УДК 343.1:343.3:004.056:004.77:004.93(477)
DOI https://doi.org/10.24144/2788-6018.2025.05.3.37

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ДОКАЗИ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: ПРОЦЕСУАЛЬНІ ПРОБЛЕМИ ТА ЄВРОПЕЙСЬКІ СТАНДАРТИ

Погорецький М.А.,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений діяч науки і техніки України,
проректор з науково-педагогічної роботи
Київського національного університету імені Тараса Шевченка
ORCID: 0000-0003-0936-0929

Погорецький М.А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти.

Стаття пропонує системно-інтегровану процесуально-правову модель використання цифрових технологій та доказів у провадженнях про злочини проти основ національної безпеки України. Показано, що дефіцит автономної дефініції «цифрових доказів» у КПК, нерозробленість процедур одержання, автентифікації та збереження, а також нестача сертифікованих інструментів і підготовлених кадрів спричиняють правову невизначеність та ризики недопустимості. На тлі міжнародних стандартів ЄСПЛ (зокрема *Benedik v. Slovenia, Uzun v. Germany*) та підходу Суду ЄС у справі *C-670/22 (EncroChat)* обґрунтовано: (1) уніфікований тест допустимості електронних доказів – «походження – відкриття – відтворюваність» – і його інструменталізацію у вигляді спеціалізованрнр довідково-методичного посібника для суддів (довідника – *benchbook*); (2) процедуру цифрової криміналістики відкритих джерел (OSINT-forensics**)** із вимогами до фіксації, *ланцюга збереження доказів* та *журналу аудиту (audit trail)*; (3) алгоритм судової перевірки координат (подвійна проєкція; крос-валідація з телеком-логами/офіційними довідками; журнал доступу) для верифікації геоданих і картографічних матеріалів. Запропоновано нормативне закріплення мінімальних стандартів процесуального обігу цифрових доказів у КПК (у т.ч. правила огляду вебресурсів і роботи з даними хмарних сервісів/мобільних застосунків), підзаконні міжвідомчі інструкції цифрової криміналістики та інституційні механізми (акредитовані лабораторії, реєстр валідованих методик). Доведено, що системна імплементація цих рішень підвищує доказову надійність цифрових матеріалів, забезпечує сумісність із принципом «внутрішньої еквівалентності» в транскордонному обігу електронних доказів і зміцнює гарантії справедливого судового розгляду.

Ключові слова: цифрові докази; цифрова криміналістика відкритих джерел (OSINT-forensics); допустимість; відтворюваність; *chain of custody*; *audit trail*; суддівський довідник (*benchbook*); геодані; картографічні сервіси (Google Maps); верифікація координат; глибокі підробки (*deepfake*); ЄСПЛ; Суд ЄС; C-670/22 (EncroChat); Benedik v. Slovenia; Uzun v. Germany; внутрішня еквівалентність; національна безпека; Верховний Суд України; Протокол Берклі.

Pohoretskyi M.A. Digital technologies and evidence in the investigation of crimes against the fundamentals of national security of Ukraine: procedural problems and european standards.

The article advances a system-integrated procedural and legal model for the use of digital technologies and evidence in criminal proceedings concerning offences against the foundations of Ukraine's national security. It shows that the lack of an autonomous definition of "digital evidence" in the Criminal Procedure Code (CPC), the underdevelopment of procedures for collection, authentication and preservation, as well as shortages of certified tools and trained personnel, generate legal uncertainty and risks of inadmissibility. Against the backdrop of international standards of the ECtHR (notably Benedik v. Slovenia, Uzun v. Germany) and the CJEU's approach in Case C-670/22 (EncroChat), the article substantiates: (1) a unified admissibility test for electronic evidence–"provenance – disclosure – reproducibility"–and its operationalisation through a judicial benchbook with model reasoning; (2) a procedure for open-source digital forensics (OSINT-forensics) with requirements for capture, chain of custody, and audit trail; (3) an algorithm for judicial verification of coordinates (double projection; cross-validation with telecom logs/official statements; access logging) to verify geodata and cartographic materials. It proposes statutory incorporation of minimum standards for the procedural circulation of digital evidence in the CPC (including rules for inspecting web resources and handling data from cloud services/mobile apps), sub-statutory interagency digital-forensics instructions, and institutional mechanisms (accredited laboratories; a register of validated methods). It is

demonstrated that systemic implementation of these measures enhances the probative reliability of digital materials, ensures compatibility with the "internal equivalence" principle in the cross-border circulation of electronic evidence, and strengthens guarantees of a fair trial.

Key words: digital evidence; open-source digital forensics (OSINT-forensics); admissibility; reproducibility; chain of custody; audit trail; judicial benchbook; geodata; cartographic services (Google Maps); coordinate verification; deepfakes; ECtHR; CJEU; C-670/22 (EncroChat); Benedik v. Slovenia; Uzun v. Germany; internal equivalence; national security; Supreme Court of Ukraine; Berkeley Protocol.

Постановка проблеми. Злочини проти основ національної безпеки України відзначаються особливою суспільною небезпечністю, оскільки вони спрямовані на підрив конституційного ладу, суверенітету та територіальної цілісності держави. В умовах гібридної війни та високої цифровізації суспільних процесів ці злочини дедалі частіше супроводжуються використанням сучасних інформаційно-комунікаційних технологій. Це призводить до того, що саме цифрові сліди стають ключовими носіями доказової інформації. Водночас українське кримінальне процесуальне право поки що не забезпечує належної регламентації їх статусу, а правозастосовна практика залишається непослідовною.

Актуальність дослідження зумовлюється необхідністю вирішення двоєдиного завдання: по-перше, підвищення ефективності розслідування злочинів проти основ національної безпеки шляхом широкого й обґрунтованого застосування цифрових технологій; по-друге, гарантування захисту прав людини при втручанні держави у сферу приватності, комунікацій та персональних даних. Відсутність чітких норм щодо допустимості, належності та автентичності цифрових доказів створює ризик їх відхилення судами та водночас загрозу зловживань при їх збиранні.

Проблема полягає у дисбалансі між швидкістю реагування на загрози національній безпеці та потребою забезпечення належного судового контролю і процесуальних гарантій. Європейські стандарти, сформульовані у практиці ЄСПЛ (*Roman Zakharov v. Russia*, *Big Brother Watch v. the UK*, *Bykov v. Russia та ін.*) та Суду ЄС (справа *C-670/22, EncroChat*), визначають критерії пропорційності, прозорості й сумісності доказів у транскордонному вимірі. Досягнення цих стандартів для України є не лише правовим викликом, а й стратегічною необхідністю у процесі євроінтеграції та реформування кримінальної юстиції.

Таким чином, постановка проблеми полягає у пошуку оптимальної моделі регламентації цифрових доказів у кримінальному процесі України, яка б одночасно забезпечувала ефективність переслідування злочинів проти основ національної безпеки та дотримання фундаментальних прав і свобод людини.

Аналіз останніх досліджень і публікацій. Проблемні питання застосування цифрових технологій та електронних доказів у кримінальному провадженні щодо злочинів проти основ національної безпеки України послідовно перебували у фокусі вітчизняної доктрини, де їх розглядали крізь призму верховенства права, гарантій приватності й таємниці комунікацій, інституційного балансу процесуальних повноважень сторін та функціональної ролі слідчого судді в досудовому провадженні, а також критеріїв допустимості, належності, достовірності й збереження «ланцюга володіння» цифровими слідами. Значний внесок у розвиток цієї проблематики зробили: О.Ф. Бантишев, О.В. Бех, В.С. Бондар, І.В. Гловюк, О.М. Дуфенюк, І.В. Гора, О.В. Капліна, В.В. Малюк, О.П. Метелев, Ю.М. Одажиу, В.Ю. Парфьонов, М.М. Погорецький, В.І. Присяжний, О. Пчеліна, Т. Фоміна, О.Ю. Татаров, Г.К. Тетерятник, С.С. Чернявський, А.М. Черняк, Д.Б. Сергєєва, О.С. Старенький, О.М. Стрільців, М.С. Цуцкіридзе та ін.

Зокрема, В.С. Бондар та В.Ю. Парфьонов висвітлили особливості впровадження новітніх технологій у документуванні та розслідуванні окремих категорій злочинів, акцентуючи на проблемі їх допустимості та доказової сили [1]. О.М. Дуфенюк дослідив виклики та інноваційні стандарти розслідування, пов'язані з цифровими слідами, у контексті міжнародних зобов'язань України [2]. О.Ф. Бантишев, І.В. Гора, В.В. Малюк, А.М. Черняк та ін. у колективному посібнику систематизували підходи до кваліфікації та розслідування злочинів проти основ нацбезпеки, наголошуючи на процесуальній інтеграції цифрових джерел доказів у досудовому провадженні [3]. О.П. Метелев дослідив проблемні аспекти фіксації відомостей із транспортних телекомунікаційних мереж і окреслив вимоги до їх процесуальної легітимації та автентичності [4]. О. Пчеліна, Т. Фоміна розкрили специфіку огляду місця події з урахуванням виявлення та збереження електронних слідів, релевантних для посягань на основи нацбезпеки [5]. Г.К, Тетерятник, О.В. Бех, та Ю.М. Одажиу поєднали теоретичні та прикладні підходи до доказування, акцентуючи на процесуальних гарантіях при використанні цифрових технологій [6].

Значний внесок у розробку проблем цифрових технологій та електронних доказів у кримінальному провадженні зробили зарубіжні вчені: Кетрін Робертс (Catherine Roberts), Деніел Сенг (Daniel Seng), Іоганн Кейсі (Eoghan Casey), Єрун Й. Оерлеманс (Jeroen J. Oerlemans), Джонатан Клаф (Jonathan Clough), Орін С. Керр (Orin S. Kerr), Радіна Стойкова (Radina Stoykova), Стівен Манн (Stephen Mann), Стівен Мейсон (Stephen Mason), Сюзан В. Бреннер (Susan W. Brenner), Том ван Тоор (Tom van Toor) та ін. Так, Іоганн Кейсі (Eoghan Casey) запропонував криміналістичну рамку для роботи з цифровими

доказами (ідентифікація, фіксація, збереження, аналіз), підкресливши критичність автентичності та «chain of custody» у кримінальному процесі [8]. Стівен Мейсон (Stephen Mason) та Деніел Сенг (Daniel Seng) систематизували стандарти електронних доказів і електронних підписів, акцентуючи на доказовій силі цифрових записів і вимогах до їхнього представлення в суді [9]. Єрун Й. Оерлеманс (Jeroen J. Oerlemans) та Том ван Тоор (Tom van Toor) на матеріалі EncroChat показали архітектуру «data-driven investigations» та процесуальні фільтри відбору/мінімізації даних у транскордонних справах [10]; у правознавчому аналізі ці ж автори довели значення тесту внутрішньої еквівалентності й правозахисних гарантій для допустимості перехоплених комунікацій [11]. Радіна Стойкова (Radina Stoykova) дослідила межі феномену «хакера з ордером» і справедливого судового розгляду, окресливши процесуальні ризики масового збору комунікацій і критерії їхнього судового контролю [12].

Поряд із зарубіжними та вітчизняними підходами окремі аспекти проблеми застосування цифрових технологій та електронних доказів у кримінальному провадженні розроблялися й в авторських працях, які, спираючись на власну концепцію доказів та доказування, стали методологічною основою для подальшого аналізу зазначеної проблематики у контексті злочинів проти основ національної безпеки України [13–23].

Проведений огляд наукових напрацювань показує, що питання цифрових технологій та електронних доказів у кримінальному процесі вже дістали значний розвиток як у вітчизняній, так і в зарубіжній літературі. Українські дослідники переважно зосереджуються на прикладних аспектах документування та розслідування злочинів, підкреслюючи потребу нормативного закріплення процесуального статусу цифрових доказів. Зарубіжні вчені пропонують універсальні моделі автентифікації, оцінки й збереження електронної інформації, які потенційно можуть бути адаптовані до українських реалій. Водночас жодне з досліджень не дає комплексної відповіді на ключове питання – як забезпечити баланс між ефективністю розслідування злочинів проти основ національної безпеки та гарантіями прав людини в умовах застосування новітніх цифрових технологій. Саме ця наукова лакуна визначає актуальність подальшого дослідження.

Метою цієї статті є комплексне дослідження процесуальних проблем використання цифрових технологій та електронних доказів у розслідуванні злочинів проти основ національної безпеки України з урахуванням практики Верховного Суду, ЄСПЛ та Суду ЄС, а також вироблення пропозицій щодо вдосконалення кримінального процесуального законодавства з метою одночасного підвищення ефективності розслідування й забезпечення належних гарантій прав людини.

Методологічно стаття спирається на доктринальний та порівняльно-правовий аналіз, аналітико-правовий огляд судової релевантної практики ЄСПЛ і Суду ЄС (із точними посиланнями на ключові §§ рішень) та емпіричне узагальнення правових позицій Верховного Суду України на основі аналізу конкретних справ [42; 44–45; 49–51; 55–56]. Джерельна база охоплює міжнародні договори (Конвенція про кіберзлочинність і Другий додатковий протокол) [24; 25], акти права ЄС (Директива 2014/41/ЄС) [26], прецеденти ЄСПЛ і СЄС (*зокрема Benedik v. Slovenia, Uzun v. Germany, Roman Zakharov v. Russia, Big Brother Watch and Others v. the United Kingdom*) [29–33; 36–37], а також перевірені приклади національної практики. Для підвищення відтворюваності висновків використано перехресну верифікацію: зіставлення доктрини, судової практики та запропонованих процесуальних алгоритмів (цифрова криміналістика відкритих джерел (OSINT-forensics); валідація координат). Обмеження дослідження полягають у фокусі на доступних рішеннях і відкритих матеріалах без залучення закритої частини проваджень.

Виклад основного матеріалу. Злочини проти основ національної безпеки України утворюють особливий розділ кримінально-правових заборон, закріплений у статтях 109–114-2 Кримінального кодексу України, безпосереднім об'єктом яких є конституційний лад, державний суверенітет, територіальна цілісність, обороноздатність і функціонування органів публічної влади. Вони характеризуються підвищеною суспільною небезпечністю, оскільки спрямовані на підрив основ існування держави та підрив довіри до її інституцій.

Класичні форми таких злочинів – державна зрада, шпигунство, колабораційна діяльність, пособництво державі-агресору – в умовах сучасних гібридних загроз отримали якісно новий вимір. Сьогодні вони дедалі частіше реалізуються у поєднанні з кібернетичними та інформаційними атаками, які проявляються у здійсненні кіберактивності проти критичної інфраструктури, несанкціонованому втручанні в інформаційні ресурси, розповсюдженні дезінформації та психологічному впливі на суспільну свідомість. У такий спосіб відбувається інтеграція традиційних складів злочинів із цифровими технологіями, що зумовлює виникнення нового рівня складності їх документування та доказування.

Особливістю зазначених правопорушень є їх високий рівень латентності та специфіка доказової бази. Якщо у минулому визначальними були агентурні відомості, матеріальні носії чи особисті свідчення, то нині ключовими стають цифрові сліди: електронна переписка, дані операторів мобільного зв'язку, записи камер відеоспостереження, геолокаційні треки, транзакції у блокчейні. Саме ці дже-

рела фактичних даних визначають успішність доведення вини, але водночас породжують складні процесуальні питання щодо їх автентичності, збереження та допустимості.

У цьому контексті доцільно системно окреслити коло обставин, що підлягають доказуванню з опорою на відкриті цифрові джерела (OSINT) у кримінальних провадженнях про посягання на основи національної безпеки. По-перше, йдеться про головний предмет доказування за ст. 91 КПК України: подію кримінального правопорушення (час, місце, спосіб), винуватість особи, форму вини, мотив і мету. Судова практика підтверджує, що саме відкриті електронні матеріали – аудіоповідомлення з месенджерів, скриншоти комунікаційних каналів, геопозначки на цифрових картах, відеофіксація – можуть відігравати провідну роль у доведенні об'єктивної та суб'єктивної сторін складу. Зокрема, у справах за ч. 2 ст. 111 КК такі дані дозволяють одночасно встановити механізм комунікації з представниками держави-агресора (голосові повідомлення, кореляції за IMEI/IP) та просторову прив'язку переданих координат до реальних місць дислокації підрозділів, що підтверджено використанням у доказуванні аудіофайлів, добровільно наданих або вилучених із мобільних пристроїв, їхніх стенограм, а також картографічних матеріалів з позначеними геокоординатами за умови належної процесуальної фіксації та технічної верифікації цілісності (відсутності монтажу) [42]. До цього блоку належать також «візуальні» електронні свідчення участі в діяльності окупаційних адміністративних утворень (самопроголошених органів): фото- і відеозаписи публічних виступів, цифрові копії розпорядчих документів, відомості з офіційних вебресурсів таких утворень, які безпосередньо підтверджують факт обіймання посади (у значенні ч. 7 ст. 111-1 КК) та дозволяють ідентифікувати здійснення організаційно-розпорядчих функцій. [44].

По-друге, відкриті цифрові джерела мають самостійне доказове значення у межах локального предмета доказування – під час вирішення окремих процесуальних питань поза межами вирішення справи по суті. Йдеться, зокрема, про обґрунтування ризиків за ст. 170, 177 КПК (факти переховування, спроби впливу чи знищення електронних слідів, засвідчені публічною цифровою активністю), про встановлення підстав для застосування спеціального досудового розслідування та спеціального судового провадження (сталі індикатори перебування підозрюваного на тимчасово окупованій території або на території держави-агресора), а також про верифікацію належного повідомлення особи (публікації повісток і процесуальних повідомлень на офіційних державних порталах з додатковими відкритими ознаками обізнаності). Практика засвідчує, що огляди офіційних вебресурсів і публічних інтернет-матеріалів можуть логічно та процесуально коректно підкріплювати висновок про тривале перебування особи поза підконтрольною територією та її процесуальну доступність для інститутів заочного кримінального провадження (in absentia) [44].

По-третє, OSINT слугує для доказування допоміжних фактів – локалізації осіб, речей і документів; спростування чи підтвердження альтернативних версій; підготовки до слідчих (розшукових) дій; оперативного виявлення релевантних джерел. Особливе значення тут мають геопросторові дані (Google Maps, супутникові знімки, геомітки в метаданих), які національні суди визнають прийнятними за умови належної процесуальної фіксації: складання протоколу огляду з додатками (скриншоти або відеозапис екрану), фіксації URL і часу доступу, збереження оригінальних файлів та їхніх контрольних сум. Така практика вже сформульована у рішеннях, де суди акцентували на способі отримання та документування електронних картографічних матеріалів як на ключовому чиннику їх допустимості [45].

З огляду на зазначене вважаємо необхідним послідовно процесуалізувати OSINT-джерела як інструмент кримінального доказування, який системно інтегрує дані з мобільних пристроїв (аудіо, листування, метадані), картографічні сервіси (геомітки, маршрути), відеоконтент з відкритих платформ та відомості з офіційних вебресурсів. Це зумовлено тим, що у провадженнях із формальним складом (наприклад, ч. 2 ст. 111 КК) зміст і спосіб комунікації (голосові повідомлення, передані координати, послідовність цифрових подій) часто є самодостатніми для встановлення об'єктивної сторони; натомість у провадженнях із «змішаною» структурою (зокрема, ч. 7 ст. 111-1 КК та ст. 438 КК) відкриті джерела забезпечують доказування контекстуальних елементів – статусу, функцій, наявності міжнародного збройного конфлікту та просторово-часової «прив'язки» діяння [42; 44; 45]. Такий підхід є сумісним із конституційним імперативом недопустимості доказів, одержаних незаконним шляхом (ч. 3 ст. 62 Конституції України) [34], а також із критеріями належності та допустимості, які Верховний Суд послідовно конкретизує щодо аудіо- та картографічних матеріалів, скриншотів і відеозаписів за умови їх отримання і документування відповідно до вимог КПК [42; 44; 45].

Міжнародні стандарти послідовно формулюють критерії правомірного використання цифрових доказів. Європейський суд з прав людини у рішеннях *Benedik v. Slovenia* [29], *Uzun v. Germany* [30], *Big Brother Watch and Others v. UK* [31], *Bykov v. Russia* [32], *Roman Zakharov v. Russia* [36], наголосив на тому, що збирання та використання інформації з приватної сфери особи можливе лише за умови законності, необхідності та пропорційності втручання.

У розвиток наведеної тези слід звернути особливу увагу на два рішення, які чітко артикулюють стандарти правомірного використання цифрових доказів. У справі *Benedik v. Slovenia* ЄСПЛ визнав, що деанонімізація користувача за динамічною IP-адресою становить втручання у приватне життя і можлива лише за наявності якісної правової підстави та ефективних процесуальних запобіжників: закон має бути доступним і передбачуваним щодо умов отримання ідентифікаційних даних; національні норми мають прямо регулювати зв'язок IP-адреси з конкретною особою; як правило, потрібен судовий дозвіл. Відсутність достатньої ясності закону та гарантій від свавілля призвела до висновку про порушення статті 8 (див. орієнтири Суду щодо «якості закону» і вимоги судового контролю: §§ 116–120, 127, 133–134) [29].

У справі *Uzun v. Germany* (GPS-стеження) Суд системно нагадав триєдиний тест: втручання має бути відповідно до закону (*«in accordance with the law»)*, тобто спиратися на зрозумілу і передбачувану норму та супроводжуватися *достатніми і ефективними гарантіями від зловживань* (визначеність підстав, межі за обсягом/тривалістю, компетентні органи дозволу й контролю, наявність дієвого засобу юридичного захисту), а також бути *необхідним і пропорційним* легітимній меті. Застосовуючи ці критерії, Суд визнав, що в тих фактичних обставинах GPS-стеження відповідало вимогам ст. 8 § 2: воно було часово обмеженим, стосувалося тяжких злочинів і менш інвазивні заходи виявилися неефективними (§§ 60–63, 94–95, висновок про пропорційність та «необхідність у демократичному суспільстві» – §§ 75–81, особливо § 81) [30].

З огляду на наведені стандарти, українська модель роботи з цифровими доказами має бути синхронізована щонайменше у трьох площинах. По-перше, *якість закону*: спеціальні норми повинні прямо регулювати деанонімізацію мережевих ідентифікаторів (динамічні IP, IMSI/IMEI тощо) з вимогою *ex ante судового контролю*, чіткими порогами підозри та вузько цільовою метою. По-друге, *процедурні запобіжники*: фіксований *chain of custody* (хеш-ідентифікація, журнал дій, відтворюваність методики), межі за тривалістю/масштабом збору, правило «найменш інвазивного засобу», пост-фактум повідомлення особи, коли ризики минають, і реальний засіб оскарження. По-третє, *судова оцінка*: суд має перевіряти не лише зміст цифрових даних, а *якість методики* їх отримання та збереження, відсікаючи результати, здобуті поза вимогами законності, необхідності й пропорційності. Запропоноване інституційно-процедурне налаштування забезпечує відповідність національної практики підходам, сформульованим ЄСПЛ у справах *Benedik v. Slovenia* [29] та *Uzun v. Germany* [30], і водночас узгоджується з уже наведеною у Вашому тексті прецедентною лінією *Roman Zakharov v. Russia* [36], *Big Brother Watch and Others v. the United Kingdom* [31] та *Bykov v. Russia* [32].

У транскордонному вимірі ці підходи корелюють із практикою Суду ЄС у справі *C-670/22, M.N. (EncroChat),* який закріпив концепт «*внутрішньої еквівалентності*»: цифрові дані, отримані за кордоном, визнаються допустимими лише за умови дотримання стандартів, еквівалентних національним [37].

На рівні національної правозастосовчої практики наведені орієнтири підтримуються підходами Верховного Суду України, який у низці рішень [42; 44–45; 49–51; 55–56] формує уніфіковані критерії оцінки електронних доказів (перевірюваність методики збирання, безперервність ланцюга збереження, релевантність і достовірність), що має бути інституційно закріплено шляхом кодифікації зазначених вимог у КПК України.

Щоб таке інституційне закріплення було змістовним і передбачуваним, насамперед слід окреслити місце цифрових доказів у національній моделі доказування. У сучасному кримінальному процесі цифрові докази посідають особливе місце як новітня форма відображення фактичних даних. Відповідно до положень КПК України, доказами є будь-які фактичні дані, отримані у порядку, визначеному законом, на підставі яких встановлюються обставини, що мають значення для кримінального провадження. Водночас вітчизняне законодавство не містить спеціальної дефініції цифрових доказів, що породжує дисбаланс між швидкістю технологічних змін та ефективністю правового регулювання.

Конкретизуючи предмет регулювання, цифрові докази охоплюють електронні дані, зафіксовані, передані чи збережені в інформаційно-комунікаційних системах: метадані, електронну переписку, дані мобільних операторів, записи камер відеоспостереження, GPS-треки, інформацію про транзакції у блокчейні. Їх характерною рисою є можливість оперативного копіювання, обробки та поширення, що водночас створює переваги (швидкість отримання, багатофакторність аналізу) і ризики (фальсифікація, модифікація, втрата автентичності), які й обумовлюють потребу в чітких нормативних визначеннях та процесуальних гарантіях.

У підсумку, правова природа злочинів проти основ національної безпеки України нині поєднує класичні форми підривної діяльності з цифровими проявами гібридної агресії. Це вимагає від законодавця й правозастосувача в сфері кримінального процесу переосмислення підходів до доказування, формування нових гарантій автентичності та процесуальної надійності цифрових слідів, а також запозичення європейських стандартів у сфері доказового права – у логічному продовженні вже окреслених Верховним Судом критеріїв і їх майбутнього нормативного закріплення в КПК України.

У цьому контексті ключовим є дотримання вимог автентичності та допустимості. Європейський суд з прав людини у рішеннях *Bykov v. Russia* [32] та *Khan v. UK* [33] наголосив, що спосіб отримання електронних даних має не менше значення, ніж їхній зміст: саме процесуальні гарантії убезпечують від маніпуляцій і довільного втручання держави. Суд послідовно вимагає оцінювати, чи було втручання *відповідно до закону*, чи воно було *необхідним і пропорційним*, і чи не підриває використання таких даних загальної справедливості провадження; за відсутності належних гарантій та вирішального характеру таких відомостей для обвинувачення вони мають бути вилучені з доказової бази як недопустимі [32; 33].

Важливу роль у формуванні європейських стандартів відіграє Директива 2014/41/ЄС про Європейський наказ про розслідування [26], яка визначає правила транскордонного доступу до цифрових даних. Своєю чергою, Будапештська конвенція про кіберзлочинність 2001 року та Другий додатковий протокол 2022 року [24; 25] заклали міжнародні стандарти криміналізації кібердіянь і механізми належного обміну електронними доказами між державами. Для України, що протидіє збройній агресії, ці акти є дороговказом для побудови внутрішнього процесуального режиму цифрових доказів, сумісного з європейськими підходами, і для подальшого *нормативного закріплення* вироблених критеріїв у КПК України.

У науковому дискурсі дедалі більше уваги приділяється технологічним аспектам доказування. Наприклад, Європейське агентство з кібербезпеки (ENISA) у своїй доповіді 2023 року підкреслило ризики застосування штучного інтелекту та машинного навчання, які можуть призвести як до підвищення ефективності розслідування, так і до появи нових форм маніпуляцій доказами [27]. Стандарти Національного інституту стандартів і технологій США (National Institute of Standards and Technology – NIST) [28] акцентують на необхідності інтеграції криміналістичних методів у систему реагування на інциденти, включно з документуванням ланцюга збереження («*chain of custody*») для забезпечення доказової надійності.

Отже, цифрові докази слід розглядати як самостійну процесуальну категорію, що потребує законодавчого визначення й уніфікації. Вони поєднують у собі нові можливості для кримінальної юстиції та значні ризики для прав людини, що зумовлює необхідність удосконалення національного законодавства шляхом гармонізації з європейськими та міжнародними стандартами.

Однією з найскладніших проблем кримінального провадження із застосуванням цифрових технологій є гарантування автентичності електронних даних та збереження безперервного «ланцюга збереження доказів» (chain of custody). На відміну від класичних речових доказів, цифрові дані є надзвичайно вразливими до модифікації, копіювання чи знищення. Будь-яке втручання – навіть технічне з боку операційної системи чи автоматичного оновлення програмного забезпечення – може змінити часові мітки чи структуру файлу, що ставить під сумнів його достовірність і процесуальну придатність.

Європейський суд з прав людини у справі *Bykov v. Russia* [32] наголосив, що відсутність належно задокументованого ланцюга передачі аудіозаписів позбавила їх доказової сили, оскільки суд не мав можливості перевірити умови їхнього отримання та збереження. У рішенні *Roman Zakharov v. Russia* [36] Суд звернув увагу на ризик свавільного доступу до телекомунікаційних даних без належних гарантій контролю, що робить такі дані непридатними для використання у кримінальному процесі. Аналогічна логіка простежується у справі *Big Brother Watch and Others v. UK* [31], де Суд прямо вказав на необхідність незалежного контролю та чітких процедур збереження електронних даних, аби уникнути їхньої недостовірності.

Міжнародні стандарти, зокрема Рекомендації NIST [28], визначають обов'язкові елементи ланцюга збереження: фіксацію початкової хеш-суми даних, ведення журналу доступу, ідентифікацію кожної особи, яка мала доступ до носія, та використання сертифікованого програмного забезпечення для копіювання й аналізу. Ці вимоги повністю узгоджуються з положеннями Другого додаткового протоколу до Будапештської конвенції [25], який акцентує на прозорості транскордонного обігу електронних доказів та їх автентифікації.

У контексті кіберзагроз і гібридної війни для України питання автентичності цифрових доказів набуває особливого значення. Недостатня процесуальна фіксація чи порушення ланцюга зберігання (володіння) «*chain of custody*» може призвести до втрати ключових матеріалів у справах про державну зраду чи шпигунство, що не лише ускладнює доведення вини, а й створює ризик уникнення кримінальної відповідальності осіб, які посягають на основи національної безпеки.

Отже, проблема автентичності цифрових доказів та безперервності їх «ланцюга володіння» є одним із центральних викликів сучасного кримінального процесу. Її вирішення потребує поєднання законодавчого закріплення спеціальних процедур, впровадження національного стандарту цифрової криміналістики та гармонізації з європейськими вимогами щодо прозорості та надійності доказування.

У межах запропонованої моделі національного стандарту «*chain of custod*y» доцільно виокремити спеціальний ризик-профіль для відкритих цифрових джерел (OSINT), оскільки їхня доказова сила без-

посередньо залежить від відтворюваності кроків доступу та збереження, підтвердження первинності публікації і контролю за незмінністю вмісту. По-перше, *первинність публікації* має фіксуватися у самому протоколі (ідентифікація платформи, акаунта/каналу, первісного посту/відео, наявних ідентифікаторів, часу першого виявлення), із докладною прив'язкою *дата-часу доступу/завантаження* у форматі UTC та вказівкою використовуваного середовища (браузер/агент, мережеві налаштування). По-друге, кожен елемент доступу повинен супроводжуватися фіксацією *URL/URI* (включно з параметрами запиту), контрольним знімком екрану/відеозахопленням процесу доступу, а також збереженням вихідних файлів *у форматі, що не змінює метадані* (оригінальні контейнерні формати або «forensic-friendly» образи), із *контрольними сумами (хеш-значеннями)*, обчисленими на момент первинного захоплення і перевіреними під час кожного наступного відтворення. По-третє, має вестися *журнал аудиту* (*audit trail*) до електронних копій і носіїв, де вказуються особа, дата-час, мета та обсяг операції, а також застосовані програмні засоби і їх версії, що забезпечує простежуваність і незалежну верифікацію. По-четверте, забезпечується *дублювання копій у захищених репозиторіях* (географічно та організаційно рознесені сховища/сейфи даних) із контрольованим доступом та політикою незмінності (WORM-режим, цифрові відбитки, кваліфікований час).

Окремого врегулювання потребує уніфікована процедура «OSINT-forensics», яка деталізує процесуальні та технічні кроки збору, збереження і документування відкритих цифрових матеріалів як різновиду електронних документів. У складових цієї процедури доцільно: (1) встановити обов'язкові елементи протоколу огляду відкритих вебресурсів (ідентифікація джерела; URL/URI; дата-час у UTC; опис середовища доступу й версій ПЗ/плагінів; спосіб фіксації; хешування; долучення «службової картки» з технічними атрибутами та даними про ланцюг збереження доказів); (2) передбачити спеціальні правила роботи з картографічними сервісами (Google Maps тощо), у межах яких судова перевірка координат має здійснюватися за таким алгоритмом: а) первинна фіксація – експорт «сирих» точок у WGS84 (EPSG:4326) із зазначенням масштабу/zoom, джерела тайлів/знімків, часу отримання (UTC), параметрів пристрою/браузера та негайним хешуванням файлів; б) подвійна проєкція – пряме й зворотне перетворення координат між EPSG:4326 та щонайменше однією альтернативною проєкцією (напр., EPSG:3857 Web Mercator і/або відповідною національною/UTM-зоною), з автоматичним обчисленням відхилення в метрах і фіксацією параметрів трансформації; в) встановлення допустимої похибки – визначення порогу розбіжності з урахуванням природи джерела (для GNSS без диференціації типовий діапазон кількох метрів; для базових телеком-ідентифікаторів – десятки/сотні метрів; значення конкретизуються у звіті методики); г) крос-валідація з телеком-даними – зіставлення координат із офіційними довідками/логами оператора (CDR; Cell-ID/eNodeB/gNodeB; LAC/TAC; сектор, азимут і кут розкриття антени; показники на кшталт *Timing Advance*/RTT), за можливості – з *EXIF*-метаданими, журналами Wi-Fi (BSSID/MAC, RSSI), Bluetooth-маяками, записами відеоспостереження та (за потреби) супутниковими зображеннями; **ґ)** дублювання джерел – збереження тайлів/знімків у декількох масштабах/датах, із фіксацією контроль-точок (*ground control points*) для візуальної верифікації; **д)** повний журнал аудиту (доступу) – хто/коли/звідки (IP/ідентифікатор робочого місця) здійснював перегляд/експорт/обробку; версійність файлів; цифрові підписи/мітки часу; е) підсумковий звіт – опис відтворюваної методики, інструментів і параметрів перетворення, обґрунтування встановленої похибки, таблиця крос-звірок і висновок про відповідність координат; (3) регламентувати допустимі способи збереження з мережевих платформ (API-вивантаження, *forensic capture*) з мінімізацією втручання у структуру файлів і з дотриманням вимог до метаданих; (4) уніфікувати вимоги до репродукції доказу в суді (публічне відтворення; перевірка хеш-значень; надання суду й стороні захисту покрокових інструкцій та пакета даних для незалежного повторення експерименту, включно з файлами проєкцій/параметрами трансформації та витягами з *журналу аудиту*).

Запропонований ризик-орієнтований підхід до OSINT інтегрується з пропозиціями щодо національного стандарту *«chain of custody»,* забезпечуючи сумісність процесуальних (протоколювання, відкриття, доступ для контрперевірки) і техніко-криміналістичних (хешування, журнали доступу, захищені сховища, відтворюваність) вимог. Така інтеграція, по-перше, *знижує ентропію джерел* (розмаїття платформ і форматів) до стандартизованих кроків, придатних для незалежної верифікації; по-друге, *переносить акцент оцінювання допустимості* з формального носія на доведену цілісність, походження і можливість репродукції; по-третє, *узгоджує національну практику* з європейськими орієнтирами щодо прозорості і процесуальної справедливості у сфері електронних доказів. У підсумку OSINT, оформлений за єдиною процедурою «OSINT-forensics», стає не «сірим» інструментом оперативного реагування, а повноцінним компонентом доказування з прогнозованою доказовою силою у справах про посягання на основи національної безпеки.

Судовий контроль є ключовим інструментом забезпечення справедливості та законності під час збирання і використання цифрових доказів у кримінальному провадженні щодо злочинів проти основ національної безпеки. На відміну від класичних слідів злочину, цифрова інформація потребує не лише

технічної верифікації, а й ретельного процесуального оцінювання. Слідчий суддя, надаючи дозвіл на доступ до даних або оцінюючи їхню допустимість у судовому розгляді, фактично виступає гарантом дотримання конституційних прав людини на приватність, таємницю комунікацій та захист персональних даних.

Європейський суд з прав людини неодноразово наголошував, що саме незалежний судовий контроль є необхідною умовою правомірного втручання у сферу цифрових комунікацій. Так, у справі *Roman Zakharov v. Russia* [36] Суд підкреслив, що загальні повноваження спецслужб щодо прослуховування без належних процесуальних гарантій створюють серйозну загрозу для верховенства права. У рішенні *Big Brother Watch and Others v. UK* [31] Суд встановив, що масове перехоплення даних можливе лише за умови наявності ефективних механізмів судового контролю і прозорості процедур. У справі *Barbulescu v. Romania* [30] зроблено акцент на необхідності належної мотивації судових рішень, що обмежують право на приватність у сфері цифрової комунікації.

У цій площині, спираючись на наведені конвенційні орієнтири, доцільно підкреслити дві практичні площини судового контролю, тісно пов'язані з особливостями проваджень щодо злочинів проти основ національної безпеки. По-перше, у процедурах спеціального досудового розслідування та спеціального заочного судового провадження відкриті цифрові джерела інформації (OSINT) виконують не лише допоміжну, а й самостійну доказову функцію для встановлення факту переховування підозрюваного/обвинуваченого на тимчасово окупованій території України чи на території держави-агресора. За умови належної процесуальної фіксації (протокол огляду вебресурсу з позначенням URL/URI, дати й часу доступу за UTC, технічних параметрів відтворення та збереження контрольних хеш-сум) цифрові сліди (геомітки, сталі цифрові індикатори місцеперебування, публічні профілі та їх активність) можуть утворювати достатню основу для висновку про реальну недоступність особи для очного провадження та легітимувати застосування інститутів заочного провадження. По-друге, у площині належного повідомлення особи про виклики і процесуальні рішення формальне опублікування повісток у загальнодержавних ЗМІ та на офіційних вебресурсах повинно доповнюватися додатковими відкритими підтвердженнями фактичної обізнаності адресата (зокрема, відбитками перегляду, кореляціями цифрової активності, власними публічними заявами особи про відомість їй змісту обвинувачення). Така багатошарова модель повідомлення зменшує ризики для гарантій, закріплених у статті 6 § 3 (a) Конвенції, і робить висновок суду про належність повідомлення не формальним, а матеріально вмотивованим.

Водночас судовий контроль має поширюватися не лише на законність доступу до цифрових матеріалів, а й *на методологічну якість* OSINT-масивів. Йдеться про вимогу прозорості та відтворюваності способу одержання цифрової інформації: ідентифікація джерела (provenance), фіксація інструментів та середовища збору, документування незмінності (хешування первинних файлів і створених образів), можливість незалежного повторення кроків збору (replicability), ведення журналу доступу, а також експлікація критеріїв надійності джерела (source assessment) і тріангуляція з іншими доказами. У цьому сенсі суд має орієнтувати сторони на дотримання процедурних кроків, рекомендованих Протоколом Берклі для розслідувань з використанням відкритих цифрових джерел: протоколювання ланцюга збереження доказів, збереження оригінальних копій з контрольними сумами, фіксація метаданих і часових міток, опис алгоритмів/застосунків, якими здійснювався захват контенту, та додання службової картки методичних дій. Невиконання цих вимог не обов'язково зумовлює автоматичну недопустимість, однак істотно знижує доказову вагу матеріалу й може вимагати компенсаторних процесуальних гарантій (призначення технічної експертизи, надання захисту реального часу й доступу для контрперевірки).

З огляду на це пропонується сформулювати в національній практиці «міні-тест» судової перевірки OSINT-доказів у заочних провадженнях: (1) *походження* – належне ідентифіковане джерело, відсутність квазіоперативної діяльності приватних осіб; (2) *процедура* – документований спосіб доступу, фіксація метаданих, хешів, часу, інструментів; (3) *верифікованість* – технічна відтворюваність кроків збору, можливість незалежної перевірки; (4) *контрперевірка* – наданий стороні захисту реальний доступ до матеріалів і часу для спростування. Такий підхід поєднує конвенційні стандарти «прозорості та пропорційності» із процесуальною економією й дозволяє легітимно інтегрувати OSINT у доказову систему, не знижуючи планки гарантій справедливого судового розгляду.

Українська судова практика поступово формує власні підходи до використання цифрових технологій і доказів у кримінальному процесі, орієнтуючись на судову практику країн ЄС та ЄСПЛ. В основі цієї еволюції лежить конституційний імператив недопустимості доказів, здобутих «незаконним шляхом» (ч 3 ст. 62 Конституції України), який, у тлумаченні Конституційного Суду України, охоплює як порушення конституційних прав і свобод або встановленої законом процедури, так і «приватну оперативно-розшукову діяльність» осіб, не уповноважених на застосування відповідних заходів. Водночас Суд наголосив: фактичні дані можуть бути випадково або з ініціативи приватних осіб зафіксовані фото-, відео- чи звукозаписами, зокрема з камер спостереження; питання їх допустимості вирішується з

урахуванням поваги до прав людини та перевірюваності походження [34]. Саме цей подвійний підхід – суворість до процесуальних порушень державних органів і водночас відкритість до приватних цифрових слідів – став видимим у справах про злочини проти основ національної безпеки.

Показовою є позиція Касаційного кримінального суду у провадженні щодо державної зради, де ключовим доказовим масивом стали аудіофайли з мобільних телефонів обвинуваченого: голосові повідомлення в Telegram, запис розмови у форматі m4a, а також скриншоти з Google Maps із геопозначками. Суд наголосив, що негласні слідчі (розшукові) дії не проводилися; файли вилучені з пристроїв, добровільно переданих слідству; отже, не йдеться про втручання держави у приватне спілкування, а про фіксацію добровільно розкритої інформації, яка втрачає статус таємниці [42]. Такий підхід збігається з правовою позицією ЄСПЛ: питання допустимості належить до національної компетенції, однак вирішальним є те, чи не порушено загальної справедливості провадження; використання записів, отриманих поза незаконним втручанням держави, не суперечить статті 8 Конвенції за умови забезпечення засад статті 6 (**Khan** v. the United Kingdom; Schenk v. Switzerland) [33; 43]. З огляду на формальний характер ч. 2 ст. 111 КК, коли для кримінальної відповідальності не вимагається настання матеріальної шкоди, цифрові сліди – зміст і адресність голосових повідомлень, часові мітки та координати – виконують функцію демонстрації умислу та добровільності участі у сприянні підривній діяльності й, у підсумку, забезпечують досягнення стандарту «поза розумним сумнівом».

Розширення прийнятності OSINT як окремого каналу доказування також проступає у справах про злочини проти основ національної безпеки України. Верховний Суд визнав, що протоколи огляду веб-сторінок, скриншоти й завантажені відеофайли з відкритих джерел (соціальні мережі, відеохостинги, офіційні сайти окупаційних адміністрацій), оформлені за дорученням слідчого згідно зі ст. 40 КПК і належно приєднані до провадження, є документами у розумінні ст. 99 КПК та можуть бути покладені в основу висновків. У справі щодо колабораційної діяльності та організації «референдуму» сукупність таких електронних матеріалів – інтерв'ю на YouTube, публікації на офіційному сайті «адміністрації», впізнання особи за фотознімками – була визнана достатньою для доведення ролі та умислу обвинуваченої, а закиди захисту про «недостовірність інтернет-даних» відхилено через відсутність ініційованої спеціальної перевірки та внутрішню узгодженість масиву з іншими доказами [44].

Комплементарно адміністративна юрисдикція підтвердила можливість покладання на дані Google Maps як на достовірний електронний документ: сервіс систематизує інформацію з різних джерел із постійним оновленням і верифікацією; відтак за належного процесуального оформлення такі відомості придатні для встановлення фактичних обставин. [45]. У цьому контексті простежується застосування конвенційного тесту: ключового значення набуває не матеріальний носій інформації, а достовірність його джерела та забезпечення реальної можливості ефективної контрперевірки стороною захисту. Такий підхід послідовно відображено у практиці ЄСПЛ, зокрема у справах *Doorson v. the Netherlands* [46] та *Al-Khawaja and Tahery v. the United Kingdom* [47], де Суд наголосив, що допустимість доказів визначається передусім критеріями надійності й забезпечення змагальності, а не їх формальною природою чи технічним способом фіксації.

Проблема «оригінальності» цифрового доказу в українській судовій практиці отримала предметне вирішення на перетині Закону «Про електронні документи та електронний документообіг» [48] і ст. 99 КПК. По-перше, «оригіналом» електронного документа є його відображення (дані), а не конкретний фізичний носій; ідентичні примірники на різних носіях можуть визнаватися оригіналами за умови забезпечення цілісності та перевірюваності походження [49]. По-друге, суд відмовляється від «фетишизації» технічної специфікації: відсутність відомостей про марку камери, її сертифікацію або канал передавання не нівелює доказову силу відео, якщо воно належно витребуване запитом, оглянуте протоколом і відтворене в суді (зокрема записи «Безпечного міста») [50]. По-третє, водночас застосовується підвищений стандарт до копій, достовірність яких неможливо перевірити через невстановлене джерело або знищення первинних записів: у таких випадках похідні експертні висновки, що спираються на сумнівний відеофайл, не можуть підтримати обвинувачення [51].

У свою чергу, такий підхід узгоджується з функціональною логікою ЄСПЛ: визначальним є не формальна ідентичність чи «копійність» доказу, а оцінка ризику його недостовірності та потенційного впливу на загальну справедливість провадження відповідно до стандартів статті 6 Конвенції [52] (Schenk v. Switzerland [43]; Gäfgen v. Germany [53]). При цьому, як слушно підкреслює ЄСПЛ, йдеться про пошук балансу між вимогами процесуальної економії та гарантіями сторони захисту, адже надмірний формалізм у підході до доказів може перетворитися на перешкоду доступу до правосуддя, тоді як ігнорування ризиків недостовірності – на загрозу реальному змісту права на справедливий суд [53, 54].

Процесуальний режим цифрових доказів у значній мірі детермінується правилами відкриття матеріалів та фіксації результатів НСРД. Велика Палата Верховного Суду обґрунтовано сформулювала імператив своєчасного розсекречення та відкриття правових підстав для проведення НСРД (ухвали слідчих суддів, клопотання, доручення), невиконання якого зумовлює недопустимість не лише без-

посередніх результатів, але й похідних доказів [55]. У цьому ж контексті касаційна практика підтвердила, що використання копійних носіїв НСРД без можливості ідентифікувати первинний носій та застосовані технічні засоби суперечить вимогам ч. 3 ст. 254 КПК України й породжує наслідок, відомий у доктрині як «плоди отруєного дерева» [51]. Водночас Об'єднана палата Касаційного кримінального суду внесла суттєве уточнення: складання протоколу НСРД поза межами 24-годинного строку саме по собі не тягне недопустимості доказу; визначальним у такому випадку є відсутність обмеження прав сторін провадження та збереження можливості перевірки достовірності й цілісності відповідного матеріалу [56].

Зіставлення вітчизняної судової практики з європейською практикою свідчить про концептуальну спорідненість: так, у німецькому кримінальному процесі § 100e(6) StPO встановлює чіткі вимоги до документування й збереження даних, акцентуючи на їх цілісності та можливості верифікації [57]; натомість ЄСПЛ у справах *Bykov v. Russia* (10.03.2009) [32] та *Roman Zakharov v. Russia* (04.12.2015) [36] сформував стандарт, згідно з яким недоліки у фіксації або невідкриття правових підстав для втручання становлять ризик порушення статей 6 і 8 Конвенції [52], оскільки підривають довіру до належності й достовірності цифрових доказів. Таким чином, українська практика дедалі більше тяжіє до загальноєвропейського підходу, що поєднує вимоги процесуальної дисципліни із захистом фундаментальних прав сторони захисту.

Додатково Верховний Суд деталізував, що відкриття процесуальних документів, які стали підставою проведення НСРД, уже під час судового розгляду не є автоматичною підставою для визнання недопустимими результатів самих негласних слідчих (розшукових) дій та похідних від них доказів, якщо стороні захисту було надано реальний час і можливість для ефективного їх оспорення [55]. Такий підхід відображає конвенційний стандарт оцінки «процесуальних збоїв»: визначальною є не формальна вада процедури, а її вплив на рівність сторін і справедливість провадження в цілому (Schatschaschwili v. Germany [58]; Al-Khawaja and Tahery v. the United Kingdom [47]).

У цьому аспекті можна погодитися з тим, що надмірний процесуальний формалізм не відповідає меті кримінального процесу, адже його результативність має оцінюватися крізь призму забезпечення права на справедливий судовий розгляд. Водночас допустимість використання результатів НСРД не може тлумачитися як бланкетне схвалення будь-яких процесуальних відхилень: баланс полягає у відмежуванні тих недоліків, які справді позбавляють сторону захисту можливості ефективної контрперевірки, від процедурних огріхів, що не мають істотного впливу на реалізацію засад змагальності й рівності сторін. Саме у цьому полягає зміст конвенційного тесту «справедливості в цілому», який послідовно імплементує Верховний Суд, спираючись на стандарти ЄСПЛ.

У сфері виявлення та кваліфікації явища «провокації злочину» [59] українські суди також наближаються до стандарту, сформульованого у справі Teixeira de Castro v. Portugal [60]: якщо відсутня об'єктивна підозра до початку оперативних заходів, а правоохоронні органи діють не пасивно, а фактично ініціюють збут, результати НСРД визнаються недопустимими, а виправдувальні вироки залишаються чинними.

Натомість у «звичайних» епізодах поза сферою нацбезпеки касація відхиляє закиди щодо ст. 290 КПК, коли диск/документи долучено і досліджено в суді без заперечень сторони захисту, а відео, надане свідком добровільно, розцінюється як належний доказ за умови протокольного огляду і безпосереднього перегляду в засіданні [50]. Водночас там, де відтворюються лише фрагменти відеозапису, які не фіксують інкримінованої події, або де неможливо перевірити цілісність, Верховний Суд послідовно апелює до стандарту «поза розумним сумнівом» і не дозволяє «дотягувати» доказування за рахунок неперевірюваних файлів [51].

У підсумку цифрові технології – OSINT, Google Maps, мобільні месенджери, системи відеоспостереження – стали для національної практики не лише новими каналами збирання (отримання) доказів, а насамперед полем уточнення процесуальних гарантій: від конституційного фільтра недопустимості «незаконних» доказів [1] до матеріального наповнення поняття «оригіналу» електронного документа [49–50] і гнучкого, але вимогливого підходу до НСРД [55–56]. Для злочинів проти основ національної безпеки цей комплекс набуває особливої ваги: формальний склад ч. 2 ст. 111 КК зміщує центр тяжіння з «наслідків» на доказ умислу й добровільності, а отже саме електронні сліди – голосові повідомлення, геомітки, публічні заяви в мережі – забезпечують досягнення необхідного рівня переконливості [42; 44–45]. Рухаючись у фарватері практики ЄСПЛ – справедливого судового розгляду («fair trial first»), пріоритет реальної змагальності над формалізмом – українські суди поступово витворюють стійку модель цифрового доказування, що зберігає процесуальні запобіжники і відповідає викликам гібридних загроз національній безпеці.

На рівні міжнародних актів вирішальним орієнтиром у використанні цифрових технологій та доказів у розслідуванні злочинів проти основ національної безпеки для України є Будапештська конвенція про кіберзлочинність та Другий додатковий протокол до неї [24; 25], які прямо передбачають судовий

контроль як обов'язкову умову для доступу до електронних даних. Директива 2014/41/ЄС щодо Європейського наказу про розслідування [26] також встановлює, що будь-яке транскордонне отримання цифрових доказів має відбуватися за рішенням незалежного органу, що відповідає стандарту судової влади.

У цьому контексті судовий контроль виконує двоєдину функцію: він є, з одного боку, процесуальним запобіжником від свавілля державних органів, а з іншого – гарантією збереження належності та допустимості цифрових доказів у судовому розгляді. Відсутність чітких правил чи формалізований підхід до оцінки електронних даних ставить під загрозу як ефективність розслідування, так і захист прав людини, що особливо небезпечно у справах, пов'язаних із національною безпекою.

Таким чином, забезпечення належного судового контролю є визначальним чинником допустимості цифрових доказів у кримінальному процесі. Його вдосконалення має включати: закріплення спеціальних процедур у КПК України, підвищення незалежності слідчих суддів, обов'язковість повного і мотивованого обґрунтування ухвал, а також адаптацію до стандартів, сформованих ЄСПЛ і Судом ЄС.

Міжнародні стандарти відіграють фундаментальну роль у формуванні національного режиму поводження з цифровими доказами, особливо у справах, що стосуються злочинів проти основ національної безпеки. Україна як держава-учасниця Ради Європи та держава, що прагне інтеграції у правовий простір Європейського Союзу, зобов'язана гармонізувати своє кримінальне процесуальне законодавство з усталеними європейськими підходами.

Ключовим міжнародним документом є Конвенція про кіберзлочинність (Будапештська конвенція) 2001 року [24], яка вперше на міждержавному рівні закріпила обов'язок держав створювати ефективні процедури збирання та збереження електронних доказів. Її Другий додатковий протокол 2022 року [25] уточнив механізми транскордонного доступу до даних, передбачивши вимоги щодо прозорості процедур, захисту приватності та міжнародного судового контролю.

Не менш важливе значення має Директива 2014/41/ЄС про Європейський наказ про розслідування [26], що встановлює уніфіковані правила транскордонного обміну цифровими доказами в межах ЄС. Її положення особливо релевантні для України, оскільки інтеграція в європейський правовий простір вимагає запровадження сумісних процедур отримання й передачі електронних доказів.

У цій площині принциповим видається звернення до Протоколу Берклі щодо розслідувань з використанням відкритих цифрових джерел як до «м'якого» (*soft law*) орієнтира, який практично заповнює прогалину між загальними конвенційними вимогами та щоденною процесуальною рутиною роботи з OSINT у кримінальному провадженні. Його методологічна рамка пропонує те, що в національній юрисдикції бракує на рівні прямої норми: процесуалізацію відкритих джерел через чіткий опис кроків збирання, забезпечення відтворюваності (*reproducibility*) та перевірюваності (*verifiability*) доступу, фіксацію первинності публікації, часу й способу отримання матеріалів, технічну охорону метаданих і контрольних сум, ведення журналів доступу, а також документування застосованих інструментів і параметрів середовища. Унаслідок цього суд отримує не «знімок» мережевого артефакту як такого, а процесуально прозору історію його походження й оброблення, що дозволяє відсікти недостовірні або неперевірені об'єкти та зберегти доказову силу релевантних матеріалів. На мою думку, імплементація рекомендацій Протоколу Берклі у внутрішні методики (із відповідним відображенням у процесуальних протоколах огляду, вилучення та збереження) має подвійний ефект: по-перше, уніфікує підхід до OSINT як різновиду електронних документів із прогнозованою доказовою спроможністю; по-друге, узгоджує національну практику з конвенційними критеріями законності, необхідності та пропорційності втручання у приватну сферу, сформульованими ЄСПЛ. Саме цей зв'язок «процесуальної прозорості» з тестом законності/необхідності/пропорційності, на який орієнтує Європейський суд з прав людини, у поєднанні з вимогами Суду ЄС щодо «внутрішньої еквівалентності» (*internal equivalence*) у транскордонному обігу електронних доказів (*EncroChat*), формує у нас рамку сумісності: доказ, зібраний за стандартом, що забезпечує відтворюваність і перевірюваність методики OSINT, легше інтегрується у процедури взаємної правової допомоги та Європейського наказу про розслідування без ризику втрати допустимості. Інакше кажучи, «берклійська» процесуальна дисципліна щодо відкритих джерел – разом із конвенційними запобіжниками та вимогами Другого додаткового протоколу – підсилює нашу претензію на транскордонну сумісність електронних доказів і водночас знижує ризики для справедливості провадження у розумінні статті 6 Конвенції. Саме тому пропонована мною гармонізація має включати і нормотворчий компонент (мінімальні процесуальні вимоги до огляду вебресурсів, збереження метаданих, хешування, журналювання доступу, опис застосованих інструментів) і організаційний (єдині міжвідомчі протоколи «*OSINT-forensics*», підготовка слідчих суддів, слідчих і прокурорів до оцінки методологічної якості відкритих цифрових джерел). Такий підхід не підміняє закон, але фактично надає українському кримінальному процесу універсальну «мову взаємосумісності» («мову інтероперабельності») з європейськими партнерами й одночасно зміцнює внутрішні процесуальні гарантії, яких вимагає як сучасна цифрова доказова реальність, так і стандарти ЄСПЛ та Суду ЄС.

Значну увагу питанню надійності цифрових слідів приділяють міжнародні стандарти. Так, Європейське агентство з кібербезпеки (ENISA) у звіті *Artificial Intelligence Threat Landscape* [27] наголосило на необхідності оцінки ризиків, пов'язаних із застосуванням штучного інтелекту, зокрема створенням діпфейк-записів та маніпуляцією даними. Національний інститут стандартів і технологій США (NIST) у своєму керівництві з інтеграції криміналістичних методик [28] окреслив вимоги до документування «chain of custody», підкресливши, що лише детальна фіксація всіх етапів доступу до електронного носія може гарантувати збереження доказової сили цифрових даних.

Практика міжнародних судів формує обов'язкові орієнтири для оцінки цифрових доказів. ЄСПЛ у справах *Khan v. UK* [33], *Bykov v. Russia* [32] та *Roman Zakharov v. Russia* [36] послідовно наголошував, що цифрова інформація, здобута з порушенням гарантій приватності, не може вважатися допустимою. У справі *Big Brother Watch and Others v. UK* [31] Суд визнав, що навіть у випадках загрози національній безпеці масове збирання цифрових даних має супроводжуватися пропорційними обмеженнями та ефективними процедурами нагляду.

Особливе значення для України має практика Суду Європейського Союзу. У справі *C-670/22, M.N. (EncroChat)* [37] Суд закріпив концепцію «внутрішньої еквівалентності», відповідно до якої електронні докази, здобуті в іншій державі, можуть визнаватися допустимими лише за умови їхньої відповідності мінімальним гарантіям, прийнятим у національному праві. Подібну логіку простежуємо у рішеннях вищих судів держав ЄС: Федерального суду Німеччини (BGH) [38], Конституційного суду ФРН (BVerfG) [39] та Верховного суду Нідерландів [40], які визнали допустимим використання даних, отриманих у межах операції EncroChat, але за умови дотримання суворих процедурних гарантій.

Таким чином, міжнародні стандарти й судова практика формують базові орієнтири для розвитку українського кримінального процесуального законодавства у сфері цифрових доказів. Їхня імплементація є необхідною умовою забезпечення належного балансу між ефективністю переслідування злочинів проти національної безпеки та захистом фундаментальних прав людини.

Висновки. Умови збройної агресії рф проти України зробили цифрові сліди одним із ключових сегментів доказування у провадженнях про посягання на основи національної безпеки, водночас актуалізувавши три взаємопов'язані блоки проблем – нормативні, інституційні та технологічні. На нормативному рівні все ще відчутною є прогалина у вигляді відсутності автономної дефініції цифрових доказів у кримінальному процесі та деталізованої процедури їх одержання, фіксації, автентифікації та збереження. Це породжує правову невизначеність і підвищує ризик втрати доказового значення або недопустимості значущих електронних масивів через формальні вади. Інституційно брак єдиних стандартів і розірвана координація між слідчими підрозділами та кіберкомпонентами різних оперативних, контррозвідувальних та оперативно-технічних підрозділів Служби безпеки України та інших органів правопорядку призводять до дублювання функцій, втрати темпу і фрагментації практик, особливо в зоні бойових дій та на прилеглих територіях.

У технологічному вимірі правоохоронні органи стикаються з викликами, пов'язаними із застосуванням систем шифрування, анонімізаторів, месенджерів із функцією тимчасового зберігання повідомлень (*disappearing messages*), хмарних екосистем та феномену діпфейку (діпфейк, технології створення штучних аудіо- та відеопідробок із використанням алгоритмів штучного інтелекту). Водночас відчутним залишається дефіцит сертифікованих програмно-апаратних інструментів, ресурсів для безпечного зберігання даних, а також належної фахової підготовки кадрів для роботи з мобільними пристроями, джерелами OSINT (*Open Source Intelligence* – розвідка з відкритих джерел), картографічними сервісами та масивами великих даних.

Розв'язання цього трикомпонентного комплексу проблем вимагає цілісної архітектоніки подальших змін щодо нормативного визначення цифрових доказів, інституційної спроможності органів досудового розслідування та технологічного забезпечення їх автентичності й збереження.

У підсумку обґрунтовується теза, що розвідка з відкритих джерел (OSINT) у провадженнях щодо злочинів проти основ національної безпеки не лише доповнює, а й структурно розширює систему доказування. Вона є релевантною одночасно для головного предмета доказування, визначеного статтею 91 КПК України, для локальних процесуальних рішень (обрання/продовження запобіжних заходів, санкціонування слідчих (розшукових) дій, визначення обсягу тимчасового доступу), а також для встановлення допоміжних фактів – атрибуції, просторово-часової локалізації подій, верифікації джерел і контролю внутрішньої узгодженості цифрових слідів. Придатність OSINT як доказового матеріалу зумовлюється дотриманням методологічної дисципліни та належною процесуальною «документованістю» кожного кроку збору й обробки відкритих даних: постановкою пошукового завдання, фіксацією алгоритмів/запитів, відтворюваним збереженням артефактів із хеш-ідентифікацією, журналюванням дій і належним зберіганням; ці вимоги кореспондують Протоколу Берклі щодо цифрових OSINT-розслідувань.

Звідси випливає необхідність нормативної уніфікації OSINT-процедур у КПК України у поєднанні з національним стандартом «ланцюга збереження доказів», а також покладення на суд обов'язку перевіряти не лише зміст відкритих цифрових масивів, а й якість застосованої методики їх збирання, фіксації та збереження (критерії відтворюваності, цілісності, атрибуції та прозорості). За відсутності такої уніфікації зберігатиметься ризик відсікання ключових цифрових масивів як недопустимих, що спотворюватиме доказову картину у кримінальних провадженнях щодо злочинів, передбачених розділом I Особливої частини КК України («Злочини проти основ національної безпеки України») і знижуватиме ефективність кримінального провадження без доданої цінності для гарантій прав людини.

На рівні закону доцільно закріпити у КПК України самостійне поняття цифрових доказів і мінімальні стандарти їх процесуального обігу: визначити «оригінал» електронного документа як його відображення; встановити презумпцію допустимості технічно відтворюваних копій за умови фіксації цілісності; прописати обов'язкові елементи «ланцюга збереження» (хешування при первинному захопленні, кваліфіковані часові мітки, журнал доступу, опис середовищ зберігання); уніфікувати порядок огляду вебресурсів та OSINT (протоколювання URL/URI, дати й часу в UTC, способу доступу, параметрів відображення, метаданих), а також спеціальні правила роботи з даними хмарних сервісів і мобільних застосунків, включно з транскордонним отриманням електронних доказів у синхронізації з міжнародними інструментами. Паралельно мають бути імплементовані процесуальні запобіжники пропорційності для доступу до приватного контенту – чіткий опис мети, мінімізація обсягу вилучення, деперсоналізація третіх осіб, окреме зберігання надлишкових файлів, прозора процедура судового контролю.

На підзаконному рівні потрібні єдині міжвідомчі інструкції з цифрової криміналістики: стандарти ізоляції пристроїв від мереж і екстракції даних з мобільних телефонів сертифікованими інструментами; методики фіксації OSINT (скриншот із вбудованим хешем і службовою карткою метаданих, повторюваність збору); політика збереження первинних носіїв або верифікованих образів; типові протоколи для огляду, відтворення, копіювання та передачі електронних масивів; уніфіковані правила документування картографічних даних і координат (Google Maps тощо) для їх подальшої верифікації.

Інституційний контур змін має передбачати створення мережі спеціалізованих центрів цифрової криміналістики з акредитованими лабораторіями, національний реєстр валідованих методик і сертифікованих програмних засобів, а також механізм незалежної технічної верифікації спірних електронних об'єктів. Для справ про злочини проти основ національної безпеки доцільно сформувати міжвідомчі групи швидкого реагування, здатні оперативно працювати з OSINT-джерелами, мобільними терміналами, телеком-логами та даними бойової обстановки; для прокурорів і суддів – запровадити постійні навчальні модулі з оцінювання цифрових даних: читання метаданих, перевірки безперервності записів, відмежування приватної ініціативної фіксації від негласних заходів, коректної інтерпретації координат і часових міток.

Технологічний вимір повинен спиратися на модель «дані з атрибутами довіри»: рутинне хешування й збереження контрольних сум у незалежному реєстрі, електронний підпис процесуальних документів, ведення аудиту доступу, захищені сховища для великих масивів і стандартизована технічна документація до кожної серії файлів (джерело, інструмент, версія ПЗ, параметри пристрою, маршрут мережевої доставки).

Окремий блок – протидія штучно модифікованому контенту: можливість призначення «вузьких» технічних перевірок справжності аудіо/відео, стандарти звітування експертів про межі впевненості, обов'язок сторін розкривати використані алгоритми, фільтри й програмні засоби попередньої обробки.

Судовій практиці доцільно запровадити для суддів спеціалізований довідково-методичний посібник *(benchbook)* у справах із цифровими доказами та OSINT, що містить систематизовані роз'яснення, алгоритми дій та узагальнення судової практики з метою забезпечення єдності правозастосування й підвищення ефективності судового контролю. Це забезпечуватиме єдність правозастосування через чіткі алгоритми перевірки й типові формулювання мотивів судового рішення. Мінімальний зміст такого *посібника* має охоплювати: по-перше, чек-лист за тріадою «походження – процедура – верифікація», де суддя послідовно встановлює: ідентифіковане походження даних (уповноваженість суб'єкта на збирання цифрових доказів; відсутність делегування квазіоперативних функцій приватним особам; фіксація ланцюга збереження доказів*)* й журнал аудиту від першого доступу до долучення в матеріали), законність і прозорість процедури здобуття (правові підстави, технічна методика, хеш-ідентифікація, незмінність «сирих даних» (файлів), а також незалежну верифікацію результату (можливість стороннього повторення за наданими інструкціями, контрольними сумами та метаданими); по-друге, уніфікований тест допустимості електронних доказів із трьох вузлів: *походження* (суд перевіряє правосуб'єктність і повноваження того, хто збирав дані, та відсутність прихованої «оперативної» активності з боку приватних осіб; безперервність ланцюга збереження й незмінність *«сирі (raw) дані» (далі – «сирі дані»)* підтверджуються хешами, журналами доступу та описом середовища), *відкриття* (стороні захисту своєчасно надано достатній доступ до «сирих даних» (файлів), методики та інструментів, що забезпечує реалістичну

можливість незалежної експертизи; відсутність доступу або надання лише скриншотів без метаданих тягне сумнів у справедливості провадження), *відтворюваність* (за долученими інструкціями, версіями ПЗ, параметрами та контрольними сумами незалежний фахівець може отримати ідентичний результат; суд встановлює межі похибки та джерела її виникнення); по-третє, короткі алгоритми для специфічних підвидів цифрових даних, зокрема для картографії/Google Maps: подвійна проєкція координат (WGS84 ↔ альтернативна/національна система) з прямим і зворотним перетворенням і порівнянням відхилення; крос-валідація з телеком-логами та/або офіційними довідками оператора (CDR, Cell-ID/IMSI, сектор, *Timing Advance*), за можливості – з *EXIF*, Wi-Fi/BSSID і відеоспостереженням; ведення повного журналу аудиту з позначками часу та цифровими підписами. Для забезпечення однакової аргументації довідково-методичний посібник для суддів має містити й типові формули мотивувальної частини для OSINT: у випадку прийняття доказу – «Суд установив, що електронні дані походять від уповноваженого суб'єкта; спосіб їх одержання був *відповідно до закону* та технічно прозорий; стороні захисту надано своєчасний і достатній доступ до «сирих даних» (файлів), метаданих і методики; результат відтворюваний за наданими інструкціями та контрольними сумами, межі похибки визначені», – та у випадку відхилення – «Суд відхиляє цифрові дані як недопустимі через неідентифіковане/неуповноважене походження, ненадання «сирих даних» (файлів) і метаданих для перевірки та/або неможливість незалежного відтворення результату, що підриває справедливість провадження». Такий підхід одночасно підвищує доказову цінність надійних цифрових джерел і дисциплінує практику, мінімізуючи ризики маніпуляцій, процесуальних пасток і випадкового відсікання релевантних даних.

Оптимізація кримінального провадження в умовах воєнного стану передбачає впровадження процесуальних механізмів пріоритетного розгляду, які забезпечують баланс між оперативністю судового розгляду та дотриманням фундаментальних гарантій прав людини (гарантії): стандартизовані шаблони протоколів огляду вебресурсів і картографічних сервісів, порядок підтвердження координат OSINT з офіційних карт і довідок компетентних органів, типові форми запитів до військових частин, спеціальний режим збереження конфіденційних і класифікованих цифрових матеріалів із контрольованим доступом і процесуальною логістикою їх дослідження в суді. Така ж логіка має поширюватися на роботу з даними мобільних телефонів і месенджерів: чіткі стандарти фіксації, збереження і відтворення голосових повідомлень, листування та системних журналів, а також правила поєднання таких даних із картографічними прив'язками та відкритими джерелами.

У підсумку, наукова новизна та практична значущість дослідження полягають у тому, що запропоновано: (а) уніфікований тест допустимості електронних доказів – «походження – відкриття – відтворюваність» – і його інструменталізацію у вигляді спеціалізованого довідково-методичного посібника для суддів з типовими формулами мотивування; (б) процедуру цифрової криміналістики відкритих джерел (OSINT-forensics) з чіткими вимогами до фіксації, ланцюга збереження ланцюга збереження доказів та журналу аудиту; (в) алгоритм судової перевірки координат (подвійна проєкція, крос-валідація з телеком-логами/офіційними довідками, журнал доступу) як окремий інструмент верифікації; (г) перенесення стандартів Benedik/Uzun і принципу «внутрішньої еквівалентності» зі справи C-670/22 (EncroChat) у конкретні пропозиції щодо нормативного закріплення в КПК України. Сукупно це забезпечує єдність і передбачуваність правозастосування, підвищує доказову надійність цифрових матеріалів та узгоджує національну практику з європейськими стандартами справедливого судового розгляду.

Узгоджена реалізація цих кроків забезпечить подвійний ефект. З одного боку, вона підвищить ефективність розслідування злочинів проти основ національної безпеки України, де цифрова тканина події часто є головним носієм інформації, а доказування нерідко має справу з формальним складом діяння, коли вирішальними стають OSINT-масиви, координати з картографічних сервісів і вміст мобільних пристроїв. З іншого – зміцнить процесуальні гарантії і стандарти справедливого суду шляхом прозорої фіксації походження, належного відкриття та перевірюваної відтворюваності електронних даних, що кореспондує із європейськими підходами до допустимості доказів і пропорційності втручання у приватне життя. У підсумку саме поєднання ефективності та гарантій, підсилене уніфікованою технічно-процесуальною рамкою і здатністю судів працювати з цифровою доказовою реальністю, надасть українській кримінальній юстиції легітимності й стійкості в умовах гібридної війни та пришвидшить зближення з кращими практиками європейського правового простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бондар В.С., Парфьонов В.Ю. Про особливості застосування новітніх технологій у документуванні воєнних злочинів. *Прикарпатський юридичний вісник.* 2024. №6. С. 118–123. URL: http://pjv.nuoua.od.ua/v6_2024/24.pdf.
2. Дуфенюк О.М. Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації. *Baltic Journal of Legal and Social Sciences.* 2022. № 1. С. 46–56. URL: http://baltijapublishing.lv/index.php/bjlss/article/view/1771/1789.

3. Кваліфікація та розслідування окремих видів злочинів проти основ національної безпеки та воєнних злочинів: навч. посіб. / О.Ф. Бантишев, І.В. Гора, В.В. Малюк, М.А. Погорецький та ін.; за ред. В.А. Колесника. Київ: 7БЦ, 2022. 356 с.
4. Метелев О.П. Проблемні аспекти фіксації відомостей, отриманих з транспортних телекомунікаційних мереж. *Вісник кримінального судочинства.* 2022. № 3–4. С. 28–37. URL: https://vkslaw.knu.ua/ua/3-4-2021-aktualni-problemy-kryminalnoho-sudochynstva/322-problemy-kryminalnoho-protsesu/1089-problemni-aspekty-fiksatsii-vidomostei-otrymanykh-z-transportnykh-telekomunikatsiinykh-merezh.
5. Пчеліна О., Фоміна Т. Особливості проведення огляду місця події під час досудового розслідування злочинів, пов'язаних зі збройною агресією проти України. *Науковий вісник ДДУВС.* 2023. № 2. С. 254–258. URL: https://dspace.univd.edu.ua/entities/publication/d3255a0f-e170-4dfc-8ef0-6b2f8ca04d82.
6. Тетерятник Г.К., Бех О.В., Одажиу Ю.М. Розслідування воєнних злочинів: окремі теоретико-прикладні питання. *Юридичний науковий електронний журнал.* 2023. № 6. С. 95–105. URL: http://lsej.org.ua/6_2023/161.pdf.
7. Чернявський С.С., Присяжний В.І., Стрільців О.М. та ін.; за ред. М.С. Цуцкіридзе. *Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: метод. рек.* Київ: НАВС, 2023. 92 с. URL: https://elar.navs.edu.ua/items/02907f6a-e6b8-47b8-aa5d-9a747b24a7d3.
8. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Burlington: Academic Press, 2011. 840 p. ISBN 978-0-12-374268-1 (print); eBook ISBN 978-0-08-092148-8. URL: https://shop.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-08-092148-8.
9. Mason S., Seng D. (eds.). Electronic Evidence and Electronic Signatures. 5th ed. London: University of London, 2021. 604 p. URL: https://library.oapen.org/bitstream/handle/20.500.12657/55755/9781911507246.pdf?sequence=1&isAllowed=y.
10. Oerlemans, J.J.; Royer, S. The future of data-driven investigations in light of the Sky ECC operation. *New Journal of European Criminal Law*, 2023. URL: https://journals.sagepub.com/doi/full/10.1177/20322844231212661.
11. Oerlemans J.J., van Toor T. Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime*, *Criminal Law and Criminal Justice*. 2022. 30. P. 309–328. DOI: 10.1163/15718174-bja10037. URL:https://www.researchgate.net/publication/366687140_Legal_Aspects_of_the_EncroChat_Operation_A_Human_Rights_Perspective.
12. Stoykova R. EncroChat: The Hacker with a Warrant and Fair Trials*? Forensic Science International: Digital Investigation.* 2023. Vol. 46. Art. 301602. URL: https://www.sciencedirect.com/science/article/pii/S2666281723001142.
13. Погорецький М.А. Проблеми використання матеріалів оперативно-розшукової діяльності в кримінальному процесі: монографія. Київ: РВВ НА СБУ, 2004. 336 с.
14. Погорецький М.А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Харків: Арсіс ЛТД, 2007. 576 с.
15. Погорецький М.А. Оперативно-розшукова діяльність і кримінальний процес: проблеми взаємозв'язку: монографія: у 2 ч. Луганськ: ЛДУВС ім. Е.О. Дідоренка, 2008. Ч. 1. 216 с.
16. Погорецький М.А. Теоретичні й практичні проблеми використання матеріалів ОРД у кримінальному процесі (за матеріалами СБУ): автореф. дис. … д-ра юрид. наук. Київ: КНУВС, 2006. 36 с.
17. Погорецький М.А. Докази у кримінальному процесі. *Вісник прокуратури.* 2003. № 2. С. 59–65.
18. Погорецький М.А. Прослуховування телефонних розмов: європейські стандарти. *Вісник прокуратури.* 2003. № 9. С. 45–51.
19. Погорецький М.А., Шумило М.Є. Проблеми використання матеріалів ОРД у доказуванні у кримінальних справах. *Вісник Луганського ін-ту внутр. справ.* 2001. Вип. 3. С. 199–209.
20. Погорецький М.А. Закон України «Про оперативно-розшукову діяльність»: проблеми застосування окремих норм*. Вісник Академії правових наук України.* 2001. №3. С. 205–213.
21. Погорецький М.А., Лисаченко Є.І. Допустимість доказів у праві країн ЄС та його вплив на кримінальне судочинство України. Вісник кримінального судочинства. 2022. № 3–4. С. 20–34. URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3-4_22_231024_avt%20(2)-20-34.pdf.
22. Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). Вісник кримінального судочинства. 2023. № 3–4. С. 84–102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf.

23. Погорецький М.А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. Аналітично-порівняльне правознавство. 2025. № 4 (ч. 3). С. 269–279. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42-2.pdf.
24. Convention on Cybercrime (Budapest Convention). ETS No. 185, 23 November 2001. Council of Europe. URL: https://www.coe.int/web/conventions/full-list?module=treaty-detail&treatynum=185.
25. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. CETS No. 224, 12 May 2022. Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.
26. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. *Official Journal of the European Union*, L 130, 1 May 2014, p. 1–36. URL: https://eur-lex.europa.eu/eli/dir/2014/41/oj.
27. European Union Agency for Cybersecurity (ENISA). *Artificial Intelligence Threat Landscape*. 15 December 2020. ENISA Publications. URL: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.
28. National Institute of Standards and Technology (NIST). Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86. Gaithersburg, MD: NIST, August 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.
29. Benedik v. Slovenia. № 62357/14, Judgment of 24 April 2018. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-182455.
30. Uzun v. Germany. № 35623/05, Judgment of 2 September 2010. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-100293.
31. Big Brother Watch and Others v. the United Kingdom. №№ 58170/13, 62322/14, 24960/15, Judgment of 25 May 2021. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-210077.
32. Bykov v. Russia. № 4378/02, Judgment of 10 March 2009. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-91561.
33. Khan v. the United Kingdom. № 35394/97, Judgment of 12 May 2000. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-58527.
34. Конституція України: Закон України від 28 червня 1996 року № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80.
35. Prade v. Germany. № 71891/10, Judgment of 3 March 2016. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-160313.
36. Roman Zakharov v. Russia. № 47143/06, Judgment of 4 December 2015. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-159324.
37. Court of Justice of the European Union (CJEU). Case C-670/22, M.N., Judgment of 30 April 2024 (EncroChat). URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=283677&pageIndex=0&doclang=EN.
38. Bundesgerichtshof (BGH). Urteil vom 2. März 2022 – 5 StR 457/21 (EncroChat). Bundesgerichtshof, Germany. URL: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2022_en/2022038.html.
39. Bundesverfassungsgericht (BVerfG). Order of 1 November 2024, 2 BvR 684/22 (EncroChat). Federal Constitutional Court of Germany. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2024/11/rs20241101_2bvr068422en.html.
40. Hoge Raad der Nederlanden. Supreme Court ruling in EncroChat and SkyECC cases, 13 June 2023. Supreme Court of the Netherlands. URL: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2023:913.
41. Конституційний Суд України. Рішення від 20.10.2011 № 12-рп/2011 (справа № 1-31/2011) «…обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом…». Офіційна публікація. URL: https://zakon.rada.gov.ua/laws/show/v012p710-11/print.
42. Верховний Суд (Касаційний кримінальний суд, Третя судова палата). Постанова від 13.03.2024 у справі № 953/3558/22 (провадження № 51-6103км23). ЄДРСР. URL: https://reyestr.court.gov.ua/Review/117757857.
43. Schenk v. Switzerland. № 10862/84, Judgment of 12 July 1988. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-57572.
44. Верховний Суд (Касаційний кримінальний суд, Третя судова палата). Постанова від 12.06.2024 у справі № 569/1908/23 (провадження № 51-1430км24). ЄДРСР. URL: https://reyestr.court.gov.ua/Review/119741340.

45. Верховний Суд (Касаційний адміністративний суд). Постанова від 20.06.2023 у справі № 420/4540/22 (адміністративне провадження № К/990/32869/22). ЄДРСР; iPlex. URL: https://iplex.com.ua/doc.php?regnum=111663260.
46. Doorson v. the Netherlands. № 20524/92, Judgment of 26 March 1996. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-57972.
47. Al-Khawaja and Tahery v. the United Kingdom. № 26766/05, 22228/06, Judgment of 15 December 2011. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-108778.
48. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.
49. Верховний Суд (Касаційний кримінальний суд, Третя судова палата). Постанова від 20.06.2022 у справі № 646/8454/17 (провадження № 51-381км22). ЄДРСР; iPlex. URL: https://iplex.com.ua/doc.php?regnum=105012014.
50. Верховний Суд (Касаційний кримінальний суд, Третя судова палата). Постанова від 08.02.2023 у справі № 201/2609/20 (провадження № 51-3907км22). ЄДРСР; iPlex. URL: https://iplex.com.ua/doc.php?regnum=108930823.
51. Верховний Суд (Касаційний кримінальний суд, Друга судова палата). Постанова від 31.10.2019 у справі № 404/700/17 (провадження № 51-4451км19). ЄДРСР. URL: https://reyestr.court.gov.ua/Review/85390646.
52. Конвенція про захист прав людини і основоположних свобод від 04.11.1950, ратифікована Законом України від 17.07.1997 № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
53. Gäfgen v. Germany. № 22978/05, Judgment of 1 June 2010. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-99145.
54. Погорецький М.А., Гриценко І.С. Право на справедливий суд. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2012. № 91. С. 4–7.
55. Велика Палата Верховного Суду. Правові позиції щодо відкриття матеріалів НСРД (застосування ст. 290 КПК) у зв'язку з постановою від 16.10.2019 у справі № 640/6847/15-к (провадження № 13-43кс19). База правових позицій ВС. URL: https://lpd.court.gov.ua/legal-position/4313/document/12960.
56. Об'єднана палата Касаційного кримінального суду. Постанова від 25.09.2023 у справі № 208/2160/18 (щодо наслідків порушення строку, передбаченого ч. 3 ст. 252 КПК). База правових позицій ВС. URL: https://lpd.court.gov.ua/legal-position/4315/document/4520.
57. Strafprozessordnung (StPO). German Code of Criminal Procedure of 7 April 1987 (BGBl. I S. 1074, 1319), as amended up to BGBl. I S. 3009, 2021. § 100e(6). URL: https://www.gesetze-im-internet.de/stpo/__100e.html.
58. Schatschaschwili v. Germany. № 9154/10, Judgment of 15 December 2015. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-159324.
59. Погорецький М.А. Застосування провокації в ході негласних розслідувань: питання правомірності. *Вісник кримінального судочинства*. 2016. № 1. С. 33-43.
60. Teixeira de Castro v. Portugal. № 25829/94, Judgment of 9 June 1998. European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-58100.