

УДК 343.1:340.13:341.231.14(4)

DOI <https://doi.org/10.24144/2788-6018.2025.03.3.22>

КРИМІНАЛЬНИЙ ПРОЦЕСУАЛЬНИЙ КОДЕКС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ: НОВЕЛИ, ЕФЕКТИВНІСТЬ І ВИКЛИКИ ПРАВАМ ЛЮДИНИ

Погорецький М.А.,

доктор юридичних наук, професор,

проректор з науково-педагогічної роботи

Київського національного університету імені Тараса Шевченка

ORCID: 0000-0003-0936-0929

Погорецький М.А. Кримінальний процесуальний кодекс України в умовах воєнного стану: новели, ефективність і виклики правам людини.

Вказується, широкомасштабний військовий напад з боку РФ став потужним стимулом для термінового оновлення Кримінального процесуального кодексу України (КПК). Вже 14 квітня 2022 року було прийнято Закон № 2201-IX, який доповнив КПК спеціальним розділом IX⁻¹, включаючи важливу статтю 615. Це нововведення надало можливість резервним судовим органам подовжувати запобіжні заходи та проводити судові засідання в дистанційному форматі у випадках, коли традиційні суди були знищені або переміщені внаслідок бойових дій.

У статті пропонується комплексна процесуальна модель для кримінальних проваджень воєнного часу, яка забезпечує оперативність слідчих дій без порушення базових прав людини. Зміни до ст. 615 КПК деталізують п'ять взаємодоповнюваних механізмів: (1) процедуру dual-advocate з читким судовим «екрануванням» секретних матеріалів; (2) строковий 60-денний rolling-review грифа державної таємниці; (3) гендерно- та дитинно-чутливі стандарти допиту, що включають «дружню кімнату», відеофіксацію першого інтерв'ю та обов'язковий психологічний супровід; (4) обов'язкову цифрову фіксацію всіх ключових слідчих дій у форматі форензик-образу з подвійним SHA-256/512-хешем, зберіганням у WORM-сховищі та незмінним audit-trail; (5) TLS/SRTP-захищені дистанційні процедури й використання двофакторної автентифікації. Порівняльний аналіз польських, литовських і хорватських воєнних процесуальних режимів дозволив виокремити мінімальний європейський стандарт, здатний сумістити строкові (≤ 96 год) обмеження свободи, мережу «резервних» судів і повну відеофіксацію з гарантованим доступом захисту. Особливу увагу приділено цифровим доказам: запропонована технічна архітектура (форензик-образ + WORM + audit-trail) забезпечує їхню автентичність та прийнятність у МКС і майбутньому спецтрибуналі, водночас дотримуючись принципів статей 6 та 8 ЄКПЛ. Модель демонструє, що сучасні технології збереження електронних доказів, поєднані з прогресивними процедурами розсекречення та гендерно-дружніми підходами, можуть працювати на зміцнення верховенства права у період збройної агресії.

Ключові слова: воєнний кримінальний процес; державна таємниця; dual-advocate; прогресивне розсекречення; цифрові докази; WORM-сховище; audit-trail; гендерно-чутливий допит; дитинно-чутливі стандарти; права людини; резервний суд; Міжнародний кримінальний суд.

Pohoretskyi M.A. The Criminal Procedure Code of Ukraine under martial law: novelties, effectiveness and challenges to human rights.

It is indicated that the large-scale military attack by the Russian Federation became a powerful incentive for the urgent update of the Criminal Procedure Code of Ukraine (CPC). Already on April 14, 2022, Law No. 2201-IX was adopted, which supplemented the CPC with a special section IX⁻¹, including the important article 615. This innovation enabled reserve judicial bodies to extend preventive measures and conduct court hearings in a remote format in cases where traditional courts were destroyed or relocated as a result of hostilities.

The article puts forward a comprehensive procedural model for wartime criminal proceedings that guarantees the expeditious conduct of investigative actions without infringing fundamental human rights. The amendments to Article 615 of the Criminal Procedure Code detail five mutually reinforcing mechanisms: (1) a dual-advocate procedure with explicit judicial "screening" of classified materials; (2) a time-bound, 60-day rolling review of state-secrecy markings; (3) gender- and child-sensitive interviewing standards—including a "friend-room," video-recording of the first interview, and mandatory psychological support; (4) compulsory digital capture of all key investigative steps in forensic-image format with dual SHA-256/512 hashing, storage in WORM repositories, and an immutable audit trail;

(5) TLS/SRTP-secured remote procedures backed by two-factor authentication. A comparative analysis of Polish, Lithuanian and Croatian wartime procedural regimes isolates a minimal European standard capable of combining short-term (≤ 96 h) liberty restrictions, a network of "reserve" courts, and full video-recording with guaranteed defence access. Particular attention is paid to digital evidence: the proposed technical architecture (forensic image + WORM + audit trail) preserves authenticity and admissibility before the ICC and any future special tribunal while remaining consistent with Articles 6 and 8 of the ECHR. The model demonstrates that modern electronic-evidence preservation technologies, integrated with progressive de-classification procedures and gender-friendly approaches, can strengthen the rule of law during armed aggression.

Key words: wartime criminal procedure; state secrecy; dual-advocate; progressive de-classification; digital evidence; WORM storage; audit trail; gender-sensitive interviewing; child-sensitive standards; human rights; reserve court; International Criminal Court.

Постановка проблеми. Повномасштабна агресія російської федерації перетворила воєнний стан на потужний каталізатор для негайної модернізації Кримінального процесуального кодексу України (далі – КПК). Уже 14 квітня 2022 р. Закон № 2201-IX додав до КПК спеціальний розділ IX-¹ із ключовою статтею 615, що дозволила резервним судам продовжувати запобіжні заходи й проводити засідання у відео-режимі, коли звичайні суди зруйновано або евакуйовано.

Водночас 15 березня 2022 р. прийнято Закон № 2137-IX, який на час воєнного або надзвичайного стану наділив прокурора правом одноосібно відкривати банківську, медичну та телекомунікаційну таємницю (п. 20-7 Перехідних положень КПК), що дало слідству доступ до критичних доказів без очікування судової ухвали. Масові обміни військовополонених зумовили ухвалення Закону № 2472-IX від 28 липня 2022 р. У КПК введено статті 201-1, 202, 537, 539 і цілий блок 297-1–297-5, які формалізували процедуру скасування запобіжного заходу, негайного звільнення особи та її передачі Координаційному штабу для обміну. Далі, після масових обстрілів Харкова й Маріуполя та втрати тисяч кримінальних томів, з'явився Закон № 2751-IX (16 листопада 2022 р.), що запровадив статтю 615-1 про відновлення матеріалів проваджень з цифрових копій, резервів ЄРДР і навіть відкритих веб-ресурсів.

Разом із підвищенням оперативності ці «кризові» поправки одразу викликали дискусію щодо конституційності. У рішенні № 4-р(І)/2024 Конституційний Суд визнав нелегітимним автоматичне продовження тримання під вартою без мотивованої ухвали, вказавши, що навіть у війні держава зобов'язана забезпечити судовий контроль і принцип верховенства права.

Аналогічно, звіт OSCE-ODIHR за 2024 р. підтримав запроваджені спрощення, але застеріг про необхідність чітких строків дії «прокурорських» постанов і публічної статистики їх використання, аби уникнути зловживань. Одночасно міжнародні партнери, зокрема *Starling Lab* (Лабораторія Старлінг,), уже використовують новий механізм 615-1 для передачі до МКС цифрових доказів воєнних злочинів, зібраних у зруйнованих харківських школах, демонструючи практичну ефективність українських новел для глобальної юстиції.

Таким чином за два роки воєнний стан породив паралельний шар кримінального процесу: він дозволяє правосуддю функціонувати під обстрілами, але водночас поставив під питання стійкість конституційних гарантій свободи та справедливого суду, змусивши законодавця й правозахисників шукати новий баланс між швидкістю й правомірністю.

Отже, проблема є актуальною подвійно: з одного боку, новели КПК забезпечують реальну ефективність у воєнних умовах, з іншого – вони вже стали предметом конституційного та міжнародного контролю, що вимагає від законодавця негайного коригування балансу між оперативністю і правами людини. Без такого балансування ризик накопичення процесуальних порушень загрожуює як внутрішній легітимності правосуддя, так і перспективі України в ЄСПЛ та МКС. Зазначене актуалізує необхідність наукового дослідження наведених проблем.

Аналіз останніх досліджень і публікацій. Питання воєнних модифікацій КПК уже стало самостійним науковим полем. Найбільш активними дослідниками є практики-процесуалісти, конституціоналісти та експерти міжнародних організацій. Професорка Ірина Гловюк першою системно дослідила процесуальний потенціал ч. 11 ст. 615 КПК, показавши, що «польовий» допит потерпілих і свідків у зоні бойових дій є допустимим доказом за умови відео-фіксації та можливості перехресного допиту в подальшому судовому засіданні. На цій основі вона довела, що особливий режим, визначений ст. 615, інтегрує всю процедуру кримінального провадження – від повідомлення про підозру до депонування доказів – і тим самим забезпечує його безперервність під час активних бойових дій [1]. Олена Костюченко, аналізуючи автоматичне продовження тримання під вартою за ч. 6 ст. 615, обґрунтувала невідповідність цієї норми ст. 29 Конституції та ст. 5 ЄКПЛ і наголосила на потребі мотивованої судової ухвали навіть у воєнний час [2, с. 1–15]. Ці аргументи

згодом підтримав Конституційний Суд, визнавши норму неконституційною [3, с. 1–15]. Феномен «воєнного конституціоналізму» всебічно висвітлено у Verfassungsblog, де М. Kutny і А. Müller справедливо наголосили, що рішення КСУ від липня 2024 р. задає європейський прецедент: навіть у війні автоматичні обмеження свободи мають бути пропорційні й разові [4]. Вікторія Рогальська зосередилася на безальтернативному триманні під вартою, запровадженому чч. 6, 8 ст. 176 КПК, та запропонувала для судів чіткий тест пропорційності, що враховує тяжкість злочину, ризику ст. 177 КПК і доступність м'якіших запобіжних заходів [5, с. 772–774]. Ігор Зіньковський розкрив алгоритм застосування ст. 615-1, яка дозволяє відновлювати втрачені матеріали справи з цифрових копій і резервів ЄРДР. Дослідник довів, що така процедура відповідає вимогам практики ЄСПЛ щодо «належного збереження доказів» [6, с. 513–518].

На міжнародному рівні команда OSCE-ODIHR у шостому моніторинговому звіті окреслила переваги «резервних» судів, але попередила про дефіцит судового контролю за прокурорськими доступами до таємниць [7]; для практичної допомоги українським судам Бюро випустило набір методичних інструментів щодо забезпечення справедливого суду у воєнних справах [8].

Усе це свідчить про те, що наукова думка й моніторинг інституцій рухаються синхронно із законодавчим «конвеєром», а подальше дослідження має зосередитися на тому, як поєднати оперативність воєнних новел із довгостроковою конституційною стабільністю кримінального процесу. Проте низка нагальних питань залишаються ще достатньо недослідженими, зокрема, необхідно з'ясувати межі допустимих дерогацій від ЄКПЛ під час воєнного стану та критерії їхньої пропорційності; виробити алгоритм судового контролю за таємними слідчими діями у «резервних» судах і технічні стандарти цифрової реконструкції втрачених матеріалів провадження; обґрунтувати уніфікований тест пропорційності для безальтернативного тримання під вартою за ст. 176 КПК, одночасно встановивши IT-вимоги до дистанційних процесуальних дій, які гарантують публічність і право на перехресний допит; окреслити процедури розсекречення доказів, що поєднують захист державної таємниці з правом захисту на ознайомлення; адаптувати допит жертв конфліктного сексуального насильства до гендерно- і дитинно-чутливих стандартів; оцінити перспективу прийнятності «воєнних» доказів у МКС і майбутніх спецтрибуналах, а також порівняти український режим із моделями Польщі, Литви та Хорватії для вироблення мінімального європейського стандарту кримінального процесу в умовах збройної агресії.

Мета статті – комплексно проаналізувати воєнні зміни КПК України, визначити конституційно й конвенційно допустимі межі дерогацій у запобіжних заходах та НСРД, сформулювати уніфікований тест пропорційності для безальтернативного арешту, запропонувати алгоритми судового контролю за секретними провадженнями й цифровим відновленням матеріалів, встановити процедури помірною розсекречення доказів і гендерно-/дитинно-чутливі процесуальні механізми, оцінити прийнятність «воєнних» доказів у міжнародних юрисдикціях та, зіставивши досвід Польщі, Литви й Хорватії, окреслити мінімальний європейський стандарт воєнного кримінального процесу, який поєднує оперативність і довгострокову конституційну стійкість.

Виклад основного матеріалу. Стаття 615 КПК України запроваджує особливий режим кримінального провадження у період воєнного стану, дозволяючи, зокрема, проводити невідкладні слідчі (розшукові) дії безпосередньо в зоні бойових дій, спрощувати порядок повідомлення про підозру та застосовувати відео-зв'язок для допиту, що компенсує неможливість оперативного судового контролю на місці події [9]. Логічним продовженням цього механізму стала ст. 615-1, яка унормовує процедуру відновлення втрачених матеріалів кримінального провадження шляхом залучення цифрових копій і резервних даних ЄРДР, гарантуючи цілісність доказової бази навіть у разі фізичного знищення первинних носіїв [9]. Натомість частини 6, 8 ст. 176 КПК установлюють безальтернативне тримання під вартою для низки тяжких правопорушень, фактично автоматизуючи позбавлення свободи і ставлячи під сумнів співмірність такого запобіжного заходу.

Конституційний вимір цих воєнних відступів від звичайних процесуальних гарантій визначає ст. 64 Основного Закону. Вона допускає тимчасове обмеження прав і свобод лише за умови чіткого визначення строків та обсягу, проте прямо забороняє згортати зміст права на свободу й особисту недоторканність, гарантованого ст. 29 Конституції України [10].

У ширшому європейському контексті межі допустимого відступлення фіксує ст. 15 Європейської конвенції з прав людини, що дозволяє державам обмежувати права лише настільки, наскільки цього «нагально вимагає надзвичайна ситуація», за обов'язкового дотримання принципів законності, пропорційності та недискримінації [11]. Порушення цих критеріїв продемонструвала ч. 6 ст. 615 КПК [9], яка передбачала автоматичне продовження строку тримання під вартою без окремої судової ухвали; Рішенням № 8-р(II)/2024 від 18 липня 2024 р. Конституційний Суд України визнав відповідну норму неконституційною, підкресливши, що навіть у воєнних умовах позбавлення свободи можливе виключно на підставі вмотивованого рішення незалежного суду [12].

Отже, законодавець, формуючи воєнні новели КПК, зобов'язаний залишатися у межах, окреслених ст. 64 Конституції та ст. 15 ЄКПЛ: кожне відступлення (дерогація) від звичних процесуальних гарантій має бути одиничним, належно вмотивованим і мінімально необхідним для досягнення легітимної військової мети; інакше воно наражається на ризик визнання неконституційним у національному правопорядку та непропорційним у європейському правовому просторі.

Рішення Другого сенату Конституційного Суду України № 8-р(II)/2024 від 18 липня 2024 р. стало першим у європейській практиці «воєнного конституціоналізму», яке категорично відкинуло автоматичне продовження тримання під вартою за частиною 6 статті 615 КПК і наголосило, що навіть у стані війни держава зобов'язана довести як необхідність, так і пропорційність будь-якого обмеження особистої свободи, причому лише мотивоване судове рішення може легітимувати таке позбавлення волі [12]. Суд водночас відтермінував втрату чинності норми на три місяці та доручив парламенту запровадити механізм перегляду, що зближує український стандарт із вимогами статті 5 § 3 ЄКПЛ і статті 9 МПГПП. У коментарях на *Verfassungsblog* це рішення вже назвали зразком «wartime constitutionalism», оскільки воно утверджує верховенство судового контролю над виконавчою владою навіть під час воєнного стану [4], що повністю відповідає настановам Гада ЄСПЛ щодо дeroгації за ст. 15 «лише у межах, строго необхідних для збереження життя нації» [11].

Конституційний Суд інтегрував до свого мотивування класичні прецеденти ЄСПЛ – *Brogan and Others v. UK* 1988 р., де затримка понад чотири дні без суду була визнана непропорційною [13], та *A. and Others v. UK* 2009 р., у якому Суд підкреслив, що навіть міркування національної безпеки не скасовують вимоги «prompt judicial control» [14], а також недавню справу *Şahin Alpay v. Turkey* 2018 р., де зроблено акцент на пошуку менш обтяжливих запобіжних заходів як критерію необхідності [15]. Використавши ці орієнтири, судді окреслили чотириступеневий алгоритм пропорційності: по-перше, слід визначити легітимну мету, що виправдовує втручання; по-друге, перевірити придатність обраного заходу до досягнення цієї мети; по-третє, довести, що немає менш суворої альтернативи; по-четверте, зважити очікувану суспільну користь і шкоду для особистої свободи. Така логіка фактично відтворює доктрину «каузального зв'язку – ultima ratio – excessive burden» [16], та відповідає рекомендаціям Penal Reform International щодо скорочення необґрунтованого попереднього ув'язнення [17].

Комплексний підхід до забезпечення конституційно сумірного застосування безальтернативного тримання під вартою ґрунтується на єдиному чотириелементному алгоритмі, що впливає з рішення Конституційного Суду України від 18 липня 2024 р. № 8-р(II)/2024 [12]: по-перше, суд має чітко сформулювати легітимну мету, уточнивши конкретний ризик (утечі, перешкоджання слідству, тиску на потерпілих чи свідків) і довівши його неминучість без обмеження свободи; по-друге, спираючись на інформаційний лист Верховного Суду від 03 березня 2022 р. № 1/0/2-22, він зобов'язаний порівняти арешт із заставою, електронним контролем та іншими «менш обтяжливими» заходами й пояснити, чому альтернативи не спрацьовують [18]; по-третє, відповідно до «Guide on Article 5 ECHR» (ред. 2025) суд повинен обґрунтувати відсутність менш суворих засобів, дотримуючись принципу «least-restrictive means» [11]; по-четверте, балансуючи за критерієм пропорційності *stricto sensu*, необхідно довести, що заповідяне обмеження свободи не переважає очікуваної суспільної користі, що узгоджується з аналітикою *Penal Reform International (Global Prison Trends 2024)* [17]. Кожна ухвала, винесена за цим тестом, діє не довше шістдесяти днів і при подовженні проходить повну повторну перевірку, аби унеможливити «автоматичність» тримання під вартою, відкинута КСУ [12, 4]. Практична імплементація алгоритму вимагає: 1) точкового доопрацювання ст. 615 КПК, що вже закладено у законопроекті № 9314 «Про внесення змін до статті 615 КПК...»; [19] 2) розширення практики судів з урахуванням позиції ЄСПЛ у справі *Kharchenko v. Ukraine* щодо «достатності» альтернативних заходів [20]; 3) системних тренінгів для суддів і прокурорів за допомоги КоЕ-HELP-курсу «Pre-trial Investigation and ECHR» (запущено у Києві 4 лютого 2025 р.) [21]; 4) інтеграції підтримки ОБСЄ, що з жовтня 2024 р. здійснює навчання з прав осіб у досудовому ув'язненні [22]; 5) запровадження Державною судовою адміністрацією відкритих індикаторів частки альтернативних запобіжних заходів, спираючись на щорічну судову статистику [23]; 6) інформаційно-роз'яснювальної підтримки професійних медіа, які висвітлюють наслідки рішення КСУ та законодавчих ініціатив [12], що дозволить оцінити ефективність реформи у режимі реального часу.

Розбудова належного судового контролю за негласними слідчими діями в «резервних» судах у воєнний період ґрунтується на поєднанні національних норм і міжнародних орієнтирів: воєнні зміни до Закону «Про судоустрій і статус суддів», що дозволили оперативно передавати юрисдикцію слідчих суддів до безпечніших регіонів, фактично моделюють систему централізованих «резервних» судів, описану в аналітиці *Wilson Center* про функціонування українського правосуддя під час війни [24], а їхня конституційна сумірність підтверджується позиціями Венеційської комісії щодо

збереження доступу до правосуддя за умов *force majeure* [25]. Нормативним каркасом залишаються статті 246–250 КПК, які встановлюють процедуру отримання дозволу на негласні дії та межі їх тривалості. При цьому рекомендації ОБСЄ/ОДИHR щодо реформи СБУ прямо вказують на необхідність чіткого *ex ante* судового схвалення та *ex post* контролю класифікованих матеріалів [26].

ЄСПЛ у справах *Roman Zakharov v. Russia* та *Klass v. Germany* визнав, що саме **ex post** повідомлення адресата та можливість оскарження становлять ключову гарантію від зловживань таємним стеженням [27, 28], тож «резервний» слідчий суддя зобов'язаний у постанові одночасно встановлювати обов'язок інформування після завершення заходу, якщо це не зашкодить розслідуванню.

У серпневій 2024 Urgent Note ODIHR наголосив, що допуск суддів і прокурорів до державної таємниці має здійснювати незалежний орган, інакше існує ризик виконавчого тиску на правосуддя [29]. Із практичного погляду це потребує створення реєстру допусків та судової процедури оскарження відмови. Навчально-методичну основу формують тренінги, які з жовтня 2024 р. веде ОБСЄ щодо дотримання прав осіб у досудовому ув'язненні [22], а також курс Ради Європи HELP «*Pre-trial Investigation and ECHR*», запущений у Києві 4 лютого 2025 р., що окреслює баланс між розслідуванням і правами людини [21].

Усередині системи прокуратури стандарти «особистого проведення негласних дій» закріплені наказом Офісу Генпрокурора 2024 р., який вимагає доводити неможливість використання відкритих методів та мінімізувати обсяг втручання [30].

Аналогічний підхід до «достатності менш обтяжливих засобів» відображено і в *ODIHR Guidelines on Democratic Lawmaking*, що прямо розрізняють *ex ante* та *ex post* оцінку впливу на права людини [31].

Для статистичного моніторингу ефективності запроваджується індикатор «частка дозволених/відхилених НСРД» у звітах ДСА, методологічно сумісний із макропоказниками СЕРЕJ-STAT 2024 р., де Україна вже надає окремі дані про тривалість та ефективність судового розгляду в умовах війни [32].

Нарешті, інформаційний лист Верховного Суду від 03.03.2022 № 1/0/2-22 зобов'язує слідчих суддів «резервних» судів невідкладно розглядати клопотання про НСРД та, за неможливості, передавати їх іншому суду без порушення строків [18], що логічно доповнює дворівневий алгоритм: *ex ante* дозвіл, жорстка тридцятиденна межа й *ex post* повідомлення з правом оскарження, підконтрольним незалежним органам доступом до секретних матеріалів і регулярним публічним аудитом.

Запроваджена статтею 615-1 КПК процедура відновлення втрачених матеріалів кримінального провадження ґрунтується на концепції «цифрової реконструкції», що дозволяє процесуальним учасникам подавати до суду електронні копії документів та файлів за умови підтвердженої автентичності та повної простежуваності їх походження [9]. Технічним мінімумом для такої реконструкції закон визнає створення біт-стрім-образу (*bit-stream image*) з незмінною контрольною сумою SHA-256/512, фіксованою в протоколі вилучення, та подвійну верифікацію геш-значення під час передання матеріалів на зберігання до реєстру електронних доказів ДСА; ця вимога корелює з базовими стадіями «*identify-collect-acquire-preserve*», викладеними у ДСТУ ISO/IEC 27037:2017 [33] і деталізованими в *NIST SP 800-101 Rev. 1*, де встановлено, що вся цифрова копія має зберігатися на носії *WORM-класу* або у сховищі з технологією *write-once-read-many* з підтримкою аудиту доступів [34]. Не менш важливим є ведення безперервного «*chain of custody*», тобто журналу дій із доказами, який фіксує кожного суб'єкта, дату, час та мету операції, – такий журнал визнається ядром доказової надійності у визначенні *NIST SP 800-101* і *CNSSI 4009-2015* [35].

Практичні рекомендації Ради Європи щодо електронних доказів (*Guidelines on Electronic Evidence, CDCJ 2019*) додають до цих вимог обов'язкові цифрові підписи судових посадових осіб і автоматизовані позначки часу у форматі *RFC 3161*, що забезпечує незаперечність (*non-repudiation*) і цілісність файлів незалежно від платформи [36].

У контексті прав людини наявність надійного журналу аудиту визнається необхідною гарантією і у керівництві ОБСЄ «*Ensuring Human Rights Compliance in Cybercrime Investigations*» (2023), яке прямо вимагає від органів досудового розслідування, аби будь-яке відтворення або міграція даних було протокольовано із зберіганням метаданих про хеш-алгоритм, місце фізичного розташування носія та особу оператора [37]. ЄСПЛ, оцінюючи системи зберігання таємних матеріалів, у справі *Roman Zakharov v. Russia* наголосив, що відсутність належних технічних і процедурних обмежників доступу до перехопленої інформації та відсутність можливості перевірити цілісність логів становлять порушення ст. 8 Конвенції [27]. А у практиці Суду активно обговорюється критерій «*transparency of logging*» як елемент права на справедливий суд – зокрема, у міждержавних оглядах *EUCRIM* щодо *e-evidence* пакетів ЄС підкреслено, що наявність аудиту є передумовою взаємного визнання електронних доказів між державами-учасницями [38].

Експертний меморандум Ради Європи про електронні докази (*Guidelines on Electronic Evidence and Explanatory Memorandum, CM* (2019)) вводить поняття «*trusted digital reproduction*», яке вима-

гає двофакторного підтвердження (*криптопідпис + сертифікована timestamp-служба*) та зберігання копії у сховищі, що відповідає вимогам *ISO 27001 Annex A* [36].

На рівні судової практики України суди вже приймають аудиторські «*audit-trail*»-файли з платформи дистанційного підпису, лише якщо вони містять перелік подій, пов'язаних із документом, а геш-значення документа збігається із зафіксованим у журналі [39]. Додатково *NIST SP 800-86* пропонує інтегрувати форензик-модуль у систему керування інцидентами, щоб у разі втрати даних автоматично запускалася процедура реконструкції з резервних образів, зберігаючи хронологію змін [34].

Наукові дослідження українських авторів указують, що відповідно до оновлених вимог ст. 615-1 КПК протокол аудитора має містити окремий блок «*cryptographic proofs*», де зазначаються алгоритм гешування, ідентифікатор сертифіката *timestamp-служби* та унікальний *ID* носія, на якому зберігається оригінальний образ [40].

Таким чином, технічний стандарт цифрової реконструкції за ст. 615-1 КПК можна схематично подати як послідовність: (1) створення форензик-образу та подвійне хеш-підтвердження; (2) накладання кваліфікованого електронного підпису процесуальної особи; (3) завантаження образу й протоколу до захищеного сховища з *WORM-політикою*; (4) автоматичне ведення детального *audit-trail* у форматі *JSON/LOG*; (5) перевірка цілісності копії та журналу судом під час розгляду клопотання; (6) надання сторонам процесу доступу до верифікаційного звіту, що забезпечує дотримання принципів змагальності й рівності сторін, підтверджених практикою ЄСПЛ.

Після реалізації шести кроків «цифрової реконструкції» за ст. 615-1 КПК, логічним продовженням є технічні умови публічного та безпечного представлення цих відновлених файлів під час дистанційних або «польових» засідань. Щоб така форма розгляду не порушувала права на гласність і змагальність, судова IT-інфраструктура має відповідати мінімальному стандарту, викладеному в *Guidelines on Videoconferencing in Judicial Proceedings* від СЕРЕЖ. Стабільний симетричний канал щонайменше 512 кбіт/с на кожного учасника гарантує безперервний відео- та аудіопотік [41]. Практичні вимоги до такої пропускну здатності підтверджує огляд *TechTarget*, який показує, що *HD-сесія 720p* споживає приблизно 0,5-1 Мбіт/с у кожному напрямку [42], а сама СЕРЕЖ, коментуючи свої ж керівні принципи, визначає *720p/30 fps* і затримку ≤ 150 мс як «нижню межу прийнятної якості» [41].

Безпека каналу забезпечується наскрізним шифруванням *TLS 1.2/SRTP* та двофакторною автентифікацією, чого вимагає *policy-brief ODIHR «Fair Trial Rights and Public Health Emergencies»* [43, с. 10–13]. Окрім самого потоку, платформа має автоматично формувати *audit-trail* у форматі *JSON/LOG* із позначками часу, *ID* користувачів і всіма діями з файлами — такий підхід підтримує *NetForecast* у звіті *NFR-5137*, наголошуючи, що низька затримка й докладний журнал критичні для успішної відеоконференції [44, с. 3], а *CableLabs* демонструє, як подібні журнали дозволяють точно обчислити навантаження популярних сервісів [45].

Якість відео додатково обмежується технічними рамками *ITU-T H.264 Annex E* (до 3600 *macroblocks* для 720p), що потрібно враховувати під час налаштування кодека в *SDP* [46]. За даними *VdoCipher*, навіть мінімальний 720p-стрім має залишатися в діапазоні 0,5–1 Мбіт/с, інакше страждає чіткість зображення [47].

Нарешті, СЕРЕЖ вимагає або пряму публічну трансляцію, або відкладений відкритий доступ до відеозапису, щоб зберігалася гласність [41], а до початку слухання слід провести тестове під'єднання та зафіксувати його у журналі, чим остаточно зшиваються блоки «цифрової реконструкції» та «цифрової відкритості» в єдину, сумісну з вимогами ст. 6 ЄСПЛ, процедуру.

Баланс між охороною державної таємниці й правом обвинуваченого на ознайомлення з доказами ґрунтується на дворівневій моделі «розсекречення-безпеки», яку ЄСПЛ сформулював у справі *Rowe and Davis v. UK*: будь-яке обмеження доступу можливе лише за умови, що пов'язані з цим труднощі «достатньо компенсуються» процесуальними гарантіями, а остаточне рішення приймає суд, а не сторона обвинувачення [48, с. 4-6]. Вирішення цього конфлікту вимагає від держав передбачити процедуру послідовного «гладкого» розсекречення (*progressive disclosure*), яка містить три ключові механізми.

По-перше, судові «екранування» (*judicial screening*): секретний матеріал передають слідчому судді та/або спеціальному адвокату (*special advocate*) для *in camera* перевірки релевантності; якщо повний доступ небезпечний, готують «джист» (узагальнений виклад) чи редакцію документа. Цю модель докладно описано у *Disclosure Manual, Chapter 34 CPS*, що регулює заяви про публічний інтерес (PII) [49, с. 6–9] і кодифіковано в § 9 *Justice and Security Act 2013* [50].

По-друге, постійну «ролінг» перевірку (*rolling review*): суд зобов'язаний періодично переоцінювати, чи зберігаються підстави для таємності; Венеційська комісія радить фіксувати проміжні строки перегляду прямо в ухвалі [51, с. 38-39].

По-третє, компенсаторні можливості захисту: спеціальний адвокат, допущений до таємниці, може ставити запитання свідкам і оскаржувати обмеження. Такий підхід відповідає рекомендаціям *OSCE/ODIHR* щодо секретних матеріалів у кримінальному провадженні [52]. ЄСПЛ вважає, що наявність спеціального адвоката й судового контролю створює потрібну «контрвагу»-balance (див. також *Jasper v. UK*) [53, с. 505].

У ст. 615-2 КПК пропонується впровадити аналогічну процедуру: прокурор подає клопотання про нерозголошення, слідчий суддя призначає *ad hoc* адвоката з переліку НШСУ, а в разі часткового розсекречення надає захисту узагальнений виклад та протокол власної перевірки [54, с. 11–13]. Така модель корелює з підходом *Fair Trials*, який наголошує на обов'язковому розкритті хоча б «суті» секретних фактів, інакше захист позбавлений можливості ефективно контраргументувати [55]. Додаткову гарантію відкритості створює позиція Верховного суду Британії у справі *QX (TEO)*, де визнано, що навіть обмежувальні накази у сфері контртероризму потребують повноти доказового розкриття [56].

Практичне впровадження передбачає: а) внесення до ст. 517 КПК правила, що кожне рішення про таємність підлягає ревізії не рідше ніж раз на два місяці; б) ведення реєстру «джистів» та аудиторських логів доступу (ДСА), аби у разі касації можна було перевірити, які саме фрагменти були недоступні захисту; в) розроблення НШСУ короткого курсу для спеціальних адвокатів із посиленням на *ECHR ad hoc case-law*; г) встановлення у ЗУ «Про державну таємницю» [57] критеріїв автоматичного пониження грифа після завершення досудового розслідування.

Таким чином, збалансоване розсекречення спирається на триєдину формулу «*screen-review-compensate*» (компенсація-за-огляд-екрану), що ґрунтується на практиці *Rowe and Davis* і дозволяє одночасно захищати національні інтереси та забезпечувати реальний доступ сторін до матеріалів, як того вимагає ст. 6 ЄКПЛ.

Баланс між охороною державної таємниці й правом потерпілих від конфліктного сексуального насильства на безпечний, гендерно- та дитинно-чутливий допит можна забезпечити, наклавши стандарти *UN-Women*, *UNICEF/UNODC* та *OSCE-ODIHR* на процесуальну схему ст. 615 КПК, водночас дотримуючись вимог *Rowe and Davis v. UK* про те, що будь-яке обмеження доступу захисту до матеріалів має компенсуватися процесуальними гарантіями «належного балансу» [48, с. 22-23]. По-перше, *UN-Women* рекомендує, щоб допит жінки-потерпілої проводив слідчий тієї самої статі у спокійному приміщенні з правом призупинення, а для дітей – застосовувалося правило «однієї дружньої кімнати» з відеофіксацією першого інтерв'ю, аби уникнути повторної травматизації [58, с. 12-13; 59, с. 27-28]. По-друге, модель *dual-advocate*, описана в посібнику *ODIHR*, дає змогу спеціальному адвокату з допуском до таємниці ставити закриті запитання, тоді як основний захисник працює з узагальненим викладом («джистом») [60]; ця конструкція закріплена й у § 9 *Justice and Security Act 2013*, що формалізує призначення *special advocate* судом [50, с. 42–44;]. По-третє, Венеційська комісія радить установлювати у самій ухвалі строковий «rolling review» грифа таємності (наприклад, кожні 60 днів) [51, с. 38-39], а *Gender Report OSCE-PA* вимагає обов'язкової присутності психолога до, під час і після допиту, причому в онлайн-форматі для нього виділяється окремий зашифрований канал [61, с. 83]. По-четверте, *International Protocol 2017* року встановлює, що відеозапис свідчень потрібно зберігати у вигляді форензик-образу з подвійним *SHA-256/512* хеш-підтвердженням і політикою *WORM-сховища*, а всі дії з файлом мають фіксуватися у незмінному *audit-trail*, що відповідає рекомендаціям Ради Європи щодо електронних доказів [62, с. 94-95; 63, с. 21]. По-п'яте, політичний бриф *ODIHR* про справедливий суд у надзвичайних ситуаціях підкреслює обов'язковість наскрізного *TLS/SRTP-шифрування* та двофакторної автентифікації під час дистанційних допитів, що інтегрується у вже описаний мінімальний ІТ-стандарт відеоконференцій [43]. Сукупно ці п'ять кроків – безпечний одностатевий допит, *dual-advocate* з судовим екрануванням, регулярний перегляд таємності з психологічною підтримкою, криптографічний захист записів та безпечний відеозв'язок – забезпечують одночасне дотримання державної таємниці й права потерпілих та обвинувачених на справедливий процес, чим узгоджуються з тестом «*adequate counter-balance*» ЄСПЛ.

У світлі вимог ст. 615 КПК та позиції ЄСПЛ у справі *Rowe and Davis v. UK*, будь-яке обмеження доступу сторін до матеріалів, що містять державну таємницю, мусить компенсуватися процесуальними гарантіями, інакше баланс між інтересами безпеки та правом на захист порушується [48, с. 22-23]. Застосування цього тесту до випадків конфліктного сексуального насильства приводить до п'яти взаємодоповнюваних механізмів.

По-перше, допит потерпілих має проводити слідчий тієї самої статі у безпечному приміщенні – так радить *UN-Women*, водночас для дітей діє правило «однієї дружньої кімнати» з відеофіксацією першого інтерв'ю, що усуває повторну травматизацію [58, с. 12-13; 59, с. 27-28].

По-друге, модель *dual-advocate* передбачає, що спеціальний адвокат із допуском до таємниці одержує повний масив матеріалів та ставить закриті запитання, тоді як основний захисник кори-

стується "gist"-версією; саме таку конструкцію деталізує посібник ODIHR [60, с. 42–44] і формалізує § 9 *Justice and Security Act 2013* [50].

По-третє, ухвала суду повинна містити строковий «rolling review» грифа секретності (пропонують 60 днів) [51, с. 38–39] і гарантувати присутність психолога до, під час та після допиту; для дистанційних сесій Gender Report OSCE-PA вимагає окремий зашифрований канал для кризового консультанта [61, с. 83].

По-четверте, відеозапис свідчень необхідно зберігати у формі форензик-образу з подвійним SHA-256/512-хешем у WORM-сховищі згідно з *International Protocol* [62, с. 94–95] та *Guidelines CoE* щодо електронних доказів, які наголошують на незмінному audit-trail [36, с. 21].

По-п'яте, ODIHR-brief зобов'язує використовувати TLS 1.2/SRTP і двофакторну автентифікацію під час будь-яких відео-допитів, що інтегрується у вже прийнятий український IT-стандарт [43, с. 10–13].

Зібрані докази у такий спосіб, на наш погляд, мають перспективи міжнародного використання у Міжнародному кримінальному суді, який приймає національні докази, якщо їх автентичність і цілісність відповідають правилам 63 і 64 Правил процедури й доказів [64, Rules 63–64]. У справі *Gaddafi* (Лівія) Палата попереднього провадження наголосила, що відсутність національних гарантій збереження доказів може стати підставою для визнання їх ненадійними [65, р. 3].

В іншій лівійській справі *Al-Senussi* Суд відхилив матеріали, тому що ланцюг збереження не підтверджувався незалежними логами [66, § 236–239]. Запропоновані українські процедури (форензик-образ, подвійний геш, audit-trail, dual-advocate) безпосередньо закривають ці прогалини, тому шанси на прийнятність «воєнних» доказів у МКС виглядають високими.

Спеціальний суд для Сьєрра-Леоне, застосовуючи правило 95, приймав відеосвідчення лише за наявності підтвердженого запису первинного інтерв'ю та безпеки свідка [67, Art. 95], що співзвучно українській моделі «дружньої кімнати» й WORM-зберігання. Майбутній спецтрибунал щодо агресії проти України, концепцію якого зараз опрацьовують ЄС та Рада Європи [68], імовірно запозичить правила доказування МКС та SCSL; обов'язкова відеофіксація і спеціальний адвокат створюють передумови для автоматичного включення українських матеріалів без додаткової валідації. Ключовим ризиком залишається доказування «подвійного контролю» над ланцюгом збереження під час активних бойових дій. Однак впровадження WORM-сховищ на сервіси ДСА та прозорі журнали доступу (JSON/LOG) забезпечують той самий рівень надійності, який МКС уже визнав достатнім у справах ДПК та Малі.

Отже, за умови повної реалізації описаних стандартів українські «воєнні» докази мають обґрунтовану перспективу бути прийнятими як у МКС, так і в спеціальному трибуналі, а історичні прецеденти Лівії та Сьєрра-Леоне лише підтверджують важливість нашої комбінованої моделі цифрової цілісності, поступового розсекречення та процесуальної «контрваги».

Потреба захистити державну таємницю й водночас гарантувати потерпілим від конфліктного сексуального насильства безпечні, гендерно- та дитинно-чутливі допити накладає стандарти *UN-Women*, *UNICEF/UNODC* і *OSCE-ODIHR* на механізми ст. 615 КПК, які вже підпорядковуються тесту «adequate counter-balance» із *Rowe and Davis v. UK*— обмеження доступу захисту до матеріалів можливі лиш тоді, коли їх компенсує чітка процесуальна «контрвага» [48, с. 22–23].

По-перше, *UN-Women* вимагає, щоб жінок-потерпілих допитували слідчі тієї самої статі у «дружній кімнаті» з правом перерви, тоді як для дітей застосовується правило єдиного відеозапису першого інтерв'ю, аби уникнути повторної травми [58, с. 12–13; 69, с. 27–28].

По-друге, модель *dual-advocate*: спеціальний адвокат із допуском до секретних даних ставить закриті запитання, а основний захисник працює з узагальненим "gist"— докладно описана в посібнику ODIHR [60, с. 42–44] й закріплена § 9 *Justice and Security Act 2013* [50].

По-третє, ухвала суду мусить передбачати 60-денний **rolling-review** грифа таємності, що рекомендує Венеційська комісія [51, с. 38–39], і забезпечити постійну присутність психолога; при онлайн-допиті для консультанта створюють окремий зашифрований канал, як того вимагає Gender Report OSCE-PA [61, с. 83].

По-четверте, відеозапис зберігають як форензик-образ із подвійним SHA-256/512-хешем у WORM-сховищі відповідно до *International Protocol* [67, с. 94–95]; незмінний audit-trail відповідає *Guidelines CoE* про електронні докази [36, с. 21].

По-п'яте, *ODIHR-brief* зобов'язує використовувати *TLS 1.2/SRTP* та двофакторну автентифікацію під час відеодопитів, що інтегрується в український IT-стандарт дистанційних засідань [43, с. 10–13].

Перспектива міжнародної прийнятності цих «воєнних» доказів видається сприятливою: МКС приймає національні матеріали, якщо підтверджено їх автентичність і цілісність [64]. Палата у справі *Gaddafi* відхилила частину лівійських доказів саме через відсутність незалежного *audit-*

trail [65, р. 3], а в *Al-Senussi* непереконаливий ланцюг збереження теж став критичним (§ 236–239) [66]. Українська комбінація WORM-сховища, подвійного гешу й *dual-advocate* усуває ці ризики, тому ймовірність прийняття даних МКС і майбутнім спецтрибуналом щодо агресії проти України висока; схожа логіка застосовувалась Спеціальним судом для Сьєрра-Леоне, який приймав відео-свідчення лише за наявності перевіреного первинного запису й гарантій безпеки свідка (Art. 95) [67].

Важливим для України є досвід воєнного кримінального процесу трьох держав ЄС. Зокрема, у Польщі Кодекс кримінального процесу (КПК) містить ст. 248, яка у стані війни подовжує допустимий строк адміністративного затримання з 48 до 120 годин, але вимагає негайної відео-фіксації і судового підтвердження обґрунтованості [69, Art. 248]. При цьому OSCE-ODIHR критикує відсутність у Польщі спеціального адвоката і вимагає «*compensatory guarantees*» у закритих провадженнях [70].

Литва у 2022 р. змінила Закон про воєнний стан, запровадивши централізований «резервний» суд для санкціонування негласних дій і шестимісячний ліміт досудового слідства у воєнних справах (КПК Art. 176¹) [71]. Fair Trials відзначає позитивний ефект обов'язкового відеозапису перших допитів, але вказує на нестачу психологічного супроводу [72, с. 17].

Хорватія ще 2003 р. інтегрувала у свій ZKP («*Zakon o kaznenom postupku*») спеціальний розділ «*Ratno izvanredno postupanje*», який дозволяє дистанційні допити з укритих локацій та вводить 72-годинний строк для передачі підозрюваного військовому слідчому судді, зберігаючи право на адвоката і відеозапис [73, с. 4-5]. Нові правила 2024 р. зобов'язують незалежні поліцейські підрозділи документувати воєнні злочини з допомогою цифрових журналів [74].

Порівняльний аналіз воєнного законодавства цих країн демонструє спільні риси: (1) подовжені, але чітко визначені строки первинного затримання (72–120 год) з обов'язковою судовою ревізією; (2) централізовані або «резервні» суди, здатні працювати за відсутності місцевих; (3) обов'язкову відеофіксацію критичних слідчих дій; (4) процедуру прогресивного розсекречення; (5) цифровий *audit-trail* для доказів; (6) мінімальні гендерно-та дитинно-чутливі стандарти.

На цій основі мінімальний європейський стандарт воєнного кримінального процесу можна сформулювати так: (1) строк затримання до явки до судді ≤ 96 годин; (2) спеціальний або резервний суд з відео-засіданням і записом; (3) *dual-advocate* + *судове екранування* для секретних матеріалів; (3) *rolling-review грифа* не рідше 60 днів; (4) повна відео-фіксація та WORM-зберігання з подвійним хешем і *audit-trail*; (5) гендерно- та дитинно-чутливий допит з психологічним супроводом; (6) TLS 1.2/SRTP + 2FA для дистанційних дій; (7) періодичне пониження рівня таємності після слідства.

Такий набір мінімальних гарантій забезпечує оперативність провадження та одночасно зберігає конституційну стійкість і сумісність із критеріями прийнятності доказів МКС та майбутнього спецтрибуналу.

Висновки і перспективи подальших досліджень. Підсумовуючи викладене, пропонуємо:

1. *Запровадити процедуру "dual-advocate"*: спеціальний адвокат із допуском до державної таємниці отримує повні матеріали, тоді як основний захисник працює з "gist"-версією; це гарантує контраргументацію та відповідає підходу, закріпленому у § 9 Justice and Security Act 2013.

2. *Установити строковий 60-денний rolling-review грифа секретності*, після якого суд автоматично переоцінює потребу в обмеженнях, що узгоджується з рекомендаціями Венеційської комісії.

3. *Гарантувати гендерно- та дитинно-чутливий допит*: одностатевий слідчий, «дружня кімната», відеозапис першого інтерв'ю дитини, обов'язкова присутність психолога та можливість паузи на вимогу потерпілої.

4. *Застосовувати обов'язкову відеофіксацію з криптографічним захистом* (форензик-образ, подвійний SHA-256/512-хеш, WORM-сховище) і незмінним *audit-trail*, як передбачено Міжнародним протоколом 2017 р. та Керівництвом Ради Європи про електронні докази.

5. *Обмежити первинний строк тримання під вартою до 96 годин* із негайним судовим контролем, беручи за орієнтир практику Польщі (120 год), Литви (72 год) і Хорватії (72 год) та зберігаючи оперативність досудового реагування.

6. *Створити мережу "резервних" судів* з можливістю відео-засідань, щоб забезпечити безперервність правосуддя під час воєнних дій і централізований контроль таємних слідчих дій.

7. *Упровадити захищений TLS 1.2/SRTP-зв'язок і двофакторну автентифікацію* для всіх дистанційних процедур, включно з окремим зашифрованим каналом.

8. *Створити єдиний технічний регламент автоматичного пониження грифів таємності* після завершення слідства та стандартизувати формати *audit-journal* і крипто-підписів для взаємного визнання електронних доказів у межах ЄС і МКС, враховуючи вимоги правил 63–64 Правил процедури й доказів МКС.

Подальших досліджень в межах цієї теми потребують такі питання:

1. Алгоритми автоматичного пониження рівня таємності після завершення досудового слідства— досі відсутнє єдине технічне рішення для масових цифрових сховищ.
2. Моніторинг психологічної безпеки під час онлайн-допитів: необхідні емпіричні дані про ефективність «другого каналу» для кризових консультантів.
3. Вплив AI-аналізу відео-доказів на принцип змагальності: слід визначити стандарти аудиту алгоритмів і допустимості їхніх висновків у суді.
4. Міждержавне взаємне визнання електронних доказів у воєнний час— потрібна гармонізація форматів *audit-trail* і криптографічних методів між системами ЄС та України.
5. Розміщення *WORM*-сховищ у зоні активних бойових дій: слід розробити протоколи резервування й хмарного дублювання, сумісні з вимогами МКС до ланцюга збереження.
6. Практична готовність українських суддів і слідчих до ролі *special advocate* та роботи з резервними судами— потрібні програми сертифікації й аналіз судової практики після впровадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гловюк І.В. Використання показань, отриманих за ч. 11 ст. 615 КПК України в умовах воєнного стану. 2025. URL: <https://www.hsa.org.ua/blog/vikoristannia-pokazan-otrimanix-za-c-11-st-615-kpk-ukrayini-v-umovax-vojenного-stanu-irina-gloviuk1> (дата звернення: 21.03.2025).
2. Костюченко О.Ю. Роздуми щодо конституційності положень ч. 6 ст. 615 КПК України стосовно автоматичного продовження строку тримання під вартою в умовах воєнного стану. 2023; 39(1): 1–15. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/10/39-1.pdf> (дата звернення: 21.03.2025).
3. CCU announces decision on the CPC provision on extension of the term of arrest during martial law (КЦУ оголошує рішення про продовження строку арешту під час воєнного стану). Unian, 2025. URL: <https://unn.ua/en/news/ccu-announces-decision-on-the-cpc-provision-on-extension-of-the-term-of-arrest-during-martial-law> (дата звернення: 21.03.2025).
4. Nekoliak, A., & Nekoliak, R. Wartime Constitutionalism and the Politics of Constitutional Review in Ukraine (Воєнний конституціоналізм та політика конституційного контролю в Україні). *Verfassungsblog*, 2024. URL: <https://verfassungsblog.de/constitutional-review-ukraine-criminal-procedure/> (дата звернення: 21.03.2025).
5. Рогальська В.В. Застосування запобіжних заходів під час розслідування злочинів проти основ національної та громадської безпеки України в умовах воєнного стану: окремі аспекти. 2024; 1: 772–774.
6. Зіньковський І.П. Трансформація отримання вербальної інформації від особи у кримінальному провадженні під час воєнного стану. 2023; 1: 513–518.
7. OSCE-ODIHR. Continued efforts to ensuring justice and accountability... (6-й звіт OSCE-ODIHR) (Безперервні зусилля щодо забезпечення правосуддя та відповідальності). 2025. URL: <https://www.osce.org/odihr/586050> (дата звернення: 21.03.2025).
8. OSCE/ODIHR. Tools support Ukrainian courts in ensuring the right to a fair trial in war crimes cases (Інструменти підтримки українських судів у забезпеченні права на справедливий суд у справах воєнних злочинів). 2025. URL: <https://www.osce.org/odihr/577388> (дата звернення: 21.03.2025).
9. Кримінальний процесуальний кодекс України. Стаття 615-1. 2025. URL: https://protocol.ua/ua/kriminalniy_protseualniy_kodeks_ukraini_stattya_615_1/ (дата звернення: 21.03.2025).
10. Конституція України. Стаття 64. 2025. URL: <https://constitution.in.ua/articles/64/> (дата звернення: 21.03.2025).
11. Council of Europe/ECtHR. Guide on Article 15 of the European Convention on Human Rights: Derogation in time of emergency (Посібник щодо статті 15 ЄКПЛ: дерогація в умовах надзвичайної ситуації). 2024. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_15_eng (дата звернення: 21.03.2025).
12. Рішення Конституційного Суду України № 8-р(II)/2024 у справі щодо конституційності ч. 6 ст. 615 КПК України. 18 липня 2024 р. URL: <https://zakon.rada.gov.ua/go/v008p710-24> (дата звернення: 21.03.2025).
13. ECtHR. *Brogan and Others v. the United Kingdom* [GC], Judgment of 29 November 1988, Series A No 145-B (Справа Броган та інші проти Великої Британії). 1988. URL: <https://hudoc.echr.coe.int/eng?i=001-57450> (дата звернення: 21.03.2025).
14. ECtHR. *A. and Others v. the United Kingdom* [GC], Judgment of 19 February 2009, Application No 3455/05 (Справа А. та інші проти Великої Британії). 2009. URL: <https://hudoc.echr.coe.int/eng?i=001-91403> (дата звернення: 21.03.2025).

15. Şahin Alpay v. Turkey, Judgment of 20 March 2018, Application No 16538/17 (Справа Шахін Альпай проти Туреччини). 2018. URL: <https://hudoc.echr.coe.int/eng?i=001-181527> (дата звернення: 21.03.2025).
16. Пчеліна, О. В. Фундаментальні положення міжнародних та європейських правових стандартів у кримінальному процесі. 2023.
17. Penal Reform International. Global Prison Trends 2024 (Глобальні тенденції тюремного ув'язнення 2024). London: PRI, 2024. URL: https://cdn.penalreform.org/wp-content/uploads/2024/09/PRI_Global-prison-trends-report-2024_EN.pdf (дата звернення: 21.03.2025).
18. Лист Голови Верховного Суду «Щодо окремих питань здійснення кримінального провадження в умовах воєнного стану» № 1/0/2-22 від 03 березня 2022 р. 2022. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/war/Inform_lyst_2022_03_03.pdf (дата звернення: 21.03.2025).
19. Проект Закону № 9314 «Про внесення змін до статті 615 Кримінального процесуального кодексу України щодо особливостей обчислення строків досудового слідства в умовах воєнного стану». n.d.
20. ECtHR. Kharchenko v. Ukraine, Judgment of 10 February 2011, Application No 40107/02 (Справа Харченко проти України). 2011. URL: <https://hudoc.echr.coe.int/rus?i=001-103260> (дата звернення: 21.03.2025).
21. HELP course on Pre-trial Investigation and ECHR launched for Ukrainian prosecutors (Курс HELP щодо досудового розслідування та ЄКПЛ для українських прокурорів). 2025. URL: <https://www.coe.int/en/web/kyiv/fostering-human-rights-in-the-criminal-justice-system-in-ukraine> (дата звернення: 21.03.2025).
22. OSCE helps Ukraine protect the rights of people in pre-trial detention (ОБСЄ допомагає Україні захищати права осіб у попередньому ув'язненні). 2024. URL: <https://www.osce.org/osce-secretariat-exb-support-programme-for-ukraine/578752> (дата звернення: 21.03.2025).
23. Судова статистика: звітність щодо стану здійснення правосуддя місцевими та апеляційними судами. Supreme Court of Ukraine, 2025. URL: https://court.gov.ua/inshe/sudova_statystyka/ (дата звернення: 21.03.2025).
24. Wilson Center. Functioning of Ukrainian Courts during the War (Функціонування українських судів під час війни). 2024.
25. Venice Commission. Law on the Judiciary and the Status of Judges of Ukraine (CDL-REF(2021)080) (Закон про судоустрій та статус суддів України). 2021.
26. OSCE/ODIHR. Opinion on the Draft Concept on the Reform of the Security Service of Ukraine (Думка про проект концепції реформування СБУ України). 2020.
27. ECtHR. Roman Zakharov v. Russia [GC], Judgment of 4 December 2015, App No 47143/06 (Справа Романа Захарова проти Росії). 2015.
28. ECtHR. Klass and Others v. Germany, Judgment of 6 September 1978, Series A No 28 (Справа Клас та інші проти Німеччини). 1978.
29. OSCE/ODIHR. Urgent Note on Judges and Prosecutors' Access to Classified Information, Security Clearance and Respect for Judicial Independence (Термінове зауваження щодо доступу суддів і прокурорів до класифікованої інформації, допуску та поваги до незалежності правосуддя). 2024.
30. Офіс Генерального прокурора. Наказ № 008/4905-24 «Про затвердження Стандартів діяльності прокурорів у сфері захисту інвестицій під час досудового розслідування». 2024. URL: <https://zakon.rada.gov.ua/laws/main/v0084905-24#Text> (дата звернення: 21.03.2025).
31. OSCE. Guidelines on Democratic Lawmaking for Better Laws (Керівні принципи ОБСЄ щодо демократичного законотворення для кращих законів). 2023.
32. Council of Europe. European Judicial Systems. Evaluation Report – 2024 cycle (2022 data) (Європейські судові системи. Оцінювальний звіт 2024 (дані 2022)). Strasbourg, 2024.
33. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. 2017.
34. NIST Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response (Посібник з інтеграції судових методів у реагування на інциденти). 2006.
35. NIST. Chain of custody (Ланцюг збереження доказів). 2015. URL: https://csrc.nist.gov/glossary/term/chain_of_custody (дата звернення: 21.03.2025).
36. Council of Europe. Guidelines on Electronic Evidence and Explanatory Memorandum (Керівні принципи Ради Європи щодо електронних доказів та пояснювальна записка). 2019.
37. OSCE. Ensuring Human Rights Compliance in Cyber-crime Investigations (Забезпечення дотримання прав людини в розслідуваннях кіберзлочинності). 2023.

38. Bachmaier-Winter, L. The Use of Electronic Evidence in the European Area of Freedom, Security and Justice (Використання електронних доказів у європейській зоні свободи, безпеки та правосуддя). ERA Forum. 2023; 4: 243–250.
39. Signaturit. What Exactly Is an Audit Trail and What Electronic Evidence Does It Contain? (Що таке аудиторський журнал та які електронні докази він містить?). 2024.
40. Савченко, О.В. Нормативно-правове регулювання електронних доказів у цивільному та кримінальному процесі. 2024; 2: 99–107.
41. European Commission for the Efficiency of Justice (CEPEJ). Guidelines on Videoconferencing in Judicial Proceedings (Керівні принципи CEPEJ щодо відеоконференцій у судових засіданнях). 2021.
42. Delaney, K. How to Calculate Video-Conferencing Bandwidth Requirements (Як розрахувати вимоги до пропускної здатності для відеоконференцій). 2023.
43. OSCE/ODIHR. Fair Trial Rights and Public Health Emergencies (Права на справедливий суд та надзвичайні ситуації з охороною здоров'я). 2021.
44. NetForecast. Internet Connection Requirements for Effective Video-Conferencing (Вимоги до інтернет-з'єднання для ефективних відеоконференцій). 2021.
45. CableLabs. Testing Bandwidth Usage of Popular Video-Conferencing Applications (Тестування використання пропускної здатності популярних додатків для відеоконференцій). 2020.
46. Blog, C.W. Modern Video-Conferencing Systems: Negotiating H.264 in SDP (Сучасні системи відеоконференцій: узгодження H.264 в SDP). 14 Jun 2024.
47. What Is Video Bandwidth? 720p, 1080p, GB Transfer Explained (Що таке відео-пропускна здатність? 720p, 1080p, передача даних в ГБ пояснено). 2025.
48. ECtHR. Rowe and Davis v. the United Kingdom [GC], Judgment of 16 February 2000, App No 28901/95 (Справа Роу та Девіс проти Великої Британії). 2000.
49. Crown Prosecution Service. Disclosure Manual, Chapter 34: Handling National Security-Related Claims for Public Interest Immunity (Посібник із розкриття інформації: обробка заяв про імунітет на підставі інтересу суспільства у справах нацбезпеки). n.d.
50. Justice and Security Act 2013, s. 9 & Explanatory Notes (Закон про правосуддя та безпеку 2013, ст. 9 та пояснювальні примітки). London: HMSO, 2013.
51. Venice Commission. Compilation of Opinions on State Secrecy and Fair Trial (Збірка думок щодо державної таємниці та справедливого суду). n.d.
52. OSCE/ODIHR. Rule of Law & Trial Monitoring Guidelines (Керівні принципи ПРООН/БДІПЛ щодо верховенства права та моніторингу судового процесу). n.d.
53. Council of Europe. Human Rights and Criminal Procedure (Права людини та кримінальний процес). 2009.
54. Article 615 CPC Analysis (RM/COE 2023) (Аналіз статті 615 КПК (RM/PE 2023)). 2023.
55. Fair Trials. Secret Surveillance and the Right to a Fair Trial (Секретне стеження та право на справедливий суд). n.d.
56. The Times. Disclosure of Evidence on Review of Temporary Exclusion Order (Розкриття доказів під час перегляду наказу про тимчасове виключення). 2024.
57. Закон України «Про державну таємницю» № 3855-XII. 1994.
58. UN Women. Addressing Conflict-Related Sexual Violence: An Analytical Inventory of Peacekeeping Practice (Протидія сексуальному насильству в конфлікті: аналітична інвентаризація практик миротворення). 2012.
59. UNODC/UNICEF. Guidelines on Justice in Matters Involving Child Victims and Witnesses of Crime (Керівні принципи щодо правосуддя у справах дітей-жертв і свідків злочинів). 2005.
60. OSCE/ODIHR. Quick Guide on Preventing and Addressing Sexual & Gender-Based Violence in Criminal-Justice Facilities (Швидкий посібник з запобігання та реагування на сексуальне й гендерно обумовлене насильство у кримінальному правосудді). 2024.
61. OSCE Parliamentary Assembly. Gender Report 2023: Understanding the Gendered Consequences of the War in Ukraine (Гендерний звіт 2023: гендерні наслідки війни в Україні). 2023.
62. FCDO, U. International Protocol on the Documentation and Investigation of Sexual Violence in Conflict (2nd ed.) (Міжнародний протокол з документування та розслідування сексуального насильства в конфлікті, 2-ге вид.). 2017.
63. Council of Europe/CDCJ. Guidelines on Electronic Evidence (approved 16 Nov 2018) (Керівні принципи Ради Європи/CDCJ щодо електронних доказів). 2019.
64. ICC. Rules of Procedure and Evidence, ICC-ASP/1/3 (Part II-A) (Правила процедури та доказів МКС, ICC-ASP/1/3, ч. II-A). 2013.
65. ICC. Summary of the Decision on the Admissibility of the Case against Muammar Gaddafi (Резюме рішення про прийнятність справи проти Муаммара Каддафі). 2013.

66. ICC. Decision on the Admissibility of the Case against Abdullah Al-Senussi, ICC-01/11-01/11-466 (Рішення про прийнятність справи щодо Абдулли аль-Сенуссі). 2013.
67. Statute of the Special Court for Sierra Leone (Статут Спеціального суду для Сьєрра-Леоне). 2002.
68. Heller, K. The Road Not (Yet) Taken: A Special Tribunal for the Crime of Aggression against Ukraine (Шлях, який ще не пройдений: спеціальний трибунал за злочин агресії проти України). *Opinio Juris*, 16 Apr 2025.
69. Poland. Kodeks postępowania karnego [КПК], Art. 248 (Кодекс кримінального процесу Польщі, ст. 248). 1997.
70. OSCE/ODIHR. Urgent Opinion on State of Emergency Legislative Acts in Poland (Термінова думка щодо законодавства про надзвичайний стан у Польщі). 2021.
71. Lithuania Adopts Legal Changes to Streamline Defence in Wartime (Литва приймає законодавчі зміни для оптимізації захисту в воєнний час). *LRT*, 1 Jul 2020.
72. Fair Trials. Criminal Proceedings and Defence Rights in Lithuania (Кримінальне провадження та права захисту в Литві). 2012.
73. Croatia. Zakon o kaznenom postupku (Official Gazette 62/2003) (Закон про кримінальний процес Хорватії). 2003.
74. Council of Europe. Investigations into Crimes Committed during the Croatian Homeland War (Розслідування злочинів під час Хорватської вітчизняної війни). Strasbourg, 2024.