочину, передбаченого статтею 209 Кримінального кодексу України, охоплює вчинення фінансової операції чи правочину з коштами або іншим майном, одержаними внаслідок суспільно небезпечного протиправного діяння, що передувало легалізації, а також дії, спрямовані на приховання чи маскуванню незаконного походження таких коштів, володіння ними, джерела їх походження, місцезнаходження, переміщення чи зміну форми (перетворення), і, окремо, набуття, володіння або використання такого майна (Кримінальний кодекс України, 2001). Це означає, що предмет доказування в такій справі є двохарактерним: слідству потрібно довести не лише факт вчинення дій із майном самим підозрюваним, а й те, що це майно походить від суспільно небезпечного протиправного діяння, яке передувало легалізації (предикатного діяння). Притягнення особи до відповідальності за предикатне діяння не є обов'язковою передумовою кваліфікації за статтею 209 Кримінального кодексу України і може здійснюватися одночасно, раніше або взагалі окремо від кримінального провадження щодо легалізації.

Суб'єктивна сторона цього складу злочину має особливе значення для теми цього дослідження: відповідальність настає, якщо особа «знала або повинна була знати», що майно прямо чи опосередковано, повністю чи частково одержано злочинним шляхом (Кримінальний кодекс України, 2001), тобто законодавець допускає доведення суб'єктивної сторони не лише через знання, а й через недбале ставлення до походження майна за обставин, які мали викликати обґрунтовані сумніви. Електронні докази, розглянуті в цій статті, мають значення саме для доведення цього елемента: листування учасників схеми (дані про зміст

комунікації за термінологією Регламенту (ЄС) 2023/1543), історія пошукових запитів чи дій в інтерфейсі платіжного сервісу можуть свідчити про обізнаність особи з незаконним походженням активів набагато переконливіше, ніж непрямі докази традиційного характеру, тоді як метадані про час, послідовність і географію операцій (трафікові дані) дозволяють простежити рух коштів і відтворити механізм приховання чи маскуванню їх походження, необхідний для доведення об'єктивної сторони.

У цьому контексті принципове значення має чітке розмежування фінансово-розвідувальної інформації Державної служби фінансового моніторингу України та процесуальних доказів, придатних для використання в суді. Інформація, яку Державна служба фінансового моніторингу України отримує та аналізує в порядку фінансового моніторингу, має розвідувальний (аналітичний) характер і слугує передусім для виявлення ознак підозрілих операцій та ініціювання досудового розслідування, але не отримана в порядку, встановленому Кримінальним процесуальним кодексом України, а тому не може автоматично набувати статусу доказу без належного процесуального оформлення. Електронні дані, отримані за допомогою розглянутих у цій статті міжнародних інструментів, здатні виконувати роль такого належного процесуального підтвердження, зокрема, вони можуть підтверджувати чи спростовувати висновки фінансової розвідки щодо конкретних операцій, легітимізуючи їх для цілей судового розгляду, але не підміняють собою самостійного процесуального джерела доказів, яким є показання, документи, речові докази чи висновки експертів, отримані в порядку Кодексу.

7. Процесуальні гарантії та стандарти захисту прав людини

Прискорення транскордонного отримання електронних доказів, яке є головною практичною перевагою розглянутих у цій статті інструментів, не повинно оцінюватися виключно з позиції ефективності розслідування, оскільки кожен з таких заходів становить втручання у права, гарантовані статтями 6 і 8 Європейської конвенції з прав людини (надалі – «Конвенція») (Європейська конвенція з прав людини, 1950). Стаття 8 Конвенції вимагає, щоб будь-яке втручання у право на повагу до приватного життя та кореспонденції здійснювалося на підставі закону, переслідувало легітимну мету та було необхідним у демократичному суспільстві, що практично означає застосування тесту на пропорційність: обсяг і глибина втручання мають відповідати тяжкості злочину та наявним підставам підозри (Європейська конвенція з прав людини, 1950). Показово, що цей самий принцип пропорційності прямо закріплений і в самому Регламенті (ЄС) 2023/1543, який вимагає, щоб європейський наказ про надання електронних доказів був необхідним і пропорційним для цілей конкретного кримінального провадження з урахуванням прав особи, щодо якої він виноситься, а також щоб аналогічний захід був доступний

у подібній суто національній справі, що зближує стандарт права Європейського Союзу зі стандартом статті 8 Конвенції (Регламент (ЄС) 2023/1543, 2023).

Цей стандарт пропорційності не є абстрактним принципом, а послідовно застосовується в практиці як Європейського суду з прав людини, так і Суду справедливості Європейського Союзу саме стосовно доступу до даних, аналогічних розглянутим у цій статті. Пояснювальна доповідь до Другого додаткового протоколу до Конвенції про кіберзлочинність посилається на практику Європейського суду з прав людини щодо позитивного обов'язку держави забезпечити ефективне розслідування злочинів, вчинених з використанням комп'ютерних систем (Пояснювальна доповідь, 2022).

Зокрема, у Пояснювальній доповіді до Другого додаткового протоколу до Конвенції про кіберзлочинність було посилання на рішення у справі K.U. проти Фінляндії (заява № 2872/02, рішення від 2 березня 2009 року), у якій Суд визнав порушенням статті 8 Конвенції нездатність держави забезпечити розкриття особи, яка розмістила протиправне оголошення в мережі Інтернет від імені заявника, через відсутність у національному законодавстві ефективного правового механізму, який дозволяв би компетентним органам зобов'язати постачальника послуг розкрити дані, необхідні для ідентифікації особи, що розмістила протиправне оголошення (K.U. проти Фінляндії, 2009).

Суд справедливості Європейського Союзу, у свою чергу, у справі Digital Rights Ireland (об'єднані справи C-293/12 і C-594/12, рішення від 08.04.2014) визнав недійсною Директиву 2006/24/ЄС про збереження даних, зокрема через невибіркового характер передбаченого нею збереження трафікових і локалізаційних даних (Digital Rights Ireland, 2014). Європейський суд з прав людини у справі Khan v. the United Kingdom (заява № 35394/97, рішення від 12.05.2000) наголосив, що навіть якщо спосіб отримання доказів викликає питання з погляду статті 8 Конвенції, це не означає автоматичного порушення права на справедливий суд, гарантованого статтею 6 Конвенції. Вирішальним критерієм є оцінка справедливості кримінального провадження в цілому, зокрема, можливість сторони захисту оспирити допустимість і достовірність таких доказів та ефективно реалізувати свої процесуальні права (Khan v. the United Kingdom, 2000). Таким чином, відповідність механізмів отримання електронних доказів вимогам статті 8 Конвенції повинна оцінюватися у взаємозв'язку з гарантіями статті 6 Конвенції, які забезпечують особі реальну можливість поставити під сумнів законність отримання, допустимість і доказову силу таких матеріалів у судовому провадженні.

У справі Stojkovic v. France and Belgium (заява № 25303/08, рішення від 27.10.2011) Суд визнав порушенням статті 6 Конвенції

ситуацію, коли держава, яка ініціювала процесуальну дію за судовим дорученням в іншій державі, не забезпечила особі передбачені статтею 6 гарантії, попри те що сама дія фізично виконувалася іноземними органами, тобто відповідальність держави, яка звертається по транскордонну допомогу, за дотримання конвенційних стандартів не зникає лише тому, що виконання доручення здійснює інша держава.

Також варто згадати справу Tele2 Sverige (об'єднані справи C-203/15 і C-698/15, рішення від 21.12.2016), у якій суд підтвердив, що держави Європейського Союзу не можуть запроваджувати на національному рівні аналогічні невибіркового режими збереження даних, дозволяючи лише цільове збереження, обмежене за колом осіб, засобами зв'язку та строком (Tele2 Sverige, 2016); а в пізнішій справі La Quadrature du Net (об'єднані справи C-511/18, C-512/18 і C-520/18, рішення від 06.10.2020). Суд уточнив межі цього підходу, допустивши за виняткових обставин загальне і невибіркового збереження даних за умови посилення процесуальних гарантій (La Quadrature du Net, 2020). Ці позиції європейських судів стосуються оцінки правомірності застосування розглянутих у цій статті транскордонних механізмів: хоча вони й не є заходами масового невибіркового збереження даних, а стосуються цільового отримання даних у межах конкретного кримінального провадження, сформульовані судами критерії обмеженості колом осіб і наявності незалежного нагляду є придатним орієнтиром для оцінки того, чи забезпечують встановлені Другим додатковим протоколом та Регламентом (ЄС) 2023/1543 гарантії достатній рівень захисту прав особи, дані якої вилучаються. Масштабне чи невибіркового використання прищвиджених процедур навіть у справах про легалізацію доходів не повинно розглядатися як автоматично виправдане самою лише тяжкістю цієї категорії злочинів.

Регламент (ЄС) 2023/1543 передбачає власний перелік підстав відмови у виконанні наказу, які виконуючий орган держави Європейського Союзу вправі заявити в межах десяти днів у звичайному порядку або дев'яти місяців у випадках невідкладних випадках: привілеї та імунітети, встановлені правом виконуючої держави; недотримання вимоги подвійної кримінальної відповідальності для окремих категорій злочинів, тощо. Показово, що для категорії професійної (зокрема адвокатської) таємниці прямого окремого переліку підстав відмови Регламент не встановлює, а покладається на загальну категорію «імунітетів та привілеїв за правом виконуючої держави», що для держав, у праві яких адвокатура користується спеціальним нормативним захистом, включно з Україною, означає необхідність окремого визначення того, як саме ця гарантія діятиме в межах транскордонного механізму, розглянутого в цій статті. Зазначена проблема наразі залишається невирішеною на рівні національного законодавства.



Право на ефективний засіб правового захисту, що випливає зі статті 13 Конвенції у поєднанні зі статтею 8, вимагає, щоб особа, дані якої були витребувані в порядку розглянутих у цій статті механізмів, мала практичну можливість оскаржити правомірність такої особи, однак, істотно різняться між розглянутими інструментами: якщо тимчасовий доступ до речей і документів за Кримінальним процесуальним кодексом України здійснюється на підставі ухвали слідчого судді за участю зацікавлених осіб у передбачених Кодексом межах, то передбачене Регламентом (ЄС) 2023/1543 повідомлення адресоване насамперед виконуючому органу держави Європейського Союзу а, а не особі, дані якої витребувані, а питання про своєчасне повідомлення самої особи та надання їй ефективного засобу оскарження вирішується вже виключно національним законодавством видавальної держави.

Це означає, що імплементація розглянутих у цій статті інструментів у національне законодавство України не може обмежуватися визначенням компетентного органу та процесуальної форми рішення, а повинна окремо передбачати як механізм повідомлення особи, так і порядок оскарження нею відповідного рішення до слідчого судді за зразком загального механізму оскарження рішень, дій чи бездіяльності слідчого або прокурора (глава 26 Кримінального процесуального кодексу України), оскільки інститут тимчасового доступу до речей і документів не передбачає загального механізму судового перегляду таких рішень за ініціативою особи, права якої ними обмежуються, а апеляційне оскарження відповідних ухвал допускається лише у вузько визначених випадках (пункт 10 частини першої статті 309 Кримінального процесуального кодексу України).

Висновки. Проведене дослідження засвідчило, що вдосконалення інституту електронних доказів у кримінальних провадженнях, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, нерозривно пов'язане із урахуванням новітніх стандартів Ради Європи та права Європейського Союзу. У статті обґрунтовано необхідність: 1) прискорення завершення внутрішньодержавних процедур ратифікації Другого додаткового протоколу; 2) урахування підходів Регламенту (ЄС) 2023/1543 щодо скорочених строків отримання та збереження електронних доказів під час удосконалення положень Кримінального процесуального кодексу України; 3) вивчення можливості запровадження національного аналога інституту представника для цілей збору електронних доказів стосовно постачальників послуг, що діють на території України; 4) удосконалення взаємодії органів досудового розслідування з Державною службою фінансового моніторингу України щодо доказів, пов'язаних з рухом віртуальних активів, з огляду на виявлену юридичну невизначеність застосування до них Регламенту (ЄС) 2023/1543; 5) урахування виявленої специфіки предмета доказування

легалізації доходів, зокрема суб'єктивної сторони та стандартів пропорційності, вироблених практикою Європейського суду з прав людини і Суду справедливості Європейського Союзу, під час застосування розглянутих транскордонних механізмів.

Проведене дослідження також засвідчило, що значення електронних доказів виходить за межі традиційного кримінального провадження. Сучасне законодавство Європейського Союзу дедалі ширше використовує механізми отримання, збереження та обміну електронними доказами у сфері протидії відмиванню доходів, фінансуванню тероризму та регулювання ринку криптоактивів. Це свідчить про формування комплексної міжгалузевої системи правового регулювання електронних доказів, яка має бути врахована під час подальшого вдосконалення кримінального процесуального законодавства України.

Перспективи подальших досліджень пов'язані з розробленням конкретних законодавчих пропозицій щодо імплементації зазначених підходів у національне кримінальне процесуальне законодавство, а також з аналізом практики застосування Регламенту (ЄС) 2023/1543 після набуття ним чинності 18 серпня 2026 року, зокрема щодо остаточного вирішення питання його застосовності до постачальників послуг з обігу віртуальних активів.

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів.

ЛІТЕРАТУРА:

1. Погорецький М. А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесуального доказування. Аналітично-порівняльне правознавство. 2026. Том 3. № 1. С. 115–125. DOI: <https://doi.org/10.24144/2788-6018.2026.01.3.18> URL: <https://journal-app.uzhnu.edu.ua/article/view/353257> (дата звернення: 03.08.2026).
2. Конвенція про кіберзлочинність: міжнародний договір від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 03.08.2026).
3. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. URL: <https://zakon.rada.gov.ua/laws/show/2824-15> (дата звернення: 03.08.2026).
4. Другий додатковий протокол до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів (CETS No. 224): офіційний текст. Рада Європи. URL: <https://rm.coe.int/1680a49dab> (дата звернення: 03.08.2026).
5. Таблиця з переліком країн, які підписали та ратифікували Другий додатковий протокол до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів. Договірне бюро Ради Європи. URL: <https://www.coe.int/en/web/conventions/full-list/?module=signatures-by-treaty&treatynum=224> (дата звернення: 03.08.2026).
6. Огляд національної системи кібербезпеки України за 2025 рік. Рада національної безпеки і оборони України, 2026. URL: https://www.rmbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf (дата звернення: 03.08.2026).
7. Регламент (ЄС) 2023/1543 Європейського Парламенту і Ради про Європейські накази про надання електронних доказів та Європейські накази про збереження електронних

доказів у кримінальному провадженні, а також про виконання покарань у виді позбавлення волі, призначених за результатами кримінального провадження. EUR-Lex. 28.07.2023. URL: <https://eur-lex.europa.eu/eli/reg/2023/1543/oj> (дата звернення: 03.08.2026).

8. Директива (ЄС) 2023/1544 Європейського Парламенту і Ради про встановлення гармонізованих правил щодо визначення призначених установ і призначення законних представників для цілей збирання електронних доказів у кримінальному провадженні. EUR-Lex, 28.07.2023. URL: <https://eur-lex.europa.eu/eli/dir/2023/1544/oj> (дата звернення: 03.08.2026).

9. Електронні докази у кримінальному провадженні: резюме щодо Регламенту (ЄС) 2023/1543 та Директиви (ЄС) 2023/1544. EUR-Lex. URL: <https://eur-lex.europa.eu/EN/legal-content/summary/electronic-evidence-in-criminal-proceedings.html> (дата звернення: 03.08.2026).

10. Протидія легалізації доходів кримінально-правовими засобами : резюме Директиви (ЄС) 2018/1673. EUR-Lex. URL: <https://eur-lex.europa.eu/eli/dir/2018/1673/oj/eng> (дата звернення: 03.08.2026).

11. Регламент (ЄС) 2023/1114 Європейського Парламенту і Ради про ринки криптоактивів, а також про внесення змін до Регламентів (ЄС) № 1093/2010 та (ЄС) № 1095/2010 і Директив 2013/36/ЄС та (ЄС) 2019/1937. EUR-Lex., 09.06.2023. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng> (дата звернення: 03.08.2026).

12. Регламент (ЄС) 2023/1113 Європейського Парламенту і Ради про інформацію, що супроводжує перекази коштів та певні перекази криптоактивів, та про внесення змін до Директиви (ЄС) 2015/849, EUR-Lex., 09.06.2023. URL: <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng> (дата звернення: 03.08.2026).

13. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 03.08.2026).

14. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III, ст. 209. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 03.08.2026).

15. Пояснювальна доповідь до Другого додаткового протоколу до Конвенції про кіберзлочинність щодо розширеного співробітництва та розкриття електронних доказів (СДЄ № 224). Рада Європи, 2022. URL: <https://rm.coe.int/1680a49c9d> (дата звернення: 03.08.2026).

16. K.U. v. Finland: рішення Європейського суду з прав людини від 02.03.2009, заява № 2872/02. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-89964> (дата звернення: 03.08.2026).

17. Khan v. the United Kingdom: рішення Європейського суду з прав людини від 12.05.2000, заява № 35394/97. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-58841> (дата звернення: 03.08.2026).

18. Digital Rights Ireland and Others: рішення Суду справедливості Європейського Союзу від 08.04.2014, об'єднані справи C-293/12 та C-594/12, ECLI:EU:C:2014:238. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293> (дата звернення: 03.08.2026).

19. Tele2 Sverige AB and Watson and Others : рішення Суду справедливості Європейського Союзу від 21.12.2016, об'єднані справи C-203/15 та C-698/15, ECLI:EU:C:2016:970. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203> (дата звернення: 03.08.2026).

20. La Quadrature du Net and Others : рішення Суду справедливості Європейського Союзу від 06.10.2020,

об'єднані справи C-511/18, C-512/18 та C-520/18, ECLI:EU:C:2020:791. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0511> (дата звернення: 03.08.2026).

21. Stojkovic v. France and Belgium: рішення Європейського суду з прав людини від 27.10.2011, заява № 25303/08. HUDOC. URL: <https://hudoc.echr.coe.int/eng#%7B%22text%22%3A%22001-107177%22%7D> (дата звернення: 03.08.2026).

22. Мілімко Л. В., Жидовцев Ю. В. Електронні докази в кримінальному судочинстві України. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Том 3. № 88. DOI: <https://doi.org/10.24144/2307-3322.2025.88.3.45> URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/330827/320168> (дата звернення: 03.08.2026).

23. Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини): міжнародний договір від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 03.08.2026).

REFERENCES:

1. Pohoretskyi, M. A. (2026). Tsyfrovi (elektronni) dokazy ta tsyfrova (elektronna) forma dokaziv: rozmezhuвання поніат і yoho znachennia dlia kryminalnoho protsesualnoho dokazuвання [Digital (electronic) evidence and the digital (electronic) form of evidence: distinguishing the concepts and its significance for criminal procedural evidence]. *Analitichno-porivnialne pravoznavstvo — Analytical and Comparative Jurisprudence*, 3(1), 115–125. <https://doi.org/10.24144/2788-6018.2026.01.3.18>. <https://journal-app.uzhnu.edu.ua/article/view/353257>.

2. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Strasbourg, France. <https://rm.coe.int/1680081561>.

3. Verkhovna Rada of Ukraine. (2005). Pro ratyfikatsiiu Konventsii pro kiberzlochynnist [On the ratification of the Convention on Cybercrime] (Law of Ukraine No. 2824-IV). Kyiv, Ukraine. <https://zakon.rada.gov.ua/laws/show/2824-15>.

4. Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224). Strasbourg, France. <https://rm.coe.int/1680a49dab>.

5. Council of Europe Treaty Office. (n.d.). Chart of signatures and ratifications of Treaty 224. Strasbourg, France. Retrieved July 12, 2026, from <https://www.coe.int/en/web/conventions/full-list/?module=signatures-by-treaty&treaty=224>.

6. National Security and Defense Council of Ukraine. (2026). Ohliad natsionalnoi systemy kiberbezpeky Ukrainy za 2025 rik [Overview of the national cybersecurity system of Ukraine for 2025]. Kyiv, Ukraine. https://www.rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf.

7. European Parliament and of the Council (2023a). Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. EUR-Lex. Brussels, Belgium. <https://eur-lex.europa.eu/eli/reg/2023/1543/oj>.

8. European Parliament and of the Council. (2023b). Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. EUR-Lex. Brussels, Belgium. <https://eur-lex.europa.eu/eli/dir/2023/1544/oj>.

9. European Parliament and of the Council. Electronic evidence in criminal proceedings [Summary]. EUR-Lex. (2026) Brussels, Belgium. <https://eur-lex.europa.eu/EN/legal-content/summary/electronic-evidence-in-criminal-proceedings.html>.



10. European Parliament and of the Council (2018). Directive (EU) 2018/1673 on combating money laundering by criminal law. Brussels, Belgium. EUR-Lex. <https://eur-lex.europa.eu/eli/dir/2018/1673/oj/eng>
 11. European Parliament and of the Council (2023c). Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. EUR-Lex. Brussels, Belgium. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>
 12. European Parliament and of the Council (2023d). Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. EUR-Lex. Brussels, Belgium. <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>
 13. Verkhovna Rada of Ukraine. (2012). Kryminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine] (Law of Ukraine No. 4651-VI). Kyiv, Ukraine. <https://zakon.rada.gov.ua/laws/show/4651-17>
 14. Verkhovna Rada of Ukraine. (2001). Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine], Art. 209 (Law of Ukraine No. 2341-III). Kyiv, Ukraine. <https://zakon.rada.gov.ua/laws/show/2341-14>
 15. Council of Europe. (2022). Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Strasbourg, France. <https://rm.coe.int/1680a49c9d>
 16. European Court of Human Rights. (2009). K.U. v. Finland (Application No. 2872/02), judgment of 2 March 2009. Strasbourg, France. <https://hudoc.echr.coe.int/eng?i=001-89964>
 17. European Court of Human Rights. (2000). Khan v. the United Kingdom (Application No. 35394/97), judgment of 12 May 2000. Strasbourg, France. <https://hudoc.echr.coe.int/eng?i=001-58841>
 18. Court of Justice of the European Union. (2014). Digital Rights Ireland and Others, Joined Cases C-293/12 and C-594/12, judgment of 8 April 2014, ECLI:EU:C:2014:238. Luxembourg. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293>
 19. Court of Justice of the European Union. (2016). Tele2 Sverige AB and Watson and Others, Joined Cases C-203/15 and C-698/15, judgment of 21 December 2016, ECLI:EU:C:2016:970. Luxembourg. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203>
 20. Court of Justice of the European Union. (2020). La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18 and C-520/18, judgment of 6 October 2020, ECLI:EU:C:2020:791. Luxembourg. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0511>
 21. European Court of Human Rights. (2011). Stojkovic v. France and Belgium (Application No. 25303/08), judgment of October 27, 2011. Strasbourg, France. [https://hudoc.echr.coe.int/eng#%22itemid%22:\[%22001-107177%22\]](https://hudoc.echr.coe.int/eng#%22itemid%22:[%22001-107177%22])
 22. Milimko, L. V., & Zhydovtsev, Y. V. (2025). Elektronni dokazy v kryminalnomu sudochynstvi Ukrainy [Electronic evidence in the criminal justice of Ukraine]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriya Pravo, Uzhhorod National University Herald. Series Law, 3(88). <https://visnyk-pravo.uzhnu.edu.ua/article/view/330827/320168>
 23. Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms [European Convention on Human Rights] (ETS No. 5). Strasbourg, France. <https://rm.coe.int/1680a2353d>
- Дата першого надходження статті до видання: 17.07.2026*
Дата прийняття статті до друку після рецензування: 11.08.2026
Дата публікації (оприлюднення) статті: 01.09.2026