УДК 343.14:004.9
DOI https://doi.org/10.51989/NUL.2026.3.23

ВІД ВІДКРИТИХ ЦИФРОВИХ ДАНИХ ДО ДОКАЗУ: АВТОРСЬКА МОДЕЛЬ ПРОЦЕСУАЛЬНОЇ ТРАНСФОРМАЦІЇ РЕЗУЛЬТАТІВ OSINT У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Погорецький Микола Анатолійович,
orcid.org/0000-0003-0936-0929
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
перший проректор
Київського національного університету імені Тараса Шевченка

У статті обґрунтовано авторську модель процесуальної трансформації результатів OSINT у кримінальному провадженні. Вихідним є положення про те, що доказове значення не становить первинної властивості відкритої цифрової інформації: відкритість характеризує режим доступу до джерела, цифрова форма – спосіб існування та відтворення інформації, а аналітична переконливість – результат її інтерпретації. Метою дослідження є побудова цілісної доктринальної конструкції, яка пояснює перехід від виявленого цифрового матеріалу до фактичних даних, належно сформованих, перевірених, оцінених і використаних для обґрунтування процесуального рішення. Методологічну основу становлять діалектичний, системно-структурний, формально-юридичний, функціональний, герменевтичний методи та метод доктринального моделювання. Шістнадцять етапів трансформації згруповано у п'ять взаємопов'язаних рівнів: інформаційно-пошуковий, техніко-верифікаційний, аналітичний, кримінальний процесуальний і змагально-судовий. Розкрито значення збереження первинного цифрового матеріалу, встановлення походження, розмежування автентичності, цілісності й достовірності змісту, документування операцій та забезпечення відтворюваності. Доведено, що мультисенсорні й алгоритмічно сформовані результати мають похідний характер і не можуть підміняти первинні інформаційні потоки. Запропоновано поняття стандартизованого доказового пакета як організаційно-методичної системи матеріалів, яка забезпечує простежуваність і перевірюваність, але не є новим процесуальним джерелом доказів. Обґрунтовано, що процесуальне оформлення є обов'язковою, але не самодостатньою фазою трансформації, а остаточне доказове значення формується після розкриття матеріалів сторонам, реальної можливості їх змагального оспорювання, безпосереднього судового дослідження та мотивованої оцінки. Сформульовано положення про диференційовану інтенсивність трансформації, яка залежить від виду джерела, складності матеріалу, способу його одержання, технології опрацювання та характеру процесуального рішення.

Ключові слова: *OSINT, відкриті цифрові дані, кримінальне процесуальне доказування, процесуальна трансформація, цифрова форма доказової інформації, первинний цифровий матеріал, мультисенсорні дані, алгоритмічний аналіз, доказовий пакет, змагальна перевірка.*

Pohoretskyi Mykola. From Open Digital Data to Evidence: an Authorial Model of the Procedural Transformation of OSINT Results in Criminal Proceedings

The article substantiates an authorial model of the procedural transformation of OSINT results in criminal proceedings. The study proceeds from the proposition that evidentiary significance is not an inherent property of open digital information: openness characterises the access regime of a source, digital form describes the manner in which information exists and is reproduced, whereas analytical persuasiveness is the outcome of interpretation. The purpose of the study is to construct an integrated doctrinal framework explaining the transition from discovered digital material to factual data that have been properly formed, verified, assessed and used to substantiate a procedural decision. The methodology combines dialectical, system-structural, formal-legal, functional and hermeneutic methods with doctrinal modelling. Sixteen stages of transformation are grouped into five interrelated levels: information-search, technical-verification, analytical,

criminal-procedural, and adversarial-judicial. The article explains the significance of preserving the primary digital material, establishing provenance, distinguishing authenticity, integrity and substantive reliability, documenting operations and ensuring reproducibility. It is demonstrated that multisensor and algorithmically generated results are derivative and may not replace primary information streams. The concept of a standardised evidentiary package is proposed as an organisational and methodological system of materials ensuring traceability and verifiability without constituting a new procedural source of evidence. Procedural formalisation is shown to be a mandatory but not self-sufficient phase of transformation. The evidentiary significance of an OSINT result is completed only after disclosure to the parties, a genuine opportunity for adversarial challenge, direct judicial examination and reasoned assessment. The article also formulates the principle of differentiated intensity of transformation, according to which the scope and depth of required operations depend on the type of source, the complexity of the material, the manner of acquisition, the processing technology and the nature of the procedural decision.

Key words: *OSINT, open digital data, criminal procedural evidence, procedural transformation, digital form of evidentiary information, primary digital material, multisensor data, algorithmic analysis, evidentiary package, adversarial examination.*

Постановка проблеми. Цифровізація суспільних відносин, розвиток соціальних мереж, електронних реєстрів, геоінформаційних платформ, відеохостингів та інших цифрових середовищ істотно розширили масив інформації, потенційно значущої для кримінального провадження. Події, особи й об’єкти дедалі частіше залишають цифрові відображення у вигляді повідомлень, фото-, відео- й аудіоматеріалів, метаданих, геолокаційних позначок, супутникових знімків та відомостей про інформаційні зв’язки. За таких умов OSINT набув значення методологічно організованої діяльності з виявлення, збирання, фіксації, збереження, перевірки, зіставлення й інтерпретації інформації з відкритих цифрових джерел [1–2].

Результати OSINT використовуються для встановлення часу й місця події, ідентифікації осіб та об’єктів, перевірки цифрових матеріалів, реконструкції послідовності дій і виявлення взаємозв’язків між окремими обставинами. Поряд із матеріалами вебсайтів і соціальних мереж дедалі ширше застосовуються супутникові, геопросторові, телеметричні, акустичні та інші сенсорні дані, а також результати їх алгоритмічного опрацювання [3–7]. Це розширює пізнавальні можливості, але ускладнює встановлення походження матеріалів, розмежування первинних даних і похідних аналітичних продуктів та перевірку сформованих висновків.

Зростання інформаційної цінності результатів OSINT не означає автоматичного набуття ними доказового значення. У межах розробленої нами концепції кримінального процесуального доказування ми виходимо з того, що доказ формується у нормативно регламентованій пізнавально-практичній і розумово-логічній діяльності уповноважених суб’єктів, спрямованій на формування, перевірку, оцінку та використання фактичних даних для обґрунтування процесуальних рішень [8–9]. Цифрова форма визначає спосіб існування, фіксації, передавання, збереження та відтворення інформації, але сама собою не створює нового універсального виду доказів [10].

Основна суперечність полягає в тому, що відкриті цифрові матеріали та результати їх аналітичного опрацювання вже широко використовуються для встановлення обставин кримінального провадження, однак у кримінальній процесуальній доктрині відсутня цілісна модель переходу від відкритої цифрової інформації до належно сформованих, перевірених, оцінених і використаних у доказуванні фактичних даних. Унаслідок цього змішуються відкрите цифрове джерело, розміщені в ньому дані, первинний цифровий матеріал, результат OSINT-дослідження, аналітичний документ, процесуальне джерело доказів і доказ. При цьому карта, хронологія, реконструкція події чи алгоритмічно сформований висновок є похідними від первинних цифрових і сенсорних даних, залежать від критеріїв відбору, параметрів опрацювання та інтерпретаційних рішень дослідника, а тому не можуть підміняти вихідні матеріали [4–7].

КПК України, наукова доктрина та технічні стандарти містять важливі положення щодо доказів, комп'ютерних даних, їх копіювання, збереження, ідентифікації та перевірки [1–2; 11–18]. Проте вони залишаються недостатньо інтегрованими й не утворюють завершеної конструкції переходу від відкритої цифрової інформації до доказу. Отже, наукова проблема полягає не у визнанні результатів OSINT новим видом доказів, а в розробленні цілісної доктринальної моделі їх процесуальної трансформації, яка поєднує інформаційно-пошуковий, техніко-верифікаційний, аналітичний, кримінальний процесуальний і змагально-судовий рівні.

Стан наукової розробленості проблеми. Теоретичним підґрунтям дослідження є розроблена нами концепція кримінального процесуального доказування, у межах якої доказування розглядається як цілісна пізнавально-практична, розумово-логічна й нормативно регламентована діяльність, спрямована на формування, перевірку, оцінку та використання доказів [8–9]. Ці положення розвинуто у працях про верховенство права, процесуальну доброчесність, цифрову форму доказової інформації, застосування цифрових технологій у провадженнях щодо злочинів проти основ національної безпеки та процесуальне використання матеріалів оперативно-розшукової діяльності [10; 19–22]. Нормативну основу становлять конституційні гарантії, приписи КПК України й законодавства про захист персональних даних [11; 23–24].

Методологію роботи з відкритою цифровою інформацією систематизовано у Протоколі Берклі, національному підручнику з OSINT, науково-практичному пораднику та спеціальному дослідженні цифрових даних із відкритих джерел [1–2; 25–26]. Ці праці визначають вимоги до планування, пошуку, фіксації, збереження, перевірки й представлення матеріалів, однак мають переважно методичний характер і самі собою не встановлюють їх процесуального статусу.

Українська доктрина розкриває властивості цифрової інформації, особливості електронної форми доказів, цифровізацію кримінального провадження, способи збирання та використання електронних матеріалів, а також техніко-криміналістичні й теоретико-практичні аспекти їх дослідження [12–15; 27–28]. Безпосередньо проблемам відкритих джерел, OSINT, документуванню воєнних злочинів, використанню медіаданих і межам цифровізації доказування присвячено праці [29–34].

У зарубіжній доктрині системно висвітлено використання відкритої інформації для розслідування і документування міжнародних злочинів, її представлення в суді, ризики людських та машинних упереджень, втрату метаданих і контексту, проблеми відбору, розкриття та допустимості великих цифрових масивів [3–6; 35–36]. Технічні правила ідентифікації, копіювання, збереження, контролю цілісності та документування операцій закріплено у ДСТУ ISO/IEC 27037:2017, рекомендаціях NIST і стандартах SWGDE [16–18]. Національна та міжнародна судова практика підтверджує можливість використання відкритих цифрових, супутникових і відеоматеріалів, але водночас засвідчує залежність їх значення від належної фіксації, стадії провадження, застосовного стандарту доказування та кореляції з іншими джерелами [37–41]. Окремий напрям становить інтеграція мультисенсорних даних та результатів їх інтелектуального аналізу [7].

Отже, наявний доробок сформував теоретичні, нормативні, методичні й технічні засади роботи з цифровою інформацією, однак не поєднав їх у єдиний процесуальний цикл. Невирішеним залишається питання про послідовність переходу від первинного відкритого цифрового матеріалу до похідного аналітичного результату, його належного процесуального формування, змагальної перевірки та судової оцінки. Заповнення цієї прогалини шляхом розроблення авторської багаторівневої моделі становить безпосереднє завдання статті.

Мета, завдання і методологія дослідження. *Метою* статті є розроблення авторської багаторівневої моделі процесуальної трансформації результатів OSINT, яка розкриває закономірності переходу від відкритої цифрової інформа-

ції до фактичних даних, належно сформованих, перевірених, оцінених і використаних для обґрунтування процесуальних рішень. Для цього визначено структуру трансформації, систематизовано її операції за п'ятьма рівнями, розмежовано первинний цифровий матеріал, результат OSINT-дослідження та похідний аналітичний продукт, з'ясовано значення збереження, перевірки, процесуального оформлення, розкриття, змагального дослідження й судової оцінки, а також обґрунтовано диференційовану інтенсивність відповідних процедур.

Методологічну основу становлять діалектичний, системно-структурний, формально-юридичний, функціональний, герменевтичний методи та метод доктринального моделювання. Вони використані для розкриття переходу інформації до доказового використання, побудови п'ятирівневої структури, аналізу положень КПК України [11], розмежування ключових понять і поєднання теорії доказування, методології OSINT та технічних підходів до цифрових і сенсорних даних [1–10; 12–20; 36].

Виклад основного матеріалу. ***Теоретична основа авторської моделі.*** У межах розробленої нами концепції доказ не є готовим інформаційним об'єктом, що існує незалежно від установленої законом діяльності. Його формування передбачає єдність фактичних даних, належного процесуального джерела, законного способу одержання, можливості перевірки, оцінки та використання для обґрунтування процесуального рішення [8–9]. Тому виявлення у відкритому цифровому середовищі відомостей про кримінально значущу подію ще не означає формування доказу: на цьому етапі існує лише потенційно релевантна інформація, яка потребує подальшого збереження, перевірки, аналітичного опрацювання та процесуального формування.

Об'єктивне існування інформації про подію слід відрізняти від її доказового значення у конкретному провадженні. Цифровий запис, фотозображення, відеофайл, супутниковий знімок або публікація можуть виникнути до початку кримінального провадження і незалежно від його учасників. Доказового значення вони набувають лише внаслідок діяльності, у межах якої встановлюються їх походження, зв'язок із предметом доказування, цілісність, достовірність змісту, процесуальне джерело та придатність для обґрунтування рішення.

Процесуальна доброчесність потребує також послідовного розмежування інформаційного змісту і ступеня його опосередкованості. Первинний файл може безпосередньо відображати певний об'єкт або подію; метадані – містити технічні характеристики; спеціаліст – установлювати ознаки цілісності; аналітик – формулювати висновок про місце, час або зв'язок між об'єктами. Ці результати мають різну пізнавальну природу й не можуть подаватися як єдиний безпосередньо встановлений факт. Змішування вихідних даних, технічних операцій та інтерпретації підвищує ризик надання припущенню категоричного характеру і позбавляє іншу сторону можливості визначити, яка саме частина висновку ґрунтується на первинному матеріалі, а яка – на методологічному виборі дослідника [3–6; 19–20].

Другим положенням є розмежування цифрових доказів і цифрової форми доказової інформації. Цифрова форма характеризує спосіб створення, існування, фіксації, передавання, копіювання, збереження та відтворення інформації, проте сама собою не утворює нового універсального виду доказів [10]. Відкриті цифрові дані, первинний матеріал, аналітична карта, хронологія, реконструкція або алгоритмічно сформований висновок не можуть визнаватися доказами лише через цифрову форму; їх процесуальний статус визначається змістом, походженням, способом одержання та закріпленням у передбаченому КПК України джерелі [10–11].

Третім положенням є процесуальна доброчесність доказової діяльності. Вона вимагає оцінювати не лише формальне дотримання окремої процедури, а законність і справедливість усього шляху формування доказу, його правову визначеність, пропорційність, змагальність, можливість ефективного оспорювання та належний судовий контроль [19–20]. Стосовно OSINT це означає збереження

прозорого зв’язку між відкритим джерелом, первинним матеріалом, операціями перевірки, похідним аналітичним результатом і процесуально оформленими фактичними даними.

Отже, доказове значення не є внутрішньо притаманною властивістю цифрової інформації. Відкритість свідчить про режим доступу, цифрова форма – про технологічний спосіб існування, технічна цілісність – про незмінність після взяття під контроль, а аналітична переконливість – про логічну узгодженість інтерпретації. Жодна з цих характеристик окремо не створює доказу. Його значення формується поступово внаслідок виявлення, збирання, збереження, перевірки, аналітичного опрацювання, належного оформлення, розкриття, змагального дослідження та оцінки [1–2; 16–18].

Загальна структура процесуальної трансформації результатів OSINT. Процесуальну трансформацію ми розглядаємо не як одноразове долучення файла, скриншота чи звіту, а як нормативно впорядкований, організаційно й технічно забезпечений процес переходу відкритої цифрової інформації до фактичних даних, придатних для перевірки, оцінки та використання. Шістнадцять взаємопов’язаних етапів за функціональним призначенням об’єднано у п’ять рівнів: інформаційно-пошуковий, техніко-верифікаційний, аналітичний, кримінальний процесуальний і змагально-судовий [1–20; 36].

Модель не є суто лінійною: окремі операції можуть здійснюватися паралельно, повторюватися або зумовлювати повернення до попереднього рівня. Технічна перевірка може потребувати пошуку первиннішого джерела, аналітичне опрацювання – додаткових матеріалів, а змагальне оспорювання – повторного дослідження чи експертизи. Водночас кожний наступний рівень спирається на результати попереднього і не усуває необхідності самостійно перевіряти законність та обґрунтованість виконаних операцій.

Інформаційно-пошуковий рівень охоплює виникнення або оприлюднення інформації, її виявлення, первинне оцінювання та збирання. Техніко-верифікаційний – збереження первинного матеріалу, встановлення походження, технічну і змістовну перевірку. Аналітичний – систематизацію й інтерпретацію перевірених цифрових і сенсорних даних та формування стандартизованого доказового пакета. Кримінальний процесуальний рівень забезпечує закріплення фактичних даних у передбаченому законом джерелі. Змагально-судовий охоплює розкриття, оспорювання, судове дослідження, оцінку та використання у процесуальному рішенні.

Інформаційно-пошуковий рівень процесуальної трансформації результатів OSINT. Цей рівень створює вихідну інформаційну основу і ще не формує доказ. Цифрова інформація, як правило, виникає поза кримінальним провадженням і може генеруватися особами, організаціями, державними органами, платформами, супутниками, камерами або іншими системами. Уже під час створення чи оприлюднення матеріал може бути стиснутий, перекодований, помилково датований, повторно поширений або змінений, тому сам факт його існування чи публічної доступності не підтверджує автентичності та достовірності [1–2; 5].

Виявлення полягає у встановленні існування конкретного матеріалу, його місцезнаходження, режиму доступу та можливого зв’язку з досліджуваними обставинами. Пошук має бути цілеспрямованим: доцільно визначити інформаційне завдання, часові, предметні й територіальні межі, релевантні категорії джерел та очікуване значення результату. Для подальшої перевірки фіксуються пошукові запити, ключові слова, фільтри, послідовність переходів, назва і версія застосованого програмного засобу [1–2].

Первинне оцінювання має попередній і ймовірнісний характер. Воно спрямоване на визначення потенційної належності, інформаційної цінності, режиму доступу, ризику втрати та необхідності невідкладного збереження. Збіг псевдоніма, геолокаційної позначки або іншого цифрового ідентифікатора може бути підставою для подальшої перевірки, але не для категоричного висновку про особу, місце, час чи достовірність події.

Збирання на цьому рівні означає законне одержання і первинну фіксацію матеріалу в обсязі, достатньому для його збереження та подальшого дослідження. Воно може охоплювати завантаження файла, архівування вебсторінки, скриншоти, відеозапис екрана, фіксацію URL, ідентифікаторів, дати й часу доступу, характеристик профілю, каналу або платформи та доступного контексту [1–2; 16–18]. Перевага надається максимально повному збереженню цифрового об'єкта; скриншот є лише допоміжним засобом і не підміняє файла, вебархівованої сторінки чи метаданих.

Належна первинна фіксація передбачає збереження не лише змісту, а й контексту існування цифрового об'єкта. Поряд із повною URL-адресою доцільно фіксувати постійний ідентифікатор публікації, назву профілю або каналу, видимі ознаки редагування, попередні й наступні повідомлення, спосіб переходу до матеріалу, дату, час і часовий пояс доступу. Необхідно розмежовувати час створення файла, час відображеної події, час завантаження на платформу, час публікації та час доступу дослідника. Фіксація останнього підтверджує лише наявність матеріалу на ресурсі у визначений момент і не встановлює автоматично часу його створення. Якщо платформа дозволяє законне завантаження файла, перевага надається такому способу, оскільки скриншот переважно відображає лише видиму частину екрана і не зберігає повного технічного та змістового контексту [1–2; 16–18].

Первинним для конкретного OSINT-дослідження є матеріал у тому стані й контексті, в якому його фактично виявлено та взято під контроль, навіть якщо платформа раніше його стискала або перекодовувала. Результатом рівня є виявлений, попередньо оцінений, законно зібраний і первинно зафіксований цифровий матеріал, потенційний зв'язок якого з обставинами провадження потребує подальшої перевірки.

Техніко-верифікаційний рівень процесуальної трансформації результатів OSINT. Цей рівень охоплює збереження первинного матеріалу, встановлення його походження, технічну та змістовну перевірку. Первинний об'єкт має зберігатися окремо від робочих і похідних копій. Доказова копія залишається незмінною, а робоча використовується для перегляду, конвертації, аналізу метаданих та інших операцій. Разом із матеріалом зберігаються URL, дата й час доступу, контекст, доступні метадані, технічні характеристики, відомості про програмні засоби та журнал істотних операцій [1–2; 16–18].

Встановлення походження спрямоване на з'ясування інформаційного й технічного шляху матеріалу: можливого автора або системи створення, першої доступної публікації, облікових записів і платформ поширення, а також попередніх перетворень. Пошук найранішої публікації, аналіз метаданих, цифрових ідентифікаторів, зіставлення копій і зворотний пошук зображень дають змогу реконструювати інформаційну генеалогію, проте встановлення ресурсу чи акаунта не завжди означає встановлення фактичного автора [1–2; 5].

Технічна перевірка охоплює аналіз структури і формату файла, метаданих, кодеків, ознак стиснення, перекодування, редагування чи пошкодження, порівняння копій та перевірку хеш-значень [11–18]. Хешування підтверджує незмінність цифрового об'єкта між контрольованими станами, але не встановлює автора, місце й час створення, законність одержання або правдивість змісту. Метадані також можуть бути змінені чи перезаписані, тому оцінюються у взаємозв'язку з іншими матеріалами.

Технічне дослідження має здійснюватися із збереженням доказової копії та документуванням кожного істотного перетворення робочої копії. Конвертація формату, стабілізація відео, збільшення зображення, виділення кадру, корекція яскравості або нанесення позначок можуть бути методично виправданими, однак їх результат не повинен подаватися як первинний матеріал. Хеш-значення доцільно обчислювати для взятого під контроль файла та контрольних копій із зазначенням алгоритму, часу й програмного засобу. Водночас збіг хеш-значень доводить лише незмінність між двома контрольованими станами. Він не

виключає того, що файл був змінений до моменту збереження, і не підтверджує правдивості відображеної події [5; 16–18].

Змістовна перевірка цифрового матеріалу має спиратися на сукупність взаємно узгоджених методів. Геолокація може включати зіставлення будівель, доріг, рельєфу, рослинності, дорожніх знаків, ліній електропередач, цифрових карт і супутникових знімків. Хронолокація потребує розмежування різних часових позначок та врахування погодних умов, освітлення, положення тіней, сезонних ознак, телеметричних або акустичних даних. Зворотний пошук дає змогу виявити попередні публікації та повторне використання матеріалу, але найраніший знайдений результат не завжди є первинним. Автоматизовані детектори монтажу чи deepfake також не є безпомилковими; їх висновки залежать від моделі, версії програми і якості файла та за потреби мають перевірятися незалежним фахівцем [1–7].

Змістовна перевірка спрямована на відповідність відображених відомостей фактичним обставинам. Вона може включати геолокацію, хронолокацію, зіставлення архітектури, рельєфу, погодних умов і тіней, аналіз супутникових зображень, зворотний пошук, перевірку монтажу або синтетичного створення та кореляцію з документами, показаннями й незалежними сенсорними потоками [1–7]. Перевірка має охоплювати альтернативні пояснення, а формальна множинність публікацій не вважається незалежним підтвердженням, якщо вони походять від одного джерела.

На цьому рівні необхідно чітко розмежовувати походження, автентичність, цілісність і достовірність змісту. Походження відповідає на питання про джерело та інформаційний шлях; автентичність – про відповідність матеріалу тому об’єкту, за який його подають; цілісність – про відсутність недокументованих змін після взяття під контроль; достовірність – про відповідність змісту фактичним обставинам. Встановлення однієї властивості не доводить автоматично інших. Результатом рівня є збережений і перевірений матеріал із документованими операціями, обґрунтованими відомостями про походження та чітко визначеними межами висновків.

Аналітичний рівень процесуальної трансформації результатів OSINT. Аналітичний рівень охоплює систематизацію, зіставлення, інтерпретацію та узагальнення первинних матеріалів і результатів їх перевірки. Його метою є встановлення інформаційних зв’язків, просторово-часових характеристик, послідовності подій, тотожності осіб та об’єктів, перевірка версій і побудова обґрунтованої реконструкції. Визначальною вимогою є розмежування первинних відомостей, результатів технічних операцій, аналітичних припущень і підсумкових висновків [1–7].

Особливе місце посідають мультисенсорні дані – взаємопов’язана сукупність відомостей від цифрових, технічних і сенсорних систем, синхронізованих за часом, місцем та об’єктом [7]. OSINT і сенсорні дані не є тотожними: відкриті сенсорні матеріали можуть досліджуватися методами OSINT, однак включення закритих потоків до спільного масиву не змінює їх походження та правового режиму. Кожний потік підлягає окремій ідентифікації й перевірці, а інтеграція потребує врахування часових, просторових та об’єктних похибок.

Мультисенсорна інтеграція потребує не лише змістовного зіставлення, а й часової, просторової та об’єктної синхронізації. Системний час сенсора, час передавання, час створення файла й час оприлюднення можуть не збігатися; координати можуть належати до різних систем і містити різну похибку; формальний збіг часу чи місця ще не доводить, що потоки відображають той самий об’єкт. Тому в аналітичному документі мають бути зазначені способи приведення даних до спільної системи, похибки й альтернативні варіанти. Так само кілька публікацій можуть відтворювати один первинний файл, а різні звіти – ґрунтуватися на тому самому супутниковому знімку. Реальну доказову переконливість підвищує не кількість повторів, а кореляція справді незалежних інформаційних потоків та встановлення їх інформаційної генеалогії [4–7].

Алгоритмічно сформований результат є похідним продуктом автоматизованого або частково автоматизованого опрацювання. Його зміст залежить від повноти вхідних даних, критеріїв відбору, версії програмного засобу, параметрів, порогових значень, послідовності операцій і ролі людини [4–7]. Автоматизація не надає результату наперед установленої об'єктивності. Для перевірюваності необхідно зберігати вхідні та істотні проміжні дані, фіксувати програмне середовище, параметри, журнали операцій, відомі похибки та змістовний контроль людиною.

Процесуальна прозорість алгоритмічного аналізу передбачає можливість установити повну назву програми, розробника і версію, склад вхідних даних, критерії їх включення та виключення, параметри і порогові значення, послідовність попереднього очищення чи нормалізації, журнали операцій, проміжні результати та участь людини. Особливо важливо зберігати не лише збіги, що підтвердили основну версію, а й матеріали, відхилені як нерелевантні або суперечливі, оскільки вибіркове збереження унеможливлює перевірку повноти аналізу. Якщо система є недетермінованою, самонавчальною або постійно оновлюється, це має бути зазначено як обмеження відтворюваності. Чим складнішим і менш прозорим є алгоритм та чим вагомішим його результат для рішення, тим вищою є потреба в незалежній спеціальній або експертній перевірці [3–7].

Карта, схема, хронологія, таблиця зв'язків, мультисенсорна модель або алгоритмічна класифікація не підміняють первинних матеріалів. Аналітичний продукт повинен містити достатній опис завдання, джерел, критеріїв відбору, методів, параметрів, проведених операцій, альтернативних версій, похибок і меж упевненості. Його переконливість визначається не наочністю візуалізації, а прозорістю шляху формування та можливістю незалежної перевірки.

Організаційним підсумком рівня є стандартизований доказовий пакет – система первинних цифрових матеріалів, відомостей про походження, технічної документації, результатів перевірки й аналітичних документів, призначена для забезпечення цілісності, простежуваності, відтворюваності та змагальної перевірки [1–2; 5; 7; 16–18]. До нього можуть входити первинний матеріал, URL і часові позначки, метадані, хеш-значення, доказова та робоча копії, журнал операцій, опис методології, проміжні результати й відомості про виконавців. Пакет не є новим видом доказу або самостійним процесуальним джерелом і не легітимізує матеріал, одержаний незаконно.

Стандартизований доказовий пакет залежно від характеру дослідження може охоплювати первинний файл або вебархівовану сторінку, опис джерела, URL і часові позначки, метадані, контрольні значення, доказову та робочу копії, журнал операцій, опис методології, результати встановлення походження, технічної й змістовної перевірки, істотні проміжні матеріали, аналітичний документ і відомості про осіб, які виконували відповідні операції. Для мультисенсорного дослідження окремо зберігаються первинні дані кожного потоку, характеристики сенсорів, способи синхронізації та межі похибки; для алгоритмічного – програмне середовище, параметри й результати контролю відтворюваності. Термін «стандартизований» означає єдину логіку організації, а не механічну однаковість пакетів. Його обсяг має бути достатнім для простеження шляху від первинного об'єкта до висновку, але не надає компонентам наперед установленої сили [1–2; 5; 7; 16–18].

Отже, результатом аналітичного рівня є не готовий доказ, а структурований, методологічно обґрунтований і перевірюваний похідний продукт, збережений у нерозривному зв'язку з первинними цифровими й сенсорними даними.

Кримінальний процесуальний рівень процесуальної трансформації результатів OSINT. На цьому рівні фактичні дані, виявлені, збережені, перевірені або аналітично опрацьовані із застосуванням OSINT, вводяться до кримінального провадження через передбачене КПК України процесуальне джерело [8–11]. Процесуальне оформлення не є формальним посвідченням уже готового доказу, а обов'язковою фазою його

формування, під час якої визначаються суб'єкт, правова підстава, спосіб введення матеріалу, його зміст, зв'язок із конкретним джерелом та умови подальшої перевірки.

Результати OSINT не мають універсальної процесуальної форми. Найменування «OSINT-звіт», «алгоритмічний результат», «мультисенсорна реконструкція» або «доказовий пакет» характеризують спосіб опрацювання чи організації матеріалу, але не визначають його процесуальної природи. Вона залежить від змісту, способу одержання, суб'єкта та використання спеціальних знань [10–11].

Процесуально оформлені фактичні дані мають зберігати зв'язок із первинними об'єктами, відомостями про джерело, метаданими, контрольними значеннями, журналами операцій, результатами перевірки, методологією та істотними проміжними матеріалами. Оформлення не усуває дефектів попередніх рівнів: воно не відновлює втрачений файл, не підтверджує автоматично походження і достовірність та не робить прозорою нерозкриту методологію.

Процесуальна форма має забезпечувати не лише ідентифікацію кінцевого матеріалу, а й персоніфікацію операцій. Повинно бути зрозуміло, хто поставив завдання, хто виявив і зберіг цифровий об'єкт, хто здійснював технічну перевірку, хто застосовував спеціальні знання або алгоритмічні засоби та хто сформулював аналітичний висновок. Це дозволяє перевірити компетентність, межі участі та можливий вплив кожного суб'єкта. Матеріал, підготовлений журналістом, громадською організацією, спеціалістом, експертом або учасником сторони, не стає однаковим за процесуальною природою лише через використання OSINT. Назва документа не може підміняти встановлення конкретного передбаченого законом джерела й порядку його одержання [10–11].

У процесуальному документі необхідно розмежовувати безпосередньо сприйняті відомості, результати технічних операцій і аналітичні висновки, а також персоніфікувати відповідальність за виявлення, збереження, перевірку й інтерпретацію матеріалу. Результатом рівня є належно сформовані фактичні дані у передбаченому законом джерелі; однак їх остаточне доказове значення потребує розкриття, змагальної перевірки та судової оцінки.

Змагально-судовий рівень процесуальної трансформації результатів OSINT. Цей рівень охоплює розкриття матеріалів сторонам, змагальну перевірку, судове дослідження, оцінку та використання у процесуальному рішенні [11; 19–20]. Перевірці підлягає не лише кінцевий файл або аналітичний висновок, а весь істотний шлях його формування: походження первинних даних, законність доступу, способи збереження, технічні й змістовні операції, методологія та інтерпретація.

Розкриття має забезпечувати реальну можливість дослідити первинні матеріали, метадані, контрольні значення, копії, журнали операцій, методи, програмні засоби, параметри та істотні проміжні результати [1–2; 5; 16–18]. Для мультисенсорних і алгоритмічних результатів необхідно розкривати склад вхідних потоків, правила синхронізації, технічні характеристики, похибки, версію програми, параметри та роль людини [4–7]. Надання лише кінцевої візуалізації позбавляє іншу сторону можливості перевірити операції й запропонувати альтернативне пояснення.

Змагальна перевірка може включати повторний аналіз, залучення спеціаліста чи експерта, подання альтернативного дослідження та постановку питань особам, які збирали або опрацьовували інформацію. Предметом оспорювання є походження і цілісність, повнота пошуку, критерії відбору, незалежність джерел, точність геолокації чи хронолокації, коректність алгоритмічних параметрів та врахування альтернативних версій. Сторона не зобов'язана повністю відтворювати складне дослідження, але повинна мати реальну можливість критично перевірити його основу.

Право на ефективне оспорювання включає інформаційну, технічну і процесуальну складові. Інформаційна передбачає доступ до первинного матеріалу, контексту, метаданих, доказової копії, контрольних значень і методології; технічна – можливість дослідження із залу-

ченням належних засобів, спеціаліста або експерта; процесуальна – право подавати заперечення, альтернативний аналіз, ставити питання виконавцям та ініціювати додаткове дослідження. Неможливо вимагати від захисту предметного технічного спростування, одночасно не надаючи даних, необхідних для виявлення відповідного недоліку. Відсутність клопотання про експертизу може враховуватися лише після забезпечення реальної можливості перевірити матеріал, а не як засіб перенесення на захист первинного обов'язку обґрунтовувати достовірність доказів обвинувачення [11; 19–20].

Судове дослідження не може обмежуватися демонстрацією скриншота, відеофрагмента, карти або презентації. Суд має встановити їх зв'язок із первинними матеріалами, спосіб одержання та збереження, характер перетворень, методологію, компетентність виконавців, обмеження і похибки. Під час оцінки розмежовуються належність, допустимість, достовірність і доказова вага: технічна цілісність не підміняє перевірку змісту, а допустимість не означає наперед установленої переконливості.

Наочність цифрового результату потребує особливо обережної судової оцінки. Карта, граф зв'язків, синхронізована хронологія або реконструкція здатні створювати враження математичної точності, хоча можуть містити припущення, похибки та вибіркові критерії відбору. Суд має відокремити те, що безпосередньо відображено у первинних матеріалах, від того, що встановлено технічними операціями, і від аналітичної інтерпретації. Мотиване рішення повинно пояснювати, чому конкретні джерела визнано незалежними, які обмеження методології враховано, як перевірено заперечення та чи підтверджується результат сукупністю інших доказів. Недостатньо послатися на авторитет установи, кваліфікацію аналітика або використання спеціалізованої системи, не дослідивши фактичну основу й межі її висновку [3–6; 37–41].

Мотивування має відображати, які первинні дані покладено в основу висновку, як перевірено їх походження і зміст, наскільки прозорою та відтворюваною була методологія, які заперечення висловила інша сторона та яке значення матеріал має у сукупності доказів. Імовірнісний алгоритмічний результат або геолокація з певною похибкою не можуть подаватися як категорично встановлений факт.

Отже, остаточне доказове значення результату OSINT формується лише за умови реальної можливості його змагального оспорювання, безпосереднього судового дослідження та мотивованої оцінки. Йдеться не про обов'язкове фактичне заперечення кожного матеріалу, а про забезпечення стороні ефективної можливості ознайомитися з первинними даними, перевірити методологію, поставити питання й отримати мотивовану відповідь суду.

***Диференційована інтенсивність процесуальної трансформації результатів OSINT*.** Не кожний цифровий матеріал проходить усі етапи з однаковою глибиною та однаковим обсягом документування. Інтенсивність трансформації залежить від виду джерела, складності матеріалу, способу його одержання, технології опрацювання та характеру процесуального рішення.

Матеріал з офіційного реєстру зазвичай потребує менш інтенсивної перевірки походження, ніж анонімна публікація або повторно завантажене відео. Окремий документ не потребує такого обсягу операцій, як багатокомпонентна геопросторова реконструкція. Одержання файла безпосередньо з ресурсу, через третю особу або з архіву громадської організації створює різні вимоги до інформаційного шляху й ланцюга збереження. Автоматизовані та ймовірнісні системи потребують поглибленого контролю вхідних даних, версії програми, параметрів, похибок і ролі людини [4–7].

Диференціація має враховувати взаємодію п'яти чинників. Вид джерела визначає рівень довіри до його походження та стабільності; складність матеріалу – обсяг технічної документації; спосіб одержання – вимоги до ланцюга збереження; технологія опрацювання – глибину перевірки відтворюваності; характер рішення – необхідний стандарт обґрунтування. Тому

один і той самий цифровий об’єкт може на початковому етапі виконувати лише орієнтуючу функцію, а для використання у вирішальному судовому висновку потребувати повного збереження, незалежної перевірки, розкриття і безпосереднього дослідження. Такий підхід не знижує стандартів, а забезпечує співмірність процедур реальним ризикам помилки та правовим наслідкам використання матеріалу.

Чим істотнішими є правові наслідки рішення та роль OSINT у його обґрунтуванні, тим вищими мають бути вимоги до збереження, перевірки, оформлення, розкриття й мотивованої оцінки. Диференціація не дозволяє довільно відмовлятися від законності доступу, збереження доступного первинного об’єкта, фіксації джерела і контексту, достатньої перевірки, належного процесуального джерела, оспорювання та оцінки. Варіативними є обсяг і глибина операцій, необхідних для реалізації цих вимог за принципами функціональної достатності й пропорційності.

Отже, процесуальна трансформація результатів OSINT – це нормативно впорядкована, багаторівнева й диференційована за інтенсивністю діяльність, у межах якої відкрита цифрова інформація виявляється, збирається, зберігається, перевіряється й аналітично опрацьовується зі збереженням зв’язку з первинними даними, вводиться до кримінального провадження через передбачене законом процесуальне джерело, розкривається сторонам, піддається змагальній перевірці та судовій оцінці й унаслідок цього набуває значення, необхідного для обґрунтування процесуального рішення.

Наукова новизна одержаних результатів. У статті запропоновано цілісну модель, у якій шістнадцять етапів процесуальної трансформації згруповано у п’ять функціонально взаємопов’язаних рівнів. Обґрунтовано диференційовану інтенсивність трансформації, включено мультисенсорні й алгоритмічно сформовані результати до єдиного доказового циклу із збереженням самостійності первинних потоків, доведено похідний характер аналітичного продукту та визначено стандартизований доказовий пакет як організаційно-методичну, а не нову процесуальну форму доказів.

Висновки. Відкрита цифрова інформація не має первинного доказового статусу: відкритість визначає режим доступу, а цифрова форма – спосіб існування й відтворення, проте жодна з цих характеристик сама собою не створює доказу.

Результат OSINT набуває доказового значення внаслідок нормативно впорядкованої трансформації, що охоплює пошук, збереження, перевірку, аналітичне опрацювання, процесуальне формування, розкриття, оспорювання, судове дослідження та оцінку.

Шістнадцятиетапна модель концентровано об’єднується у п’ять рівнів: інформаційно-пошуковий, техніко-верифікаційний, аналітичний, кримінальний процесуальний і змагально-судовий. Кожний має самостійну функцію, а наступний спирається на належність попередніх операцій.

На інформаційно-пошуковому рівні формується не доказ, а виявлений, попередньо оцінений, законно зібраний і первинно зафіксований матеріал, потенційний зв’язок якого з провадженням потребує перевірки.

Збереження первинного цифрового матеріалу є умовою перевірюваності всього доказового циклу; скриншоти, карти, переклади й аналітичні висновки не повинні підміняти об’єкт у стані та контексті його виявлення.

На техніко-верифікаційному рівні розмежовуються походження, автентичність, цілісність і достовірність змісту. Встановлення однієї властивості не доводить автоматично інших.

Аналітичний рівень забезпечує систематизацію та інтерпретацію цифрових і сенсорних даних, але мультисенсорна реконструкція, алгоритмічна класифікація, карта чи хронологія мають похідний характер і не замінюють первинних потоків.

Стандартизований доказовий пакет забезпечує простежуваність і відтворюваність дослідження, але не є новим видом доказу або самостійним процесуальним джерелом.

Кримінальне процесуальне оформлення є обов’язковою, але не самодостат-

ньою фазою: фактичні дані мають бути введені до провадження через передбачене КПК України джерело зі збереженням зв'язку з первинними матеріалами та методологією.

Остаточне доказове значення формується на змагально-судовому рівні після розкриття матеріалів, реальної можливості оспорити їх походження, методологію та висновки, безпосереднього судового дослідження й мотивованої оцінки. Інтенсивність трансформації є варіативною і залежить від джерела, складності матеріалу, способу одержання, технології опрацювання та значення результату для процесуального рішення.

ЛІТЕРАТУРА:

1. Human Rights Center at the University of California, Berkeley, School of Law; Office of the United Nations High Commissioner for Human Rights. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York ; Geneva : United Nations, 2022. DOI: https://doi.org/10.18356/9789210053433.

2. Гаврилюк Л. В., Басиста І. В., Афонін Д. С., Шевчишин А. В. та ін. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : науково-практичний порадник. Київ : ДНДІ МВС України ; Видавництво «Політехніка», 2024. 196 с. ISBN 978-966-990-133-0.

3. Gillett M., Fan W. Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom. *Journal of International Criminal Justice.* 2023. Vol. 21. Issue 4. P. 661–693. DOI: https://doi.org/10.1093/jicj/mqad050.

4. McDermott Y., Koenig A., Murray D. Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations. *Journal of International Criminal Justice*. 2021. Vol. 19. Issue 1. P. 85–105. DOI: https://doi.org/10.1093/jicj/mqab006.

5. Fiorella G., Godart C., Waters N. Digital Integrity: Exploring Digital Evidence Vulnerabilities and Mitigation Strategies for Open Source Researchers. *Journal of International Criminal Justice.* 2021. Vol. 19. Issue 1. P. 147–161. DOI: https://doi.org/10.1093/jicj/mqab022.

6. Freeman L., Vazquez Llorente R. Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age. *Journal of International Criminal Justice.* 2021. Vol. 19. Issue 1. P. 163–188. DOI: https://doi.org/10.1093/jicj/mqab023.

7. Погорецький М. А., Меленті Є. О. Документування атак держави-агресора на об'єкти критичної інфраструктури України: методика інтелектуального аналізу мультисенсорних даних та використання його результатів у кримінальному процесуальному доказуванні. *Право і суспільство.* 2025. № 4. Т. 1. С. 251–274. DOI: https://doi.org/10.32842/2078-3736/2025.4.1.36

8. Погорецький М. А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства*. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf.

9. Погорецький М. А. Теорія кримінального процесуального доказування: проблемні питання. *Право України*. 2014. № 10. С. 12–25. URL: https://pravoua.com.ua/uk/store/pravoukr/pravoukr_10_14/Pogoretskyi_10_14.

10. 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

11. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9–10, 11–12, 13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17

12. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків : Право, 2022. 408 с. DOI: https://doi.org/10.31359/9789669982940

13. Каланча І. Г. Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект : монографія. Київ : SBA Print, 2025. 528 с.

14. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської ; НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139.

15. Гора І. В., Колесник В. А., Малюк В. В., Ходанович В. О., Черняк А. М., Щербина Л. І. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні : монографія / за заг. ред. В. А. Колесника. Київ : 7БЦ, 2024. 484 с.

16. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Київ : УкрНДНЦ, 2018. VI, 31 с.

17. Guttman B., White D. R., Williams S., Walraven T. Digital Evidence Preservation: Considerations for Evidence Handlers. NIST IR 8387. Gaithersburg, MD : National Institute of Standards and Technology, 2022. DOI: https://doi.org/10.6028/NIST.IR.8387.

18. Scientific Working Group on Digital Evidence. Best Practices for Digital Evidence Collection. SWGDE 18-F-002-2.0. Version 2.0. 20 November 2025. URL: https://swgde.org/wp-content/uploads/2025/12/2025-11-20-Best-Practices-for-Digital-Evidence-Collection-18-F-002-2.0.pdf.

19. Погорецький М. А. Верховенство права у кримінальному процесуальному доказуванні: методологія та практика застосування. *Вісник Національної академії правових наук України*. 2025. Т. 32. № 3. С. 275–299. DOI: https://doi.org/10.31359/1993-0909-2025-32-3-275

20. Погорецький М. А. Допустимість доказів у кримінальному процесі та процесуальна доброчесність: доктрини і практика (порівняльно-правове дослідження). *Вісник кримінального судочинства*. 2025. № 1–2. С. 22–59. DOI: https://doi.org/10.17721/2413-5372.2025.1-2/22-59

21. Погорецький М. А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство*. 2025. № 5. Ч. 3. С. 239–256. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.37.

22. Шумило М. Є., Погорецький М. А. Проблеми використання матеріалів оперативно-розшукової діяльності в доказуванні у кримінальних справах: теоретичний та практичний аспекти. *Вісник Луганського інституту внутрішніх справ*. Луганськ : РВВ ЛІВС, 2001. Вип. 3. С. 199–209.

23. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

24. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

25. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Видавництво «Юридика», 2024. 180 с. ISBN 978-617-8182-13-7.

26. Басиста І. В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час досудового розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького.* 2024. Вип. 17 (29). С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243.

27. Назимко Є. С., Коваленко А. В. Сучасні техніко-криміналістичні засоби доказування в кримінальному провадженні : навчально-методичний посібник. Київ : Алерта, 2024. 106 с. ISBN 978-617-566-866-5.

28. Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник Харківського національного університету внутрішніх справ*. 2023. № 3 (102). Ч. 2. С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43.

29. Бабаєва О. В., Авербах Д. В. Щодо питання про використання доказів, отриманих з відкритих джерел, у кримінальному провадженні. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 83. Ч. 3. С. 169–174. DOI: https://doi.org/10.24144/2307-3322.2024.83.3.26.

30. Коновалова Д. О. Особливості використання розвідки на основі відкритих джерел (OSINT) у кримінальному провадженні. *Юридичний науковий електронний журнал.* 2024. № 11. С. 459–465. DOI: https://doi.org/10.32782/2524-0374/2024-11/106.

31. Кульчицька Л. О. Матеріали OSINT як джерела доказів у кримінальних провадженнях за ознаками злочину агресії та воєнних злочинів. Цифровізація кримінального провадження: стан та перспективи : матеріали науково-практичного круглого столу, м. Харків, 19 вересня 2024 р. Харків : Право, 2024. С. 97–101. DOI: https://doi.org/10.31359/9786178411565.

32. Лісніченко Д. В. Використання даних з медіа та відкритих джерел (OSINT) у процесі доказування у кримінальних провадженнях. *Право та державне управління.* 2025. № 1. С. 234–239. DOI: https://doi.org/10.32782/pdu.2025.1.32.

33. Тома М. Г., Василова О. В. Інструменти OSINT: фіксація воєнних злочинів в Україні. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 905–909. DOI: https://doi.org/10.24144/2788-6018.2025.02.134

34. Черняк А. М. Цифровізація доказування у кримінальних провадженнях щодо злочинів проти основ національної безпеки України: межі допустимості та процесуальні гарантії. *Вісник кримінального судочинства*. 2026. № 1. С. 363–393. DOI: https://doi.org/10.59835/2413-5372.2026.1/363-393.

35. Dubberley S., Koenig A., Murray D. (eds.). Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability. Oxford : Oxford University Press, 2020. 360 p. DOI: https://doi.org/10.1093/law/9780198836063.001.0001.

36. Peake J. Challenges of Using Digital Evidence for War Crimes Prosecutions: Availability, Reliability, Admissibility. *AJIL Unbound*. 2024. Vol. 118. P. 57–61. DOI: https://doi.org/10.1017/aju.2024.5.

37. Постанова Касаційного кримінального суду у складі Верховного Суду від 12 червня 2024 р. у справі № 569/1908/23, провадження № 51-1430км24, ЄДРСР № 119741340. URL: https://reyestr.court.gov.ua/Review/119741340.

38. Постанова Касаційного кримінального суду у складі Верховного Суду від 21 липня 2025 р. у справі № 201/11849/23, провадження № 51-584км25, ЄДРСР № 129086893. URL: https://reyestr.court.gov.ua/Review/129086893.

39. European Court of Human Rights. Ukraine and the Netherlands v. Russia [GC], applications nos. 8019/16, 43800/14, 28525/20 and 11055/22, judgment of 9 July 2025. HUDOC no. 001-244292. URL: https://hudoc.echr.coe.int/?i=001-244292.

40. European Court of Human Rights. Georgia v. Russia (II) [GC], application no. 38263/08, judgment of 21 January 2021. HUDOC no. 001-207757. URL: https://hudoc.echr.coe.int/?i=001-207757.

41. International Criminal Court, Pre-Trial Chamber I. Warrant of Arrest for Mahmoud Mustafa Busayf Al-Werfalli, 15 August 2017, ICC-01/11-01/17-2. URL: https://www.icc-cpi.int/court-record/icc-01/11-01/17-2.

Дата першого надходження статті до видання: 20.06.2026
Дата прийняття статті до друку після рецензування: 14.07.2026
Дата публікації (оприлюднення) статті: 26.08.2026