ПРОБЛЕМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЗЛОЧИННОСТІ

УДК 343.13:340.132.6
DOI: https://doi.org/10.31359/1993-0909-2025-32-3-275

Микола Анатолійович Погорецький
Національна академія правових наук України
Харків, Україна

Київський національний університет імені Тараса Шевченка
Київ, Україна

ВЕРХОВЕНСТВО ПРАВА У КРИМІНАЛЬНОМУ ПРОЦЕСУАЛЬНОМУ ДОКАЗУВАННІ: МЕТОДОЛОГІЯ ТА ПРАКТИКА ЗАСТОСУВАННЯ

Анотація. *Стаття пропонує цілісну методологію застосування верховенства права в кримінальному процесуальному доказуванні в умовах воєнного стану та цифровізації. Верховенство права розглянуто як процедурний алгоритм оцінки доказів, реалізований через систему процесуальних фільтрів, що забезпечує законність, перевіреність і достатність сукупності. На цій основі запропоновано «паспорт доказу» – атрибуційно-реєстраційний модуль супроводу цифрового артефакта від одержання до суду (походження, технічні параметри, хеші, часові мітки, журнал доступів, можливість незалежної верифікації). Методика поєднує правові стандарти та технічні настанови й дозволяє інтегрувати результати мультисенсорного аналізу в процесуальну форму. Практична частина подає алгоритми роботи із зображеннями, аудіо, геоданими, CDR-журналами й метаданими та мікрокейси (удар по критичній інфраструктурі; провокація; верифікація листування). Запропонований підхід підвищує передбачуваність рішень, балансує ефективність провадження з дотриманням прав людини й слугує практичним інструментом для суддів, прокурорів і захисників.*

Ключові слова: *верховенство права, кримінальне процесуальне доказування, цифрові докази, процесуальні фільтри, пропорційність, ланцюг збереження цифрових даних, воєнний стан.*

Mykola A. Pohoretskyi

National Academy of Legal Sciences of Ukraine,
Kharkiv, Ukraine

Taras Shevchenko National University of Kyiv
National Academy of Legal Sciences of Ukraine
Kyiv, Ukraine

RULE OF LAW IN CRIMINAL PROCEDURAL EVIDENCE: METHODOLOGY AND PRACTICE OF APPLICATION

Abstract. *The paper develops an integrated methodology for applying the rule of law to criminal-procedural evidence under martial-law conditions and rapid digitalization. The rule of law is treated as a procedural algorithm implemented through evidentiary filters that ensure legality, verifiability and sufficiency of the evidentiary set. Building on this framework, an Evidence Passport – an attribution-and-registration module – accompanies a digital artefact from acquisition to trial (origin, technical parameters, hashes, timestamps, access logs, and options for independent verification). The methodology fuses CPC/ECHR standards with ISO/ENFSI/NIST/Berkeley guidance, translating multi-sensor analysis into admissible procedural form. The practical section outlines workflows for images, audio, geospatial tracks, connection logs and metadata, and illustrates them with micro-cases (critical infrastructure strike; entrapment; messaging verification). The approach increases the predictability of judicial decisions and balances efficiency with human-rights protection, providing a usable toolkit for judges, prosecutors and defence counsel.*

Keywords: *rule of law; criminal procedural evidence; digital evidence; evidentiary filters; proportionality; digital data chain of custody; martial law.*

ВСТУП

Цифровізація й воєнний стан істотно змінюють структуру доказування: на перший план виходять цифрові джерела, для яких вирішальними є атрибуція, цілісність і можливість незалежної перевірки. За цих умов верховенство права набуває значення операційного стандарту, що спрямовує тлумачення процесуальної форми та меж втручання в приватність [2; 12]. В європейському контексті розвинено тести «якості закону», ефективного нагляду та компенсаторних гарантій, від яких залежить справедливість процесу й допустимість цифрових даних [12; 14]. Українська практика демонструє рух до чіткішої атрибуції й перевірності електронних доказів та послідовного відсікання наслідків провокації [6; 7].

Стрімке зростання масивів даних і мультисенсорні канали фіксації (супутникові зображення, БПЛА, журнали з'єднань, системні метадані, OSINT) підвищують вимоги до процедурної дисципліни: документування походження, стабільності часових міток, незмінності вмісту, відтворюваності результатів і реального

доступу захисту до перевірки (*методичні орієнтири – розд. 4*). Водночас неврегульованість або фрагментарність національних процедур у поєднанні з воєнними обмеженнями (ущільнені строки, віддалені дії, складність доступу до носіїв) створює ризики дефектів форми. Потрібна узгоджена методична рамка, що перетворює технічний результат на процесуально легалізований доказ без зниження гарантій справедливого суду [16; 18].

У статті запропоновано модель процесуальних фільтрів, яка інтегрує доктринальні засади (належність, допустимість, достовірність, достатність) з європейськими стандартами справедливості й пропорційності та з технічними протоколами цілісності й відтворюваності. Центральний інструмент – «паспорт доказу» як атрибуційно-реєстраційний модуль супроводу цифрового артефакта від одержання до суду (походження, параметри фіксації, хеші/часові мітки, журнал доступів, умови незалежної верифікації). Такий підхід синхронізує правові та технічні вимоги, підвищує передбачуваність судових рішень і підтримує баланс між ефективністю провадження та дотриманням прав людини [4; 5; 25]. *Мета і завдання* – обґрунтувати верховенство права як методологічну основу доказування в цифрову епоху, конкретизувати фільтри оцінки, інтегрувати стандарти ЄСПЛ у національну процесуальну форму, адаптувати міжнародні технічні настанови до потреб кримінального процесу та продемонструвати застосування моделі на мікрокейсах воєнного контексту [24; 25].

1. ОГЛЯД ЛІТЕРАТУРИ

Українська доктрина верховенства права виробила два напрями. Так, концептуально-аксіологічний окреслює його як ціннісну основу правопорядку з акцентом на пріоритет прав людини, юридичну визначеність, заборону свавілля та гарантії справедливого суду [6; 7; 10; 27]. Операційно-процесуальний трансформує ці цінності в стандарти кримінального провадження: обмеження дискреції, вимоги пропорційності, передбачуваності й перевірюваності доказів [11; 19; 24].

С. Головатий тлумачить верховенство права як «правовладдя», що зобов'язує державу діяти в координатах прав людини й якісного закону, підкреслюючи роль суду [9; 10]. С. Максимов розглядає його як універсальний стандарт цивілізації з ідеальним і реальним вимірами, що матеріалізуються в стримуваннях і практиках справедливого суду [20; 21]. Б. Малишев наголошує на потребі «процесуальної якості» закону [22].

Останні дослідження акцентують значення юридичної визначеності для доказування: Ю. Корольова аналізує співвідношення «верховенства права і закону», В. Венгер – обмеження дискреції [17; 8]. В. Сущенко показує верховенство права як критерій реальності гарантій у діяльності органів розслідування та суду [28]. Європейський вимір систематизує А. Пухтецька, вказуючи на релевантність *Rule of Law Checklist* та тестів «якість закону/пропорційність» [26].

Вплив практики ЄСПЛ виявляється у справах *Roman Zakharov i Big Brother Watch* (стримуючі гарантії), *Schatschaschwili* (компенсаторні гарантії при *hearsay*), *Teixeira de Castro* (відсікання результатів провокації) [12–15]. Ці стандарти формують критерії допустимості цифрових слідів.

Окремий блок становлять настанови *ISO/IEC 27037, ENFSI BPM, NIST SP 800–101* та *Berkeley Protocol*, що встановлюють вимоги до ідентифікації, збереження, хешування й журналювання цифрових даних [2–5]. Така дисципліна забезпечує автентичність і відтворюваність результатів.

У працях автора обґрунтовано концепцію «процесуальних фільтрів» (належність, допустимість, достовірність, достатність) і судового контролю; запропоновано «паспорт доказу» як модуль атрибуції й верифікації [24; 25]. Ці підходи узгоджуються з європейськими доктринами верховенства права [26] та міжнародними технічними стандартами [2–5].

Судова практика також рухається в цьому напрямі: постанова ККС ВС від 02.04.2024 визначає критерії відсікання результатів НСРД при провокації, а постанова від 27.11.2023 встановлює вимоги до атрибуції електронних повідомлень (ідентифікація акаунтів, *CDR/GNSS*, технічна відтворюваність) [6; 7].

Отже, доктрина й практика сходяться в трьох вузлах: (1) верховенство права є набором процесуальних фільтрів; (2) цифрові джерела потребують паспортизації та дотримання *ISO/ENFSI/NIST/Berkeley-процедур* [1–5]; (3) ЄСПЛ і ККС ВС задають мінімальні гарантії допустимості та ваги доказів [20–23; 26–27]. Це й визначає методологічну рамку подальшого дослідження.

2. МАТЕРІАЛИ ТА МЕТОДИ

Застосовано міжгалузевий підхід: аналіз Конституції України та КПК (з урахуванням воєнних норм) [16; 18], практики ЄСПЛ щодо нагляду, *hearsay* і провокації [12–15], позицій ККС ВС стосовно електронних доказів [6; 7], а також SOP і стандартів цифрової форензії (ISO/IEC 27037, ENFSI BPM, NIST SP 800–101, *Berkeley Protocol*) [1–5].

Методологія поєднує нормативний, герменевтичний і порівняльно-правовий аналіз із техніко-правовим модулем: ідентифікація джерела/каналу, фіксація умов одержання, первинні та повторні хеші, журнал доступів, форензійні образи (WORM/immutable), синхронізація часу та міжканальна кореляція; для процесуальної «перекладності» використано **«паспорт доказу»** як атрибуційно-реєстраційний модуль [24; 25].

Період джерельної бази – 2010–2025 рр.; відбір здійснювався за операційною релевантністю до критеріїв законності/пропорційності/справедливості та відтворюваності процедур; виключались джерела з невизначеним процесуальним статусом або без доданої доказової ваги. Обмеження: рекомендаційний характер частини стандартів та нерівномірна деталізація національних актів; динамічність правового режиму воєнного стану [2; 5; 18].

Очікуваний результат – узгоджена матриця перевірки цифрових доказів і впровадження «процесуальних фільтрів» у судовий контроль та оцінку доказів [6; 12; 24].

3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

3.1 Верховенство права як методологічна основа доказування

3.1.1 Сучасні концепції верховенства права

Сучасні підходи виходять за межі формули «панування закону» й визначають ознаки правовладдя: законність і «якість закону» (доступність, передбачуваність, несуперечність), заборона свавілля, незалежне правосуддя, доступ до суду, рівність сторін і пропорційність втручань [10; 11].

У такому розумінні верховенство права – не лише цінність, а ***процедурна матриця*** діяльності органів досудового розслідування і суду, зокрема під час одержання та оцінки доказів [11]. Українська доктрина (правовладдя С. Головатого) підкреслює відмінність між «верховенством права» та «верховенством закону» і пріоритет змістовної справедливості над формальним легалізмом [9; 10]; праці С. І. Максимова та П. М. Рабіновича конкретизують, що ***легітимність та передбачуваність*** державного втручання є необхідними передумовами правомірності доказових дій [20; 21; 27]. Ключовий елемент – *foreseeability* – у практиці ЄСПЛ реалізується через тест «якості закону» і стримуючі гарантії (чіткість підстав/меж доступу, незалежний нагляд, запобіжники від зловживань, правила зберігання/видалення даних) [12; 13]; за їх відсутності страждають справедливість процесу, допустимість і вага цифрових слідів, тож суд перевіряє ***якість норми***, наявність контролю та компенсаторів у разі процедурних дефектів [12; 14].

В українському контексті верховенство права має й *антидискреційну* функцію: воно обмежує свавілля у виборі засобів збирання та подання доказів, вимагаючи прозорих правил і підзвітності (мотивувальні обов'язки слідчого судді й суду) [8; 22], а також такого опису кожного кроку, щоб захист мав реальний доступ до перевірки, а суд – можливість оцінити пропорційність і рівність сторін [10; 11].

3.1.2 Методологічний імператив: зв'язок предмета, форми та оцінки

Методологічний імператив верховенства права полягає в узгодженні трьох інваріантів: **що** встановлюється (предмет доказування), **як** одержується й легалізується фактичний матеріал (процесуальна форма) і **за чим** оцінюється (стандарти та фільтри) [11; 12; 16]. Предмет доказування (ст. 91 КПК) визначає межі релевантності: технічний артефакт (відеокадр, GNSS-трек, CDR-журнал) має логічно й юридично підсилювати відповідний елемент доведення [18; 24]. *Процесуальна форма* – це механізм легалізації результату: правова підстава, документування способу доступу та умов фіксації, атрибуція джерела, безперервний *ланцюг збереження цифрових даних (chain of custody*[1]*)* через хеш-ідентифікацію, часові

[1] Термін «***chain of custody***» перекладається українською як: ланцюг збереження або більш точно: ланцюг володіння й збереження цифрового доказу (цифрових даних). Це документований

мітки та журнал доступів; для цифрових слідів ці вимоги конкретизуються *«паспортом доказу»* відповідно до *ISO/IEC 27037, ENFSI BPM, NIST SP 800–101* і *Berkeley Protocol* [2; 3; 5]. *Оцінка* здійснюється через фільтри: законність/передбачуваність → належність → автентичність/цілісність → відтворюваність/достовірність → достатність → пропорційність/мінімізація → рівність сторін; дефект будь-якого рівня веде до відсікання або зниження ваги, а за потреби – до компенсаторів (підтвердження незалежними каналами, розкриття «сирих» даних тощо) [12; 14; 24].

Порушення форми (нелегітимне одержання, розрив ланцюга збереження) не компенсується змістом; так само сукупність релевантних даних без відтворюваної методики не створює достатності [10; 21]. У цифровому контексті достовірність зображення чи *месенджер-скріншоту* невіддільна від «технічної біографії» (походження, метадані, хеші, журнали доступу) і можливості незалежної реплікації захистом; нерозкриття методів і «сирих» даних підриває допустимість та вагу [7; 12]. Воєнний стан змінює організацію та строки, але ***не знижує*** тестів законності, пропорційності й змагальності; за їх браку застосовуються відсікання або компенсатори [12; 16]. Отже, зв'язок *«предмет – форма – оцінка»* матеріалізує верховенство права в доказуванні; його операціоналізація через «паспорт доказу», ланцюг збереження та фільтри стандартизує роботу з цифровими слідами й підвищує передбачуваність рішень [5; 12; 24].

3.1.3 Авторська концепція доказування: етапи, категорії, ролі судового контролю та сторін У центрі моделі – послідовність етапів і система оціночних категорій, які матеріалізують верховенство права в конкретних процесуальних діях і судових рішеннях. Вона забезпечує єдність «що доводимо – як одержуємо й легалізуємо – за якими критеріями оцінюємо», уникаючи й формального ритуалізму, і дискреційного свавілля [10; 11; 24].

Етап 1. Одержання (ідентифікація та збір). Вихідний критерій – законність і передбачуваність: наявність правової підстави з чіткими межами (об'єкт, часові «вікна», географія, селектори) та гарантіями контролю відповідно до тестів пропорційності ЄСПЛ (нагляд/доступ до комунікацій) [12; 13; 18]. Фіксуються канал доступу, суб'єкт і контекст одержання, первинні часові мітки – для атрибуції й відтворюваності наступних процедур [2; 5; 25]. Авторська позиція: збір – вибірково обґрунтований і технічно строгий (read-only/ізоляція за потреби), лише необхідний і релевантний обсяг; документування умов (місце/час/таймзона/оточення), параметрів ПЗ/обладнання, первинний форензійний образ і хешування з фіксацією джерела часу [5]. Для OSINT – кроки *Berkeley Protocol* (discovery → collection → preservation, URL/URI, таймзона, верифіковані архівні копії, опис

і верифікований процес фіксації, зберігання, передачі та доступу до цифрового доказу від моменту його одержання до пред'явлення в суді. Він гарантує, що доказ (цифрові дані) не змінено; не втрачено метадані або ідентифікатори; усі доступи до нього фіксуються; можлива перевірка кожного кроку.

інструментів) [2]; у справах про воєнні злочини це критично через волатильність цифрових слідів [25].

Мінімум дій: ідентифікація носія/каналу → перевірка мандата → безпечне одержання → первинні хеші (SHA-256/512) оригіналу й копій → фіксація джерела часу (NTP/PTP) і таймзони → протоколювання, пакування/маркування → старт «*паспорта цифрового доказу*» [2; 5; 25].

Критерії оцінки: законність, належність, мінімізація втручання; дефекти – компенсатори або зниження ваги/відсікання [5; 12; 13; 18]. *Стандарти/форми:* ухвала/ордер; протокол + додаток «паспорт доказу»; SOP – ISO/IEC 27037, ENFSI BPM, NIST SP 800–101, *Berkeley Protocol* [5; 2; 25].

Етап 2. Фіксація. Мета – збереження первісного стану й відтворюваність процедур: форензійний образ (bit-by-bit або валідований логічний), повні метадані, первинні/повторні хеші (SHA-256/512), режим лише-читання (write-blocker/ізоляція), безперервний журнал доступів, відеофіксація критичних фаз, синхронізація часу, розведення «оригіналу» і «робочих» копій; для OSINT – верифіковані архівні копії з фіксацією URL/URI і способу доступу [1–5; 18; 24].

Критерії: автентичність (ідентичність хешів), цілісність (безперервний ланцюг збереження цифрових даних – *chain of custody*), відтворюваність, повнота, мінімальне втручання, прозорість; належне процесуальне оформлення протоколом слідчої дії [1; 3; 5; 18; 24].

Етап 3. Збереження. Забезпечується незмінність від моменту первинного одержання до подання в суд: використання WORM/immutable-сховищ, поділ «оригінал»/«робочі» копії, принцип найменших повноважень і ролі custodian, перехешування при кожній операції та фіксація в журналі доступів; регулярні *fixity checks* для раннього виявлення деградації даних [1; 3; 5]. Відсутність первинного хешу, прогалини журналу чи змішування копій – процесуальний ризик, що веде до зниження ваги або відсікання [1; 3; 5].

Етап 4. Дослідження (аналіз, мультисенсорна кореляція). Побудова єдиної часової шкали, кількісна оцінка похибок і перевірка узгодженості незалежних каналів (відео/аудіо, GNSS, CDR, EXIF/XMP) з повною документацією інструментів, версій і параметрів – для гарантованої реплікації захистом і судом [3; 4; 25]. Послідовність: синхронізація часу → оцінка невизначеностей (HDOP/VDOP; радіус сектора БС; похибки стабілізації/орторектифікації) → перевірка збігів у межах допусків → фіксація алгоритмів і контрольних хешів проміжних файлів [3; 4; 25].

Етап 5. Представлення. Структуроване подання легалізує технічний результат як судовий доказ: правова підстава (ухвала/ордер, межі, строки, селектори), повний **«паспорт доказу»** (атрибуція джерела/каналу, умови фіксації, параметри ПЗ/апаратури, хеші, часові мітки, журнал доступів, опис ланцюга збереження), опис методик і параметрів (із відсиланням до SOP), об'єднана часо-просторова шкала з допусками. Додаються верифіковані додатки: хеш-реєстр raw/working,

конфігурації інструментів, версії ПЗ, журнали та контрольні логи – для забезпечення принципу процесуальної рівності сторін (*equality of arms*) й незалежної реплікації [7; 11; 12]. За обмеженого доступу – еквівалентні механізми (контрольований перегляд, віртуальний стенд, дегідентифіковані копії з відкритими метаданими). Подання має демонструвати «якість закону», пропорційність і відсутність індуктивної ролі держави; скріншоти замінюються форензійними образами з логами інструментів і хешами [20; 22; 26; 7].

Етап 6. Судова оцінка. Суд застосовує послідовні фільтри й визначає наслідки дефектів: ***належність*** (логічний/юридичний зв'язок із предметом доказування) [24; 18]; ***допустимість*** (законність способу одержання й оформлення; порушення – відсікання/зниження ваги, зокрема щодо нагляду/перехоплення і недопровокації) [6; 12; 15]; **достовірність** (цілісність через хеш-ідентичність, автентичність через метадані та безперервний ланцюг збереження, відтворюваність методик) [1; 3; 5]; ***достатність*** (міжканальна кореляція підвищує переконливість; одиничні або суперечливі сліди – знижують) [12; 25]. ***Матриця дефект → наслідок*:** немає правової підстави/перевищено межі – відсікання [12; 15; 6]; розрив ланцюга збереження, відсутність первинного хешу/метаданих – сумнів в автентичності та зниження ваги або виключення [1; 3; 5]; «фонові» або асоціативні матеріали без логічного містка – неврахування [24; 18]; внутрішня неузгодженість без міжканальної кореляції – недостатність [12; 25]. Воєнний стан не змінює цих вимог: за дефіциту часу забезпечуються законність втручання, належне документування ланцюга збереження та можливість незалежної перевірки ключових кроків [12; 18; 24].

Висновок підрозділу. Авторська концепція – це системна процедура перетворення технічного результату на судовий доказ через послідовні етапи та чіткі оціночні категорії, оперті на верховенство права, стандарти справедливого суду та актуальні методики.

3.1.4. Верховенство права як «методологічний фільтр»: як принцип спрямовує тлумачення норм КПК (процесуальна справедливість, рівність сторін, пропорційність втручання)

Як методологічний фільтр верховенство права задає судові орієнтири для тлумачення відкритих формулювань КПК: кожна процесуальна норма читається крізь призму законності, передбачуваності, заборони свавілля, доступу до правосуддя та ефективного контролю влади [11; 10; 20]. Правозастосувач пов'язує ***предмет доказування*** з належною ***процесуальною формою*** та подальшою ***оцінкою доказів***, забезпечуючи змістовну справедливість за збереження конституційних і процесуальних гарантій [16; 18].

По-перше, ***процесуальна справедливість*** у цифровому доказуванні конкретизується через «якість закону» та стримуючі гарантії: чіткі підстави й межі доступу до даних, незалежний нагляд, правила зберігання/видалення, а також

компенсатори у разі обмеженої первинної процедури (зокрема у воєнних умовах) [12; 13; 14]. Брак гарантій ставить під сумнів справедливість провадження та впливає на допустимість і вагу цифрових слідів [12; 13].

По-друге, ***рівність сторін*** вимагає реальної можливості захисту перевірити технічний результат: доступ до сирих даних або їх еквівалента, розкриття методики, відтворюваність хешів/таймстемпів, можливість контрекспертизи. Цей стандарт узгоджується з підходом ЄСПЛ до непрямих джерел і вже імплементований у практиці ККС ВС щодо електронних повідомлень та скріншотів [7; 14].

По-третє, ***пропорційність втручання*** є матеріальним порогом законності: легітимна мета, придатність засобу, необхідність (відсутність менш інвазивної альтернативи) та вузька пропорційність; невиконання тесту веде до відсікання або зниження ваги [12; 16].

У цифровому контексті ці принципи «перекладаються» на процесуальні тести: перевірка джерела й способу доступу; безперервний **ланцюг збереження цифрових даних**; цілісність/автентичність (хеш-ідентифікація, часові мітки, журнал доступів); поясненність аналітичних процедур; *міжканальна кореляція*. Порушення є дефектом форми і не компенсується переконливістю змісту – наслідок: відсікання або зниження ваги відповідно до стандартів і права [3; 5; 6].

Воєнний стан не послаблює цього фільтра, а підвищує вимоги до мотивації та компенсаторних гарантій: стислий час і утруднений доступ не звільняють від обов'язку довести необхідність, зафіксувати цілісність і забезпечити перевірність для захисту в межах процесуальної форми КПК. Це обмежує дискрецію та уніфікує практику, зближуючи її з доктриною правовладдя і національними орієнтирами доказування [18; 8; 24; 26].

3.2 Предмет доказування у воєнний час: акценти та виклики

3.2.1 Специфіка предмета доказування (ст. 91 КПК) під час воєнного стану

Предмет доказування за ст. 91 КПК – нормативно визначена сукупність фактичних обставин, без установлення яких неможливе законне вирішення провадження [18; 24]. Воєнний стан не скорочує цей зміст, а ***додає контекст нацбезпеки***: наявність, тривалість і межі воєнного стану, характер загрози, зв'язок інкримінованої поведінки з умовами збройної агресії та її вплив на охоронювані інтереси [6; 7; 25]; без їх належної фіксації суд не може ані легітимно застосувати воєнні процесуальні модифікації, ані надати коректну матеріально-правову оцінку [24].

Особливість воєнного часу – ***вимога оперативності****:* змінюються не елементи доказування, а допустимі форми й темпоральні межі збирання та перевірки доказів (розд. IX-1, ст. 615 КПК) [18]. Гнучкість не знижує стандарт: межі відступів окреслюються підходами ЄСПЛ щодо ефективних гарантій контролю, пропорційності втручань і збереження ядра права на справедливий суд, зокрема у справах про втручання в комунікації та нагляд [12; 13; 14].

Дефіцит часу створює два ключові ризики. По-перше, втрата або спотворення летких цифрових слідів (системні журнали, метадані, геолокація, відео, OSINT) вимагає негайного вилучення, фіксації часових міток і безперервності ланцюга збереження цифрових даних за NIST SP 800-101r1, *Berkeley Protocol*, ENFSI BPM, ISO/IEC 27037 [1–3; 5]. По-друге, *часовий дисбаланс* між обвинуваченням (перший доступ у зоні бойових дій) і захистом. Тому предмет доказування включає і факти, що підтверджують реальну змагальність: своєчасне відкриття матеріалів, прозоре походження цифрових доказів, доступ захисту до технічних характеристик і протоколів верифікації, ефективний і своєчасний судовий контроль [6; 7; 12; 14].

Підсумок: воєнний стан ***розширює предмет доказування контекстами*** часу й нацбезпеки без зниження стандартів. Обвинувачення доводить подію й винуватість **разом із** юридичною наявністю/межами воєнного режиму, зв'язком умов війни з прискореними рішеннями та дотриманням мінімально необхідних гарантій справедливого процесу за дефіциту часу [6; 7; 12; 25; 18].

3.2.2 Процесуальні особливості воєнного стану: строки, дистанційні дії, доступ, судовий контроль

КПК не знижує стандарт доказування, а **коригує режими**: 48 год на повідомлення про підозру затриманому, інакше – звільнення; період дії воєнного стану в провадженнях без підозри на дату його введення не зараховується до строків досудового розслідування (ст. 219) [18]. Прискорені/спрощені механізми можливі **лише** в межах і на підставах ст. 615 КПК із наступним судовим контролем; «автоматичні» продовження запобіжних заходів без судової перевірки несумісні з Конституцією та засадами верховенства права [8; 10; 11; 16; 18].

***Дистанційні процесуальні* дії** забезпечують безпеку й оперативність: на досудовій стадії – допити, впізнання тощо в режимі відеоконференції за умов належної ідентифікації та суцільної технічної фіксації (ст. 232); у суді – дистанційна участь, у винятку – допит поза приміщенням суду з власними техзасобами за відсутності іншої можливості (ст. 336) [18]. Рішення мають бути мотивованими, з гарантіями змагальності й публічності; сам відеозв'язок не порушує ст. 6 Конвенції за умови рівності сторін і ефективності захисту [14].

Ускладнений доступ до місця події/свідків зумовлює «аварійні» режими з підвищеними вимогами до фіксації: огляд/обшук без понятих – за безперервної відеофіксації з подальшим належним оформленням і внесенням відомостей до ЄРДР одразу після усунення перешкод (рамка ст. 615) [18]; техніко-криміналістична частина – за міжнародними настановами з ідентифікації, вилучення та збереження цифрових слідів [1; 3; 5]. У районах активних бойових дій важлива **процедура відновлення втрачених матеріалів** (ст. 615–1 КПК) [18]. Недосяжність свідків/потерпілих компенсується дистанційними допитами з суворою ідентифікацією й техфіксацією для подальшої перевірності [14; 18].

***Судовий контроль**:* тимчасова субституція окремих повноважень слідчого судді керівником органу прокуратури допускається лише коли суд об'єктивно не може діяти – із безумовною наступною судовою перевіркою та можливістю оскарження (ч. 4 ст. 615) [18; 16].

Територіальна підсудність адаптується (спрямування до суду за місцем органу досудового розслідування чи іншого визначеного суду) для безперервності контролю [18]. Підсумково, ***будь-яке спрощення форми*** допустиме настільки, наскільки збережено відновлюваність судового контролю, перевірність джерел і реальні можливості захисту діяти за дефіциту часу [18; 8; 10; 11; 14].

3.2.3 Баланс ефективності та прав людини: тест пропорційності (легітимна мета → придатність → необхідність → вузька пропорційність)

Умови воєнного стану не скасовують вимоги верховенства права й справедливого суду: будь-які процесуальні модифікації проходять чотириетапний тест пропорційності, виведений із конституційних засад, доктрини верховенства права та орієнтирів ЄСПЛ [10; 11; 16; 20; 21; 24].

(1) *Легітимна мета*. Обмеження процесуальних прав (скорочені строки, дистанційні дії, тимчасові відступи від «звичних» форм) допустимі лише заради захисту нацбезпеки, життя і безпеки людей, належного здійснення правосуддя – тобто з метою, яку Конституція й Конвенція визнають легітимною [10; 11; 16]. У цифровому сегменті легітимність конкретизується в матеріалах провадження (яку загрозу нейтралізує захід, який очікуваний доказовий результат), а не декларується абстрактно [24; 25].

(2) *Придатність (раціональний зв'язок*). Захід має об'єктивно сприяти досягненню мети: дистанційний допит, суцільна відеофіксація обшуку, форензійне копіювання – придатні, якщо реально забезпечують збереження та перевірність слідів у бойових умовах [18]. Оцінка спирається на визнані SOP/стандарти (NIST SP 800-101r1; *Berkeley Protocol*; ENFSI BPM; ISO/IEC 27037), що задають мінімальні вимоги надійності й відтворюваності [1–5].

(3) *Необхідність (найменше обмежувальний засіб).* Держава доводить, що серед ефективних альтернатив обрано найменш інтенсивне втручання; ЄСПЛ вимагає не «корисності», а необхідності в демократичному суспільстві із запобіжниками та можливістю незалежного контролю [12; 13]. Практично це означає пояснити, чому неможлива безпосередня участь свідка замість відеозв'язку, чому негайне копіювання даних було єдиним способом зберегти леткі сліди, або чому відступ від стандартного санкціонування був об'єктивно неминучим [6; 7; 18]. За використання непрямих джерел суд застосовує компенсатори (доступ до джерела, перехресний допит, альтернативні докази) [14].

(4) *Вузька пропорційність* (*stricto sensu*). Навіть «необхідний» захід відпадає, якщо шкода для прав людини явно переважає публічний зиск; суд зважує інтенсивність втручання (тривалість, обсяг даних, обмеження змагальності) проти

приросту доказової цінності й безпекового ефекту з урахуванням запобіжників – судового контролю, прозорого походження цифрових доказів, ланцюга збереження цифрових даних, можливості незалежної перевірки [8; 10; 11; 29]. Для цифрових доказів критичною «вагою» є технічна надійність і відтворюваність процедур (форензійні образи, хеш-верифікація, протоколи доступу) за міжнародними стандартами; за їх відсутності баланс зміщується проти втручання [1–5; 24]. Водночас ЄСПЛ наголошує: навіть за посилених загроз недопустимі процесуальна провокація та імітація доказів – така практика руйнує пропорційність і справедливість розгляду [15].

Висновок. У воєнний час тест пропорційності виконує роль процесуального «регулятора тиску»: ефективність розслідування та судового контролю підтримується лише за умов **документованого** проходження чотирьох етапів – легітимна мета → придатність → необхідність → вузька пропорційність – із належними гарантіями та фіксацією в матеріалах провадження [10–13; 18; 24; 29].

3.3 «Процесуальні фільтри» доказування: доктринальна модель

У межах методології верховенства права «процесуальні фільтри» виконують подвійну функцію: *нормалізують шлях* технічного результату до судового доказу та *задають стандарти контролю*, що забезпечують передбачуваність і справедливість провадження. Вони узгоджуються з базовими категоріями авторської концепції (належність, допустимість, достовірність, достатність) і операціоналізують вимоги *законності, пропорційності та процесуальної рівності сторін* [13; 25; 6]. Кожен фільтр має мінімум процесуальних умов, типові зони ризику й передбачувані наслідки для допустимості та ваги.

Фільтр законності та передбачуваності. *Суть:* наявність правової підстави, передбачуваних процедур доступу/санкціонування та реального судового контролю; вимога *«якості закону»* (визначеність, доступність, передбачуваність) [10; 11; 16]. *Мінімум:* пряма норма; мотивована ухвала з конкретизацією обсягу/меж/строку; дотримання процедури виконання і фіксації; контроль і оскаржуваність [10; 11; 16; 18]. *Типові помилки:* бланкетні ухвали, *ex post* легітимація, вихід за межі санкції, формальний контроль [6; 7; 11]. *Наслідок:* відсікання/зниження ваги; інколи – виключення похідних [10; 11; 18]. *Мікро*: доступ до масиву трафіку без меж і строків – недопустимий (стандарт *quality of law*, мотивування ККС) [11; 10; 6; 7; 18].

Фільтр атрибуції, автентичності та цілісності ланцюга збереження цифрових даних (chain of custody). *Суть:* атрибуція (зв'язок даних із джерелом), автентичність (незмінність), цілісність (безперервний контроль) перетворюють цифровий артефакт на процесуальне джерело [1; 3; 5]. *Мінімум:* ідентифікація носія/каналу; первинне/повторне хешування (SHA-256/512); *write-blocker*; журнал доступів; синхронізація часу; належне зберігання; протокол [1–5]. *Типові помилки:* копіювання без *write-blocker*, відсутність первинного хешу, змішування «ро-

бочих» і доказових копій, відсутність часових міток, «скріншотування» замість образу [1; 3; 5]. *Наслідок:* зниження ваги або недопустимість [1; 3; 5; 18]. *Мікро*: відео без метаданих і безперервного ланцюга – недопустиме (ENFSI–DI) [4; 3; 18; 2].

Фільтр пропорційності (легітимна мета → придатність → необхідність → вузька пропорційність). *Суть:* кожне обмеження прав проходить повний тест, що забезпечує співмірність і запобіжники [11; 10]. *Мінімум:* чітка мета; доведена придатність; аналіз менш обмежувальних альтернатив; вузька пропорційність з урахуванням тривалості/обсягу/чутливості; судовий контроль [18; 11; 10]. *Типові помилки:* автоматизм відступів, *blanket*-ухвали, «збирання про запас», *ex post* виправдання [12; 13; 11]. *Наслідок:* обмеження використання або недопустимість як непропорційного [12; 13]. *Мікро*: масовий запит до провайдера без підозрюваних – порушення «вузької» пропорційності [12; 13; 11; 10].

Фільтр змагальності та рівності сторін. *Суть:* спрощення форм не може нівелювати реальну можливість оборони; має бути доступ до джерел, перехресний допит, час на підготовку, техдані для незалежної перевірки [18; 14]. *Мінімум:* своєчасне відкриття; машинозчитувані копії/образи та протоколи; участь у ключових діях; мотивовані компенсатори для дистанційних форматів [18; 14]. *Типові помилки:* «останньомиттєве» відкриття, відмова у копіях образів, недоступність лабораторних журналів, ігнорування компенсаторів [14; 18]. *Наслідок:* перенесення, обмеження використання або відсікання; зниження ваги через утиск змагальності [14; 18].

Фільтр надійності методики (технічна валідність і відтворюваність). *Суть:* прийнятність залежить від валідованих методів, кваліфікації виконавця і можливості незалежного повторення [1–5]. *Мінімум:* SOP (NIST/ISO/ENFSI/Berkeley), калібрування/валідація інструментів, контрольні тести, повна протоколізація, реплікація [1–5]. *Типові помилки:* «чорні скриньки» без валідації, скріншоти замість образів, відсутність контрольних тестів, неузгоджені часові мітки [1; 3; 5]. *Наслідок:* зменшення ваги або недопустимість [1; 3; 5]. *Мікро*: витяг чатів лише через відображення екрана – методичний дефект (NIST/ISO/ENFSI) [1–5].

Фільтр недопровокації та заборони створення доказів державою. *Суть:* держава не може провокувати злочин чи створювати докази; такі матеріали несумісні зі справедливим судом [15]. *Мінімум:* об’єктивна підозра до втручання; пасивна роль правоохоронців; повне документування ініціативи та ходу дій; перевірність джерел [15; 6; 7]. *Типові помилки:* спонукання/обіцянки вигоди; тиск на «коливного» суб’єкта; «вкидання» предметів/даних; маніпулятивні скорочення записів [15]. *Наслідок:* недопустимість; пріоритет презумпції невинуватості [6; 7; 15].

Фільтр релевантності (належності) та допустимості. *Суть:* доказ оцінюється лише за наявності логічного зв’язку з елементами предмета доказування

та належної форми одержання/перевірки [24; 18]. *Мінімум:* місток «факт → елемент ст. 91 КПК»; дотримання форми; доступність для перевірки; належна атрибуція [18; 23; 24]. *Типові помилки:* «збирання на запас», дотичні сліди без зв'язку, підміна релевантності асоціативністю [18; 24]. *Наслідок:* відсікання або зниження ваги [18; 23; 24].

Фільтр достатності та переконливості сукупності. *Суть:* сукупність має бути несуперечною, логічно зв'язаною та достатньою; одиничний «сирий» цифровий слід рідко самодостатній [24; 29]. *Мінімум:* міжканальна кореляція, перевірка альтернатив, урахування виправдувальних даних, внутрішня логіка [6; 7; 24; 29;]. *Типові помилки:* покладання на єдине джерело, ігнорування контрдоказів, непротоколювання «летких» слідів [24; 29]. *Наслідок:* неможливість доведення поза розумним сумнівом; виправдання або повернення матеріалів [6; 7; 24; 29].

Фільтр судового контролю та мотивованості рішень. *Суть:* ефективність усіх фільтрів залежить від реального, своєчасного та мотивованого судового контролю втручань і оцінки доказів [10; 11; 18]. *Мінімум:* негайний доступ до суду; перевірка підстав/меж/пропорційності; фіксація мотивів; оскаржуваність; публічність у межах безпеки [10; 11; 18]. *Типові помилки:* «шаблонні» ухвали, дублювання клопотання, ігнорування пропорційності, відкладення контролю [6; 7]. *Наслідок:* відсікання/обмеження використання, зниження ваги, повторний розгляд [6; 7; 18]. Ілюстрація: немотивований дистанційний допит скасовується апеляцією з посиланням на *rule of law* і вимоги КПК [6; 10; 11; 18].

У підсумку фільтри утворюють цілісну систему: *законність, атрибуція/цілісність, пропорційність, змагальність, методична надійність, антипровокаційність, релевантність і достатність, а також реальний судовий контроль* – як інтегровані точки перевірки. Їх послідовне, доказово артикульоване застосування дозволяє поєднати оперативність воєнного часу з незнижуваними конституційними та конвенційними стандартами справедливого суду.

3.4 Цифрові докази: стандарти, ланцюг збереження та «паспорт доказу»

Цифрові сліди – динамічна сукупність візуальних даних (у т.ч. супутникових і з БПЛА), аудіо, GNSS, телекомунікаційних/мережевих журналів (CDR, log-files), системних метаданих (EXIF), артефактів із месенджерів і хмарних сервісів. Їх доказова спроможність залежить від швидкого «заморожування» стану, ретельного первинного опису й забезпечення можливості незалежної перевірки. Процесуальну спроможність задають взаємодоповнювані SOP: ISO/IEC 27037 (ідентифікація/збирання/одержання/збереження), ENFSI BPM (цифрова техніка; автентифікація зображень), NIST SP 800–101 (мобільна форензія) та *Berkeley Protocol* (OSINT) [1–5; 18; 24].

Ключ – безперервний ***ланцюг збереження цифрових даних***: ідентифікація джерела (пристрій/акаунт/канал), фіксація часу/місця/умов доступу, коректне

одержання (форензійний образ; WORM; write-blocker; контроль середовища), первинні хеші (як правило SHA-256/512), журнал доступів і повторна верифікація при кожній передачі/аналізі [1; 3; 5]. Для візуальних матеріалів ENFSI вимагає перевірки контейнера/метаданих, виявлення повторних компресій і часових несумісностей; для OSINT – фіксацію URL/URI, часових міток і таймзони, архівацію та опис атрибуції автора/контенту [2; 4]. Усе оформлюється за КПК – саме процесуальна форма перетворює технічний результат на судовий доказ [18; 24].

Практичний механізм «зшивання» вимог – ***«паспорт доказу»***: стислий атрибуційно-реєстраційний модуль супроводу артефакта від одержання до подання суду. ***Мінімум змісту паспорта:*** (1) ідентифікація джерела/каналу (IMEI/IMSI, MAC/UUID, URL/handle тощо); (2) суб'єкт і спосіб одержання; (3) час/місце/умови фіксації; (4) параметри ПЗ/обладнання; (5) хеш-ідентифікатори оригіналів і копій; (6) повний журнал доступів; (7) опис створення образів (WORM, write-blocker, лог-файли утиліт); (8) міжканальна кореляція для мультимодальної ф'юзії (синхронізація відео + CDR + GNSS); (9) доступність «сирих» даних для незалежної перевірки [2; 3; 5]. Паспорт не замінює процесуальної форми, але надає технічний субстрат контролю законності, достовірності та відтворюваності, слугуючи базою для змагальної перевірки [13; 24; 25].

Класи-специфіка. Для мобільних – ізоляція (airplane mode/Faraday), збереження живлення, вибір методу отримання (логічний/фізичний), форензійний звіт інструмента та контроль ланцюга при кожному переносі (NIST) [1]. Для зображень/відео – ENFSI BPM–DI: EXIF/XMP, детекція редагувань, аналіз GOP, просторово-часова узгодженість [4; 3]. Для OSINT – *Berkeley Protocol*: документований шлях ***виявлення → збирання → збереження***, верифікація (гео/хронолокація, мовні/мережеві маркери), критерії достовірності джерела [2].

Змагальна придатність паспорта перевіряється судом у трьох площинах: (а) законність доступу/санкціонування (підстави, межі, мотивованість) [18]; (б) технічна відтворюваність процедур (можливість повторити тим самим інструментом і отримати ідентичні хеші/вибірки) [1–5]; (в) логічна узгодженість мультимодальної сукупності (взаємне підтвердження відео, CDR, GNSS, системних метаданих) [3; 5]. Відсутність елементів знижує вагу, а дефекти законності або непоправна втрата автентичності – тягнуть недопустимість [18; 24]. У воєнних провадженнях пришвидшення форм не повинно руйнувати відтворюваність і перевірність – саме SOP ISO/ENFSI/NIST/*Berkeley* та належно оформлений паспорт дозволяють поєднати оперативність із вимогами допустимості та переконливості сукупності [1–5; 24].

3.5 Практика ЄСПЛ: тест справедливості та вплив на допустимість

Втручання у приватність і комунікації допустиме лише за наявності зрозумілої нормативної рамки та дієвих запобіжників. *Roman Zakharov і Big Brother Watch* окреслюють «якість закону» й стримуючі гарантії (чіткі підстави/межі, незалеж-

ний нагляд, селектори, регламентація зберігання/видалення, повідомлення, ефективні засоби захисту) [13; 12]. Дефіцит якості закону не автоматично запускає «плід отруєного дерева», але потребує або виключення, або переконливих компенсаторів (розкриття методів, незалежна перевірка, суворий огляд пропорційності); за їх відсутності провадження стає несправедливим [11–13]. У цифровому сегменті без прозорого мандата, окреслених меж і простежуваності техпроцедур (журнали доступу, час, селектори, правила зберігання/знищення) доказова цінність різко знижується [12; 13; 11; 18]. *Мікроприклад:* bulk-запит CDR «усі пристрої в квадраті 3×3 км за 24 год» без критеріїв і незалежного затвердження – надмірність; суд відсікає або мінімізує вагу, вимагаючи вузько таргетованих селекторів [11; 12; 18]. *Schatschaschwili v. Germany.* Показання неприсутнього свідка (і похідні цифрові сліди) можливі лише за достатніх компенсаторів: причина недоступності, реальна контрперевірка, підтвердження іншими джерелами, мотивована вага [14]. Для цифрових матеріалів це легітимує *мультимодальну кореляцію* (відео, GNSS, CDR, EXIF) [14; 24]. *Приклад:* відео з платформи – автор недосяжний; артефакт верифіковано за *Berkeley Protocol*, автентичність – за ENFSI BPM–DI, метадані синхронізовано з CDR/GNSS; доказ приймається з визначеною вагою [2–5; 14].

Teixeira de Castro v. Portugal. ЄСПЛ відмежував пасивне документування від активного підбурення: коли держава ініціює злочин або тисне на нерішучого суб'єкта, справедливість руйнується – матеріали НСРД відсікаються [15]. Для «цифрових закупівель» і чатів ключові: джерело ініціативи, тональність і повнота запису, можливість незалежного відтворення [6; 7; 15].

Висновок і наслідки для процесу. ЄСПЛ оцінює справедливість ***комплексно***: якість закону/контроль і пропорційність [13; 12; 11; 10], рівність сторін і контрперевірка (особливо за відсутності свідка) [14], відсутність провокації [15]. Практично це означає: на етапі санкціонування – фіксувати мету, межі, строк, селектори, правила зберігання/видалення, механізми нагляду/повідомлення [18; 10; 11; 12; 13]; при розкритті – надавати сирі дані, журнали, параметри інструментів, хеші, протоколи OSINT/форензії (ядро компенсаторів за Schatschaschwili) [1–5; 14]; при судовій оцінці – мотивовано зважувати пропорційність і вагу, перевіряти альтернативи та відсікати провокативні докази [12; 13; 15; 24].

Методичні стандарти NIST/ISO/ENFSI/*Berkeley* створюють технічні гарантії, які суд **перекладає** на мову пропорційності та справедливості; тому **«паспорт доказу»** (джерело, спосіб, хеші, журнали, міжканальна кореляція) – ключ до мінімізації ризику недопустимості [1–5; 18; 24]. Підсумок: справедливість вимагає **одночасного** доведення якісного мандата, пропорційності, реальної змагальності (доступ до сирих даних/метаданих/журналів, можливість реплікації), відсутності провокації та мотивованої ваги кожного цифрового каналу у зв'язку з іншими [10–13; 18; 24].

3.6 Український контекст: конституційно-правові орієнтири та правові позиції Верховного Суду

Конституційна рамка визначає не лише межі втручання в приватність, а й методологію тлумачення процесуальних повноважень у сфері даних і комунікацій: засади верховенства права, поваги до приватності та належного судового контролю (статті 8, 32 Конституції) [16]. На доктринальному рівні це конкретизується через правовладдя, «якість закону» та обмеження дискреції за умови реальної підконтрольності суду [8; 10; 11; 21; 20]. Звідси авторська позиція: кожна технікокриміналістична дія з цифровими слідами має спиратися на прозору правову підставу і передбачувану процедуру; воєнні відступи – лише після повного тесту пропорційності; «якість закону» і мотивований судовий контроль є матеріальними умовами допустимості в координатах належності/допустимості/достовірності/достатності [24; 11; 10].

Правові позиції ККС ВС операціоналізують цю рамку в цифровому вимірі. Постанова від 02.04.2024 у справі №450/374/18 наголошує на реальній перевірці ролі правоохоронця в комунікації та суворому дотриманні процесуальної форми фіксації НСРД: активне підбурення несумісне зі справедливим судом і тягне втрату доказової спроможності матеріалів [6; 15]. Постанова від 27.11.2023 у справі №464/472/22 підкреслює, що *скріншот ≠ доказ*: потрібні джерело й цілісність через ідентифікацію пристрою/акаунта, кореляцію з CDR/GNSS та відтворюваність результату (форензійний образ, хеш-верифікація, протоколи інструментів) [1; 3; 4; 5; 7]. Сукупно ці підходи корелюють із фільтрами законності, атрибуції/цілісності, пропорційності та змагальності [10; 11; 24].

3.7 Мікрокейси (інтегрований виклад із застосуванням «процесуальних фільтрів»)

Наведені приклади демонструють, як фільтри перетворюють технічні артефакти на переконливу сукупність і відсікають матеріали, що не витримують перевірки законності, пропорційності, автентичності та змагальності.

Кейс А (удар по об'єкту критичної інфраструктури). Вимоги – законність і вузька пропорційність: ухвала з метою, межами, строками, селекторами; суд – про придатність і відсутність менш інвазивної альтернативи [10; 11; 18]. Далі атрибуція й цілісність ланцюга збереження: для БПЛА-відео – платформа/телеметрія/EXIF, безперервна фіксація «від камери до зберігання», первинні/повторні хеші; для супутникових – джерело/параметри/геоприв'язка/хеші; для CDR – оператор/селектори/NTP – PTP/журнали/відтворюваність вибірки [3–5]. Усе зводиться у *паспорт доказу* та міжканальну кореляцію «БПЛА ↔ супутник ↔ CDR»; змагальність забезпечується відкриттям raw-файлів, телеметрії та логів [11; 18].

Кейс Б (провокація в месенджері/провокація збуту). Ключ – антипровокаційний фільтр: ініціатива контакту, спонукальна лексика, нав'язування сценарію, обіцянки вигоди, повнота логу без «обрізок» [6; 15]. Далі – законність/передба-

чуваність і атрибуція/цілісність: ідентифікація акаунтів/пристроїв, хеш-верифікація чат-логів, журнал доступів, відтворюваний експорт з протоколами інструмента, кореляція з CDR/GNSS [18; 11; 10; 1; 3; 5]. За фіксації індуктивної ролі держави – відсікання (Teixeira de Castro) [6; 15].

Кейс В («скріншот» проти форензійного образу; Telegram + EXIF). Скріншот – лише ілюстрація; прийнятний шлях – форензійний образ/експорт з логом інструмента та хешами (SHA-256/512) [1; 3; 5]. Атрибуція спирається на MSISDN/IMSI/IMEI, device ID/push-токени, події застосунку та «відбитки» пристрою у EXIF; часові мітки EXIF корелюються з CDR/GNSS і системними логами. Для змагальності – відкриття raw/метаданих/логів для незалежної реплікації [11; 18]. Позиція ККС і стандарти NIST/ENFSI/ISO: «чисті» скріншоти без образу та кореляції мають мінімальну вагу [1; 3; 4; 5; 7].

Кейс Г (кореляція CDR – GNSS – відео для верифікації БПЛА-відео). Переконливість забезпечує узгоджена множина: паспорт із хешами raw-файлів, телеметрія БПЛА, ENFSI-аналіз автентичності, валідований витяг із мобільного (NIST), CDR, що збігаються з GNSS-треком; за належної форми доказ визнається належним і переконливим [1; 3–5; 7; 24].

Підсумок. Суд і сторони щоразу мають демонструвати: «якість закону» (підстави, межі, строки, селектори, нагляд), автентичність і безперервний ланцюг збереження (первинні хеші, *write-blocker*, журнали, звіти інструментів), реальну змагальність (відкриття raw-даних і можливість незалежної перевірки), антипровокаційний стандарт та міжканальну кореляцію. Дефект будь-якої ланки веде до відсікання або критичного зниження ваги [1; 3–7; 10–16; 24].

ВИСНОВКИ

У центрі запропонованої моделі – верховенство права як методологічний критерій оцінки цифрових доказів у воєнний час. Рамка одночасно враховує конституційні засади приватності й судового контролю, процесуальні обмеження та ризики дефіциту часу, а також технічну специфіку збирання, збереження й перевірки електронних слідів. Вона синхронізує конституційно-процесуальні орієнтири (статті 8, 32 Конституції) та форму КПК [16; 18] із тестами ЄСПЛ щодо «якості закону», пропорційності, недопровокації та компенсаторів [10–15], технічними настановами ISO/ENFSI/NIST/*Berkeley* як основою відтворюваності й перевірності [1–5] та національною практикою ККС ВС [6; 7], забезпечуючи коректну оцінку допустимості й доказової ваги цифрової інформації без зниження гарантій справедливого суду.

Методологічний здобуток – формалізація **системи процесуальних фільтрів** як інструменту матеріалізації верховенства права в доказуванні:

– **законність і передбачуваність** (належний мандат, визначені межі/строки, селектори, реальний контроль);

– **атрибуція, автентичність і цілісність ланцюга збереження** (ідентифікація джерела, первинні/повторні хеші, журнали доступів);

– **пропорційність** (повний тест: легітимна мета → придатність → необхідність → вузька пропорційність);

– **змагальність** (відкриття «сирих» даних і метаданих, можливість незалежної реплікації, компенсатори).

Сукупно фільтри не лише відсікають дефектні матеріали, а й підвищують переконливість коректно зібраної мультимодальної сукупності (відео, GNSS, CDR, EXIF).

Практична цінність – готові алгоритми для всіх учасників процесу.

– Для ***обвинувачення****:* перевірка мандата; повне документування технічного треку (інструменти/версії, журнали, хеші); дотримання ISO/ENFSI/NIST при ідентифікації, збиранні та збереженні; негайні форензійні образи; синхронізація часу; демонстрація вузької пропорційності; прозора атрибуція; міжканальна кореляція для оцінки достатності.

– Для ***захисту***: запит і аналіз «сирих» даних/метаданих; перевірка інструментів і хеш-значень; застосування тесту пропорційності; оскарження провокації та дефектів ланцюга збереження.

– Для ***суду****:* мотивований контроль «якості закону» і пропорційності; перевірка відтворюваності цифрових доказів; з'ясування ролі державних агентів; застосування компенсаторів; аргументоване визначення доказової ваги кожного каналу.

Перспективи розвитку – кодифікація ***«паспорта цифрового доказу»*** як обов'язкового процесуального реквізиту (джерело/канал; інструменти й середовища; первинні та повторні хеші; журнали доступів; карти синхронізації часу; методика міжканальної кореляції); оновлення відомчих інструкцій із прямими відсиланнями до ISO/ENFSI/NIST та *Berkeley Protocol*; уніфіковані компенсатори для спрощених процедур; розвиток спеціалізованих підрозділів для роботи з шифрованими та мультисенсорними даними. Запропонована модель поєднує систему фільтрів, міжнародні стандарти та інститут «паспорта доказу», забезпечуючи практичний баланс між оперативністю воєнного часу й незнижуваними стандартами справедливого судового розгляду.

ПОДЯКИ

Немає

КОНФЛІКТ ІНТЕРЕСІВ

Немає

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ayers R., Brothers S., Jansen W. NIST Special Publication 800–101, Rev. 1: Guidelines on Mobile Device Forensics. Gaithersburg, MD: NIST. 2014. DOI: 10.6028/NIST.SP.800-101r1. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

[2] Berkeley Protocol on Digital Open Source Investigations: A Practical Guide. Geneva: OHCHR. 2022. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source
[3] ENFSI. Best Practice Manual for the Forensic Examination of Digital Technology. ENFSI-BPM-FIT-01. 2015. URL: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf
[4] ENFSI. Best Practice Manual for Digital Image Authentication. ENFSI-BPM–DI-003–1. 2021. URL: https://enfsi.eu/wp-content/uploads/2021/10/BPM_Image-Authentication_ENFSI-BPM–DI-003–1.pdf
[5] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html
[6] Постанова Касаційного кримінального суду у складі Верховного Суду від 02.04.2024 у справі № 450/374/18 (провадження № 51-3279км22). URL: https://reyestr.court.gov.ua/Review/118297021
[7] Постанова Касаційного кримінального суду у складі Верховного Суду від 27.11.2023 у справі № 464/472/22 (провадження № 51-4189км23). URL: https://reyestr.court.gov.ua/Review/115308709
[8] Венгер В. М. Обмеження дискреційних повноважень як складова принципу верховенства права. *Наукові записки НаУКМА. Юридичні науки*. 2013. Т. 144–145. С. 49–54. URL: https://ekmair.ukma.edu.ua/bitstreams/339e708d-eafe-4a26-b015-f644800fedf3/download
[9] Головатий С. П. Верховенство права: монографія у 3 кн. Київ: Фенікс. 2006. 1730 с. URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64. exe?C21COM=S&FT_PREFIX=&FT_REQUEST=&I21DBN=EC&P21DBN=EC&S21ALL=%28%3C.%3ET%3D%D0%92%D0%B5%D1%80%D1%85%D0%BE%D0%B2%D0%B5%D0%BD%D1%81%D1%82%D0%B2%D0%BE+%D0%BF%D1%80%D0%B0%D0%B2%D0%B0%24%3C.%3E%29&S21CNR=20&S21FMT=fullwebr&S21REF=10&S21SRD=&S21SRW=&S21STN=1&Z21ID=. Ірбіс НБУВ
[10] Головатий С. П. Верховенство права (правовладдя): як його тлумачить Венеційська комісія. *Право України*. 2011. № 10. С. 154–167. URL: https://ccu.gov.ua/library/verhovenstvo-prava-pravovladdya-yak-yogo-tlumachyt-veneciyska-komisiya
[11] Європейська Комісія «За демократію через право». *Мірило правовладдя: Коментар. Глосарій*. Київ: USAID. 2017. 163 с. URL: https://ccu.gov.ua/library/mirylo-pravovladdya-komentar-glosariy-rule-law-checklist
[12] *Big Brother Watch and Others v. the United Kingdom*, №№ 58170/13, 62322/14, 24960/15. Judgment of 25.05.2021. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001–210077
[13] *Roman Zakharov v. Russia*, № 47143/06. Judgment of 04.12.2015. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001–159324
[14] *Schatschaschwili v. Germany*, № 9154/10. Judgment of 15.12.2015. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001–159566
[15] *Teixeira de Castro v. Portugal*, № 25829/94. Judgment of 09.06.1998. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001–58193
[16] Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр
[17] Корольова Ю. В. Кореляція принципів верховенства права та верховенства закону в системі джерел права. *Підприємництво, господарство і право*. 2019. № 4. С. 183–186. URL: https://pgp-journal.kiev.ua/archive/2019/4/35.pdf

[18] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651–17

[19] Кучук А. М. Верховенство права як аксіологічна складова національної системи права. *Юридичний науковий електронний журнал*. 2023. № 3. С. 566–573. DOI: 10.32782/2524–0374/2023–3/127. URL: https://repository.sspu.edu.ua/server/api/core/bitstreams/d495e1b5-aaac-4c8d-ac2a-75698e84a691/content

[20] Максимов С. І. Конституційний принцип верховенства права: загальне та особливе. *Вісник Академії правових наук України*. 2009. № 3(58). С. 127–134. URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fvapny_2009_3_14.pdf&P21DBN=UJRN

[21] Максимов С. І. Верховенство права: світоглядно-методологічні засади. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія*. 2016. № 4 (31). С. 27–35. URL: https://fil.nlu.edu.ua/article/view/101652

[22] Малишев Б. В. Принцип верховенства права (теоретико-правовий аспект). *Бюлетень Міністерства юстиції України*. 2012. № 8. С. 14–20. URL: http://nbuv.gov.ua/UJRN/bmju_2012_8_4

[23] Михайленко В. В. Верховенство права як засада кримінального провадження. *Приватне та публічне право*. 2017. № 4. С. 128–133. URL: https://www.pp-law.in.ua/archive/4_2017/29.pdf

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

[25] Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства*. 2023. № 3–4. С. 84–102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf

[26] Пухтецька А. А. Принцип верховенства права: сучасні європейські доктрини як орієнтир для реформування національного законодавства. *Вісник НАН України*. 2010. № 3. С. 33–43. URL: http://nbuv.gov.ua/UJRN/vnanu_2010_3_5

[27] Рабінович П. М. Верховенство права як соціально-природний феномен (контури ідеалу). *Право України*. 2010. № 3. С. 19–23. URL: https://pravoua.com.ua/storage/files/magazines/files/content-pravoukr-2010–3-pravoukr_2010_3–1.pdf

[28] Сущенко В. М. Проблеми реалізації та захисту прав і свобод людини та громадянина в Україні (у контексті верховенства права). *Наукові записки НаУКМА. Юридичні науки*. 2012. Т. 129. С. 27–33. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/cf9f825f-1ed7-4dee-b06a-c99596bc1959/content

[29] Тертишник В. М. Гарантії істини та захисту прав і свобод людини в кримінальному процесі : монографія. Дніпропетровськ : Юридична академія МВС України. 2002. 432 с. URL: https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=F&I21DBN=EC_PRINT&P21DBN=EC&S21FMT=fullw_print&Z21MFN=253560

[30] Чепік-Трегубенко О. С. Принцип верховенства права: доктрина та судова практика. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 3. С. 121–127. DOI: https://doi.org/10.31733/2078-3566-2022-3-121-127. URL: https://er.dduvs.edu.ua/handle/123456789/10523

REFERENCES

[1] Ayers, R., Brothers, S., & Jansen, W. (2014). *NIST Special Publication 800–101, Rev. 1: Guidelines on Mobile Device Forensics*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

[2] Office of the United Nations High Commissioner for Human Rights (OHCHR). (2022). *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide*. Geneva: Author. Retrieved from https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

[3] European Network of Forensic Science Institutes (ENFSI). (2015). *Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI-BPM-FIT-01).* Retrieved from https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

[4] European Network of Forensic Science Institutes (ENFSI). (2021). *Best Practice Manual for Digital Image Authentication (ENFSI-BPM–DI-003-1).* Retrieved from https://enfsi.eu/wp-content/uploads/2021/10/BPM_Image-Authentication_ENFSI-BPM–DI-003–1.pdf

[5] International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.* Retrieved from https://www.iso.org/standard/44381.html

[6] Supreme Court of Ukraine, Criminal Cassation Court. (2024, April 2). *Judgment in case No. 450/374/18 (proceeding No. 51–3279 km22).* Retrieved from https://reyestr.court.gov.ua/Review/118297021

[7] Supreme Court of Ukraine, Criminal Cassation Court. (2023, November 27). *Judgment in case No. 464/472/22 (proceeding No. 51–4189 km23).* Retrieved from https://reyestr.court.gov.ua/Review/115308709

[8] Venger, V. M. (2013). Limitation of discretionary powers as a component of the principle of the rule of law. *Scientific Notes of the National University of Kyiv-Mohyla Academy: Legal Sciences*, 144–145, 49–54. Retrieved from https://ekmair.ukma.edu.ua/bitstreams/339e708d-eafe-4a26-b015-f644800fedf3/download

[9] Holovatyi, S. P. (2006). *Rule of Law* (3 vols.). Kyiv: Feniks. Retrieved from https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64. exe?C21COM=S&FT_PREFIX=&FT_REQUEST=&I21DBN=EC&P21DBN=EC&S21ALL=%28%3C.%3ET%3D%D0%92%D0%B5%D1%80%D1%85%D0%BE%D0%B2%D0%B5%D0%BD%D1%81%D1%82%D0%B2%D0%BE+%D0%BF%D1%80%D0%B0%D0%B2%D0%B0%24%3C.%3E%29&S21CNR=20&S21FMT=fullwebr&S21REF=10&S21SRD=&S21SRW=&S21STN=1&Z21ID=

[10] Holovatyi, S. P. (2011). Rule of law (pravovladdya): How it is interpreted by the Venice Commission. *Law of Ukraine*, 10, 154–167. Retrieved from https://ccu.gov.ua/library/verhovenstvo-prava-pravovladdya-yak-yogo-tlumachyt-veneciyska-komisiya

[11] European Commission for Democracy through Law (Venice Commission). (2017). *Rule of Law Checklist: Commentary. Glossary.* Kyiv: USAID. Retrieved from https://ccu.gov.ua/library/mirylo-pravovladdya-komentar-glosariy-rule-law-checklist

[12] European Court of Human Rights. (2021, May 25). *Big Brother Watch and Others v. the United Kingdom* (Applications Nos. 58170/13, 62322/14, 24960/15), Judgment. Retrieved from https://hudoc.echr.coe.int/eng?i=001–210077

[13] European Court of Human Rights. (2015, December 4). *Roman Zakharov v. Russia* (Application No. 47143/06), Judgment. Retrieved from https://hudoc.echr.coe.int/eng?i=001–159324
[14] European Court of Human Rights. (2015, December 15). *Schatschaschwili v. Germany* (Application No. 9154/10), Judgment. Retrieved from https://hudoc.echr.coe.int/eng?i=001–159566
[15] European Court of Human Rights. (1998, June 9). *Teixeira de Castro v. Portugal* (Application No. 25829/94), Judgment. Retrieved from https://hudoc.echr.coe.int/eng?i=001–58193
[16] Constitution of Ukraine: Law of Ukraine (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр
[17] Korolova, Y. V. (2019). Correlation between the principles of the rule of law and the rule of statute in the system of sources of law. *Entrepreneurship, Economy and Law*, 4, 183–186. Retrieved from https://pgp-journal.kiev.ua/archive/2019/4/35.pdf
[18] Criminal Procedure Code of Ukraine: Law of Ukraine (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651–17
[19] Kuchuk, A. M. (2023). The rule of law as an axiological component of the national legal system. *Juridical Scientific Electronic Journal*, 3, 566–573. Retrieved from https://doi.org/10.32782/2524–0374/2023–3/127
[20] Maksymov, S. I. (2009). The constitutional principle of the rule of law: General and special. *Bulletin of the Academy of Legal Sciences of Ukraine*, 3(58), 127–134. Retrieved from https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fvapny_2009_3_14.pdf&P21DBN=UJRN
[21] Maksymov, S. I. (2016). Rule of law: Worldview and methodological foundations. *Bulletin of the National University «Yaroslav Mudryi National Law University», Series: Philosophy*, 4(31), 27–35. Retrieved from https://fil.nlu.edu.ua/article/view/101652
[22] Malyshev, B. V. (2012). The principle of the rule of law (theoretical and legal aspect). *Bulletin of the Ministry of Justice of Ukraine*, 8, 14–20. Retrieved from http://nbuv.gov.ua/UJRN/bmju_2012_8_4
[23] Mykhailenko, V. V. (2017). The rule of law as a foundation of criminal proceedings. *Private and Public Law*, 4, 128–133. Retrieved from https://www.pp-law.in.ua/archive/4_2017/29.pdf
[24] Pohoretskyi, M. A. (2015). A new concept of criminal procedural proof. *Bulletin of Criminal Procedure*, 3, 63–79. Retrieved from https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf
[25] Pohoretskyi, M. A. (2023). The use of advanced technologies in the investigation and proving of war crimes (problematic issues). *Bulletin of Criminal Procedure*, 3–4, 84–102. Retrieved from https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf
[26] Pukhtetska, A. A. (2010). The principle of the rule of law: Modern European doctrines as a benchmark for reforming national legislation. *Bulletin of the National Academy of Sciences of Ukraine*, 3, 33–43. Retrieved from http://nbuv.gov.ua/UJRN/vnanu_2010_3_5
[27] Rabinovych, P. M. (2010). The rule of law as a socio-natural phenomenon (outlines of the ideal). *Law of Ukraine*, 3, 19–23. Retrieved from https://pravoua.com.ua/storage/files/magazines/files/content-pravoukr-2010–3-pravoukr_2010_3–1.pdf

[28] Sushchenko, V. M. (2012). Problems of realization and protection of human rights and freedoms in Ukraine (in the context of the rule of law). *Scientific Notes of the National University of Kyiv-Mohyla Academy: Legal Sciences*, 129, 27–33. Retrieved from https://ekmair.ukma.edu.ua/server/api/core/bitstreams/cf9f825f-1ed7-4dee-b06a-c99596bc1959/content

[29] Tertyshnyk, V. M. (2002). *Guarantees of truth and protection of human rights and freedoms in criminal procedure.* Dnipropetrovsk: Law Academy of the Ministry of Internal Affairs of Ukraine. Retrieved from https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=F&I21DBN=EC_PRINT&P21DBN=EC&S21FMT=fullw_print&Z21MFN=253560

[30] Chepik-Trehubenko, O. S. (2022). The principle of the rule of law: Doctrine and case-law. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, 3, 121–127. Retrieved from https://doi.org/10.31733/2078-3566-2022-3-121-127

Микола Анатолійович Погорецький
Доктор юридичних наук, професор
Член-кореспондент Національної академії правових наук України
Національна академія правових наук України
61024, вул. Григорія Сковороди, 70, Харків, Україна

Проректор з науково-педагогічної роботи
Київський національний університет імені Тараса Шевченка
01601, вул. Володимирська, 64/13, Київ, Україна

Mykola A. Pohoretskyi
Doctor of Law, Professor
Corresponding Member NALS of Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Hryhoriia Skovorody St., Kharkiv, Ukraine

Vice-Rector for Scientific and Pedagogical Work,
Taras Shevchenko National University of Kyiv
01601, 64/13 Volodymyrska St., Kyiv, Ukraine

Рекомендоване цитування: 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.

Suggested Citation: Pohoretskyi, M. A. (2025). Rule of Law in Criminal Procedural Evidence: Methodology and Practice of Application. *Journal of the National Academy of Legal Sciences of Ukraine*, 32(3), 275–299.

Стаття надійшла / Submitted: 18/07/2025
Доопрацьовано / Revised: 18/08/2025
Схвалено до друку / Accepted: 29/09/2025