УДК 343.1:343.98:341.4(477)
DOI https://doi.org/10.24144/2788-6018.2025.06.3.94

ДОКУМЕНТУВАННЯ І ДОКАЗУВАННЯ МІЖНАРОДНИХ ЗЛОЧИНІВ В УКРАЇНІ: ПРОЦЕСУАЛЬНО-КРИМІНАЛІСТИЧНІ ТА ЦИФРОВІ СТАНДАРТИ ПРИЙНЯТНОСТІ ДОКАЗІВ ДЛЯ МІЖНАРОДНОГО КРИМІНАЛЬНОГО СУДУ ТА СПЕЦІАЛЬНОГО ВІЙСЬКОВОГО ТРИБУНАЛУ

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

Погорецький М.А. Документування і доказування міжнародних злочинів в Україні: процесуально-криміналістичні та цифрові стандарти прийнятності доказів для Міжнародного кримінального суду та спеціального військового трибуналу.[1]

Стаття присвячена комплексному дослідженню теоретичних і практичних засад документування та доказування міжнародних злочинів в Україні в умовах збройної агресії російської федерації з урахуванням процесуально-криміналістичних і цифрових стандартів прийнятності доказів для Міжнародного кримінального суду та спеціального військового трибуналу. Розкрито роль органів правопорядку України – Служби безпеки України, Державного бюро розслідувань, Національної поліції, а також Офісу Генерального прокурора – у забезпеченні належної фіксації, перевірки, процесуальної оцінки та збереження доказів воєнних злочинів і злочинів проти людяності з орієнтацією на вимоги міжнародного кримінального правосуддя.

Обґрунтовано необхідність інтеграції міжнародних і європейських стандартів цифрового доказування у національну систему кримінального процесу, зокрема положень Римського статуту Міжнародного кримінального суду, Берклійського протоколу щодо розслідування цифрових відкритих джерел та Настанов належної практики Європейської мережі судово-експертних установ у сфері цифрової криміналістики. Проаналізовано принцип комплементарності (стаття 17 Римського статуту), критерії прийнятності справ і доказів (небажання, неспроможність, тяжкість, та сама особа / те саме діяння), а також практику Міжнародного кримінального суду у справах «Онгвен», «Руто та Санг», «Каддафі та Ас-Сенуссі».

Окрему увагу приділено використанню технологій штучного інтелекту в аналітичній діяльності правоохоронних органів, а також правовим і етичним обмеженням застосування алгоритмів під час перевірки достовірності та допустимості цифрових доказів. Запропоновано створення єдиної міжвідомчої платформи «Український центр цифрових доказів» для централізованого збору, перевірки, збереження та передачі доказів міжнародних злочинів. Доведено, що впровадження уніфікованих цифрових і процесуальних стандартів створює передумови для визнання доказів, зібраних в Україні, прийнятними в міжнародному кримінальному провадженні та забезпечує реалізацію принципу невідворотності відповідальності за злочин агресії, воєнні злочини й злочини проти людяності.

Ключові слова: документування міжнародних злочинів; розслідування; доказування; воєнні злочини; злочини проти людяності; допустимість доказів; комплементарність; Міжнародний кримінальний суд; Римський статут; цифрові докази; протокол Берклі; стандарти ENFSI; штучний інтелект; Український центр цифрових доказів; органи правопорядку України, прокуратура; Євроюст, ЄСПЛ.

---

[1] ***Спеціальний військовий (ad hoc) трибунал щодо злочину агресії рф*** *– Special Tribunal for the Crime of Aggression against Ukraine (STCoA)* юридично започаткований 25.06.2025 Угодою Україна–РЄ; зараз він проходить стадію інституційного розгортання, повномасштабна робота (локація, склад, процесуальні дії) – у процесі визначення/формування. Агентство ЄС з питань співробітництва у сфері кримінального правосуддя (European Union Agency for Criminal Justice Cooperation – Eurojust, Франція, Гаага) повідомляє: Міжнародний центр переслідування злочину агресії проти України (ICPA) вже готує справи до майбутнього трибуналу; у жовтні 2025 р. прокурори ЄС/України узгоджували трансфер розслідувань саме до майбутнього трибуналу. **ICPA** – координаційний центр прокурорів при Eurojust (Гаага), який збирає, зберігає та аналізує докази злочину агресії рф проти України й готує справи для подальшого кримінального переслідування злочинців.

Pohoretskyi M.A. Documentation and proof of international crimes in Ukraine: procedural, forensic, and digital standards of evidence admissibility for the International Criminal Court and a special military tribunal.

The article is devoted to a comprehensive study of the theoretical and practical foundations of documenting and proving international crimes in Ukraine in the context of the armed aggression of the Russian Federation, with due regard to procedural, forensic, and digital standards of admissibility of evidence for the International Criminal Court and a special military tribunal. The role of Ukraine's law enforcement authorities—the Security Service of Ukraine, the State Bureau of Investigation, the National Police, as well as the Office of the Prosecutor General—is examined in ensuring the proper recording, verification, procedural assessment, and preservation of evidence of war crimes and crimes against humanity, in line with the requirements of international criminal justice.

The necessity of integrating international and European standards of digital evidence into the national criminal procedure system is substantiated, in particular the provisions of the Rome Statute of the International Criminal Court, the Berkeley Protocol on Digital Open Source Investigations, and the Best Practice Manuals of the European Network of Forensic Science Institutes in the field of digital forensics. The article analyzes the principle of complementarity (Article 17 of the Rome Statute), the criteria for the admissibility of cases and evidence (unwillingness, inability, gravity, the same person / the same conduct), as well as the practice of the International Criminal Court in the cases of *Ongwen*, *Ruto and Sang*, and *Gaddafi and Al-Senussi*.

Particular attention is paid to the use of artificial intelligence technologies in the analytical activities of law enforcement agencies, as well as to the legal and ethical limitations on the use of algorithms in verifying the reliability and admissibility of digital evidence. The article proposes the establishment of a unified interagency platform—the "Ukrainian Centre for Digital Evidence"—for the centralized collection, verification, preservation, and transfer of evidence of international crimes. It is demonstrated that the implementation of unified digital and procedural standards creates the prerequisites for recognizing evidence collected in Ukraine as admissible in international criminal proceedings and ensures the realization of the principle of the inevitability of accountability for the crime of aggression, war crimes, and crimes against humanity.

Key words: documentation of international crimes; investigation; evidentiary process; war crimes; crimes against humanity; admissibility of evidence; principle of complementarity; International Criminal Court (ICC); Rome Statute of the International Criminal Court; digital evidence; Berkeley Protocol on Digital Open Source Investigations; ENFSI standards; artificial intelligence (AI); Ukrainian Centre for Digital Evidence; Ukrainian law enforcement authorities and the prosecution service; Eurojust; European Court of Human Rights (ECtHR).

Постановка проблеми. Повномасштабна збройна агресія рф проти України актуалізувала комплексну проблему документування та доказування міжнародних злочинів, передусім воєнних злочинів і злочинів проти людяності. За цих умов кримінальне провадження стикається не лише з необхідністю фіксації окремих фактів порушення норм міжнародного гуманітарного права, а з викликом побудови цілісної процесуально-криміналістичної архітектоніки доказового забезпечення, здатної трансформувати значний масив різнорідних відомостей у належні, допустимі, достовірні та достатні докази як для національного правосуддя, так і для розгляду справ у Міжнародному кримінальному суді. У цьому контексті документування міжнародних злочинів виходить за межі суто процесуальної діяльності та набуває значення елементу системи національної безпеки, спрямованого на запобігання безкарності, відновлення прав потерпілих і зміцнення довіри міжнародної спільноти до спроможності держави забезпечувати справедливе правосуддя.

Характерною рисою сучасного етапу розвитку документування та доказування міжнародних злочинів в Україні є стрімке зростання ролі цифрових доказів, зокрема відео- й фотоматеріалів, даних супутникової зйомки, телекомунікаційних і мережевих журналів подій, інформації з мобільних пристроїв та відкритих джерел (OSINT). Водночас динамічність цифрового середовища, поширення шифрування, ризики маніпуляцій і фальсифікацій (зокрема з використанням технологій deepfake), а також неоднорідність відомчих підходів до збирання й обробки таких даних істотно ускладнюють забезпечення їх процесуальної якості. Це зумовлює об'єктивну потребу в стандартизованих техніко-процесуальних рішеннях, які охоплюють увесь життєвий цикл цифрового доказу – від моменту його виявлення й вилучення до представлення та оцінки судом.

Ключовою передумовою допустимості цифрових доказів у кримінальному провадженні, зокрема з огляду на перспективу їх використання в міжнародному кримінальному правосудді, є забезпечення безперервного, процесуально простежуваного і документально підтвердженого ланцюга збереження доказів (*chain of custody*), застосування сертифікованих засобів фіксації та аналізу,

відтворюваності процесуальних і технічних процедур, а також дотримання принципів пропорційності, прозорості й підконтрольності людському контролю (*human oversight*) втручання у приватну сферу. В Україні ці вимоги поступово імплементуються шляхом оновлення кримінального процесуального та спеціального законодавства, нарощування інституційної спроможності органів, що здійснюють оперативно-розшукову, контррозвідувальну діяльність та досудове розслідування і прокуратури, а також посилення міжвідомчої координації між Службою безпеки України, Міністерством оборони, Державним бюро розслідувань, Національною поліцією, Національною гвардією, Прикордонною Службою, Офісом Генерального прокурора у взаємодії з міжнародними партнерами.

У такій ситуації сутність наукової та практичної проблеми полягає у відсутності в Україні цілісної, уніфікованої та процесуально гарантованої системи роботи з цифровими доказами міжнародних злочинів, яка б забезпечувала їх належність, допустимість і відтворюваність відповідно до стандартів національного та міжнародного кримінального правосуддя, насамперед Міжнародного кримінального суду. Фрагментарність нормативного регулювання, інституційна роз'єднаність і технологічна неоднорідність технічних засобів, форматів даних і процедур їх процесуального супроводу на різних стадіях кримінального провадження безпосередньо впливають на перспективу визнання зібраних доказів і, як наслідок, на реалізацію принципу невідворотності відповідальності за злочин агресії, воєнні злочини та злочини проти людяності.

Аналіз останніх досліджень і публікацій. Проблематика документування й доказування міжнародних злочинів у сучасній доктрині склалася у трьох взаємопов'язаних вимірах: (1) *міжнародно-правовому*, де досліджуються юрисдикційні засади, прийнятність (прийнятність) справи (*«admissibility of cases»*) та принцип комплементарності [1; 20; 31; 32; 34; 35]; (2) *кримінально-процесуальному*, що визначає критерії *законності*, *належності*, *допустимості доказів* (*«admissibility of evidence»*) і достовірності відповідно до Правил процедури і доказування Міжнародного кримінального суду (*Rules of Procedure and Evidence*) та норм національного кримінального процесу [2; 14–19]; (3) *криміналістично-цифровому*, який окреслює стандарти виявлення, фіксації, вилучення, хешування та збереження електронних слідів із забезпеченням *ланцюга збереження доказів* (*«chain of custody»*), процесуальної перевірюваності (верифікованості) й відтворюваності процедур, у тому числі під час використання розвідки з відкритих джерел (*«open-source intelligence», OSINT)* та інших цифрових інструментів, що кодифіковані Протоколом Берклі[2] [22], Настановами Європейської мережі судово-експертних установ у галузі цифрової криміналістики (ENFSI BPM–DF)[3] [23] і стандартами ISO/IEC щодо ідентифікації, збирання та збереження цифрових доказів *[56–58],* а також підходами до аналітики на основі штучного інтелекту («artificial intelligence/AI») з обов'язковими вимогами до пояснюваності *(«explainability»),* попереднього й наступного контролю *(«ex ante / ex post»)* та підконтрольності людині *(«human oversight»)* як умов процесуальної придатності результатів алгоритмічної обробки [36].

У сучасній науковій літературі сформовано цілісний авторський доктринальний підхід до кримінального процесуального доказування, у межах якого обґрунтовано функціональний зв'язок оперативно-розшукової діяльності, негласних заходів і процесуальної форми кримінального провадження як передумови легалізації результатів аналітичної та доказової діяльності [30–45]. Значна увага приділяється проблематиці допустимості й достовірності доказів у національному та європейському кримінальному процесуальному праві, з акцентом на вплив стандартів Європейського Союзу, практики міжнародних судових інституцій і принципу *верховенства права* на формування української моделі доказування, зокрема через вимоги законності способу одержання доказів, передбачуваності процедур і процесуальної доброчесності [42; 43; 48; 52; 53].

Окремий масив досліджень охоплює *використання цифрових технологій та аналітичних інструментів* у документуванні воєнних злочинів, злочинів проти людяності й злочинів проти основ націо-

---

[2] Цифрові ресурси, супутникові знімки, відкриті дані й матеріали розвідки з відкритих джерел (**OSINT**) стали невід'ємними елементами доказової бази у справах про міжнародні злочини. У відповідь на це Офіс Верховного комісара ООН з прав людини спільно з Університетом Берклі розробив ***Берклійський протокол щодо цифрових відкритих джерел розслідувань*** *(Berkeley Protocol on Digital Open Source Investigations),* який відомий в україномовному середовищі як – ***Протокол Берклі, Берклійський протокол*** (*Berkeley Protocol).* Цей протокол закріпив міжнародні стандарти роботи з цифровими доказами – від збору до їх верифікації (перевірки й оцінки достовірності). Його принципи – достовірність, відтворюваність і прозорість походження – стали фундаментом сучасної методології документування й доказування воєнних злочинів та злочинів проти людяності й геноцида, зокрема в Україні.

[3] ***ENFSI Best Practice Manuals – Digital Forensics*** *(BPM*) – це оновлена серія методичних настанов належної практики у сфері цифрової криміналістики, підготовлена профільними робочими групами Європейської мережі судово-експертних установ (ENFSI) та затверджувана Правлінням Європейської мережі судово-експертних установ **(ENFSI)**. Кожен BPM має власну редакцію й дату ухвалення (напр., 11.2015; 18.10.2021; 16.12.2022; 7.12.2023); актуальні версії оприлюднюються на офіційному сайті ENFSI (розділ *Best Practice Manuals*). Офіційний сайт ENFSI: **enfsi.eu** (European Network of Forensic Science Institutes).

нальної безпеки, де наголошується на необхідності поєднання процесуальних гарантій із технічними стандартами автентичності, ланцюга збереження доказів і відтворюваності цифрових процедур [44–47; 49]. У цьому контексті подальший розвиток національної моделі доказування пов'язується з уточненням процесуальних меж втручання у приватну сферу під час збирання цифрових доказів, насамперед у межах обшуку та онлайн-обшуку, із суворим дотриманням принципів необхідності, пропорційності та ефективного попереднього й наступного судового контролю [51].

Новітні авторські праці розвивають концепцію комплементарності, цифрових стандартів доказування та обмеженого, допоміжного використання штучного інтелекту в розслідуванні міжнародних злочинів, підкреслюючи значення міжнародної сумісності доказів і процесуальної доброчесності як визначальних умов їх допустимості та ефективного притягнення до відповідальності, з огляду на ризик трансформації будь-яких відхилень від цих вимог у підстави для визнання доказів недопустимими [50–53].

Водночас центральним теоретичним вузлом залишається *принцип комплементарності* (*«complementarity»*)[4] як організаційна конструкція співвідношення міжнародної та національної кримінальної юрисдикції. У вітчизняній науці він системно обґрунтований, зокрема у статті В. Попка, який обґрунтовано виокремлює три моделі співвідношення: *горизонтальну* (взаємодія між державами), *вертикальну* (відносини «держава – міжнародний суд» із презумпцією пріоритету міжнародної юрисдикції у разі *небажання/нездатності* держави), а також *паралельну* (похідну від практики спеціальних «*ad hoc*» трибуналів) [46].

У зарубіжній доктрині комплементарність трактується як принцип особливого (*«sui generis»*) штибу, що поєднує повагу до суверенітету з інституційними механізмами подолання безкарності; при цьому підкреслюється значення *позитивної (проактивної) комплементарності* (*«positive / proactive complementarity»*) як політики заохочення й підтримки спроможностей держав до сумлінного національного переслідування, на відміну від їх заміщення міжнародною юстицією [20; 31–35].

З методологічного погляду, на нашу думку, принципово необхідно розрізняти *два рівні*: по-перше, *прийнятність конкретної справи* перед МКС (*«admissibility of cases»*) – юрисдикційний фільтр за статтею 17 Римського статуту, що спирається на критерії небажання чи неспроможності держави, тяжкості злочину та тест «та сама особа / те саме діяння» і застосовується Палатами Суду у кожній конкретній справі [1; 14–16; 20]; по-друге, *допустимість конкретних доказів* (*«admissibility of evidence»*), яка оцінюється через призму вимог до джерела і способу отримання, автентичності, надійності та дотримання гарантій справедливого судового розгляду відповідно до Правил процедури і доказування МКС, а також приписів національного процесуального права [2; 14–19]. Юриспруденція Міжнародного кримінального суду у справах *Dominic Ongwen*, *William Ruto і Джошуа Арап Санг*, *Saif Al-Islam Gaddafi та Абдулла Аль-Сенуссі*, *Bosco Ntaganda*, *Ahmad Al Faqi Al Mahdi*, *Germain Katanga та Маттьє Нгуджоло Чуі* послідовно підтверджує таке розмежування, виробляючи «тест реальності» (*genuineness / capacity*) на рівні статті 17 та автономні критерії допустимості доказів на рівні процесуальної форми [14–19; 2]. Європейський вимір доповнює практика Європейського суду з прав людини щодо н*еобхідності* та *пропорційності* втручання і *незалежного попереднього контролю* при здобутті телекомунікаційних даних, викладена у справах *Roman Zakharov v. Russia* та *Big Brother Watch and Others v. the United Kingdom* [27; 28], а також правовий стандарт Суду Європейського Союзу у справі *C-670/22* (*M.N., EncroChat*) щодо *внутрішньої еквівалентності*: передання й використання «вже наявних» електронних даних у порядку *Європейського наказу про розслідування* (*«European Investigation Order», EIO*) можливі лише тоді, коли тотожний захід відповідав би вимогам права держави-виконавця у «порівнюваній внутрішній ситуації», із дотриманням процесуальних гарантій та засад розумної необхідності [29].

---

[4] ***Принцип комплементарності*** *(principle of complementarity)* – це фундаментальний засадничий принцип Римського статуту Міжнародного кримінального суду (ст. 17), який визначає співвідношення між юрисдикцією МКС та національними системами правосуддя. Його сутність полягає в тому, що МКС не замінює, а доповнює національні юрисдикції, здійснюючи втручання лише тоді, коли держава не бажає або не спроможна провести належне розслідування чи судовий розгляд злочинів, що належать до його компетенції. У міжнародно-правовій доктрині та практиці МКС розрізняють пасивну (негативну) та активну (позитивну, проактивну) комплементарність. ***Пасивна комплементарність*** означає невтручання Суду у випадках, коли держава виконує свій обов'язок щодо ефективного розслідування та переслідування осіб, винних у міжнародних злочинах, – у такій ситуації справа визнається неприйнятною для розгляду МКС. ***Активна або позитивна комплементарність***, навпаки, передбачає сприяння Суду державам у зміцненні їхньої спроможності самостійно здійснювати правосуддя, зокрема шляхом технічної допомоги, навчання, обміну доказовою інформацією та координації розслідувань. Зміст і практичне застосування принципу комплементарності розкрито в юриспруденції МКС – зокрема у справах *Prosecutor v. Dominic Ongwen* (Уганда, 2021), *Prosecutor v. William Ruto and Joshua Arap Sang* (Кенія, 2016), *Prosecutor v. Saif Al-Islam Gaddafi and Abdullah Al-Senussi* (Лівія, 2013), де сформульовано критерії «***щирості***» (genuineness) та «***спроможності***» (capacity) держав у забезпеченні ефективного національного правосуддя.

У *криміналістичному вимірі* дослідження збігаються в тому, що слід чітко відмежовувати технічну придатність електронного сліду (правильність ідентифікації, фіксації, *обчислення хеш-ідентифікаторів* (*«hashing»*), ведення журналів доступу та забезпечення *ланцюга збереження доказів* (*«chain of custody»*), відтворюваність) від його процесуальної долі: навіть бездоганно зафіксований цифровий артефакт має пройти перевірку на законність способу одержання, відповідність правам людини та релевантність *предметові доказування* [22–23; 40–42]. Окремо розвивається напрям криміналістики даних із використанням *штучного інтелекту* (*«artificial intelligence/AI»*), де результат алгоритмічного аналізу розглядається як допоміжне (короборaційне) свідчення, придатне до процесуального використання лише за умови забезпечення прозорості методології, перевірюваності й наглядового контролю [36].

В українських дослідженнях, у тому числі й наших авторських роботах, суттєво оновлено категоріальний апарат доказового права (система «належність – допустимість – достовірність – достатність», інститут процесуальної легалізації матеріалів оперативно-розшукової та негласної слідчої (розшукової) діяльності, посилення ролі судового контролю) і розпочато адаптацію міжнародних технічних настанов – Протоколу Берклі та Настанов ENFSI у сфері цифрової криміналістики – до потреб національного провадження [30; 44–45; 22–23]. Водночас зберігаються «*вузькі місця*», що потребують подальшої теоретичної конкретизації та нормативного врегулювання: інституціоналізація позитивної комплементарності через створення та правове забезпечення «Українського центру цифрових доказів» («Ukrainian Evidence Hub») як національного вузла надійного обігу й міжнародної передачі електронних доказів, а також остаточне розмежування між *прийнятністю справи* за статтею 17 Римського статуту та *допустимістю доказів* за Правилами МКС із урахуванням вимог пропорційності, незалежного контролю та критерію *внутрішньої еквівалентності* [1–2; 20; 27–29; 43]. Зазначені аспекти визначають межі подальшого дослідження та слугують методологічною основою для вироблення національної моделі процесуально-криміналістичних і цифрових стандартів допустимості доказів у справах про міжнародні злочини.

Метою цієї статті є розроблення національної моделі документування та доказового забезпечення міжнародних злочинів, яка інтегрує процесуально-криміналістичні, цифрові та міжнародно-правові стандарти допустимості доказів, узгоджені з засадами верховенства права і комплементарною роллю Міжнародного кримінального суду. Для досягнення цієї мети передбачено вирішити такі *завдання:* з'ясувати місце й призначення документування як елемента процесуальної форми кримінального провадження та як інструмента забезпечення національної безпеки; конкретизувати понятійно-категоріальний апарат доказового права (належність, допустимість, достовірність, достатність; предмет доказування; процесуальна легалізація результатів оперативно-розшукової та негласної слідчої (розшукової) діяльності; ланцюг збереження доказів) з урахуванням вимог Правил процедури і доказування Міжнародного кримінального суду та стандартів Європейського суду з прав людини; систематизувати міжнародні технічні настанови щодо роботи з електронними доказами та визначити механізми їх імплементації у кримінальний процес (протокол Берклі, настанови Європейської мережі судово-експертних установ у галузі цифрової криміналістики, відповідні стандарти ISO/IEC); проаналізувати ролі та повноваження органів досудового розслідування і прокуратури України в частині документування та процесуальної легалізації цифрових доказів, окреслити напрямки удосконалення судового контролю й міжвідомчої координації; запропонувати інституційне рішення у формі «Українського центру цифрових доказів» як національного вузла надійного обігу та міжнародної передачі електронних доказів; сформулювати пропозиції щодо корекції кримінального процесуального законодавства з метою забезпечення безперервності ланцюга збереження, верифікованості й відтворюваності процедур, а також належного врядування алгоритмічних інструментів у доказуванні з урахуванням вимог пояснюваності, пропорційності та незалежного контролю [1–2; 20; 22–23; 27–29; 40–42].

Джерельну базу становлять міжнародно-правові акти універсального та регіонального рівня (Римський статут Міжнародного кримінального суду, Правила процедури і доказування Міжнародного кримінального суду, Конвенція про захист прав людини і основоположних свобод, судова практика Європейського суду з прав людини; акти Європейського Союзу щодо Європейського наказу про розслідування й взаємного визнання доказів), національне законодавство України у сфері кримінального провадження, оперативно-розшукової діяльності та кібербезпеки, прецеденти Міжнародного кримінального суду щодо прийнятності справ і допустимості доказів, рішення Суду Європейського Союзу у справах щодо транскордонного використання електронних доказів, а також техніко-криміналістичні настанови (протокол Берклі, настанови Європейської мережі судово-експертних установ у галузі цифрової криміналістики, стандарти сімейства ISO/IEC). *Емпіричну складову* становлять узагальнені матеріали національної практики документування та процесуальної легалізації цифрових доказів у провадженнях про воєнні злочини й злочини проти людяності, а

також релевантні публікації, аналітичні звіти і методичні документи компетентних органів України та міжнародних інституцій [1–11; 14–19; 20; 22–23; 27–32; 40–42; 47–50].

Методологія дослідження ґрунтується на поєднанні загальнонаукових і спеціально-правових підходів. Застосовано *діалектичний* та *системно-структурний* підходи для виявлення внутрішніх зв'язків між процесуальними, криміналістичними та міжнародно-правовими елементами доказового процесу; *порівняльно-правовий метод* для зіставлення національних правил допустимості доказів із відповідними приписами та практикою Міжнародного кримінального суду і Європейського суду з прав людини; *формально-юридичний* та *герменевтичний* аналіз для тлумачення норм кримінального процесуального законодавства і міжнародних актів; *метод аналізу* судової практики (кейс-стаді) для виокремлення релевантних критеріїв «прийнятності справи» та «допустимості доказів» у конкретних справах; *методи емпіричного узагальнення, контент-аналізу* та *елементів даних-орієнтованого аналізу* для опрацювання матеріалів національної практики документування цифрових доказів; *елементи ризик-орієнтованого підходу* для оцінки впливу технологічних інструментів на права людини і процесуальні гарантії [1–2; 14–23; 27–29; 40–42].

Виклад основного матеріалу. Документування міжнародних злочинів у сучасному кримінальному провадженні становить нормативно й методологічно врегульовану діяльність з виявлення, фіксації, вилучення, збереження, аналітичної перевірки та процесуального закріплення фактичних даних, що набувають статусу доказів за умови відповідності критеріям належності, допустимості доказів (*«admissibility of evidence»*), достовірності й достатності [11; 2; 30; 44–45]. У структурі кримінального процесуального пізнання ця діяльність поєднує дві взаємопов'язані ролі: *по-перше*, елементу процесуальної форми кримінального провадження, що забезпечує законність отримання та легалізації відомостей*; по-друге*, інструмента державної протидії безкарності за воєнні злочини та злочини проти людяності, необхідного для досягнення завдань правосуддя на національному рівні та в межах юрисдикції Міжнародного кримінального суду [1–2; 11; 14–19].

Зміст документування охоплює послідовні, детально протоколювані дії з фіксації події, виявлення й вилучення речових та електронних носіїв інформації, забезпечення безперервного ланцюга збереження доказів (*«chain of custody»*), проведення первинної та поглибленої верифікації, а також процесуальної легалізації (*«procedural legalization»*) результатів оперативно-розшукової та негласної слідчої (розшукової) діяльності через передбачені законом джерела доказів – показання, речі й документи, висновки експертів, протоколи слідчих (розшукових) дій та інші носії інформації [8; 11; 22–23; 40–45]. У межах цієї послідовності принциповим є розмежування технічної придатності електронного сліду (ідентифікація, хешування (*«hashing»*), ведення журналів доступу, відтворюваність процедур) та його подальшої процесуальної долі: навіть технічно бездоганно зафіксований цифровий артефакт підлягає судовій оцінці щодо законності способу одержання, дотримання прав людини та зв'язку з обставинами, що підлягають доказуванню [2; 11; 27–28; 40–42].

Специфіка міжнародних злочинів зумовлює розширений спектр джерел і методів фіксації. Поряд із традиційними слідчими діями активно застосовуються *техніко-криміналістичні засоби*: цифрова зйомка і звукозапис, супутникові спостереження, розвідка з відкритих джерел (*«open-source intelligence», OSINT*), аналіз телекомунікаційних та мережевих журналів подій, вилучення даних з мобільних пристроїв і хмарних сервісів, використання спеціалізованих інструментів комп'ютерно-технічної експертизи та аналітики даних [22–23; 40–42]. Такі дії мають здійснюватися із застосуванням сертифікованих засобів, повним протоколюванням кожного доступу до носія, контролем цілісності файлів і дотриманням принципів необхідності, пропорційності (*«proportionality»*) та незалежного попереднього контролю, що випливають із конституційних гарантій і практики Європейського суду з прав людини [11; 27–28].

Місце документування у механізмі доказування визначається також взаємодією національних і міжнародних процедур. На рівні Міжнародного кримінального суду питання про прийнятність конкретної справи (*«admissibility of cases»*) вирішується за критеріями небажання або неспроможності держави, тяжкості злочину та формули «та сама особа / те саме діяння», тоді як питання про допустимість окремих доказів (*«admissibility of evidence»*) розглядається автономно крізь призму законності джерела, автентичності й надійності, а також відповідності принципам справедливого судового розгляду [1–2; 14–19]. Для електронних матеріалів особливу вагу має дотримання вимог до походження, верифікованості й відтворюваності, кодифікованих Протоколом Берклі та Настановами Європейської мережі судово-експертних установ у галузі цифрової криміналістики, а також узгодженість із приписами національного законодавства щодо одержання і використання доказів [22–23; 11].

Предмет доказування у справах про воєнні злочини та злочини проти людяності включає сукупність фактичних даних про подію, спосіб та наслідки діяння, суб'єктний склад і форму вини, наявність збройного конфлікту та зв'язок діяння з ним, а також ознаки широкомасштабності або

систематичності нападу на цивільне населення і наявність відповідної політики держави чи організації [1; 11; 14–19]. Це зумовлює підвищені вимоги до повноти й послідовності фіксації, зокрема до просторово-часової прив'язки електронних матеріалів, їх співвіднесення з незалежними джерелами та забезпечення можливості зовнішньої перевірки й контролю, у тому числі в межах національного судового контролю і процедур міжнародної правової допомоги, що реалізуються через Європейський наказ про розслідування («*European Investigation Order*») з дотриманням критерію внутрішньої еквівалентності примусових заходів [29; 11].

Отже, *документування міжнародних злочинів* водночас є елементом процесуальної форми кримінального провадження і засобом державної політики протидії безкарності; воно спирається на технічно вивірені та етично легітимні процедури роботи з доказами, які забезпечують їхню належність, допустимість, достовірність і достатність у національній та міжнародній юрисдикції [1–2; 11; 22–23; 27–29; 40–45]. У цьому контексті доцільно звернути увагу на формування в Європейському Союзі спеціалізованих цифрових інституційних механізмів, покликаних забезпечити стандартизоване накопичення, захищене зберігання та аналітичну обробку доказів щодо основних міжнародних злочинів. Одним із таких механізмів є Core International Crimes Evidence Database (CICED) – міжнародна цифрова платформа, що функціонує в межах мандату Євроюсту та спрямована на створення єдиного доказового простору щодо воєнних злочинів, злочинів проти людяності, геноциду та злочину агресії. CICED не замінює національне розслідування, але виступає інституційною «точкою синхронізації» між розслідуваннями різних держав і міжнародних структур, забезпечуючи технічну відтворюваність і доказову сумісність цифрових матеріалів [21; 26; 45; 46; 60].

Функціональна логіка CICED полягає у тому, що цифрові матеріали, отримані в межах міжнародної взаємодії, проходять стандартизований цикл технічної обробки: фіксацію метаданих і часових міток; криптографічний захист і хешування; маркування та верифікацію цілісності файлів; структуроване зберігання в захищеному середовищі; встановлення технічних зв'язків між окремими елементами доказового масиву для полегшення подальшого кореляційного аналізу. Таким чином, CICED формує «*доказову інфраструктуру довіри*», у межах якої автентичність і цілісність цифрових доказів підтверджуються не декларативно, а технологічно – через контроль ланцюга збереження, протоколювання дій і операцій доступу доступів і відтворюваність технічних параметрів доказового об'єкта [22; 23; 26].

Підвалини сучасного підходу до документування й доказування міжнародних злочинів були закладені практикою Міжнародного військового трибуналу в Нюрнберзі [3] та Міжнародного військового трибуналу для Далекого Сходу (Токійського трибуналу) [4]. Саме там уперше системно артикульовано індивідуальну кримінальну відповідальність за «*злочини проти миру*», «*воєнні злочини*» і «*злочини проти людяності*», сформульовано елементи складів, визнано неприпустимість посилання на офіційний статус як виправдання та апробовано спрощені, але формалізовані правила збирання і оцінки доказів. Наступний етап пов'язаний із створенням міжнародних кримінальних трибуналів для колишньої Югославії та для Руанди – спеціальних *ад хок* (*«ad hoc»*) юрисдикцій, статути яких закріпили «первинність» міжнародного суду над національними судами та сприяли виробленню процесуальних стандартів щодо допиту свідків, автентифікації документів і матеріальних слідів, а також окресленню меж застосування спеціальних засобів здобуття інформації [5; 6]. Кульмінацією зазначеної еволюції стала кодифікація Римського статуту Міжнародного кримінального суду, що заснував постійну юрисдикцію та концепцію *комплементарності* (*«complementarity»*), за якої пріоритет належить національному правосуддю, а *прийнятність справи* (*«admissibility of cases»*) перед Судом визначається за критеріями небажання чи неспроможності держави провести належне переслідування та за тестом «та сама особа / те саме діяння» [1]. Одночасно *Правила процедури і доказування* (*«Rules of Procedure and Evidence»*) надали загальним засадам доказування нормативної форми, закріпивши вимоги до допустимості доказів (*«admissibility of evidence»*), їхньої законності, автентичності та справедливості розгляду, що згодом отримало подальший розвиток у юриспруденції Міжнародного кримінального суду [2; 14–19]. Так сформувався нинішній стандарт: від перших прецедентів, де пріоритет мав міжнародний «наддержавний» контроль, – до римської моделі постійного суду з комплементарною роллю щодо національних органів та з розмежуванням між вирішенням питання про юрисдикційну прийнятність і процесуальною оцінкою доказів. Логічним продовженням цієї національної цифрової архітектури є інтеграція доказових потоків України з наднаціональними платформами ЄС, які забезпечують транснаціональну обробку та збереження цифрових матеріалів у кримінальних провадженнях щодо основних міжнародних злочинів *(core international crimes)*. Саме в цій площині CICED може розглядатися як «європейський рівень» доказового обігу, що доповнює національні цифрові платформи документування

міжнародних злочинів, зокрема державний інформаційний ресурс Warcrimes.gov.ua[5], та створює технічні передумови для взаємного визнання цифрових доказів у межах спільних слідчих груп, координаційних механізмів Євроюсту та взаємодії з Офісом Прокурора МКС. Відтак Warcrimes.gov.ua та майбутній Український доказовий хаб мають бути концептуалізовані не як ізольовані інформаційні ресурси, а як національні процесуальні вузли європейської та глобальної доказової екосистеми, що забезпечують відповідність доказів стандартам технічної автентифікації, інформаційної безпеки, процесуальної простежуваності та безперервного процесуально зафіксованого ланцюга збереження доказів, як необхідної умови їх допустимості у національному та міжнародному кримінальному провадженні [21; 22; 23; 26; 32].

Національна модель документування та доказування міжнародних злочинів спирається на розмежування повноважень і узгоджену взаємодію ключових суб'єктів кримінальної юстиції. Служба безпеки України, що здійснює *контррозвідувальну діяльність* і *оперативно-розшукову діяльність*, а також уповноважена на проведення *негласних слідчих (розшукових) дій* (*«covert investigative measures»*) за спеціальними законами та *Кримінальним процесуальним кодексом України* (КПК), забезпечує виявлення й фіксацію фактичних даних у справах про злочини проти основ національної безпеки та міжнародні злочини [7–9; 11; 44]. Державне бюро розслідувань провадить досудове розслідування щодо злочинів, учинених військовослужбовцями та посадовими особами, тоді як Національна поліція зосереджується на первинному *огляді місця події*, фіксації наслідків діяння, роботі з потерпілими й свідками та взаємодії з органами місцевого самоврядування і службами порятунку [9–11; 33]. Офіс Генерального прокурора здійснює *процесуальне керівництво*, формує єдині методичні підходи до *процесуальної легалізації* (*«procedural legalization»*) результатів ОРД і НС(Р)Д, координує міжвідомчу взаємодію та міжнародну співпрацю, у тому числі в межах *Меморандуму про взаєморозуміння* з Офісом Прокурора Міжнародного кримінального суду й спільних слідчих груп [11; 21; 26; 59].

Операційно-процесуальний цикл доказування охоплює виявлення, фіксацію, вилучення, зберігання та аналітичну перевірку електронних і матеріальних носіїв інформації, їх перетворення на передбачені КПК *джерела доказів* (показання, речі й документи, висновки експертів, протоколи слідчих (розшукових) дій) і подальше судове представлення. На всіх етапах забезпечується *ланцюг збереження доказів* (*«chain of custody»*) як безперервний, документований облік доступу до носіїв і трансформацій їхнього змісту; застосовуються сертифіковані засоби фіксації, *обчислення хеш-ідентифікаторів* (*«hashing»*), протоколювання доступів, процедури верифікації та відтворюваності, а також впроваджуються *Настанови Європейської мережі судово-експертних установ у галузі цифрової криміналістики* (ENFSI) і відповідні стандарти *ISO/IEC* [22–23; 40–42]. Разом із тим, зазначена «інфраструктура перевірюваності» у сучасних умовах набуває ще одного виміру – виміру цифрових доказів міжнародного походження, що проходять технічну обробку, збереження та аналітичну кореляцію в межах інституційних систем ЄС. CICED у цьому сенсі є практичним прикладом того, як формуються стандартизовані траєкторії руху доказу між державами: від первинної фіксації та верифікації цифрового об'єкта – до його структурованого зберігання і подальшого використання у транснаціональних провадженнях. Змістовно це означає, що «перевірюваність» у міжнародному кримінальному правосудді дедалі частіше забезпечується не лише процесуальною формою, а й технологічно контрольованими механізмами відтворюваності [20; 22; 23; 26].

Утім, для української системи кримінального процесу тут постає принципово важливий виклик: навіть за наявності технічно верифікованого доказу міжнародного походження залишається питання його процесуальної легалізації в межах КПК України. Відсутність спеціально визначеного механізму залучення та оцінки результатів наднаціональних доказових платформ (зокрема CICED) створює ризик, що технологічно «чистий» доказовий матеріал може втратити доказову силу через прогалини у процесуальній формі його введення до провадження та забезпечення прав сторін на доступ і перевірку [11; 20; 31; 32].

Важливим елементом є *процесуальна легалізація* результатів НС(Р)Д та *розвідки з відкритих джерел* (*«open-source intelligence», OSINT*): інтеграція електронних матеріалів у процес доказу-

---

[5] **Warcrimes.gov.ua** – державний онлайн-ресурс України, запущений у квітні 2022 року за ініціативи Офісу Генерального прокурора України у співпраці з правоохоронними органами та за підтримки міжнародних партнерів, для централізованого збору, первинної фіксації та систематизації повідомлень і матеріалів про воєнні злочини, вчинені в контексті збройної агресії Російської Федерації проти України. Ресурс інституційно підпорядкований Офісу Генерального прокурора, наповнюється шляхом подання інформації громадянами, органами державної влади, правоохоронними органами та правозахисними організаціями і використовується для подальшої процесуальної перевірки, кримінального переслідування та міжнародної правової співпраці, зокрема у взаємодії з Міжнародним кримінальним судом

вання здійснюється через належні процесуальні форми з дотриманням вимог законності одержання, належності, допустимості та достовірності [8; 11; 22–23; 44–45].

Судовий контроль (*«judicial review/control»*) є системною гарантією законності та справедливості втручання у права людини під час здобуття й використання доказів. Санкціонування окремих слідчих і негласних заходів здійснюється слідчим суддею за критеріями *необхідності* та *пропорційності* (*«necessity», «proportionality»*), а на стадії судового розгляду перевіряється відповідність способу отримання доказів вимогам КПК, їхня *автентичність* та *надійність* [11]. Практика Європейського суду з прав людини у справах про перехоплення комунікацій і обробку електронних даних (зокрема *Roman Zakharov v. Russia* та *Big Brother Watch and Others v. the United Kingdom*) формує обов'язкові стандарти незалежного попереднього контролю, меж втручання у приватність і процесуальної рівноваги сторін, що безпосередньо впливають на оцінку допустимості таких доказів у національному провадженні [27–28].

Міжнародний компонент національної моделі реалізується через інструменти *міжнародної правової допомоги* та *Європейський наказ про розслідування* (*«European Investigation Order», «EIO»*), а також діяльність спільних слідчих груп. Передавання «вже наявних» електронних матеріалів можливе за умови дотримання критерію *внутрішньої еквівалентності* (застосовності ідентичного заходу у «порівнюваній внутрішній ситуації») і принципу пропорційності, що відповідає підходу Суду Європейського Союзу у справі *C-670/22 (M.N., EncroChat)* та вимогам національного права [29; 11]. Така побудова забезпечує водночас ефективність досудового розслідування на національному рівні й відповідність матеріалів критеріям *прийнятності справи* та *допустимості доказів* у міжнародному вимірі, з урахуванням юриспруденції Міжнародного кримінального суду та технічних настанов щодо роботи з цифровими доказами [14–19; 20; 22–23; 29; 40–42; 44–45].

Сучасні вимоги до роботи з електронними доказами в справах про міжнародні злочини кодифіковано, насамперед, у *Протоколі Берклі* (*Berkeley Protocol on Digital Open Source Investigations*) та *Настановах Європейської мережі судово-експертних установ у галузі цифрової криміналістики* (ENFSI, модуль *Digital Forensics – Best Practice Manuals*) [22; 23]. Ці документи формують узгоджену рамку для виявлення, фіксації, зберігання та процесуальної перевірки *електронних доказів*, забезпечуючи їх *автентичність*, *надійність* і *відтворюваність* у значенні *допустимості доказів* (перш згад.: *«admissibility of evidence»*) згідно з *Правилами процедури і доказування Міжнародного кримінального суду* [2; 22–23].

Протокол Берклі встановлює три базові засади: *достовірність* (перевірка джерела, походження, часу та способу створення і відсутності неправомірних змін), *відтворюваність* (*«reproducibility»*) як можливість незалежно повторити аналітичні дії з тим самим результатом, та *прозорість* документування (повний *журнал дій* (*«audit trail»*), що фіксує кожну операцію з даними) [22]. *Настанови ENFSI (Digital Forensics)* деталізують алгоритми *ідентифікації*, *вилучення*, *хешування* (*«hashing»* із використанням стійких функцій, зокрема *SHA-256*), *зберігання*, *транспортного пакування* і *аналізу* цифрових носіїв; вимагають суворого *ланцюга збереження доказів* (*«chain of custody»*), контрольованого середовища (чисті носії, write-blockers), а також *валідації* інструментів та *калібрування* методик у відповідності до стандартів *ISO/IEC 17025* (компетентність випробувальних та калібрувальних лабораторій), *ISO/IEC 27037* (ідентифікація, збирання, одержання та зберігання цифрових доказів) і *ISO/IEC 27043* (принципи та процеси розслідування інцидентів) [23; 40–42].

Вказані міжнародні настанови кореспондують із конвенційними гарантіями *необхідності* й *пропорційності* (*«necessity», «proportionality»*) втручання у приватну сферу, а також з вимогами до *незалежного попереднього контролю*, що випливають із практики Європейського суду з прав людини (зокрема *Roman Zakharov v. Russia*; *Big Brother Watch and Others v. the United Kingdom*) [27; 28]. Їх імплементація у національні процедури (санкціонування, *процесуальна легалізація* результатів, судова перевірка способу одержання і надійності електронних даних) є передумовою не лише внутрішньої, а й транскордонної прийнятності матеріалів, що особливо важливо для виконання *Європейського наказу про розслідування* (*European Investigation Order*) та дотримання критерію *внутрішньої еквівалентності* під час передання «вже наявних» цифрових даних [2; 22–23; 29; 40–42].

Для української практики ключовим є послідовне вбудовування зазначених вимог у *процедури огляду, обшуку, доступу до речей і документів (виїмки), призначення та проведення експертиз* і в регламентацію *життєвого циклу електронного доказу* – від первинної фіксації до судового дослідження. Це потребує: уніфікованих протоколів хешування та протоколювання доступу; чітких правил пакування, маркування й транспортування носіїв; обов'язкової *процесуальної перевірки придатності* застосованих інструментів і *контрольного підтвердження достовірності* отриманих результатів; закріплення вимоги про *відтворюваність* експертних дій; забезпечення *підконтрольності людині* під час застосування алгоритмічних засобів аналізу даних і фіксації параметрів їх виконання [22–23; 40–42]. Синхронізація цих елементів із *Правилами процедури і доказування Міжна-*

родного кримінального суду та з національним процесуальним правом підсилює доказову цінність електронних матеріалів і мінімізує ризики їх відхилення з мотивів порушення процесуальної форми або прав людини [2; 11; 22–23; 27–28; 40–42].

У структурі доказування у справах про міжнародні злочини *електронні (цифрові) докази* (*«digital evidence»*) набули статусу самостійного й наскрізного носія інформації, що відтворює як зміст комунікацій і поведінкові патерни, так і технічні параметри подій. До кола релевантних видів належать *дані змісту* (тексти, аудіо-, відеозаписи, зображення), *дані про з'єднання й трафік* (*«traffic data»*), *метадані* (*«metadata»*, час/місце/джерело створення, ідентифікатори файлів і пристроїв, параметри мережевої взаємодії), *ідентифікаційні дані абонентів* (*«subscriber information»*), машинні журнали подій операційних систем і застосунків, дані *хмарних сервісів* (*«cloud service logs»*), а також відомості з *розвідки з відкритих джерел* (*«open-source intelligence/OSINT»*) та сліди у *розподілених реєстрах* (записи про транзакції у блокчейнах). Процесуальне значення кожної категорії визначається її зв'язком із предметом доказування, *можливістю достовірного встановлення джерела походження* та наявністю притаманних їй технічних підтверджень автентичності й цілісності [22–23; 40–42].

Вимоги до процедур поводження з такими даними відображають подвійний – технічний і процесуальний – характер допустимості. Початковий етап охоплює виявлення носія та його безпечне вилучення із застосуванням *пристроїв блокування запису* (*«write-blockers»*) та документуванням обставин доступу. На цій фазі формуються первинні *контрольні суми (хеш-ідентифікатори)* (*«hash values»*) за стійкими алгоритмами (зокрема *SHA-256*), фіксується *журнал доступу* (*«audit trail»*), забезпечується фізична та логічна ізоляція копій від змін, визначається стратегія зберігання, резервування та подальшого аналізу [23; 40–42]. Наступна фаза – аналітичне опрацювання – передбачає відтворювані, методично описані дії з обробки даних: розшифрування (за наявності правомірних ключів або на підставі судового дозволу), відновлення видаленого, виділення релевантних фрагментів, побудову часових ланцюжків, кореляцію з незалежними джерелами та підготовку *пояснювального звіту експерта/спеціаліста*, у якому кожна операція відображена у спосіб, що дозволяє стороні захисту її самостійне відтворення і перевірку [22–23; 40–42].

Особливу увагу слід приділяти ризикам, притаманним цифровому середовищу. Висока *мінливість* і *крихкість* електронних масивів зумовлює необхідність невідкладного та коректного хронографування, інакше змінені часові мітки, кеш або тимчасові файли можуть викривити причинно-наслідкові зв'язки. Поширення *глибинних підробок* (*«deepfake»*) і синтетичних даних вимагає процедурної й технічної верифікації автентичності (аналіз структурних артефактів, перевірка метаданих, порівняння з контрольними зразками, використання валідованих інструментів детекції, двофакторне підтвердження через незалежні канали). Ризики *алгоритмічного упередження* у системах аналізу на основі *штучного інтелекту* (*«artificial intelligence/AI»*) нейтралізуються шляхом обов'язкового *людського контролю* (*«human oversight»*), прозорого опису моделей, їх *валідації* (*«validation»*) та *перевірюваності* (*«verifiability»*), фіксації версій програмного забезпечення й налаштувань, а також заборони використання неперевірених «чорних скриньок» як самодостатніх підстав для доведення [25; 36].

Процесуальний вимір роботи з електронними доказами зумовлений вимогами до законності отримання, захисту прав людини та дотримання *необхідності* і *пропорційності* (*«necessity», «proportionality»*). Доступ до телекомунікаційних даних, змісту повідомлень, локаційних і реєстраційних відомостей можливий лише на підставі належної судової санкції з конкретизацією обсягу, строків і мети втручання; порушення цих вимог тягне процесуальні наслідки у вигляді визнання доказів недопустимими, що прямо випливає з приписів національного процесуального закону та практики Європейського суду з прав людини щодо меж втручання у приватну сферу (зокрема *Roman Zakharov v. Russia*, *Big Brother Watch and Others v. the United Kingdom*) [11; 27–28]. У транскордонному вимірі застосовуються механізми *Європейського наказу про розслідування* (*European Investigation Order*), за якими передання «вже наявних» електронних даних можливе лише за дотримання критерію *внутрішньої еквівалентності* (тобто придатності ідентичного заходу у «порівнюваній внутрішній ситуації») та відповідних процесуальних гарантій, як це закріплено у справі *C-670/22 (M.N., EncroChat)* [29].

З огляду на вказані вимоги й ризики, національна практика має забезпечувати безперервний *ланцюг збереження доказів* з моменту виявлення носія до його дослідження судом; уніфіковані протоколи *хешування*, маркування й транспортування; ретельний *журнальний* облік дій із носіями; належне *процесуальне оформлення* кожного етапу роботи з електронним об'єктом; використання *сертифікованих інструментів* і регулярний *аудит* методик. Лише поєднання технічно вивірених процедур із повнокровним судовим контролем та дотриманням прав людини конвертує цифрову інформацію в належні, допустимі, достовірні й достатні докази, спроможні витримати як національ-

ний, так і міжнародний стандарт перевірки, включно з вимогами Правил процедури і доказування Міжнародного кримінального суду та Настановами ENFSI [2; 22–23; 27–29; 40–42].

Залучення штучного інтелекту (*«artificial intelligence/AI»*) та методів машинного навчання (*«machine learning/ML»*) до аналітичних етапів документування міжнародних злочинів посилює спроможність органів правопорядку швидко опрацьовувати великі масиви даних, виявляти приховані кореляції, патерни переміщень і комунікацій, здійснювати пріоритизацію слідчих версій, ідентифікувати об'єкти та суб'єкти на зображеннях і відео, виконувати семантичний пошук у масивах *розвідданих з відкритих джерел* (*«open-source intelligence/OSINT»*) та телекомунікаційних журналах [25; 36]. Водночас результати алгоритмічної обробки мають суто *допоміжний (кооборационний) характер*: вони не підміняють ані *предмет доказування*, ані судову оцінку доказів за критеріями належності, *допустимості доказів* (*«admissibility of evidence»*), достовірності та достатності, що випливають із приписів Правил процедури і доказування Міжнародного кримінального суду [2], норм КПК України [11] і стандартів Європейського суду з прав людини щодо необхідності, пропорційності та ефективного незалежного контролю [27–28]. Будь-яке алгоритмічне твердження потребує людського підтвердження, перехресної перевірки іншими джерелами та процесуального закріплення у відповідній формі (протокол, висновок експерта/спеціаліста, показання свідка, речовий або письмовий доказ) з дотриманням *ланцюга збереження доказів* (*«chain of custody»*) і вимог до верифікованості та відтворюваності, зафіксованих у Протоколі Берклі та Настановах ENFSI (модуль *цифрова криміналістика*) [22–23; 40–42].

Ключовою запорукою процесуальної придатності аналітики на основі штучного інтелекту є пояснюваність (*«explainability»*) та перевірюваність (*«verifiability»*) моделей. Під час першого застосування алгоритму у провадженні має бути детально задокументовано його призначення, архітектуру, версію, параметри навчання, джерела та якість навчальних даних, метрики точності й хибних спрацьовувань, а також налаштування порогів прийняття рішень; цей журнал дій та змін (*«audit trail»*) повинен зберігатися як складова матеріалів провадження для подальшої експертної перевірки та реалізації права сторони захисту на ознайомлення й ефективне спростування [25; 36]. Результати роботи моделі мають бути *відтворюваними* (*«reproducibility»*): незалежний експерт, діючи за описаною методикою і використовуючи ідентичні вхідні дані та параметри, повинен отримати тотожний (або еквівалентний у межах статистичної похибки) результат. Непрозорі рішення «чорної скриньки», що не допускають реконструкції логіки виводу, не можуть бути єдиною підставою для висновків, які обмежують права й свободи особи; їх допустимість має оцінюватися з огляду на *пропорційність* та *необхідність* втручання і наявність альтернативних, менш інвазивних засобів [2; 27–28; 36].

Окремої уваги потребує *аудит моделей* – системна перевірка алгоритмів на предмет алгоритмічної упередженості, стійкості до збурень (ризик «*адверсарних*» прикладів) та узагальнювальної здатності щодо даних, відмінних від навчальних (зсув розподілу даних). Аудит включає незалежну валідацію вибірок, тестування на різнорідних датасетах (щоб уникнути перенавчання під специфічний контент), оцінку чутливості моделі до шуму й маніпуляцій, а також контроль за дотриманням принципів мінімізації даних і підконтрольності людині (*«human-in-the-loop»*) на всіх критичних етапах – від формування гіпотез до ухвалення рішень [25; 36]. Впровадження процедур аудиту має бути інституційно закріплене у внутрішніх регламентах органів досудового розслідування та експертних установ, а технічні інструменти, що застосовуються для аналізу цифрових доказів, повинні проходити *валідацію* відповідно до вимог ISO/IEC 17025 та суміжних стандартів, із фіксацією результатів і періодичним оновленням методик [56–58].

З метою недопущення порушення процесуальної чистоти доказів (процесуальної «токсичності» длоказів) аналітичні продукти штучного інтелекту інтегруються в доказовий масив через: *по-перше*, чітке позначення їх як допоміжних відомостей, що потребують підтвердження незалежними джерелами (свідчення, речові та письмові докази, висновки експертів); *по-друге*, забезпечення безперервного *ланцюга збереження* як для первинних даних, так і для вихідних файлів та проміжних артефактів; *по-третє,* формалізований *життєвий цикл* моделі (ініціалізація, навчання, застосування, оновлення, архівація) з визначенням відповідальних осіб і меж доступу; *по-четверте*, дотримання приписів національного законодавства щодо судового санкціонування доступу до інформації та стандартів міжнародного права з прав людини щодо пропорційності і необхідності [11; 22–23; 27–28; 36]. У підсумку алгоритмічні інструменти можуть істотно прискорювати й поглиблювати *аналітичну перевірку* та *кореляцію* даних, однак їх використання має залишатися підпорядкованим принципам *верховенства права*, *справедливого судового розгляду* та *процесуальної відтворюваності*, аби збережені й проаналізовані електронні сліди трансформувалися в належні, допустимі, достовірні й достатні докази, придатні як для національної, так і для міжнародної юрисдикції [2; 22–23; 25; 36; 40–42].

Національна спроможність до ефективного документування та процесуальної легалізації міжнародних злочинів потребує інституційної конфігурації «єдиного вікна», що консолідує збір, верифікацію, зберігання й передання матеріалів у межах єдиної *цифрової архітектури доказування*. Доцільним є створення «Українського центру цифрових доказів» (*Ukrainian Evidence Hub*) як державної платформи з функціями *централізованого приймання*, *маркування*, *хешування* (*«hashing»*), *ведення ланцюга збереження доказів* (*«chain of custody»*), *верифікації та відтворюваності* цифрових слідів, а також їх *процесуальної легалізації* для використання у національному провадженні та для належної *міжнародної передачі* (зокрема за процедурами *Європейського наказу про розслідування* (*European Investigation Order, «EIO»*)) [11; 22–23; 29; 40–42]. З урахуванням формування в Європейському Союзі CICED як наднаціональної інфраструктури накопичення та технічної верифікації доказів щодо core international crimes, Український доказовий хаб доцільно проєктувати не лише як внутрішньодержавну платформу, а як національний доказовий «шлюз» (gateway) між КПК України та міжнародними інституційними системами. Такий шлюз має забезпечувати процесуально коректне введення до національного провадження цифрових доказів міжнародного походження з дотриманням вимог допустимості, належності та достовірності, а також стандартів технічної автентифікації і chain of custody [11; 20; 22; 23; 26; 43].

У цьому ж контексті обґрунтованою є ідея створення окремого державного реєстру цифрових доказів міжнародного походження як проміжної ланки між національною системою кримінального провадження та міжнародними платформами, зокрема CICED. Такий реєстр має забезпечувати централізований облік хеш-ідентифікаторів, часових міток, ключових метаданих і протоколів передачі доказів, що дозволить мінімізувати ризики втрати або недопустимості цифрових матеріалів та забезпечити практичну реалізацію інституційної комплементарності між Україною та міжнародними органами кримінальної юстиції [20; 22; 23; 35; 43]. У перспективі створення спеціальної юрисдикції щодо злочину агресії особливого значення набуває довгострокове збереження та міжнародна сумісність цифрових доказів. У цьому вимірі платформи на кшталт CICED виконують функцію попереднього доказового архіву, що забезпечує безперервність збереження доказової інформації, знижує ризики повторного отримання доказів і створює умови для їх оперативного використання в різних міжнародних юрисдикційних форматах [13; 21; 26; 44].

Моделі управління таким центром мають передбачати, з одного боку, інституційне лідерство Офісу Генерального прокурора як центрального координатора процесуального обігу матеріалів, відповідального за уніфікацію методик легалізації та взаємодію з міжнародними органами (зокрема в рамках *позитивної комплементарності* (*«positive complementarity»*) і реалізації Меморандуму про взаєморозуміння з Офісом Прокурора Міжнародного кримінального суду) [20; 21]; з другого боку – чітке визначення ролей Служби безпеки України як провідного збирача й первинного верифікатора контррозвідувальних та негласних матеріалів, Державного бюро розслідувань як органу досудового розслідування тяжких злочинів військовослужбовців і посадових осіб, та Національної поліції як суб'єкта первинної фіксації місця події, роботи з потерпілими й свідками [7–11; 26; 44–45]. Для забезпечення технічної й процедурної єдності доцільно затвердити *єдиний довірчий перелік* сертифікованих програмно-апаратних засобів для копіювання, аналізу та зберігання електронних даних, а також міжвідомчі протоколи і формати обміну метаданими, контрольними сумами та логами доступу, узгоджені з Настановами Європейської мережі судово-експертних установ (модуль цифрова криміналістика) і стандартами *ISO/IEC* [22–23; 40–42; 11].

Ключовим елементом діяльності центру має стати інституціоналізований *ланцюг збереження доказів* із використанням захищених модулів *протоколювання дій* (*«audit trail»*), багаторівневою автентифікацією доступу, *контрольним хешуванням* кожної операції та обов'язковим формуванням *профілю походження* (джерело, час, місце, засіб отримання, службова особа, контрольні суми до/після) – як для первинних носіїв, так і для робочих копій та похідних артефактів. Така конфігурація забезпечує технічну надійність і процесуальну *допустимість доказів* (*«admissibility of evidence»*), узгоджену з вимогами *Правил процедури і доказування Міжнародного кримінального суду*, Протоколу Берклі та Настанов ENFSI [2; 22–23; 40–42].

З погляду зовнішньої взаємодії *У*країнський центр цифрових доказів має бути сумісним з інфраструктурами міжнародної співпраці (платформи *Євроюсту* для спільних слідчих груп, механізми EIO), підтримувати *матчинг* метаданих і контрольних сум, а також процедури перевірки *внутрішньої еквівалентності* заходів, результати яких передаються за кордон. Наявність уніфікованого *пакета пересилання* (структуровані дані, контрольні суми, технічні характеристики носіїв, протоколи доступу, довідки про застосовані засоби та санкції слідчого судді) зменшує ризик відхилення матеріалів за межами юрисдикції, підвищує прогнозованість міжнародної оцінки та сприяє реалізації *позитивної комплементарності* як системної підтримки національних переслідувань, що відбиває сучасну політику Міжнародного кримінального суду [20; 22–23; 26; 29].

Паралельно з технічною інфраструктурою необхідна сталість кадрової спроможності. Рекомендовано запровадити *цільову спеціалізацію* аналітиків цифрових доказів, експертів з розвідки з відкритих джерел (*open-source intelligence*), фахівців з міжнародного кримінального права та технічних аудиторів алгоритмів. Підготовка й підвищення кваліфікації мають здійснюватися на базі Національної академії Служби безпеки України, Національної академії внутрішніх справ і Тренінгового центру прокурорів України у співпраці з навчальними підрозділами Міжнародного кримінального суду та Євроюсту, із включенням модулів щодо Протоколу Берклі, Настанов ENFSI, стандартів ISO/IEC та процедур EIO; обов'язковим елементом має стати навчання *пояснюваності* алгоритмів, методам незалежного *аудиту моделей* і належної *процесуальної легалізації* результатів аналітики на основі *штучного інтелекту* [11; 22–23; 25–26; 40–42].

Нормативна модернізація повинна закріпити у КПК спеціальні інструменти роботи з електронними доказами: процесуальну форму *онлайн-обшуку* як різновид *негласного доступу* з чіткими критеріями *необхідності* та *пропорційності*, обов'язком фіксувати *журнал дій*, *контрольні суми* і параметри застосованих технічних засобів; розширення переліку *документів* як джерел доказів за рахунок *електронних комунікаційних даних*, отриманих у результаті спеціальних технічних операцій в Україні або правомірно переданих іноземними компетентними органами; імплементацію принципу *внутрішньої еквівалентності* для транскордонних доказів; процесуальні запобіжники для застосування алгоритмічних інструментів (обов'язкове *попереднє* і *наступне* погодження методики, *пояснюваність* та *перевірюваність* результатів, заборона використання «*чорних скриньок*» як самодостатніх підстав для вирішення питання про винуватість) [2; 11; 22–23; 29; 40–42; 44–45].

Запропонована конфігурація – *і*нституціоналізований національний центр обігу цифрових доказів, уніфіковані міжвідомчі протоколи та стандартизований *ланцюг збереження*, а також цілеспрямована підготовка кадрів і нормативне закріплення *онлайн-обшуку*, *внутрішньої еквівалентності* та *аудиту моделей* – створює цілісну «екосистему довіри», у межах якої цифрові сліди набувають як технічної надійності, так і процесуальної легітимності. У розвитку цього підходу міжнародні інституційні платформи на кшталт CICED фактично задають еталон технічної реалізації принципу chain of custody у транскордонному масштабі. Для цифрових доказів міжнародного походження ключового значення набувають стандартизовані механізми фіксації метаданих, автоматизованого хешування, протоколювання дій і операцій доступів і документування кожної операції з цифровим об'єктом у захищеному середовищі. Водночас транснаціональний характер обігу такого доказу висуває підвищені вимоги до процесуальної відтворюваності, що потребує нормативного закріплення спеціальних механізмів легалізації цифрових доказів міжнародного походження в національному кримінальному процесі [22; 23; 31; 35]. Така *екосистема* сприяє одночасно підвищенню ефективності національного розслідування та відповідності отриманих доказів стандартам прийнятності в Міжнародному кримінальному суді й механізмах міжнародної правової допомоги, забезпечуючи реальну дієвість принципу невідворотності відповідальності за воєнні злочини та злочини проти людяності [1–2; 20–23; 26; 29; 40–45].

Висновки. Сформована у дослідженні *концептуальна модель* переконливо засвідчує, що документування міжнародних злочинів у національному кримінальному провадженні має подвійну правову природу. З одного боку, воно є невід'ємним елементом процесуальної форми кримінального провадження, підпорядкованим вимогам законності, судового контролю та захисту прав людини; з другого – виконує функцію стратегічного інструменту державної політики протидії безкарності за воєнні злочини, злочини проти людяності та, у перспективі, злочин агресії. Саме ця подвійність зумовлює необхідність поєднання внутрішньодержавних процесуальних гарантій із міжнародними стандартами доказування та збереження доказової інформації.

Методологічну визначеність забезпечує чітке розмежування між прийнятністю справи (*admissibility of cases*) перед Міжнародним кримінальним судом і допустимістю доказів (*admissibility of evidence*) у межах національної процесуальної форми. Перша категорія функціонує як юрисдикційний фільтр, пов'язаний із критеріями небажання або нездатності держави здійснювати переслідування та з оцінкою тяжкості злочинів, тоді як друга залежить від дотримання конкретних процесуальних і технічних вимог до збирання, фіксації, зберігання та перевірки матеріалів. У сфері цифрових слідів вирішальне значення набувають безперервний і належно задокументований ланцюг збереження доказів (*chain of custody*), коректне формування хеш-ідентифікаторів (*hashing*), повне протоколювання дій і операцій доступу (*audit trail*), відтворюваність процедур і водночас неухильне дотримання гарантій прав людини та вимог справедливого судового розгляду.

Концептуальним каркасом узгодження національного й міжнародного вимірів доказування виступає принцип комплементарності (*complementarity*), у межах якого диференціюються горизонтальна, вертикальна та паралельна моделі співвідношення юрисдикцій. Особливого значення набуває позитивна (проактивна) комплементарність (*positive / proactive complementarity*), зорі-

єнтована не на заміщення, а на посилення національних механізмів переслідування шляхом гармонізації процесуальних і технічних стандартів, розвитку інституційної спроможності та забезпечення довіри до результатів внутрішніх розслідувань.

У цьому контексті обґрунтовано доведено, що створення Українського центру цифрових доказів (*Ukrainian Evidence Hub*) та пов'язаних із ним уніфікованих міжвідомчих протоколів має розглядатися не лише як внутрішня адміністративно-процесуальна реформа, а як формування національного доказового «шлюзу» (*gateway*) між КПК України та наднаціональними інфраструктурами, зокрема платформами на кшталт *CICED*. Така модель забезпечує процесуально коректне введення до національного провадження цифрових доказів міжнародного походження, їх довгострокове збереження, технічну автентифікацію та міжнародну сумісність, що є критично важливим у перспективі створення спеціальної юрисдикції щодо злочину агресії та тривалого функціонування міжнародних механізмів відповідальності.

Доведено також, що інтеграція аналітичних інструментів на основі штучного інтелекту (*artificial intelligence / AI*) може підвищувати ефективність документування і кореляції цифрових масивів лише за умови їх підпорядкування процесуальним вимогам пояснюваності (*explainability*), перевірюваності (*verifiability*) та обов'язкового людського контролю (*human oversight*). Алгоритмічні результати мають допоміжний характер і набувають доказового значення виключно через їх процесуальну легалізацію, відтворюваність і перевірку в суді, що унеможливлює підміну доказування технократичним «процесуальним автоматизмом».

У підсумку сформована модель – інституціоналізований центр обігу цифрових доказів, стандартизований ланцюг збереження, уніфіковані протоколи, сумісні з міжнародними платформами, та нормативно закріплені запобіжники використання високих технологій – утворює цілісну *екосистему довіри*. Саме в межах такої екосистеми цифрові сліди трансформуються в належні, допустимі, достовірні й достатні докази, здатні витримати як національний судовий контроль, так і міжнародну перевірку, забезпечуючи реальну дієвість принципу невідворотності відповідальності за найтяжчі міжнародні злочини.

Перспективи подальших досліджень пов'язані, *по-перше*, з поглибленою деталізацією процесуальних і технічних вимог до *онлайн-обшуку* (*online search*) як різновиду негласного доступу до цифрової інформації, з акцентом на критерії *необхідності* (*necessity*), *пропорційності* (*proportionality*), а також на інституціоналізацію належного попереднього та наступного судового контролю за такими заходами. Особливого значення в цьому аспекті набуває розроблення уніфікованих протоколів фіксації втручання, протоколювання дій і операцій доступу (*audit trail*) та перевірки відтворюваності результатів у контексті захисту права на приватність і справедливий судовий розгляд.

По-друге, перспективним є формування національних критеріїв *пояснюваності* (*explainability*), *перевірюваності* (*verifiability*) та інституційного *аудиту* моделей аналітики на основі *штучного інтелекту* (*artificial intelligence / AI*) з обов'язковою *підконтрольністю людині* (*human oversight*). Подальші дослідження мають бути спрямовані на нормативне розмежування допоміжного (кооборационного) характеру алгоритмічних результатів і власне доказів, а також на вироблення процедур їх процесуальної легалізації з урахуванням вимог відтворюваності та можливостей ефективного спростування стороною захисту.

По-третє, актуальним напрямом є поглиблення методик процесуальної легалізації результатів *розвідки з відкритих джерел* (*open-source intelligence / OSINT*) із урахуванням стандартів атрибуції джерел, перевірки автентичності контенту, запобігання маніпуляціям і забезпечення захисту *персональних даних* у цифровому середовищі. У цьому вимірі перспективними є міждисциплінарні дослідження на стику кримінального процесу, цифрової криміналістики та інформаційного права.

По-четверте, подальшого наукового опрацювання потребує *нормативне закріплення принципу внутрішньої еквівалентності* під час транскордонного обігу «вже наявних» електронних матеріалів, зокрема у взаємодії з наднаціональними доказовими інфраструктурами та в межах реалізації *позитивної комплементарності* (*positive complementarity*). Це включає дослідження процесуальних моделей взаємодії національних органів із платформами на кшталт *CICED* та формування доказового «шлюзу» (*gateway*) між КПК України й міжнародними юрисдикційними механізмами.

По-п'яте, перспективним залишається подальше вдосконалення й стандартизація національних протоколів *хешування* (*hashing*), *протоколювання* (*audit trail*) і збереження цифрових носіїв (*chain of custody*) відповідно до міжнародних технічних орієнтирів і стандартів цифрової криміналістики. Окремої уваги потребує дослідження довгострокового збереження та міжнародної сумісності цифрових доказів у контексті можливого створення спеціальної юрисдикції щодо злочину агресії та тривалих у часі міжнародних переслідувань.

Реалізація зазначених наукових напрямів сприятиме підвищенню надійності, передбачуваності й конституційної орієнтованості національної моделі доказування, забезпечить її сумісність із

найкращими європейськими та міжнародними практиками та зміцнить інституційну спроможність України ефективно доводити відповідальність за найтяжчі міжнародні злочини в національних і міжнародних юрисдикціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Rome Statute of the International Criminal Court. *International Criminal Court*. 17 July 1998. URL: https://www.icc-cpi.int/resource-library/Documents/RS-Eng.pdf.
2. Rules of Procedure and Evidence of the International Criminal Court. *International Criminal Court*. 2021. URL: https://www.icc-cpi.int/sites/default/files/RulesProcedureEvidenceEng.pdf.
3. Charter of the International Military Tribunal (Nuremberg). *Avalon Project, Yale Law School*. 8 August 1945. URL: https://avalon.law.yale.edu/imt/imtconst.asp.
4. Charter of the International Military Tribunal for the Far East (Tokyo Charter). *United Nations*. 1946. URL: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.2_Tokyo%20Charter.pdf.
5. Statute of the International Criminal Tribunal for the former Yugoslavia (ICTY). *United Nations*. UN Doc. S/RES/827 (25 May 1993). URL: https://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf.
6. Statute of the International Criminal Tribunal for Rwanda (ICTR). *United Nations*. UN Doc. S/RES/955 (8 November 1994). URL: https://legal.un.org/avl/pdf/ha/ictr/ictr_statute_e.pdf.
7. Закон України «Про Службу безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.
8. Закон України «Про оперативно-розшукову діяльність». URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
9. Закон України «Про Державне бюро розслідувань». URL: https://zakon.rada.gov.ua/laws/show/794-19#Text.
10. Закон України «Про Національну поліцію». URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
11. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
12. Agreement between the Government of Ukraine and the Council of Europe on the Establishment of the Register of Damage Caused by the Aggression of the Russian Federation against Ukraine. *Council of Europe*. 2023. URL: https://www.coe.int/en/web/kyiv/registry-of-damage.
13. Council of Europe. Establishment of a Special Tribunal for the Crime of Aggression against Ukraine: Concept Note and Legal Framework. *Council of Europe*. 2023. URL: https://www.coe.int/en/web/portal/ukraine-special-tribunal.
14. International Criminal Court. Prosecutor v. Dominic Ongwen. Judgment, Trial Chamber IX, 4 February 2021. *International Criminal Court*. URL: https://www.icc-cpi.int/case/uganda/dominic-ongwen.
15. International Criminal Court. Prosecutor v. William Samoei Ruto and Joshua Arap Sang. Decision, Trial Chamber V(A), 5 April 2016. *International Criminal Court*. URL: https://www.icc-cpi.int/case/kenya/ruto.
16. International Criminal Court. Prosecutor v. Saif Al-Islam Gaddafi and Abdullah Al-Senussi. Decision on Admissibility, Appeals Chamber, 21 October 2013. *International Criminal Court*. URL: https://www.icc-cpi.int/case/libya.
17. International Criminal Court. Prosecutor v. Bosco Ntaganda. Judgment, 8 July 2019. *International Criminal Court*. URL: https://www.icc-cpi.int/case/ntaganda.
18. International Criminal Court. Prosecutor v. Ahmad Al Faqi Al Mahdi. Judgment and Sentence, 27 September 2016. *International Criminal Court*. URL: https://www.icc-cpi.int/case/almadhi.
19. International Criminal Court. Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui. Judgment of the Appeals Chamber, 25 June 2020. *International Criminal Court*. URL: https://www.icc-cpi.int/case/katanga-ngudjolo.
20. International Criminal Court, Office of the Prosecutor. Policy Paper on Complementarity. *International Criminal Court*. 2023. URL: https://www.icc-cpi.int/resources/otp-policy-complementarity.
21. Office of the Prosecutor of the International Criminal Court; Office of the Prosecutor General of Ukraine. Memorandum of Understanding on Cooperation and Evidence Sharing. 2023. URL: https://www.icc-cpi.int/news/ukraine-memorandum-of-understanding-signed.
22. Berkeley Protocol on Digital Open Source Investigations. *OHCHR; UC Berkeley Human Rights Center*. 2020. 56 p. URL: https://www.ohchr.org/sites/default/files/Documents/Publications/BerkeleyProtocol.pdf.

23. ENFSI. Best Practice Manuals – Digital Forensics. *European Network of Forensic Science Institutes*. 2025. URL: https://enfsi.eu/documents/best-practice-manuals.
24. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. *Council of Europe*. 2018. 22 p. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.
25. Europol. AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. *Europol*. 2023. 28 p. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf.
26. Eurojust; Office of the Prosecutor General of Ukraine. Joint Investigation Teams for Core International Crimes in Ukraine. *Eurojust*. 2023. URL: https://www.eurojust.europa.eu/joint-investigation-team-support.
27. European Court of Human Rights. Roman Zakharov v. Russia, no. 47143/06, Judgment of 4 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001-159324.
28. European Court of Human Rights. Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, Judgment of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001-203614.
29. Court of Justice of the European Union. Case C-670/22 (M.N., EncroChat), Judgment of 30 April 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0670.
30. Погорецький М.А.; Шеломенцев В.П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2 (2). С. 77–81. URL: https://ir.library.knu.ua/handle/15071834/8415.
31. Погорецький М.А.; Сергєєва Д.Б. Криміналістична тактика: щодо визначення поняття. *Часопис Національного університету «Острозька академія». Серія «Право»*. 2012. № 1 (5). 8 с. URL: https://lj.oa.edu.ua/articles/2012/n1/12pmasvp.pdf.
32. Погорецький М.А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства України*. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf.
33. Погорецький М.А.; Сергєєва Д.Б. Тактика захисника: поняття, зміст та місце в системі криміналістичної тактики. *Вісник кримінального судочинства*. 2016. № 2. С. 113–123. URL: https://vkslaw.knu.ua/images/verstka/2_2016_Sergeeva.pdf.
34. Pohoretskyi M.; Cherniak A.; Serhieieva D.; Chernysh R.; Toporetska Z. Detection and proof of cybercrime. *Amazonia Investiga*. 2022. Vol. 11 (53). P. 259–269. DOI: https://doi.org/10.34069/AI/2022.53.05.26. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/2142.
35. Погорецький М.А.; Лисаченко Є.І. Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України. *Вісник кримінального судочинства*. 2022. № 3–4. С. 20–34. DOI: https://doi.org/10.17721/2413-5372.2022.3-4/20-34. URL: https://vkslaw.knu.ua/en/3-4-2022-actual-problems-of-criminal-justice/problems-of-the-criminal-process/admissibility-of-evidence-in-the-criminal-procedure-law-of-the-european-union-and-its-impact-on-criminal-justice-in-ukraine.
36. Погорецький М.А.; Лисаченко Є.І. Встановлення достовірності цифрових доказів Міжнародним кримінальним судом: окремі проблемні питання та шляхи їх вирішення. *Вісник кримінального судочинства*. 2023. № 1–2. С. 54–73. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/54-73. URL: https://vkslaw.com.ua/index.php/journal/article/view/35.
37. Погорецький М.А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства*. 2023. № 3–4. С. 84–102. DOI: https://doi.org/10.17721/2413-5372.2023.3-4/84-102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf.
38. 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. URL: https://visnyk.kh.ua/uk/journals/visnik-naprnu-3-2025-r/verkhovenstvo-prava-u-kriminalnomu-protsesualnomu-dokazuvanni-metodologiya-ta-praktika-zastosuvannya.
39. 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.DOI: https://doi.org/10.24144/2788-6018.2025.04.3.40. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42-2.pdf.
40. 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. URL: https://app-journal.in.ua/wp-content/uploads/2025/10/APP_05_2025_part-3-2.pdf.
41. Погорецький М.А.; Меленті Є.О. Документування атак держави-агресора на об'єкти критичної інфраструктури України: методика інтелектуального аналізу мультисенсортних даних та використання його результатів у кримінальному процесуальному доказуванні. *Право і суспільство*. 2025. № 4. С. 251–274. DOI: https://doi.org/10.32842/2078-3736/2025.4.1.36. URL: http://pravoisuspilstvo.org.ua/archive/2025/4_2025/part_1.
42. Погорецький М.А. Використання даних EncroChat у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий електронний журнал*. 2025. № 8. С. 223–229. DOI: https://doi.org/10.32782/2524-0374/2025-8. URL: http://lsej.org.ua/8_2025/48.pdf.
43. Погорецький М.А. Цифрові та процесуально-криміналістичні стандарти документування злочинів проти людяності в діяльності Служби безпеки України. *Злочини проти людяності та геноцид: практичний погляд на окремі аспекти російської агресії в контексті ратифікації Римського Статуту*. Київ: Алерта, 2025. С. 8–32.
44. Погорецький М.А. Допустимість доказів у кримінальному процесі та процесуальна доброчесність: доктрини і практика (порівняльно-правове дослідження). *Вісник кримінального судочинства*. 2025. № 1–2. С. 60–82. DOI: https://doi.org/10.17721/2413-5372.2025.1-2/22-59. URL: https://vkslaw.com.ua/index.php/journal/issue/view/37/1-2-2025-pdf.
45. Погорецький М.А. Забезпечення прав людини в цифровому доказуванні як умова реалізації принципу верховенства права та постановлення справедливого вироку. *Право України*. 2025. № 9. С. 60–74. URL: https://pravoua.com.ua/uk/store/pravoukr/pravo_2025_9/pravo_2025_9-s4490.
46. Попко В.В. Принцип комплементарності у міжнародному кримінальному праві. *Актуальні проблеми держави і права*. 2019. Вип. 82. С. 164–174. URL: http://www.apdp.in.ua/v82/26.pdf.
47. Ambos K. Treatise on International Criminal Law. Vol. III: International Criminal Procedure. *Oxford University Press*. 2021. 704 p.
48. Schabas W. The International Criminal Court: A Commentary on the Rome Statute. 2nd ed. *Oxford University Press*. 2016. 1360 p.
49. Cryer R.; Friman H.; Robinson D.; Wilmshurst E. An Introduction to International Criminal Law and Procedure. 4th ed. *Oxford University Press*. 2022. 732 p.
50. Kleffner J. Complementarity in the Rome Statute and National Criminal Jurisdictions. *Oxford University Press*. 2008. 398 p.
51. de Souza Dias T. Positive Complementarity and the ICC: Towards a More Proactive Approach. *Journal of International Criminal Justice*. 2020. Vol. 18 (2). P. 341–363. DOI: https://doi.org/10.1093/jicj/mqaa011.
52. Stigen J. The Relationship between the International Criminal Court and National Jurisdictions. *Martinus Nijhoff Publishers*. 2008. 548 p.
53. Bekou O.; Birkett D. Cooperation and Complementarity: National Implementation of the Rome Statute. *Cambridge University Press*. 2020. 412 p.
54. Ligeti K. et al. CRIM_AI – Unpacking AI Evidence and (Re-)Defining Authentication in Criminal Justice. *University of Luxembourg*. 2024. 27 p. URL: https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/Unpacking-AI-Evidence_Ligeti.pdf.
55. Human Rights Watch. Making Justice Count: Lessons from the ICC's Early Years on Complementarity. *Human Rights Watch*. 2021. 58 p.
56. ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories. Geneva: *International Organization for Standardization*.
57. ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: *International Organization for Standardization*.
58. ISO/IEC 27043:2015. Incident investigation principles and processes. Geneva: *International Organization for Standardization*.
59. International Criminal Court. Ukraine and International Criminal Court sign an agreement on the establishment of a country office (Press Release ICC-CPI-20230323-PR1713). *International Criminal Court*. 23 March 2023. URL: https://www.icc-cpi.int/news/ukraine-and-international-criminal-court-sign-agreement-establishment-country-office.
60. Eurojust. Agreement to extend the joint investigation team into alleged core international crimes in Ukraine for two years (Press Release). *Eurojust*. 29 February 2024. URL: https://www.eurojust.europa.eu/news/agreement-extend-joint-investigation-team-alleged-core-international-crimes-ukraine-two-years.