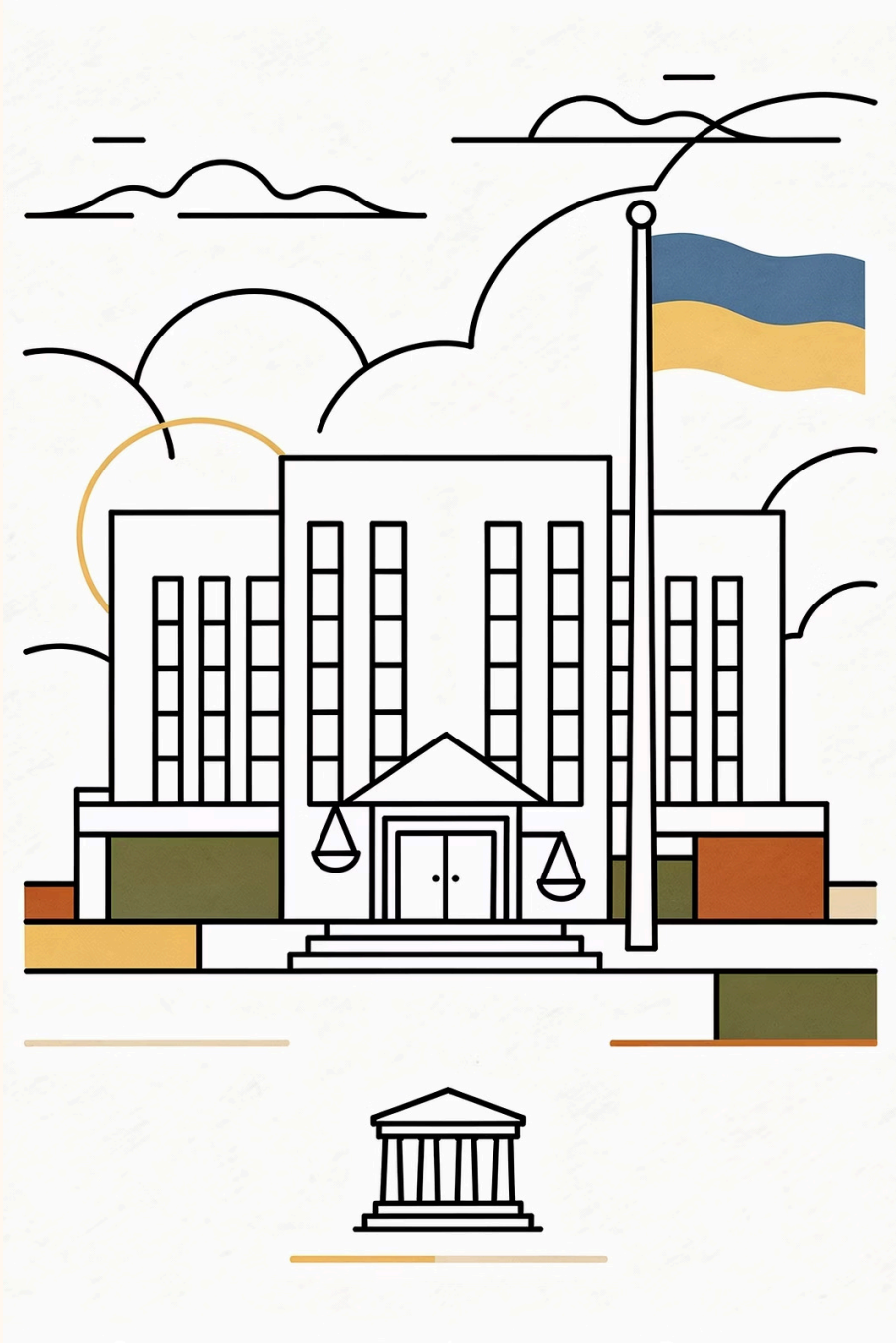
Документування і доказування воєнних злочинів в Україні



Міжнародно-правовий контекст: трибунал та інституційна база

Спеціальний трибунал (STCoA)

Спеціальний трибунал щодо злочинів агресії РФ — Special Tribunal for the Crime of Aggression against Ukraine (STCoA) — юридично започаткований **25.06.2025** Угодою Україна–РФ. Наразі перебуває на стадії інституційного розгортання: локація, склад, процесуальні дії — у процесі визначення та формування.

ICPA та Eurojust

Агентство ЄС з питань співробітництва у сфері кримінального правосуддя (**Eurojust**, Гаага) повідомляє: Міжнародний центр переслідування злочинів агресії проти України (**ICPA**) вже готує справи до майбутнього трибуналу. У жовтні 2025 р. прокурори ЄС/України узгоджували трансфер розслідувань саме до цього трибуналу.

ICPA — координаційний центр прокурорів при Eurojust (Гаага), який збирає, зберігає та аналізує докази злочинів агресії РФ проти України й готує справи для подальшого кримінального переслідування.

Нюрнберзька спадщина

Підвалини сучасного підходу закладені практикою Міжнародного військового трибуналу в Нюрнберзі та Токійського трибуналу: кримінальна відповідальність за «злочини проти миру», «воєнні злочини» і «злочини проти людяності», неприпустимість посилання на офіційний статус як виправдання, формалізовані правила збирання й оцінки доказів.

Документування міжнародних злочинів: поняття та зміст

Повномасштабна збройна агресія РФ актуалізувала комплексну проблему документування та доказування міжнародних злочинів. Кримінальне провадження стикається з викликом побудови цілісної **процесуально-криміналістичної архітектоніки доказового забезпечення**, здатної трансформувати різнорідні відомості у належні, допустимі, достовірні та достатні докази — як для національного правосуддя, так і для МКС.

Визначення документування

Нормативно й методологічно врегульована діяльність з виявлення, фіксації, вилучення, збереження, аналітичної перевірки та процесуального закріплення фактичних даних, що набувають статусу доказів за умови відповідності критеріям **належності, допустимості (*admissibility of evidence*), достовірності й достатності**.

Зміст документування

Послідовні, детально протоколювані дії: фіксація подій, виявлення й вилучення речових та електронних носіїв, забезпечення *chain of custody*, первинна та поглиблена верифікація, процесуальна легалізація результатів ОРД та НС(Р)Д через передбачені законом джерела доказів — показання, речі й документи, висновки експертів, протоколи слідчих дій.

Стратегічне значення

Документування 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.

Предмет доказування та джерела фіксації

Предмет доказування у справах про міжнародні злочини

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
- ознаки широкомасштабності або систематичності нападу на цивільне населення
- наявність відповідної політики держави чи організації

Це зумовлює підвищені вимоги до повноти й послідовності фіксації, просторово-часової прив'язки електронних матеріалів та забезпечення можливості зовнішньої перевірки.

Техніко-криміналістичні засоби фіксації

Поряд із традиційними слідчими діями активно застосовуються:

- Цифрова зйомка і звукозапис
- Супутникові спостереження
- Розвідка з відкритих джерел (**OSINT**)
- Аналіз телекомунікаційних та мережевих журналів подій
- Вилучення даних з мобільних пристроїв і хмарних сервісів
- Спеціалізовані інструменти комп'ютерно-технічної експертизи та аналітики даних

Такі дії мають здійснюватися із застосуванням **сертифікованих засобів**, повним протоколюванням кожного доступу до носія, контролем цілісності файлів і дотриманням принципів необхідності, пропорційності та незалежного попереднього контролю.

Цифрові докази: види, ризики та процесуальний вимір

У структурі доказування у справах про міжнародні злочини електронні (цифрові) докази набули статусу **самостійного й наскрізного носія інформації**, що відтворює як зміст комунікацій і поведінкові патерни, так і технічні параметри подій.

Види цифрових доказів

- Дані змісту: тексти, аудіо-, відеозаписи, зображення
- Дані про з'єднання й трафік (*traffic data*)
- Метадані: час/місце/джерело створення, ідентифікатори файлів
- Машинні журнали подій ОС і застосунків
- Дані хмарних сервісів (*cloud service logs*)
- OSINT та сліди у розподілених реєстрах (блокчейн)

Ключові ризики

- **Мінливість і крихкість** — необхідність невідкладного хронографування; змінні часові мітки можуть викривити причинно-наслідкові зв'язки
- **Deepfake і синтетичні дані** — вимагають процедурної й технічної верифікації: аналіз артефактів, перевірка метаданих, валідовані інструменти детекції, двофакторне підтвердження
- **Шифрування та неоднорідність підходів** — ускладнюють забезпечення процесуальної якості

Процесуальний вимір

- Доступ до телекомунікаційних даних — лише на підставі **належної судової санкції** з конкретизацією обсягу, строків і мети
- Порушення вимог тягне визнання доказів **недопустимими**
- Практика ЄСПЛ (*Roman Zakharov v. Russia*; *Big Brother Watch v. UK*) — обов'язкові стандарти незалежного попереднього контролю та меж втручання у приватність

Міжнародні стандарти: Протокол Берклі та Настанови ENFSI

Протокол Берклі

Розроблений Офісом Верховного комісара ООН з прав людини спільно з Університетом Берклі (*Berkeley Protocol on Digital Open Source Investigations*). Закріпив міжнародні стандарти роботи з цифровими доказами — від збору до верифікації.

Три базові засади:

- **Достовірність** — перевірка джерела, походження, часу та способу створення, відсутність неправомірних змін
- **Відтворюваність** (*reproducibility*) — можливість незалежно повторити аналітичні дії з тим самим результатом
- **Прозорість** — повний журнал дій (*audit trail*), що фіксує кожну операцію з даними

Настанови ENFSI (Digital Forensics BPM)

Оновлена серія методичних настанов належної практики у сфері цифрової криміналістики, підготовлена профільними робочими групами **Європейської мережі судово-експертних установ (ENFSI)**. Кожен BPM має власну редакцію й дату ухвалення (11.2015; 18.10.2021; 16.12.2022; 7.12.2023). Офіційний сайт: **enfsi.eu**.

Настанови деталізують алгоритми **ідентифікації, вилучення, хешування** (SHA-256), зберігання, транспортного пакування й аналізу цифрових носіїв; вимагають суворого *chain of custody*, контрольованого середовища (чисті носії, write-blockers), валідації інструментів та калібрування методик відповідно до стандартів:

- **ISO/IEC 17025** — компетентність випробувальних та калібрувальних лабораторій
- **ISO/IEC 27037** — ідентифікація, збирання, одержання та зберігання цифрових доказів
- **ISO/IEC 27043** — принципи та процеси розслідування інцидентів

Для української практики ключовим є послідовне вбудовування зазначених вимог у процедури огляду, обшуку, призначення та проведення експертиз і в регламентацію **життєвого циклу електронного доказу** — від первинної фіксації до судового дослідження.

Принцип комплементарності та допустимість доказів у МКС

Принцип комплементарності (ст. 17 Римського статуту)

Фундаментальний засадничий принцип: МКС **не замінює, а доповнює** національні юрисдикції, здійснюючи втручання лише тоді, коли держава не бажає або не спроможна провести належне розслідування чи судовий розгляд.

- **Пасивна комплементарність** — невтручання Суду у випадках, коли держава ефективно розслідує та переслідує осіб, винних у міжнародних злочинах; справа визнається неприйнятною для МКС
- **Активна (позитивна) комплементарність** — сприяння Суду державам: технічна допомога, навчання, обмін доказовою інформацією, координація розслідувань

Допустимість доказів у МКС

Питання про **прийнятність справи** (*admissibility of cases*) вирішується за критеріями небажання або неспроможності держави, тяжкості злочину та формули «та сама особа / те саме діяння».

Питання про **допустимість окремих доказів** (*admissibility of evidence*) розглядається автономно крізь призму:

- законності джерела
- автентичності й надійності
- відповідності принципам справедливого судового розгляду

Для електронних матеріалів особливу вагу має дотримання вимог до **походження, верифікованості й відтворюваності**, кодифікованих Протоколом Берклі та Настановами ENFSI, а також узгодженість із приписами національного законодавства.

Національна модель: суб'єкти та операційний цикл доказування

Служба безпеки України

Здійснює *контрозвідувальну діяльність* і *оперативно-розшукову діяльність*, уповноважена на проведення *негласних слідчих (розшукових) дій* (*covert investigative measures*). Забезпечує виявлення й фіксацію фактичних даних у справах про злочини проти основ національної безпеки та міжнародні злочини. Є провідним збирачем і первинним верифікатором контррозвідувальних та негласних матеріалів.

Офіс Генерального прокурора

Здійснює **процесуальне керівництво**, формує єдині методичні підходи до *процесуальної легалізації* результатів ОРД і НС(Р)Д, координує міжвідомчу взаємодію та міжнародну співпрацю, у тому числі в межах *Меморандуму про взаєморозуміння* з Офісом Прокурора МКС й спільних слідчих груп.

ДБР та Національна поліція

Державне бюро розслідувань проводить досудове розслідування щодо злочинів, учинених військовослужбовцями та посадовими особами.
Національна поліція зосереджується на первинному огляді місця події, фіксації наслідків діяння, роботі з потерпілими й свідками та взаємодії з органами місцевого самоврядування.

На всіх етапах забезпечується **ланцюг збереження доказів** (*chain of custody*) як безперервний, документований облік доступу до носіїв; застосовуються сертифіковані засоби фіксації, обчислення хеш-ідентифікаторів (*hashing*), протоколювання доступів, процедури верифікації та відтворюваності, а також впроваджуються Настанови ENFSI і стандарти ISO/IEC.

Цифрові інституційні механізми ЄС: CICED та Warcimes.gov.ua

Core International Crimes Evidence Database (CICED)

Міжнародна цифрова платформа в межах мандату **Євроюсту**, 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.

Функціональний цикл CICED:

- Фіксація метаданих і часових міток
- Криптографічний захист і хешування
- Маркування та верифікація цілісності файлів
- Структуроване зберігання в захищеному середовищі
- Встановлення технічних зв'язків між елементами доказового масиву для кореляційного аналізу

Таким чином, CICED формує **«доказову інфраструктуру довіри»**, де автентичність і цілісність підтверджуються технологічно, а не декларативно.

Warcimes.gov.ua

Державний онлайн-ресурс України, запущений у **квітні 2022 року** за ініціативи Офісу Генерального прокурора у співпраці з правоохоронними органами та за підтримки міжнародних партнерів. Призначений для централізованого збору, первинної фіксації та систематизації повідомлень і матеріалів про воєнні злочини.

Ресурс 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 МКС.

Warcimes.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 та процесуальної простежуваності.

Штучний інтелект у документуванні міжнародних злочинів

Залучення **штучного інтелекту (*AI*) та методів машинного навчання (*ML*)** до аналітичних етапів документування посилює спроможність органів правопорядку швидко опрацьовувати великі масиви даних, виявляти приховані кореляції, патерни переміщень і комунікацій, здійснювати пріоритезацію слідчих версій, ідентифікувати об'єкти та суб'єкти на зображеннях і відео, виконувати семантичний пошук у масивах OSINT та телекомунікаційних журналах.

1

Позначення як допоміжних відомостей

Аналітичні продукти ШІ чітко позначаються як допоміжні відомості, що потребують підтвердження незалежними джерелами: свідчення, речові та письмові докази, висновки експертів.

2

Безперервний ланцюг збереження

Забезпечення *chain of custody* як для первинних даних, так і для вихідних файлів та проміжних артефактів аналізу ШІ.

3

Формалізований життєвий цикл моделі

Ініціалізація, навчання, застосування, оновлення, архівація — з визначенням відповідальних осіб і меж доступу.

4

Судове санкціонування та пропорційність

Дотримання приписів національного законодавства щодо судового санкціонування доступу до інформації та стандартів міжнародного права з прав людини щодо пропорційності і необхідності. Заборона використання «чорних скриньок» як самодостатніх підстав для вирішення питання про винуватість.

Пропозиція: Український центр цифрових доказів (Evidence Hub)

Концепція та функції

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
- Процесуальної легалізації для використання у національному провадженні
- Належної міжнародної передачі за процедурами *Європейського наказу про розслідування (EIO)*

З урахуванням формування CICED, Український доказовий хаб доцільно проєктувати як національний доказовий **«шлюз» (gateway)** між КПК України та міжнародними інституційними системами.

Обґрунтованою є також ідея створення **окремого державного реєстру цифрових доказів міжнародного походження** як проміжної ланки між національною системою та міжнародними платформами (зокрема CICED), що забезпечить централізований облік хеш-ідентифікаторів, часових міток і протоколів передачі.

Управління та розподіл повноважень

Управління центром покладається на **Офіс Генерального прокурора** як центрального координатора процесуального обігу матеріалів, відповідального за уніфікацію методик легалізації та взаємодію з міжнародними органами в рамках Меморандуму з Офісом Прокурора МКС.

Чітко визначені ролі інших суб'єктів:

- **СБУ** — провідний збирач і первинний верифікатор контррозвідувальних та негласних матеріалів
- **ДБР** — орган досудового розслідування тяжких злочинів військовослужбовців і посадових осіб
- **Національна поліція** — суб'єкт первинної фіксації місця події, роботи з потерпілими й свідками

Зовнішня сумісність

Центр має підтримувати *матчинг* метаданих і контрольних сум, процедури перевірки *внутрішньої еквівалентності* заходів, а також уніфікований пакет пересилання (структуровані дані, контрольні суми, технічні характеристики носіїв, протоколи доступу, довідки про застосовані засоби та санкції слідчого судді).

Нормативна модернізація та кадрова спроможність

Нормативна модернізація КПК

Закріпити у КПК спеціальні інструменти роботи з електронними доказами: процесуальну форму **онлайн-обшуку** як різновид негласного доступу з критеріями необхідності та пропорційності; розширення переліку документів за рахунок **електронних комунікаційних даних**; імплементацію принципу **внутрішньої еквівалентності** для транскордонних доказів; процесуальні запобіжники для алгоритмічних інструментів — обов'язкове попереднє і наступне погодження методики, пояснюваність та перевірюваність результатів.

Цільова спеціалізація кадрів

Рекомендовано запровадити цільову спеціалізацію: аналітиків цифрових доказів, експертів з OSINT, фахівців з міжнародного кримінального права та технічних аудиторів алгоритмів. Підготовка — на базі **Національної академії СБУ, Національної академії внутрішніх справ і Тренінгового центру прокурорів України** у співпраці з навчальними підрозділами МКС та Євроюсту.

Модулі підготовки

Обов'язкові модулі: Протокол Берклі, Настанови ENFSI, стандарти ISO/IEC, процедури EIO. Обов'язковим елементом має стати навчання **пояснюваності алгоритмів**, методам незалежного аудиту моделей і належної процесуальної легалізації результатів аналітики на основі штучного інтелекту.

Висновки: документування як елемент державної політики протидії безкарності

Процесуальна форма і державна політика

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.

Стандарти якості доказів

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 національний, так і міжнародний стандарт перевірки.

Позитивна комплементарність

Наявність уніфікованого пакета пересилання 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 МКС.

25.06

Дата заснування STCoA

Спеціальний трибунал щодо злочинів агресії РФ юридично започаткований 25 червня 2025 року

2022

Рік запуску Warcimes.gov.ua

Державний ресурс для централізованого збору матеріалів про воєнні злочини запущено у квітні 2022 р.

6

Ключових суб'єктів

СБУ, МО, ДБР, Нацполіція, Нацгвардія, Прикордонна служба, ОГП у взаємодії з міжнародними партнерами

Список використаних джерел

I. Міжнародно-правові акти та інституційні документи

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. 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.
5. 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.
6. 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.

II. Законодавство України

1. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
2. Закон України «Про Службу безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.
3. Закон України «Про оперативно-розшукову діяльність». URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
4. Закон України «Про Державне бюро розслідувань». URL: https://zakon.rada.gov.ua/laws/show/794-19#Text.
5. Закон України «Про Національну поліцію». URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

III. Міжнародні стандарти та протоколи

1. 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.
2. ENFSI. Best Practice Manuals – Digital Forensics. European Network of Forensic Science Institutes. 2025. URL: https://enfsi.eu/documents/best-practice-manuals.
3. 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.
4. 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.

IV. Наукові праці

1. 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.
2. 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.
3. 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.
4. Погорецький М.А. Судовий контроль у забезпеченні справедливості 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.
5. 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.
6. Погорецький М.А. Використання даних EncroChat у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. Юридичний науковий електронний журнал. 2025. № 8. С. 223–229. DOI: https://doi.org/10.32782/2524-0374/2025-8. URL: http://lsej.org.ua/8_2025/48.pdf.
7. 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.

Презентацію підготовлено з використанням інструменту штучного інтелекту Gamma AI. Усі наведені джерела, нормативні акти та бібліографічні відомості верифіковані автором. Відповідальність за зміст і точність посилань несе автор презентації.