

УДК 341.24:004.056:343.346(477)

DOI <https://doi.org/10.32782/2307-1745.2026.82.33>

Белкін Л. М.,

*кандидат технічних наук,
старший науковий співробітник, адвокат,
адвокат індивідуальної практики*
ORCID: <https://orcid.org/0000-0001-8672-8147>

Криволап Є. В.,

PhD, спеціаліст з IT
ORCID: <https://orcid.org/0000-0003-2599-2520>

Юринець Ю. Л.,

*доктор юридичних наук, професор,
професор кафедри права та публічного управління
Київського національного університету будівництва та архітектури*
ORCID: <https://orcid.org/0000-0003-0281-3251>

Белкін М. Л.,

*кандидат юридичних наук,
доцент кафедри адміністративного,
фінансового та банківського права
Міжрегіональної Академії управління персоналом, адвокат*
ORCID: <https://orcid.org/0000-0003-0805-9923>

ОСНОВНІ ЗАСАДИ ДРУГОГО ДОДАТКОВОГО ПРОТОКОЛУ ДО КОНВЕНЦІЇ РАДИ ЄВРОПИ «ПРО КІБЕРЗЛОЧИННІСТЬ» (CETS № 224) І ПИТАННЯ ЙОГО РАТИФІКАЦІЇ УКРАЇНОЮ

Анотація. У статті досліджено основні засади Другого додаткового протоколу до Конвенції Ради Європи про кіберзлочинність щодо посилення співробітництва та розкриття електронних доказів, а також перспективи його ратифікації Україною. Обґрунтовано актуальність цього міжнародно-правового інструменту з огляду на зростання ролі електронних доказів у кримінальних провадженнях та недостатню ефективність традиційних механізмів міжнародної правової допомоги в умовах транскордонного характеру цифрової інформації. Розглянуто основні механізми співробітництва, передбачені Протоколом, зокрема вдосконалення процедур взаємної правової допомоги, співробітництво у невідкладних ситуаціях, безпосередню взаємодію компетентних органів із постачальниками послуг, отримання інформації про абонентів і даних про трафік, використання сучасних засобів електронної комунікації та інші форми міжнародної взаємодії. Окрему увагу приділено гарантіям захисту персональних даних, приватності та інших прав людини, а також дотриманню принципів законності, необхідності й пропорційності під час транскордонного отримання електронної інформації. Проаналізовано стан ратифікації Протоколу та процес підготовки Україною відповідних законодавчих змін. Обґрунтовано, що незавершеність ратифікації Україною зумовлена передусім необхідністю комплексної адаптації національного законодавства та практики до передбачених Протоколом механізмів. Визначено значення Протоколу для України в контексті протидії кіберзлочинності, документування кримінальних правопорушень та отримання електронних доказів з іноземних юрисдикцій.

Ключові слова: кіберзлочинність, електронні докази, Другий додатковий протокол, Будапештська конвенція, міжнародне співробітництво, міжнародна правова допомога, постачальники послуг, дані про абонента, дані про трафік, транскордонне отримання доказів, персональні дані, приватність.

Постановка проблеми. У сучасному світі, з розвитком мережі Інтернет, з'явився новий вид злочинності – кіберзлочинність. Чим більше стає користувачів мережі Інтернет, тим більше шахраїв, які стають більш досвідченими і вигадують нові види шахрайства. Кіберзлочинність становить реальну небезпеку для суспільства і держави, вона здатна спричинити незворотні наслідки [1, с. 219]. У даний час протидія кіберзлочинності є однією з найактуальніших проблем у всьому світі [2, с. 3]. На це спрямовано дію Конвенції Ради Європи (далі – РЄ) «Про кіберзлочинність» (Будапештська конвенція, далі – Конвенція), яку укладено 23.11.2001 р. в м. Будапешті й до якої нещодавно приєдналась Україна [3, с. 3]. Розвитком положень Конвенції є, зокрема, Другий додатковий протокол до Конвенції про кіберзлочинність щодо посилення співробітництва та розкриття електронних доказів (Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence). Основна мета документа – пристосувати міжнародне співробітництво у кримінальних провадженнях до ситуації, коли необхідні докази зберігаються в електронній формі, перебувають у іншій державі або контролюються приватним постачальником цифрових послуг.

Протокол у присутності кількох міністрів 12.05.2022 року підписали такі держави-члени РЄ: Австрія, Бельгія, Болгарія, Естонія, Фінляндія, Ісландія, Італія, Литва, Люксембург, Чорногорія, Нідерланди, Північна Македонія, Португалія, Румунія, Сербія, Іспанія та Швеція, а також державами, які не є державами-членами: Чилі, Колумбія, Японія, Марокко та США. Протокол відкритий для підписання Сторонами Конвенції і набуде чинності після ратифікації п'ятьма державами. Станом на тепер, 20.08.2026 року, протокол підписали 52 держави, у тому числі Україна (дата підписання – 30.11.2022). Станом на 09.08.2026 року протокол ратифікували лише 4 держави (Сербія – 09.02.2023 року; Японія – 10.08.2023 року; Угорщина – 05.02.2026 року; Коста-Рика – 15.04.2026 року. Україна Протокол не ратифікувала, Планом законопроектної роботи Верховної Ради України на 2026 рік ратифікація планується на 4 квартал 2026 року [4, с. 6].

Аналіз останніх досліджень і публікацій. Підписання Україною Другого додаткового протоколу до Конвенції про кіберзлочинність, покладає початок нового законотворчого процесу щодо удосконалення національного законодавства України відповідно до міжнародних стандартів [5, с. 141]. В Стратегії кібербезпеки України, затвердженій Указом Президента України від 26.08.2021 року № 447/2021, передбачено забезпечення участі України у доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах. Не дивлячись на актуальність зазначеної проблеми, у юридичній науці значенню ратифікації Другого додаткового протоколу до Конвенції про кіберзлочинність приділяється недостатньо уваги. Так, стаття [6] присвячена аналізу новел міжнародного співробітництва щодо збору доказів в електронній формі, відповідно до Другого додаткового протоколу Конвенції про кіберзлочинність, який забезпечує правову основу для розкриття інформації про реєстрацію доменних імен, для прямого співробітництва з постачальниками послуг для одержання інформації про абонентів, про трафік, співробітництво в надзвичайних ситуаціях, оновлює процедуру відеоконференцій [6, с. 188]. У статті [7] аналізується необхідність гармонізації українського законодавства з європейськими стандартами у боротьбі з кіберзлочинністю, з акцентом на імплементації положень Конвенції про кіберзлочинність та її Другого додаткового протоколу. Підкреслюється важливість запровадження чітких процедур обробки електронних доказів та узгодження законодавства України із Регламентом ЄС про електронні докази [7].

Отже, подальше дослідження основних засад Другого додаткового протоколу до Конвенції Ради Європи «Про кіберзлочинність» і перспектив його ратифікації Україною є актуальним.

Результати дослідження. Поява Другого додаткового протоколу пов'язана з тим, що традиційні механізми міжнародної правової допомоги дедалі менше відповідають особливостям цифрового середовища. Електронна інформація може фізично зберігатися в одній країні, належати компанії, зареєстрованій в іншій державі, а особа, щодо якої проводиться розслідування, перебувати взагалі в третій державі. Крім того, місце зберігання даних іноді неможливо швидко встановити. У таких умовах отримання електронних доказів за традиційною процедурою міжнародної правової допомоги може тривати значний час. За цей період дані можуть бути видалені, змінені або стати недо-

ступними. Саме тому Протокол спрямований на створення більш оперативних каналів співробітництва між компетентними органами держав та на встановлення спеціальних правил отримання електронних доказів. РЄ прямо визначає його мету як посилення міжнародного співробітництва та розкриття електронних доказів.

Важливо, що Протокол стосується не лише власне кіберзлочинів. Його механізми можуть застосовуватися також у розслідуванні інших кримінальних правопорушень, якщо для такого розслідування необхідні електронні докази. Таким чином, сфера його практичного значення значно ширша за боротьбу з хакерськими атаками чи іншими злочинами, безпосередньо пов'язаними з комп'ютерними системами.

Протокол передбачає декілька взаємопов'язаних механізмів міжнародного співробітництва.

Перший напрям – удосконалення традиційної взаємної правової допомоги. Держави повинні отримати можливість швидше обмінюватися електронними доказами та використовувати сучасні засоби комунікації між компетентними органами.

Другий напрям – співробітництво у невідкладних ситуаціях, коли зволікання може призвести до втрати або знищення електронної інформації.

Третій напрям – безпосередня взаємодія компетентних органів держав із постачальниками послуг, які володіють або контролюють відповідні електронні дані.

Четвертий напрям – пряме співробітництво між компетентними органами різних держав у передбачених Протоколом випадках.

П'ятий напрям – створення додаткових гарантій захисту прав людини, персональних даних та інших законних інтересів особи при транскордонному отриманні інформації.

Одним із практично важливих положень Протоколу є механізм отримання інформації про абонента без необхідності проходження повної традиційної процедури міжнародної правової допомоги. Йдеться про відомості, які дають можливість встановити особу користувача певного цифрового сервісу. Наприклад, це може бути інформація про ім'я користувача, адресу, контактні дані, платіжну інформацію або інші відомості, які перебувають у розпорядженні постачальника послуг.

Протокол створює правові підстави для того, щоб компетентний орган однієї держави міг звертатися до постачальника послуг в іншій державі без необхідності щоразу застосовувати складну процедуру міждержавного запиту. Це особливо важливо у випадках, коли цифровий сервіс працює глобально, а його користувачі перебувають у різних країнах.

При цьому Протокол не встановлює принципу необмеженого доступу правоохоронних органів до інформації. Навпаки, відповідні заходи повинні здійснюватися відповідно до умов самого Протоколу та внутрішнього права держави.

Окрему увагу приділено **даним про трафік**. Такі відомості дозволяють встановити, наприклад, джерело та напрямки електронної комунікації, час її здійснення, використовувані технічні засоби та інші обставини передачі інформації.

Особливість електронних комунікацій полягає в тому, що маршрут передачі інформації може проходити через декілька держав. Тому для слідства може бути принципово важливим встановити, через якого постачальника або яку інфраструктуру проходила комунікація.

Протокол передбачає механізми співробітництва, які мають дозволити компетентним органам швидше отримувати такі дані.

Водночас доступ до них повинен відповідати визначеним правовим умовам та гарантіям.

Одним із найбільш нових елементів Протоколу є розвиток **прямого співробітництва між державними органами та постачальниками цифрових послуг**.

У сучасному Інтернеті значна частина інформації знаходиться не в державних установах, а у приватних компаній – операторів зв'язку, соціальних мереж, хмарних сервісів, поштових платформ, реєстраторів доменних імен тощо. Тому ефективність кримінального розслідування часто залежить від можливості оперативно отримати інформацію саме від такого постачальника. Протокол створює правову основу для відповідних запитів та встановлює процедури, за допомогою яких держава може звертатися до суб'єкта, що володіє або контролює потрібну інформацію. При цьому йдеться не про автоматичне надання правоохоронним органам усієї інформації, якою володіє компанія. Запит має відповідати встановленим вимогам, а держава, до якої належить постачальник або де знаходиться відповідна інформація, зберігає визначені механізми контролю.

Особливого значення набувають положення про **надзвичайні або невідкладні ситуації (екстрене співробітництво)**.

У цифровому середовищі проблема часу має особливе значення. Наприклад, постачальник послуг може зберігати певні дані протягом обмеженого періоду. Якщо компетентний орган чекатиме завершення всіх процедур звичайної міжнародної правової допомоги, інформація може бути втрачена. Тому Протокол передбачає можливість використання спеціального механізму співробітництва в екстрених випадках. Його призначення полягає у тому, щоб компетентні органи могли діяти швидко, коли існує реальний ризик значної шкоди або втрати електронних доказів. Водночас екстрений характер ситуації не означає повної відмови від правових гарантій. Надзвичайний механізм має застосовуватися лише за визначених умов.

Протокол також орієнтований на ширше використання **сучасних технологій у міжнародному кримінальному співробітництві**. Зокрема, передбачаються можливості використання відеоконференцій та інших електронних засобів комунікації для отримання показань та проведення процесуальних дій. Це відповідає загальній логіці документа: якщо злочин і докази існують у цифровому середовищі, міжнародна процедура їх отримання також повинна бути здатною функціонувати в цифровому форматі.

Протокол розвиває й інші форми безпосередньої взаємодії держав. Йдеться, зокрема, про можливість формування **спільних слідчих груп та інших форм координації** у відповідних випадках. Це особливо важливо для злочинів, які одночасно зачіпають декілька юрисдикцій. Наприклад, злочинець може перебувати в одній державі, потерпілий – у другій, сервер – у третій, а фінансові операції проходити через четверту.

За традиційної моделі кожна держава проводить окреме розслідування, а обмін інформацією відбувається через формалізовані канали. Протокол прагне зробити таку взаємодію більш оперативною та практичною.

Оскільки Протокол створює додаткові можливості для транскордонного отримання електронної інформації, особливого значення набуває **захист персональних даних**.

Документ передбачає гарантії того, що передача та використання інформації не повинні перетворитися на необмежений транскордонний доступ державних органів до приватного життя

людини. При застосуванні механізмів Протоколу повинні враховуватися принципи необхідності та пропорційності втручання, цільове використання отриманої інформації, а також інші гарантії, передбачені міжнародним правом і національним законодавством. Таким чином, Протокол намагається знайти баланс між двома конкуруючими інтересами: з одного боку, ефективністю кримінального переслідування, а з іншого – захистом приватності та інших основоположних прав людини.

Важливо й те, що Протокол не встановлює абсолютного обов'язку виконувати будь-який запит іншої держави.

У визначених випадках держава може відмовити у співробітництві або поставити його здійснення в залежність від певних умов. Це необхідно для захисту суверенітету держави, прав людини, національної безпеки та інших охоронюваних законом інтересів.

Тобто Протокол не скасовує принцип територіального суверенітету. Він створює спеціальні механізми подолання практичних труднощів, які виникають через транскордонний характер електронних доказів.

Значення Протоколу для кримінального процесу. У цілому Другий додатковий протокол можна розглядати як спробу перейти від класичної моделі міжнародної правової допомоги до **більш гнучкої та багаторівневої системи отримання електронних доказів**. Його принципова особливість полягає в тому, що міжнародне співробітництво більше не обмежується взаємодією державних органів. До системи фактично включаються **приватні суб'єкти цифрової економіки**, які контролюють значний обсяг інформації, необхідної для кримінальних розслідувань. Це змінює саму модель міжнародного кримінального співробітництва. Якщо раніше центральним елементом був запит однієї держави до іншої держави, то тепер поряд із цим механізмом з'являються прямі канали взаємодії правоохоронних органів із постачальниками послуг.

Водночас Протокол не замінює Будапештську конвенцію, а **доповнює та модернізує її механізми**. Його завдання полягає в тому, щоб зробити положення Конвенції придатними для умов, коли електронна інформація стала одним із найважливіших видів доказів у кримінальному процесі.

Отже, Другий додатковий протокол до Конвенції про кіберзлочинність спрямований на вирішення однієї з головних проблем сучасного кримінального процесу – як швидко та законно отримати електронні докази, якщо вони знаходяться за межами держави, яка проводить розслідування.

Його значення виходить далеко за межі власне кіберзлочинності. Електронні докази сьогодні можуть мати вирішальне значення у справах про тероризм, організовану злочинність, корупцію, шахрайство, незаконний обіг наркотиків, торгівлю людьми та багато інших кримінальних правопорушень. Основна новизна Протоколу полягає у поєднанні **традиційної міжнародної правової допомоги, прискорених процедур, екстреного співробітництва та прямої взаємодії з приватними постачальниками цифрових послуг**. При цьому передбачено систему правових гарантій, покликану не допустити перетворення транскордонного доступу до електронних даних на необмежене втручання держави у приватне життя.

Таким чином, Протокол формує сучасну міжнародно-правову модель отримання електронних доказів, у якій **швидкість і ефективність кримінального розслідування мають поєднуватися з вимогами законності, пропорційності, захисту**

персональних даних та прав людини. Саме в цьому полягає його основне практичне та правове значення.

Разом із тим, станом на **31 липня 2026 року** Протокол ще не набув чинності: за умовами самого договору для набрання ним чинності потрібні **п'ять ратифікацій**. Як зазначено вище, станом на 09.08.2026 року протокол ратифікували лише 4 держави. Україна відноситься до держав, які станом на цю дату ще не ратифікувала Другий додатковий протокол. У парламентських документах на 2026 рік проект закону про ратифікацію визначений як новий законопроект, а строк його внесення/розгляду запланований на IV квартал 2026 року [4]. Метою прямо названо приведення українського законодавства у відповідність до Протоколу для посилення співробітництва українських постачальників електронних комунікаційних послуг з уповноваженими органами держав – підписантів Конвенції.

Тобто станом на зараз причина «не ратифікації» виглядає не як принципова відмова України від Протоколу, а як незавершеність внутрішньої законодавчої підготовки до його ратифікації та імплементації. Насправді Другий протокол передбачає досить серйозну перебудову механізмів роботи з електронними доказами, зокрема:

- безпосередню взаємодію правоохоронних органів із постачальниками послуг;
- процедури отримання інформації про абонента;
- отримання та збереження даних про трафік;
- транскордонний обмін електронними доказами;
- спеціальні механізми міжнародного співробітництва;
- гарантії захисту персональних даних і приватності.

У 2025 році (29–30 вересня 2025 року) українська делегація взяла участь у спільному семінарі Ради Європи та Євроюсту, присвяченому імплементації Другого додаткового протоколу [8]. Основною метою зустрічі був обмін практичним досвідом та обговорення правових і організаційних механізмів, спрямованих на поглиблення міжнародного співробітництва та забезпечення доступу до електронних доказів. Україну на семінарі представляли п'ятеро експертів, делегованих Міністерством юстиції України, Офісом Генерального прокурора, Службою безпеки України та Міністерством внутрішніх справ України. Участь представників зазначених органів засвідчила зацікавленість України у подальшому узгодженні національного законодавства та правозастосовної практики у сфері протидії кіберзлочинності з відповідними міжнародними стандартами.

Під час семінару розглядалися як правові, так і практичні питання реалізації положень Другого додаткового протоколу. Особливу увагу приділено механізмам безпосередньої взаємодії компетентних органів із постачальниками послуг, оптимізації процедур отримання електронних даних, а також забезпеченню належного рівня захисту персональних даних, приватності та інших основоположних прав людини. Окремим предметом обговорення стало практичне використання передбачених Протоколом механізмів під час проведення транскордонних розслідувань.

Українська сторона поінформувала учасників заходу про здійснювану в Україні роботу з підготовки законодавчих змін, необхідних для імплементації Другого додаткового протоколу та його подальшої ратифікації. Зокрема, розробляється законопроект про внесення змін до Кримінального процесуального кодексу України та інших законодавчих актів, спрямованих на врегулювання питань безпосередньої взаємодії з постачальниками послуг, а також на забезпечення належних гарантій захисту персональних даних і права на приватність.

Передбачені законодавчі зміни мають сприяти спрощенню та прискоренню процедур обміну інформацією між українськими постачальниками послуг і компетентними органами іноземних держав, визначенню належного порядку роботи з електронними доказами та посиленню процесуальних і судових гарантій їх використання. Важливу роль у цьому процесі відіграє проект CyberUA, у межах якого надається підтримка в адаптації українського законодавства до положень Другого додаткового протоколу та розвитку міжнародного співробітництва України у сфері протидії кіберзлочинності.

А в липні 2026 року Рада Європи знову повідомляла, що в Україні триває робота над законодавчими змінами щодо електронних доказів, їх допустимості, обробки та chain of custody, причому ці зміни мають забезпечити відповідність Будапештській конвенції та Другому протоколу. Відзначалося, що розробка та прийняття законодавства, що вдосконалює процедури, пов'язані зі збором та використанням електронних доказів у кримінальному провадженні, залишається пріоритетом для України. Такі реформи необхідні, щоб дозволити українським органам влади отримати доступ до електронних доказів та забезпечити їх допустимість у кримінальному провадженні. Ці зміни відповідають процесуальним повноваженням згідно з Будапештською конвенцією, включаючи статті 16-18, а також відповідним положенням Другого додаткового протоколу до Конвенції про кіберзлочинність щодо посиленої співпраці та розкриття електронних доказів [9].

Тобто українська сторона розглядає питання не просто як ратифікацію міжнародного договору, а як комплексну реформу законодавства. Зокрема, стаття [7] прямо розглядає необхідність гармонізації українського законодавства з Конвенцією про кіберзлочинність та її Другим додатковим протоколом. Автор наголошує на необхідності чітких процедур поводження з електронними доказами та узгодження українського законодавства з європейськими стандартами.

Значення Другого додаткового протоколу для України. Для України питання ефективного доступу до електронних доказів має особливе значення.

Після початку повномасштабної агресії російської федерації кіберпростір став одним із напрямів протистояння. Українські державні органи, критична інфраструктура та приватні компанії регулярно зазнають атак, які потребують швидкого встановлення джерел походження, збору цифрових доказів та міжнародної координації.

У таких умовах Другий додатковий протокол може стати важливим інструментом:

- документування кіберзлочинів;
- ідентифікації осіб, причетних до атак;
- отримання інформації від іноземних цифрових платформ;
- забезпечення доказової бази у кримінальних провадженнях.

Для української правової системи його положення також актуалізують питання подальшого вдосконалення кримінального процесуального законодавства, зокрема щодо:

- процедури отримання електронних доказів;
- взаємодії із закордонними провайдерами;
- гарантій захисту персональних даних;
- процесуального статусу цифрової інформації.

Висновки. Виконані дослідження дозволяють дійти наступних висновків.

1. Другий додатковий протокол до Будапештської конвенції є закономірним етапом розвитку міжнародної системи протидії

кіберзлочинності. Якщо сама Конвенція створила основу для криміналізації кіберзлочинів і міжнародної співпраці, то Протокол спрямований на вирішення однієї з найбільш складних сучасних проблем – швидкого та законного отримання електронних доказів у транскордонних кримінальних провадженнях. Його значення для України полягає у створенні додаткових можливостей міжнародної взаємодії, що особливо важливо в умовах зростання кіберзагроз та необхідності ефективного документування злочинів у цифровому середовищі.

2. Попри підписання Україною 30.11.2022 року Другого додаткового протоколу до Конвенції про кіберзлочинність, його ратифікація Україною станом на серпень 2026 року не завершена. Аналіз наукових публікацій та офіційних матеріалів свідчить, що затримка пов'язана не з відмовою України від приєднання до Протоколу, а передусім із необхідністю комплексної адаптації національного законодавства та правозастосовної практики до передбачених ним механізмів транскордонного отримання електронних доказів. Особливого врегулювання потребують питання безпосередньої взаємодії компетентних органів із постачальниками послуг, отримання даних про абонентів і трафік, процедур поводження з електронними доказами, їх зберігання та забезпечення ланцюга їх збереження, а також гарантій захисту персональних даних і приватності.

3. Станом на 26 липня 2026 року сам Протокол теж ще не набув чинності міжнародно – його ратифікували лише чотири держави, тоді як для набрання чинності потрібно п'ять ратифікацій. Україна входить до числа підписантів, але не ратифікаторів. Натомість ратифікація протоколу саме Україною надала б йому міжнародної чинності.

Література:

1. Долженко Л. Ю. Кіберзлочинність: криміналістична характеристика та особливості розслідування. *Молодий вчений*. 2020. № 5 (81). С. 219–223. DOI: <https://doi.org/10.32839/2304-5809/2020-5-81-45>.
2. Піщенко Г. І., Шопіна Ю. О. Кібербезпека та кіберзлочинність в Україні: сучасні тенденції. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2025. Вип. 92. Ч. 4. С. 193–199.
3. Орлов Ю. Ю. Реалізація вимог міжнародної конвенції про кіберзлочинність у законодавстві України. *Науковий вісник національної академії внутрішніх справ*. 2011. № 6. С. 3–9.
4. План законопроектної роботи Верховної Ради України на 2026 рік. URL: https://research.rada.gov.ua/uploads/documents/33968.pdf?utm_source=chatgpt.com
5. Ахтирська Н. М. Правова регламентація електронних доказів та практика їх використання в судочинстві України. *Науковий вісник Ужгородського Національного Університету*. 2023. Том 2. № 75. С. 141–150. DOI: <https://doi.org/10.24144/2307-3322.2022.75.2.23>.
6. Ахтирська Н. М. Одержання доказів в електронній формі в світлі Другого додаткового протоколу до Конвенції про кіберзлочинність. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 188–200. DOI: <https://doi.org/10.33994/kndise.2022.67.21>.
7. Гуцалюк М. Імплементация европейских стандартов в борьбе с киберзлочинністю: проблеми правового регулювання електронних доказів в Україні. *Слово Національної школи суддів України*. 2025. № 2 (51). С. 167–176. DOI: [10.37566/2707-6849-2025-2\(51\)-16..](https://doi.org/10.37566/2707-6849-2025-2(51)-16..)

8. CyberUA та CyberEast+: Україна посилює міжнародно-правове співробітництво у сфері протидії кіберзлочинності... Гаага, 29–30 вересня 2025. URL: https://www.coe.int/uk/web/kyiv/-/cyberua-and-cybereast-ukraine-strengthens-international-cybercrime-co-operation-at-the-council-of-europe/eurojust-joint-workshop-on-the-second-additional-protocol-to-the-convention-on-cybercrime?utm_source=chatgpt.com
9. CyberEast+ and CyberUA: Ukrainian law enforcement authorities and the Verkhovna Rada assessed the improvements to the Criminal Code of Ukraine, in line with international standards. 7–8 July 2026. URL: https://www.coe.int/en/web/cybercrime/-/cybereast-and-cyberua-ukrainian-law-enforcement-authorities-and-the-verkhovna-rada-assessed-the-improvements-to-the-criminal-code-of-ukraine-in-line-with-international-standards?utm_source=chatgpt.com

Belkin L., Kryvolap E., Iurynets Ju., Belkin L. The main principles of the Second additional protocol to the Council of Europe convention on cybercrime (CETS no. 224) and the issue of its ratification by Ukraine

Summary. The article examines the principal provisions of the Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, as well as the prospects for its ratification by Ukraine. The relevance of this international legal instrument is substantiated in view of the increasing importance of electronic evidence in criminal proceedings and the limited effectiveness of traditional mutual legal assistance mechanisms in cases involving cross-border digital information. The article considers the main mechanisms of co-operation provided for by the Protocol, including enhanced mutual legal assistance procedures, co-operation in emergency situations, direct interaction between competent authorities and service providers, access to subscriber information and traffic data, the use of modern electronic communication technologies, and other forms of international co-operation. Particular attention is paid to safeguards for the protection of personal data, privacy and other human rights, as well as compliance with the principles of legality, necessity and proportionality when obtaining electronic information across borders. The state of ratification of the Protocol and Ukraine's ongoing legislative preparations for its implementation are analysed. It is argued that the delay in Ukraine's ratification is primarily related to the need for comprehensive adaptation of national legislation and law enforcement practice to the mechanisms established by the Protocol rather than to any principled refusal to join it. The significance of the Protocol for Ukraine is determined in the context of combating cybercrime, documenting criminal offences and obtaining electronic evidence from foreign jurisdictions.

Key words: cybercrime, electronic evidence, Second Additional Protocol, Budapest Convention, international co-operation, mutual legal assistance, service providers, subscriber information, traffic data, cross-border evidence, personal data, privacy.

Використання штучного інтелекту. Під час підготовки статті інструменти штучного інтелекту використовувалися виключно для мовного редагування, перевірки граматики, перекладу або інших допоміжних завдань, без використання згенерованих ними об'єктів як результатів академічної діяльності.

Дата першого надходження статті до видання: 20.07.2026
Дата прийняття статті до друку після рецензування: 15.08.2026

Дата публікації (оприлюднення) статті: 01.10.2026



Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)