Проблеми автентичності та допустимості електронних доказів у кримінальних провадженнях, пов'язаних із корупцією

Ростислав Бундз[1], Григорій Мартинишин[2], Богдан Грещук[3]

Опубліковано	Секція	УДК
25.02.2025	Право	343.98:343.352(477)

DOI: https://doi.org/10.5281/zenodo.18074683

Анотація. У статті досліджено комплекс проблем, що виникають під час оперування цифровими відомостями у процесі розслідування службових злочинів. Авторами проаналізовано сучасний стан вітчизняного законодавства та виявлено термінологічні суперечності, які створюють ризики для визнання матеріалів допустимими у судовому розгляді. Особливу увагу приділено технічним аспектам верифікації первинних даних, зокрема використанню криптографічних алгоритмів та хешування для підтвердження незмінності об'єктів. Висвітлено концепцію «ланцюга збереження» як засадничого принципу роботи з віртуальним простором у криміналістиці. Розглянуто роль міжнародних стандартів та транскордонної співпраці у контексті подолання латентних правопорушень. За результатами роботи запропоновано шляхи вдосконалення процесуальних норм через впровадження обов'язкового залучення фахівців та технічну модернізацію правоохоронної системи, що сприятиме підвищенню якості доказової бази.

Ключові слова: цифрові сліди, кримінальний процес, верифікація даних, хешування, ланцюг збереження, кібербезпека, криптографічні методи, судова експертиза, антикорупційна діяльність, процесуальна фіксація.

[1] кандидат юридичних наук, доцент,
доцент кафедри міжнародного та кримінального права
Навчально-наукового інституту права,
психології та інноваційної освіти,
Національний університету «Львівська політехніка»,
https://orcid.org/0000-0002-3651-4068

[2] кандидат юридичних наук,
в.о. доцента кафедри права
Львівського національного університету ветеринарної медицини та біотехнологій імені С.З. Ґжицького,
https://orcid.org/0009-0000-7723-8007

[3] здобувач першого (бакалаврського) рівня вищої освіти
спеціальності 081 Право, факультету права
Львівського торговельно-економічного університету
https://orcid.org/0009-0008-5893-9033

Issues of authenticity and admissibility of electronic evidence in criminal proceedings related to corruption

Annotation. The article provides a comprehensive scientific analysis of the challenges associated with the authenticity and admissibility of electronic evidence within criminal proceedings, specifically focusing on corruption-related offenses. In the context of global digitalization, digital traces such as emails, messenger records, and financial transactions have become fundamental components of the evidentiary base in anti-corruption investigations. The authors emphasize that corruption schemes often utilize sophisticated digital tools for concealment, making traditional investigative methods insufficient and necessitating advanced forensic approaches.

A significant portion of the research is dedicated to the legal and technical aspects of ensuring the integrity of digital data. The study identifies a critical gap in Ukrainian legislation regarding the precise procedures for authenticating electronic evidence. To address this, the authors advocate for the mandatory implementation of the «chain of custody» principle, ensuring that every stage of data handling is documented to prevent tampering or loss. Furthermore, the article explores technical verification methods, including hash functions, digital signatures, and asymmetric cryptography, as essential tools for confirming that evidence has not been altered since its creation.

The research also addresses the cross-border nature of modern corruption, where data is often stored on remote servers in multiple jurisdictions. The authors highlight the importance of international cooperation, citing the Budapest Convention on Cybercrime as a vital framework for mutual legal assistance and information exchange. The study concludes by proposing concrete recommendations for legislative reform, specifically emphasizing the need for terminological unification between the concepts of «information», «data» and «intelligence» in the Criminal Procedure Code of Ukraine to eliminate legal uncertainty. The findings suggest that only a symbiosis of legal regulation and advanced technological expertise can ensure the effectiveness of the justice system in combating high-level corruption.

Keywords: digital traces, criminal procedure, data verification, hashing, chain of custody, cybersecurity, cryptographic methods, forensic examination, anti-corruption activity, procedural fixation.

Вступ

Постановка проблеми. У сучасному світі, де цифрові технології стали невід'ємною частиною життя суспільства, питання використання електронних доказів у кримінальних провадженнях набуває особливої актуальності. Зокрема, це стосується справ, пов'язаних із корупцією, які часто супроводжуються складними схемами приховування злочинної діяльності, що реалізуються за допомогою цифрових засобів. Електронні докази, такі як електронні листи, повідомлення в месенджерах, записи телефонних розмов, банківські транзакції та інші цифрові сліди, стають ключовими елементами доказової бази у таких провадженнях. Однак їх використання породжує низку проблем, пов'язаних із автентичністю та допустимістю таких доказів.

Проблема автентичності електронних доказів полягає в необхідності забезпечення їх достовірності, тобто підтвердження того, що вони не були змінені чи підроблені. У цифровому середовищі існує безліч способів маніпуляції даними, що ускладнює процес перевірки їхньої автентичності. Крім того, відсутність єдиних стандартів щодо фіксації, зберігання та передачі електронних доказів створює ризики їхнього спотворення або втрати.

Допустимість електронних доказів є ще однією важливою проблемою. Згідно з принципами кримінального процесуального права, докази повинні бути отримані законним шляхом. У випадку електронних доказів це означає дотримання процедур

збору інформації, визначених законодавством. Проте на практиці часто виникають суперечності щодо того, чи були такі докази зібрані відповідно до встановлених норм, що може призводити до їхнього виключення з розгляду в суді.

Окремо слід зазначити проблему недостатньої правової регламентації питань, пов'язаних із електронними доказами в Україні. Хоча законодавство передбачає можливість використання таких доказів у кримінальних провадженнях, відсутність детальних норм щодо їхньої автентифікації та допустимості створює правову невизначеність. Це ускладнює роботу правоохоронних органів і судів, а також може негативно впливати на результати розгляду справ.

Таким чином, проблеми автентичності та допустимості електронних доказів у кримінальних провадженнях, пов'язаних із корупцією, є багатовимірними та потребують комплексного наукового аналізу. Вирішення цих проблем має важливе значення для забезпечення ефективності боротьби з корупцією та дотримання принципів верховенства права.

Стан дослідження проблеми автентичності та допустимості електронних доказів у кримінальних провадженнях, пов'язаних із корупцією, є актуальною темою для сучасної правової науки. З розвитком цифрових технологій і зростанням обсягу електронної інформації, яка використовується у кримінальних розслідуваннях, виникає необхідність у чіткому визначенні стандартів автентичності та допустимості таких доказів. Особливо це стосується справ, пов'язаних із корупційними правопорушеннями, де електронні докази часто є ключовими для розкриття злочинів.

На сьогоднішній день значна кількість наукових робіт присвячена загальним аспектам використання електронних доказів у кримінальному процесі. Зокрема, досліджуються питання правового регулювання, технічних стандартів, а також процесуальних гарантій їх використання. У цьому контексті слід зазначити роботи таких вчених, як В. Тропіна, О. Костенко, С. Гончаренка та інших, які аналізують загальні проблеми правового статусу електронних доказів. Їхні дослідження закладають основу для розуміння загальних принципів роботи з цифровими даними у кримінальному процесі.

Однак проблема автентичності електронних доказів залишається недостатньо дослідженою. Автентичність передбачає підтвердження того, що електронний доказ є оригінальним або таким, що не зазнав змін після його створення. У цьому аспекті важливу роль відіграють технічні методи перевірки, такі як використання хеш-функцій, електронного підпису чи блокчейн-технологій. Проте, як зазначають деякі автори, наприклад, О. Мельник та І. Бондаренко, на практиці часто виникають труднощі із забезпеченням належного документування процесу отримання та зберігання електронних доказів, що може поставити під сумнів їхню автентичність у суді.

Ще однією важливою проблемою є допустимість електронних доказів. У науковій літературі наголошується на тому, що для визнання доказу допустимим необхідно дотримуватися вимог законності його отримання. Наприклад, І. Коваленко у своїх роботах акцентує увагу на тому, що порушення процедури вилучення або аналізу електронних даних може призвести до їх відхилення судом. Це особливо актуально для справ про корупцію, де сторони часто оспорюють законність отримання доказів.

Окрему увагу заслуговують питання забезпечення конфіденційності та захисту персональних даних під час роботи з електронними доказами. Як зазначають дослідники, такі як Н. Соловйова та М. Литвиненко, сучасне законодавство не завжди враховує специфіку цифрових даних і ризики їх витоку або неправомірного використання. Це може створювати додаткові перешкоди для використання електронних доказів у кримінальних провадженнях.

У контексті боротьби з корупцією проблема автентичності та допустимості електронних доказів набуває особливого значення. Корупційні злочини часто характеризуються складністю доказової бази, адже вони можуть включати аналіз великого обсягу фінансових транзакцій, електронного листування чи записів телефонних розмов. У цьому аспекті важливо забезпечити належний рівень співпраці між правоохоронними органами та експертними установами, які здійснюють аналіз цифрових даних.

Таким чином, стан дослідження проблеми автентичності та допустимості електронних доказів у кримінальних провадженнях демонструє значний науковий інтерес і водночас вказує на низку нерозв'язаних питань. Подальші дослідження в цій галузі мають бути спрямовані на розробку чітких критеріїв оцінки автентичності та допустимості таких доказів, удосконалення нормативно-правової бази та інтеграцію сучасних технологій у процес кримінального розслідування.

Метою статті є дослідження проблем автентичності та допустимості електронних доказів у кримінальних провадженнях, пов'язаних із корупцією, аналіз сучасного стану нормативно-правового регулювання цієї сфери, виявлення ключових викликів, що виникають у процесі збирання, зберігання та використання електронних доказів, а також розробка рекомендацій щодо вдосконалення правозастосовної практики та законодавства з метою забезпечення ефективності боротьби з корупційними правопорушеннями.

Результати

Корупційні правопорушення є одними з найбільш небезпечних загроз для функціонування державних інституцій, економіки та суспільства загалом. Ефективна протидія корупції потребує сучасних підходів до розслідування, зокрема використання електронних доказів, які стають ключовим інструментом у розкритті злочинів. Загальні тенденції свідчать про зростання використання електронних доказів у судових процесах, зокрема у справах, пов'язаних із корупцією. Електронні докази, такі як електронні листи, записи телефонних розмов, дані з мобільних пристроїв, банківські транзакції та інші цифрові сліди, дедалі частіше стають ключовими елементами у розгляді таких справ.

В Україні запровадження антикорупційних органів, таких як Національного антикорупційного бюро (НАБУ) та Спеціалізованої антикорупційної прокуратури (САП), сприяло активнішому використанню електронних доказів у розслідуваннях, зокрема у вигляді записів переговорів або аналізу фінансових потоків. У світі аналогічні підходи застосовуються в країнах із розвиненою правовою системою, зокрема в країнах ЄС та США, де цифрові технології широко інтегровані в юридичну практику і електронні докази також відіграють важливу роль у боротьбі з корупцією, і їх використання регламентується відповідними законодавчими нормами.

Однак використання таких доказів у кримінальних провадженнях стикається з низкою правових, технічних та організаційних проблем. Зокрема, питання автентичності та допустимості електронних доказів викликають значні дискусії як серед науковців, так і серед практиків.

Сучасними завданнями цифрової криміналістики є пошук і аналіз цифрових слідів, аналіз даних (зокрема – метаданих), збирання доказової інформації у цифровому середовищі. Найбільш складними й масштабними є завдання із пошуку у відкритому доступі й аналізу потенційних джерел доказів – величезної кількості загальнодоступних відео- та аудіозаписів, фото- та супутникових знімків, текстів, звітів, публікацій у соціальних мережах [1].

В чинному національному та міжнародному кримінально-процесуальному законодавстві не сформовано чіткого визначення поняття електронних доказів. У статті 84 Кримінального кодексу України визначено в широкому розумінні, що доказами є фактичні дані, які отримані відповідним чином, належать до справи та достовірні Тому в науковому і в правовому полі існує множинність підходів до тлумачення суті електронних доказів [2]. Комітет Міністрів Ради Європи трактує поняття електронних доказів як будь які докази, отримані з даних, що містяться в будь-якому пристрої або вироблені ним, функціонування якого залежить від програмного забезпечення або даних, що зберігаються або передаються через комп'ютерну систему чи мережу [3].

Більшість фахівців наукового середовища під електронними доказами розуміють дані або інформацію, яка з'явилася внаслідок використання цифрової техніки і відповідного програмного забезпечення, та може бути використана в судовому процесі [4; 5].

Інші дослідники визначають електронні докази як об'єкти цифрового (електронного) виміру, що можуть мати значення для кримінального провадження [6, с. 44].

Згідно з частиною першою статті 96 Господарського процесуального кодексу України [7], частиною першою статті 99 Кодексу адміністративного судочинства України [8] та частиною першою статті 100 Цивільного процесуального кодексу України [9], електронні докази визначаються як «інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи». До таких доказів належать електронні документи (зокрема текстові файли, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші електронні дані. Аналогічне визначення наведено у частині першій статті 1001 законопроєкту «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів», де електронний доказ визначається як «інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [10]. Ці положення демонструють найпоширеніший підхід до визначення електронних доказів.

Водночас у зазначених дефініціях спостерігається певна термінологічна невідповідність, зокрема необґрунтоване протиставлення таких понять, як «інформація», «дані» та «відомості». Відповідно до статті 1 Закону України «Про інформацію», інформацією вважаються «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [11].

Отже, електронна форма інформації є нематеріальною версією інших форм інформації (письмової, графічної, аудіовізуальної тощо) і здатна відтворювати всі її елементи. Крім того, електронна форма має певні переваги, наприклад можливість збереження метаданих, які недоступні для інших форм.

Проаналізувавши законодавчу базу та наукові дослідження, докази в електронній формі можна визначити як інформацію, створену, оброблену, збережену або передану за допомогою аналогових чи цифрових сигналів і яка має значення для кримінального провадження.

У кримінальних провадженнях, пов'язаних із корупцією, електронні докази є особливо важливими через специфіку таких злочинів. Корупційна діяльність часто здійснюється із використанням сучасних технологій, що робить традиційні методи збору доказів менш ефективними. Водночас електронні докази можуть стати вирішальними для доведення фактів хабарництва, незаконного збагачення чи інших корупційних правопорушень.

Проблема автентичності електронних доказів у справах, пов'язаних із корупційними діяннями, є однією з ключових у сучасній юридичній практиці. Електронні докази, такі як електронні листи, записи телефонних розмов, файли, збережені на цифрових носіях, або дані з соціальних мереж, дедалі частіше використовуються як основа для розслідування та судового розгляду корупційних справ. Однак їх автентичність викликає серйозні питання як у правозастосовній практиці, так і в наукових дослідженнях.

Згідно з чинним законодавством України, електронні докази є допустимими у кримінальному процесі відповідно до статті 99 Кримінального процесуального кодексу України (КПК) [2]. Вони можуть бути представлені у вигляді електронних документів, даних, отриманих з електронних пристроїв, або інших цифрових носіїв інформації. Проте законодавство не дає чітких процедур для перевірки автентичності таких доказів, що створює простір для маніпуляцій або фальсифікацій.

Одним із ключових аспектів є проблема забезпечення цілісності електронного доказу. Згідно з міжнародними стандартами, такими як ISO 27037 [12], важливо забезпечити дотримання принципу «ланцюга збереження доказів». Це означає, що кожен етап роботи з електронним доказом має бути документально зафіксований, а доступ до нього – суворо регламентований. Проблематичним у національній практиці є те, що такі процедури часто ігноруються або виконуються формально, що ставить під сумнів достовірність отриманих даних.

Науковці все частіше звертають увагу на технічні аспекти автентифікації та ризики, що виникають у зв'язку з цим. У сучасному цифровому середовищі електронні документи стали невіддільною частиною комунікацій, але їхня безпека та автентичність залишаються питанням, яке викликає занепокоєння. Одним із ключових ризиків є можливість підробки документів за допомогою спеціалізованого програмного забезпечення. Такі програми дозволяють змінювати текст, зображення і навіть метадані файлів, що ускладнює процес верифікації.

Метадані, які зазвичай використовуються для підтвердження часу створення, змінення чи авторства документа, також можуть бути змінені без залишення слідів втручання. Це створює додаткові виклики для забезпечення цілісності інформації. Наприклад, дослідження вітчизняних фахівців у сфері інформаційної безпеки демонструють, що методи маніпуляції метаданими можуть бути настільки складними, що їхнє виявлення вимагає застосування спеціалізованих інструментів і знань.

У цьому контексті використання криптографічних методів захисту інформації стає надзвичайно важливим. Одним із найбільш ефективних способів забезпечення автентичності документів є застосування цифрового підпису. Цифровий підпис базується на використанні асиметричної криптографії, де для створення підпису використовується приватний ключ, а для перевірки – публічний. Це забезпечує високий рівень захисту, оскільки підробити підпис без доступу до приватного ключа практично неможливо.

Ще одним важливим методом є хешування – процес перетворення даних у фіксований рядок символів (хеш). Хеш-функції мають властивість уникальності: навіть найменша зміна у вхідних даних призводить до значної зміни хеш-значення. Це дозволяє швидко перевіряти цілісність файлів і виявляти будь-які несанкціоновані зміни.

Дослідження українських науковців також підкреслюють необхідність інтеграції цих методів у різні сфери діяльності, включаючи державне управління, фінансовий сектор і медицину. Наприклад, у сфері електронного урядування застосування цифрових підписів дозволяє забезпечити довіру до електронних послуг та документів. У фінансовій сфері криптографічні методи допомагають захищати транзакції від

шахрайства, а в медицині – забезпечувати конфіденційність і автентичність медичних записів.

Однак впровадження таких технологій потребує не лише технічного забезпечення, але й правового регулювання. Законодавство має враховувати специфіку використання цифрових підписів і хешування, а також передбачати відповідальність за порушення правил автентифікації. Зокрема, важливо розробляти стандарти для захисту електронних документів, які могли б бути застосовані на національному рівні.

Таким чином, ризики, пов'язані з технічними аспектами автентифікації, потребують комплексного підходу до їхнього вирішення. Використання криптографічних методів, таких як цифровий підпис і хешування, у поєднанні з правовим регулюванням та освітніми ініціативами може значно зменшити вразливість електронних документів до маніпуляцій і забезпечити їхню надійність. Ще одним викликом є правове регулювання залучення експертів для перевірки автентичності електронних доказів. У КПК України визначено загальні положення щодо експертизи, але спеціалізовані методики дослідження цифрових доказів залишаються недостатньо розробленими [2]. Це призводить до неоднозначності у висновках експертів і може стати підставою для оскарження доказів у суді.

Окремо варто зазначити проблему транскордонного характеру багатьох корупційних діянь. Проблема транскордонного характеру корупційних діянь є важливим аспектом, який потребує детального розгляду в контексті боротьби з корупцією на міжнародному рівні. У сучасному глобалізованому світі, де інформація може зберігатися на серверах у різних країнах, виникають значні труднощі з доступом до даних, необхідних для розслідувань. Це ускладнює процес виявлення та притягнення до відповідальності осіб, причетних до корупційних правопорушень.

Одним із ключових інструментів для подолання таких викликів є міжнародна співпраця. Вона включає взаємодію між правоохоронними органами, обмін інформацією та координацію дій у рамках міжнародних угод. Зокрема, Будапештська конвенція про кіберзлочинність є важливим документом, який регулює питання співробітництва у сфері кібербезпеки та боротьби зі злочинами, що здійснюються з використанням інформаційних технологій [13]. Ця конвенція передбачає механізми взаємної правової допомоги, що дозволяють країнам-учасницям ефективно обмінюватися даними та забезпечувати доступ до інформації, необхідної для розслідувань.

Однак успішна реалізація таких механізмів вимагає дотримання ряду умов. По-перше, країни повинні гармонізувати своє законодавство відповідно до положень міжнародних угод. По-друге, необхідно забезпечити належний рівень технічної підготовки фахівців, які працюють у сфері боротьби з кіберзлочинністю та корупцією. По-третє, важливо створити довірливі відносини між державами для оперативного й ефективного обміну інформацією.

Таким чином, вирішення проблеми транскордонного характеру корупційних діянь потребує комплексного підходу, який включає як удосконалення національного законодавства, так і активну участь у міжнародній співпраці. Лише за таких умов можна досягти суттєвого прогресу в боротьбі з корупцією на глобальному рівні.

З цією проблемою пов'язано ще низку питань, які мають комплексний вплив на подолання корупційних схем, зокрема і на допустимість електронних доказів. У контексті глобалізації та поширення цифрових технологій, корупційні схеми все частіше виходять за межі національних кордонів, створюючи серйозні виклики для державних інституцій та міжнародного співтовариства.

Як зазначає Бойко О., сучасні корупційні діяння нерідко мають глобальний масштаб. Використання цифрових технологій дозволяє здійснювати фінансові операції через юрисдикції різних країн, зберігати дані на серверах за межами національного

контролю та приховувати сліди незаконної діяльності. Це ускладнює роботу правоохоронних органів, які стикаються з бар'єрами доступу до інформації. Вчена наголошує, що міжнародна співпраця є ключовим елементом у боротьбі з такими викликами [14]. Ефективний обмін інформацією між країнами, гармонізація правових механізмів і створення спільних баз даних можуть значно підвищити ефективність антикорупційних заходів.

Коваленко І. у своїх роботах підкреслює необхідність вдосконалення українського законодавства відповідно до міжнародних стандартів [15]. Вона зазначає, що гармонізація нормативно-правових актів дозволить Україні ефективніше співпрацювати з іншими державами у боротьбі з корупцією. Зокрема, це стосується створення механізмів швидкого реагування на запити щодо доступу до даних, які можуть зберігатися за кордоном. Також важливим є впровадження прозорих процедур для відстеження фінансових потоків і посилення відповідальності за корупційні злочини.

Мельник А. звертає увагу на технічний аспект боротьби з транскордонною корупцією. Він наголошує, що правоохоронні органи потребують високого рівня технічної компетентності та доступу до сучасних технологій аналізу даних [16]. Використання спеціалізованого програмного забезпечення для моніторингу фінансових операцій, аналізу великих обсягів даних і виявлення аномалій може значно підвищити ефективність розслідувань. Крім того, важливим є навчання фахівців новітнім методам роботи в умовах цифрової трансформації.

Висновки

У результаті проведеного дослідження можна констатувати, що розв'язання проблем автентичності та допустимості електронних доказів у кримінальних провадженнях щодо корупційних правопорушень потребує комплексного підходу, який включає міжнародну співпрацю, адаптацію законодавства та технічне вдосконалення правоохоронних органів.

Насамперед, для подолання існуючої правової невизначеності вкрай важливо здійснити уніфікацію термінології, усунувши суперечливі невідповідності між поняттями «інформація», «дані» та «відомості» у КПК України та суміжних законах. Це дозволить створити єдиний понятійний апарат, що унеможливить неоднозначне трактування правової природи цифрових слідів. Разом із цим, критичною необхідністю є чітке процесуальне закріплення процедур збирання та зберігання електронних доказів безпосередньо у нормах Кримінального процесуального кодексу України, зокрема у статті 99.

Особливу увагу слід приділити законодавчому впровадженню обов'язкового дотримання ланцюга збереження доказів, що виступатиме гарантією незмінності інформації з моменту її вилучення до представлення суду. Проте варто наголосити, що належний рівень автентичності не може бути забезпечений виключно юридичними інструментами. Ефективне правосуддя у цій сфері можливе лише через техніко-правовий симбіоз, який передбачає обов'язкове застосування криптографічних методів, таких як хешування та електронний цифровий підпис, у поєднанні із залученням кваліфікованих експертів.

Таким чином, лише за умови комплексного підходу, що поєднує гармонізацію законодавства, технічну модернізацію та міжнародну співпрацю, можна досягти реального прогресу у підвищенні ефективності розслідування корупційних злочинів у цифрову епоху.

Список використаних джерел

1. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 1 (30). URL: https://khrife-journal.org/index.php/journal.
2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 .
3. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings : adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c .
4. Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти правозастосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247–253.
5. Свистун Я. В. До питання правової природи електронних доказів. *Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану* : тези доповідей Міжнар. наук.-практ. конф. (м. Харків, 25 листоп. 2022 р.). Харків, 2022. С. 363–368.
6. Рябущенко Д. Ю. Концептуально-теоретична проблематика категорії «цифрових (електронних)» доказів у кримінальному провадженні. *Економіка. Фінанси. Право*. 2023. № 5. С. 42–47.
7. Господарський процесуальний кодекс України : Закон України від 06.11.1991 № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12 .
8. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15 .
9. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15 .
10. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : проєкт Закону України № 1001.
11. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 .
12. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva : ISO, 2012. 38 p.
13. Будапештська конвенція про кіберзлочинність : Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 .
14. Бойко О. В. Міжнародне співробітництво у сфері запобігання і протидії корупції: теоретико-правовий аспект. *Часопис Київського університету права*. 2019. № 2. С. 238–242.
15. Коваленко І. П. Гармонізація законодавства України з міжнародними стандартами у сфері боротьби з корупцією. *Право та державне управління*. 2021. № 1. С. 154–160.

16. Мельник А. М. Техніко-криміналістичне забезпечення розслідування злочинів, учинених у кіберпросторі: проблеми та перспективи. *Юридичний часопис Національної академії внутрішніх справ*. 2022. № 1 (23). С. 89–97.