збільшує ефективність роботи аналітиків, мінімізує вчинення помилок та оптимізує затрати сил й часу при опрацюванні однотипних, рутинних операцій. Використання таких рішень є невід'ємною частиною майбутнього правоохоронних органів.

Список використаних джерел

1. Махницький О. В., Мирошниченко В. О., Кочеткова І. Б. Використання відеоаналітики у роботі Національної поліції : метод. рекомендації / Кафедра економічної та інформаційної безпеки ОДУВС. Одеса, 2020. 38 с.

2. Штучний інтелект у правовій практиці: межі та можливості : зб. тез круглого столу. Львів : ЛьвДУВС, 2025. 238 с.

3. Briefcam. Програмне забезпечення для відеоаналітики. URL: https://www.briefcam.com/solutions/review-search/

Погорецький Микола Анатолійович,
перший проректор Київського національного університету імені Тараса Шевченка, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України

ДОКАЗИ В ЦИФРОВІЙ ФОРМІ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО ЕКОНОМІЧНИХ ПРАВОПОРУШЕНЬ: ВІД ОДЕРЖАННЯ ІНФОРМАЦІЇ ДО ЇЇ ІНТЕГРОВАНОЇ СУДОВОЇ ПЕРЕВІРКИ

Цифровізація економічних, фінансових і корпоративних відносин істотно змінює інформаційне середовище кримінального провадження. Значна частина відомостей про кримінальні правопорушення у сфері економіки сьогодні виникає, існує, передається та зберігається первинно у цифровій формі. Йдеться про банківські й платіжні записи, відомості про рух коштів, електронний документообіг, бухгалтерські та корпоративні інформаційні системи, ERP/EDMS-записи, журнали доступу, електронне листування, дані месенджерів, хмарних сервісів, інформацію про віртуальні активи, цифрові сліди операцій із корпоративними правами та інші масиви електронних даних.

Особливої актуальності ця проблематика набуває для протидії складним формам економічної злочинності, у тому числі

корупційним, фінансовим, корпоративним, банківським, податковим та майновим кримінальним правопорушенням. Раніше проблеми протидії окремим проявам такої злочинності, зокрема рейдерству, досліджувалися передусім крізь призму причин, організаційних та правових засобів протидії [4]. Сучасна цифровізація корпоративних і фінансових відносин додає до цієї проблеми якісно нового доказового виміру, оскільки значущі для кримінального провадження фактичні відомості дедалі частіше утворюються не в паперовому документі, а безпосередньо в інформаційній системі.

Водночас сама технологічна новизна способу існування інформації не повинна призводити до механічного конструювання нового виду доказів. На нашу думку, методологічною основою для вирішення цієї проблеми залишається сформульоване раніше положення про необхідність розмежування пізнання і кримінального процесуального доказування. Пізнавальна діяльність є ширшою за доказування, а відомості, одержані в результаті пошукової, оперативної, інформаційно-аналітичної чи іншої діяльності, не набувають автоматично процесуальної якості доказу лише внаслідок їх інформаційної цінності [1; 2].

Саме в цьому контексті нами свого часу досліджувалася проблема використання матеріалів оперативно-розшукової діяльності у кримінальному процесі [2], а також судового контролю і прокурорського нагляду за використанням протоколів оперативно-розшукових заходів як доказів [3]. Подальший розвиток кримінального процесуального законодавства актуалізував ту саму методологічну проблему вже стосовно негласних слідчих (розшукових) дій. Нами спільно з О. С. Стареньким обґрунтовувалося, що НСРД мають розглядатися як процесуальні засоби отримання доказової інформації, використання результатів яких потребує дотримання нормативно встановленої процедури та гарантій прав учасників кримінального провадження [5].

Отже, перехід від матеріалів ОРД до результатів НСРД, а нині до великих масивів цифрових даних не скасовує базового закономірного зв’язку між пізнанням і доказуванням. Змінюються технічні засоби одержання, фіксації, накопичення та аналізу інформації, проте незмінною залишається потреба у її належному процесуальному включенні, перевірці та оцінці.

З цих позицій вважаємо методологічно більш точним вести мову не про формування універсальної автономної категорії «цифрових доказів», а передусім про **докази у цифровій**

(електронній) формі. Цифрова форма є техніко-юридичним способом фіксації, збереження, передавання та відтворення доказової інформації, але сама по собі не змінює процесуальної природи фактичних даних [7]. Тому необхідно послідовно розмежовувати: фактичні дані як інформаційний зміст; передбачене законом процесуальне джерело; цифрову форму існування та відтворення інформації; матеріальний або технічний носій, на якому вона в певний момент зафіксована.

Такий підхід має не лише теоретичне, а й безпосереднє практичне значення. Цифрова інформація може бути скопійована на інший носій без зміни її змісту; один і той самий електронний документ може існувати одночасно на декількох технічних носіях; зміна формату або місця зберігання не означає автоматичної втрати інформаційної ідентичності. Відповідний підхід простежується й у практиці Об'єднаної палати Касаційного кримінального суду Верховного Суду у справі № 554/5090/16-к, у якій акцент перенесено з фізичної унікальності носія на інформаційну тотожність електронного документа [13].

Проте відмова від ототожнення доказу з його матеріальним носієм не означає послаблення вимог до цифрової інформації. Навпаки, цифрова форма формує особливий комплекс ризиків, пов'язаних із простотою копіювання та модифікації, змінюваністю метаданих, складністю встановлення конкретного користувача цифрового об'єкта, залежністю від програмного забезпечення, автоматизованим пошуком і фільтруванням, можливістю вибіркового вилучення інформації, транскордонним характером її зберігання та передавання. Технічні аспекти поводження з цифровими слідами, включно з копіюванням у режимі read-only, хешуванням, фіксацією метаданих та забезпеченням ланцюга збереження, мають у цьому аспекті істотне значення [9].

Водночас технічно правильно вилучений або збережений цифровий об'єкт ще не означає, що отримана з нього інформація є достатньо перевіреною для обґрунтування процесуального чи судового рішення. На нашу думку, ключовою категорією для сучасного доказового права має бути **процесуальна придатність доказової інформації у цифровій формі**, яка не може бути зведена до одного критерію, зокрема лише до законності одержання або технічної автентичності.

Передусім необхідно розрізняти допустимість, достовірність та доказову вагу. Допустимість пов'язана насамперед із правовою підставою, компетентністю суб'єкта, способом одержання та

належним процесуальним включенням інформації. Достовірність характеризує здатність встановити її реальне походження, атрибуцію, автентичність, цілісність, повноту та контекст. Доказова вага стосується того, наскільки перевірена інформація у сукупності з іншими доказами здатна підтвердити або спростувати певну обставину. Такий підхід узгоджується із запропонованим нами переходом від надмірно формального розуміння допустимості до оцінювання процесуальної доброчесності способу одержання, перевірки та використання доказової інформації [8].

Для кримінальних проваджень щодо економічних правопорушень особливого значення набуває **атрибуція** цифрової інформації. Належність банківського рахунку, телефонного номера, електронної адреси, облікового запису, криптовалютної адреси чи корпоративного логіна певній особі ще не завжди доводить фактичне здійснення цією особою конкретної операції. Цифрова атрибуція повинна за можливості формуватися на основі сукупності незалежних ознак: технічних ідентифікаторів, інформації банку чи оператора, часу і місця доступу, даних пристрою, змісту комунікації, характеру наступної поведінки та інших доказів. Для цифрового доказування особливо небезпечним є перехід від формального зв'язку «акаунт зареєстровано на особу» до категоричного висновку «дію здійснила ця особа» без належного проміжного доказування.

Самостійної уваги потребують автентичність, цілісність і метадані. Не кожне розходження у часових характеристиках, властивостях файла чи метаданих автоматично свідчить про його фальсифікацію. Метадані можуть змінюватися внаслідок копіювання, експорту, роботи програмного забезпечення або технічної трансформації. Тому вони мають оцінюватися разом зі змістом, контрольними сумами, журналами подій, історією версій, даними пристрою та іншими об'єктивними відомостями. З іншого боку, конкретне й технічно обґрунтоване заперечення щодо зміни цифрового об'єкта повинно зумовлювати поглиблення його перевірки.

У кримінальних провадженнях щодо економічної злочинності особливо гостро постає проблема **великих цифрових масивів**. Банківські, бухгалтерські та корпоративні дані можуть охоплювати сотні тисяч або мільйони записів. У такій ситуації доказове значення має вже не лише автентичність окремо відібраного файла, а й спосіб, у який його було знайдено

та виокремлено з первинного масиву. Дослідження цифрового розкриття матеріалів у кримінальному процесі підтверджують, що великий обсяг даних потребує спеціальних механізмів судового управління та реальної, а не формальної можливості сторони захисту працювати з відповідним масивом [12].

У зв'язку з цим вважаємо перспективним виділення **цілісності відбору** як самостійного елемента перевірки доказової інформації у цифровій формі. Під час оцінювання документа, повідомлення, транзакції чи сукупності корпоративних записів має значення не лише те, чи є конкретний елемент автентичним, а й те, з якого первинного масиву його отримано, за якими критеріями здійснювався пошук, які ключові слова або алгоритми застосовувалися, які дані були виключені та чи була сторона захисту здатна здійснити альтернативний пошук. Інакше навіть автентичний фрагмент може створити викривлену фактичну картину.

З цілісністю відбору безпосередньо пов'язані доступ до вихідних даних та відтворюваність технічної процедури. Якщо доказовий результат утворено шляхом дешифрування, автоматизованого пошуку, фільтрації або спеціального цифрового аналізу, перевірка лише кінцевого результату створює небезпеку так званої «чорної скриньки». У сучасній зарубіжній доктрині обґрунтовується необхідність документування надійності не лише самої технології, а й методу та конкретного способу його застосування [10; 11].

Це не означає абсолютного права сторони на необмежений доступ до будь-якого цифрового масиву. Захист приватності інших осіб, професійної таємниці, безпеки інформаційних систем або методів розслідування може обґрунтовувати певні обмеження. Проте, на нашу думку, у такому випадку має існувати **функціонально рівноцінний механізм перевірки**: контрольований доступ спеціаліста, незалежна експертиза, технічний звіт із достатнім описом процедури, можливість повторити пошуковий запит або інший спосіб перевірити основу фактичного висновку. Такий підхід відповідає загальній тенденції розвитку європейських стандартів справедливого судового розгляду щодо технологічно складних доказів.

Особливо показовою у цьому аспекті є справа *Yüksel Yalçınkaya v. Türkiye*, у якій ЄСПЛ пов'язав справедливість використання складної цифрової інформації з реальною

можливістю перевірки її основи та з необхідністю належної судової відповіді на істотні заперечення сторони [15]. На рівні права Європейського Союзу у справі *M.N. (EncroChat), C-670/22* Суд ЄС розмежував первинне одержання цифрових даних та їх подальшу транскордонну передачу і використання. Саме іноземне походження інформації не усуває необхідності забезпечити стороні реальну можливість її оспорити, а суду – здійснити належний контроль [14]. Проблематика EncroChat раніше була нами проаналізована також із порівняльно-правових і кримінальних процесуальних позицій [6].

На основі зазначеного доцільно розглядати судову перевірку доказової інформації у цифровій формі як **інтегрований процес**, що охоплює три взаємопов'язані рівні. Перший становить правова і процесуальна легітимність, до якої належать походження інформації, правова підстава та спосіб одержання, компетентність відповідного органу, дотримання судового контролю, а також атрибуція. Другий рівень охоплює технічну і пізнавальну надійність: автентичність, цілісність, метадані, простежуваність, ланцюг збереження, повноту та контекст, цілісність відбору, відтворюваність і доступ до вихідних даних. Третій рівень становить змагальна та судова перевірка, що передбачає практичну можливість сторони дослідити й оспорити матеріал, його узгодженість з іншими доказами, визначення доказової ваги та належне мотивування судового рішення.

Такий підхід дає змогу уникнути двох однаково небезпечних крайнощів. З одного боку, неприпустимим є технічний формалізм, коли будь-яка відмінність носія, метаданих або способу копіювання автоматично тлумачиться як підстава для втрати доказового значення. З іншого боку, цифрове походження інформації не повинно створювати презумпції її об'єктивності або безпомилковості. Автоматизований характер створення запису не усуває ризиків неправильного налаштування системи, помилкового зв'язування даних, неповного відбору або невірної інтерпретації.

Важливим наслідком запропонованого підходу є відмова від універсальної бінарної реакції «допустимий або недопустимий» щодо будь-якого дефекту цифрової інформації. Правовий наслідок має залежати від того, яку саме функцію порушено та наскільки істотним є це порушення. Несуттєвий

технічний дефект, який не впливає на зміст, походження та можливість перевірки інформації, не повинен автоматично зумовлювати її виключення. Обґрунтовані сумніви щодо автентичності або атрибуції можуть потребувати поглибленої перевірки. Неповнота, втрата контексту або неможливість надійно пов'язати інформацію з конкретною особою можуть знижувати її доказову вагу. Натомість фундаментальна незаконність одержання або така неможливість ефективного оспорювання, яка унеможливлює справедливе використання матеріалу, здатна зумовити його недопустимість чи неврахування залежно від застосовного правового режиму [8; 14; 15].

Отже, сучасний етап розвитку доказового права підтверджує наступність основної методологічної закономірності, яка простежується від проблем використання результатів оперативно-розшукової діяльності до доказів у цифровій формі: **інформаційна цінність відомостей ще не тотожна їх процесуальній придатності**. Цифрова форма не створює самостійної процесуальної природи доказу, але істотно змінює структуру ризиків його одержання, перевірки та оцінки. У кримінальних провадженнях щодо економічних правопорушень предметом перевірки має бути не лише окремий файл, документ або транзакція, а весь доказовий шлях від виникнення цифрової інформації та її одержання до атрибуції, відбору, технічної трансформації, змагального оспорювання й мотивованого визначення її доказового значення. Саме така інтегрована модель здатна поєднати ефективність протидії сучасній економічній злочинності з належними стандартами кримінального процесуального доказування та справедливого судового розгляду.

Список використаних джерел

1. Погорецький М. А. Співвідношення пізнання і доказування у кримінальному процесі та місце в них оперативно-розшукової діяльності. *Питання боротьби зі злочинністю :* зб. наук. праць. № 7. Харків : Право, 2003. С. 114–132.

2. Погорецький М. А. *Проблеми використання матеріалів оперативно-розшукової діяльності в кримінальному процесі :* монографія. Київ : РВВ НА СБУ, 2004. 336 с.

3. Погорецький М. А. Судовий контроль та прокурорський нагляд за використанням протоколів оперативно-розшукових

заходів як доказів у кримінальному процесі. *Вісник Верховного Суду України*. 2003. № 2. С. 32–38.

4. Кальман О. Г., Погорецький М. А. Рейдерство: причини та заходи протидії. *Вісник Запорізького юридичного інституту Дніпропетровського державного університету внутрішніх справ*. 2009. № 3. С. 150–160.

5. Погорецький М. А., Старенький О. С. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України*. 2018. № 8. С. 85–106. URL: http://nbuv.gov.ua/UJRN/prukr_2018_8_9

6. Погорецький М. А. Використання даних EncroChat у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий електронний журнал*. 2025. № 8. С. 223–229. DOI: https://doi.org/10.32782/2524-0374/2025-8/46

7. Погорецький М. А. Цифрові (електронні) докази та цифрова (електронна) форма доказів: розмежування понять і його значення для кримінального процесуального доказування. *Аналітично-порівняльне правознавство*. 2026. № 1. Ч. 3. С. 115–125. DOI: https://doi.org/10.24144/2788-6018.2026.01.3.18

8. Погорецький М. А. Допустимість доказів у практиці Касаційного кримінального суду у складі Верховного Суду: перехід від формальної законності до процесуальної доброчесності. *Вісник Національної академії правових наук України*. 2026. Т. 33. № 1. С. 267–302. DOI: https://doi.org/10.31359/1993-0909-2026-33-1-267

9. Сергєєва Д. Б. Виявлення і документування способів учинення службових правопорушень: методика, тактика, цифрові сліди та ланцюг збереження доказів. *Науковий вісник Ужгородського Національного Університету. Серія «Право»*. 2025. Вип. 91. Ч. 4. С. 438–451. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.60

10. Stoykova R. A. A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*. 2024. Vol. 55. Article 106040. DOI: https://doi.org/10.1016/j.clsr.2024.106040

11. Stoykova R., Franke K. Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*. 2023. Vol. 45. Article 301554. DOI: https://doi.org/10.1016/j.fsidi.2023.301554

12. Turner J. I. Managing digital discovery in criminal cases. *Journal of Criminal Law and Criminology*. 2019. Vol. 109. No. 2. P. 237–312. URL: https://scholarlycommons.law.northwestern.edu/jclc/vol109/iss2/3

13. Постанова Об'єднаної палати Касаційного кримінального суду у складі Верховного Суду від 29 березня 2021 р. у справі № 554/5090/16-к, провадження № 51-1878кмо20. ЄДРСР. № 96074938. URL: https://reyestr.court.gov.ua/Review/96074938

14. Court of Justice of the European Union. *M.N. (EncroChat)*, Case C-670/22, Judgment of 30 April 2024, ECLI:EU:C:2024:372.

15. European Court of Human Rights. *Yüksel Yalçınkaya v. Türkiye* [GC], Application no. 15669/20, Judgment of 26 September 2023. HUDOC No. 001-227636.

Рижков Едуард Володимирович,
професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ШІ-АГЕНТИ ЯК ІНСТРУМЕНТ АВТОМАТИЗАЦІЇ КРИМІНАЛЬНОГО АНАЛІЗУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Фундаментальною перешкодою для оперативного розкриття та всебічного розслідування злочинів у цифрову епоху є біологічні та психологічні обмеження людського аналітичного апарату. Концепт «інформаційного перевантаження», вперше введений у науковий обіг соціологом Бертрамом Гроссом, описує стан системи, за якого вхідний потік даних суттєво перевищує обчислювальні та пропускні можливості системи щодо їх обробки та засвоєння [1, с. 23]. У контексті індивідуальної роботи кримінального аналітика, слідчого або оперативника цей феномен трансформується у когнітивне перевантаження – стан, коли вимоги до обробки інформації виснажують доступні когнітивні ресурси та ємність робочої пам'яті людини [2, с. 1178]. На сьогодні можливості генерації та збору цифрових слідів багаторазово перевищують фізичні можливості людського мозку щодо їх обробки.