ЦИФРОВІ ТА ПРОЦЕСУАЛЬНО-КРИМІНАЛІСТИЧНІ СТАНДАРТИ ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ ПРОТИ ЛЮДЯНОСТІ В ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Микола ПОГОРЕЦЬКИЙ,
головний науковий співробітник науково-організаційного центру Національної академії Служби безпеки України,
проректор з науково-педагогічної роботи Київського національного університету імені Тараса Шевченка
доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України,
заслужений діяч науки і техніки України
ORCID ID: 0000-0003-0936-0929

Документування злочинів проти людяності, вчинених у ході збройної агресії рф проти України, є одним із ключових напрямів діяльності органів сектору безпеки та правосуддя, зокрема Служби безпеки України. Саме від ефективності та достовірності цієї роботи залежить не лише майбутнє судове переслідування винних у вчиненні таких злочинів у міжнародних юрисдикціях, а й формування історичної пам'яті, відновлення справедливості для жертв і зміцнення міжнародного правопорядку.

У сучасних умовах документування злочинів проти людяності, вчинених у ході збройної агресії рф проти України, набуває принципово нового змісту. Воно поєднує класичні криміналістичні прийоми фіксації та перевірки доказів із цифровими технологіями, оперативно-розшуковими та контррозвідувальними засобами СБУ. Ця діяльність виходить за межі традиційного національного кримінального процесу, оскільки зібрані матеріали мають слугувати доказами у провадженнях Міжнародного кримінального суду та потенційного спеціального військового трибуналу щодо злочинної агресії рф проти України[1]. Саме тому формування єдиних цифро-

[1] Спеціальний військовий (ad hoc) трибунал щодо злочину агресії рф юридично започат-

вих і процесуально-криміналістичних стандартів документування є питанням державного і міжнародного значення.

Служба безпеки України, виконуючи завдання із захисту державного суверенітету, територіальної цілісності та конституційного ладу, водночас є одним із провідних суб'єктів доказової діяльності у справах про злочини проти людяності. Її спеціальні підрозділи здійснюють контррозвідувальне спостереження, технічну фіксацію, збір цифрових слідів, аналітичне узагальнення даних та їх передачу до органів досудового розслідування і міжнародних партнерів. У цій системі СБУ є не лише органом оперативного реагування, а й ключовим елементом доказової інтеграції між національною юрисдикцією та міжнародним правосуддям.

Важливим аспектом документування злочинів проти людяності, вчинених у ході збройної агресії рф проти України, є нормативна, процесуальна й методологічна узгодженість дій різних правоохоронних і спеціальних органів. Умови воєнного стану вимагають не лише координації між СБУ, Державним бюро розслідувань, Національною поліцією та Офісом Генерального прокурора, а й адаптації української практики до міжнародних стандартів доказування. Йдеться передусім про вимоги автентичності, відтворюваності, неперервного ланцюга збереження доказів, дотримання прав людини під час їх отримання та цифрової верифікації кожного матеріалу.

Актуальність проблеми зумовлена тим, що документування злочинів проти людяності є не лише елементом процесуальної форми кримінального провадження, а й частиною національної системи безпеки. Воно виконує подвійну функцію – оперативно-захисну (як засіб запобігання новим злочинам) і доказову (як елемент майбутнього судового переслідування). У цьому аспекті особливу роль відіграють контррозвідувальні підрозділи СБУ, які володіють унікальними можливостями щодо ідентифікації організаторів та виконавців злочинів, відновлення ланцюга підпорядкованості, фіксації

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

політичних і військових рішень, що мають ознаки злочинної політики держави-агресора.

Проблематика документування злочинів проти людяності у сучасному міжнародному праві перебуває на перетині кримінально-процесуальних, криміналістичних і правозастосовних категорій. Її концептуальні основи формувалися впродовж другої половини XX століття та були кодифіковані в *Римському статуті Міжнародного кримінального суду* [11], який визначив злочини проти людяності як будь-який із передбачених актів, учинений у межах широкомасштабного або систематичного нападу проти цивільного населення. Відтоді документування таких злочинів стало не лише складовою кримінального процесу, а й інструментом реалізації принципу невідворотності міжнародної відповідальності.

З теоретико-правового погляду документування є системою цілеспрямованих дій уповноважених суб'єктів, спрямованих на виявлення, фіксацію, перевірку й збереження фактичних даних про події злочину для їх подальшої оцінки у процесуальній формі доказів. У вітчизняній науці воно розглядається як гносеологічна складова доказування, тобто як етап пізнання істини, що передує судовій перевірці [25]. Саме теорія доказів, яка лежить в основі кримінального процесуального пізнання, визначає логіку переходу від інформації про подію до юридично значущого доказу. Документування виконує роль первинного елементу доказової системи, забезпечуючи зв'язок між об'єктивними фактами та процесуальними засобами їх відображення.

У практиці міжнародних судів, починаючи з рішень *Міжнародного трибуналу щодо Руанди* (*Akayesu*, 1998) [1], вироблено уніфіковані підходи до визначення належності й допустимості доказів у справах про злочини проти людяності. Вони базуються на таких критеріях: законність отримання, автентичність джерела, зв'язок доказу з предметом обвинувачення, відсутність порушення прав людини при його здобутті. Ці вимоги відображені у правилах доказування Міжнародного кримінального суду [11] і стали взірцем для національних систем.

Розвиток технологій докорінно змінив природу процесу доказування. Цифрові ресурси, супутникові знімки, відкриті дані й матеріали OSINT стали невід'ємними елементами доказової бази у справах про міжнародні злочини. У відповідь на це Офіс Вер-

ховного комісара ООН з прав людини спільно з Університетом Берклі розробив Берклійський протокол щодо цифрових відкритих джерел розслідувань *(Berkeley Protocol on Digital Open Source Investigations),* який відомий загалу як – Протокол Берклі (*Berkeley Protocol)* [2]. Цей протокол закріпив міжнародні стандарти роботи з цифровими доказами – від збору до їх верифікації. Його принципи – достовірність, відтворюваність і прозорість походження – стали фундаментом сучасної методології документування злочинів проти людяності, зокрема на території України.

Особливе місце у доказуванні злочинів проти людяності належить органам національної юрисдикції, що виконують функції оперативного виявлення та фіксації злочинів. У цьому контексті діяльність Служби безпеки України має системне значення. Закон «Про Службу безпеки України» визначає одним із основних завдань СБУ захист державного суверенітету та протидію діяльності, спрямованій на підрив конституційного ладу [19]. Саме спеціальні підрозділи СБУ здійснюють контррозвідувальне документування злочинів, що посягають на безпеку цивільного населення, у тому числі злочинів проти людяності. Вони збирають, перевіряють і зберігають фактичні дані, які після процесуальної легалізації набувають статусу доказів у кримінальному провадженні.

Відповідно до Закону «Про оперативно-розшукову діяльність» [18] та положень Кримінального процесуального кодексу України [20], матеріали, одержані в результаті оперативно-розшукових заходів, можуть бути використані як докази за умови дотримання вимог законності, належності й достовірності. Таким чином, у системі доказування документування злочинів проти людяності виконує не допоміжну, а первинну функцію – воно створює базу для перевірки, оцінки й судового доведення.

Міжнародна практика підтверджує, що результативність документування залежить від точності технічних процедур і контролю за цілісністю доказів. У цьому аспекті провідне значення мають стандарти (*ENFSI Best Practice Manuals – Digital Forensics)* [4], які визначають методи збереження метаданих, хешування та забезпечення неперервного ланцюга збереження (*chain of custody*). Аналогічні принципи впроваджуються у спільних слідчих групах (*Joint Investigation Teams*) під егідою Євроюсту [14], де участь українських правоохоронців і СБУ гарантує інтеграцію національної доказової бази у міжнародну.

Теоретичне значення документування полягає в тому, що воно відображає еволюцію самого поняття доказу – від матеріального до цифрового, від локального до транскордонного. У роботах сучасних дослідників доведено, що використання штучного інтелекту у доказуванні сприяє підвищенню точності перевірки даних, але потребує суворого дотримання етичних і правових гарантій [9]. Цю позицію підтримує і *Європейська етична хартія про застосування штучного інтелекту в судових системах* [7], яка встановлює принципи прозорості алгоритмів, підконтрольності рішень та недопущення дискримінації при використанні аналітичних систем.

Злочини проти людяності за своєю природою мають системний характер, тому документування повинно відображати не лише окремі події, а й контекст – політичну або військову політику, у межах якої такі злочини здійснювалися. Саме контекстуальна складова є предметом доказування, який визначає логіку збору фактичних даних і структуру доказової системи. Практика Європейського суду з прав людини, зокрема у справах *Roman Zakharov v. Russia* [5] та *Big Brother Watch and Others v. the United Kingdom* [6], підкреслює необхідність забезпечення пропорційності між заходами збирання доказів і захистом права на приватність. Це положення є особливо важливим для діяльності спеціальних служб під час воєнного стану.

Таким чином, теоретико-правові основи документування злочинів проти людяності охоплюють комплекс норм і принципів, що поєднують міжнародне кримінальне право, національне процесуальне законодавство, цифрову криміналістику та етичні стандарти використання технологій. Важливу роль у забезпеченні належного документування злочинів проти людяності відіграє криміналістична тактика та комплекс негласних слідчих (розшукових) дій (НСРД) і оперативно-розшукових заходів, що проводяться підрозділами СБУ. Саме вони забезпечують своєчасне виявлення, фіксацію, збереження й перевірку доказової інформації, яка часто має цифрову природу або походить із кіберпростору. У сучасних умовах дедалі більшого значення набуває інтелектуальний аналіз мультисенсорних даних – синтез інформації, отриманої з різних джерел (аудіо-, відео-, супутникових, телекомунікаційних, мережевих), що дозволяє створити комплексну модель події та простежити ланцюг взаємозв'язків між суб'єктами злочину, його організаторами й виконавцями.

Результати такого аналізу використовуються як аналітична основа для кримінального процесуального доказування, зокрема при оцінці достовірності цифрових доказів, перевірці версій та підтвердженні системного характеру злочинної діяльності рф. Використання новітніх технологій, зокрема методів цифрової криміналістики, алгоритмів машинного навчання та криміналістичних засобів дослідження електронних доказів, забезпечує підвищення точності, оперативності та наукової обґрунтованості доказування. Кіберпростір при цьому постає не лише середовищем учинення злочинів, а й простором їх документування, у якому формується новий вимір доказового процесу – цифрове відображення злочину проти людяності. Застосування таких технологічних рішень дозволяє контррозвідувальним, оперативно-технічним, аналітичним, слідчим та іншим підрозділам Служби безпеки України інтегрувати результати контррозвідувальних, оперативно-розшукових заходів та відповідних процесуальних дій щодо документування злочинів рф проти людяності у міжнародну доказову систему, забезпечуючи їхню автентичність і відтворюваність. Вони формують методологічну основу для роботи Служби безпеки України як ключового суб'єкта фіксації та збереження доказів злочинів агресора. У поєднанні з нормами міжнародного гуманітарного права, практикою Міжнародного кримінального суду та Європейського суду з прав людини ця система гарантує не лише належну якість доказів, а й легітимність майбутніх судових рішень, спрямованих на встановлення відповідальності осіб, винних у масових порушеннях прав людини. Особливе значення у цьому контексті має судовий контроль (*judicial oversight*), який виступає основним інструментом забезпечення верховенства права у доказуванні, гарантує законність отримання, перевірки та використання доказів, а також запобігає їх фальсифікації або неправомірному втручанню в права людини [13; 21–31].

Документування злочинів проти людяності в діяльності Служби безпеки України має не лише процесуально-доказове, а й контррозвідувальне значення. У структурі СБУ саме контррозвідувальні та оперативно-технічні підрозділи здійснюють безпосередню фіксацію дій, що мають ознаки злочинів проти людяності, – масових убивств, катувань, депортацій, примусових переміщень, утримання цивільних осіб у незаконних місцях позбавлення волі. Ця діяльність

є особливою формою контррозвідувального та криміналістичного спостереження, спрямованого на виявлення та закріплення обставин злочину ще до його правової оцінки в межах кримінального провадження [19].

Контррозвідувальні заходи дозволяють виявляти структури управління злочинними діями окупаційних адміністрацій рф, осіб, які координують політику переслідувань, а також ланцюг підпорядкування між військовим і політичним керівництвом агресора. Завдяки системі агентурної та технічної розвідки СБУ здатна документувати злочини не лише за їх наслідками, а й на стадії підготовки чи реалізації. Такі матеріали набувають доказового значення після процесуальної легалізації – їх оформлення у вигляді протоколів, рапортів чи аналітичних довідок, що підтверджують достовірність отриманої інформації [18; 20].

У цьому аспекті провідне значення мають стандарти, визначені в настановах належної практики для цифрової криміналістики, зокрема в «Найкращих практичних настановах Європейської мережі судово-експертних установ (*ENFSI Best Practice Manuals – Digital Forensics*)»[2], які встановлюють вимоги до методів збору, фіксації, збереження та верифікації цифрових доказів у кримінальному провадженні. [4]. Це, зокрема, збір електронних слідів, фіксація метаданих, відновлення видалених файлів, геолокаційне позиціонування, ідентифікація цифрових артефактів і підтвердження цілісності даних за допомогою алгоритмів хешування. Важливим є забезпечення неперервного ланцюга збереження (*chain of custody*), який гарантує автентичність і відтворюваність доказів під час передачі від оперативного підрозділу до слідчого чи прокурора.

Контррозвідувальна складова документування полягає у виявленні державної політики терору як системного елементу злочинів проти людяності. У цьому контексті важливим є аналіз наказів, директив, комунікаційних мереж та інформаційних матеріалів рф, які підтверджують організований характер насильства. Такі дії

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

узгоджуються з міжнародною практикою, зафіксованою у рішеннях Міжнародного трибуналу щодо Руанди (*International Criminal Tribunal for Rwanda*) у справі Акайесу (*Akayesu*) [1] та Міжнародного кримінального суду у справі Нтаганда (*Ntaganda*) [12], де для встановлення вини використовувались дані розвідки та відомості про структуру підпорядкування військових підрозділів.

Збирання доказів злочинів проти людяності вимагає залучення аналітичних можливостей СБУ – моніторингу комунікацій, обробки відкритих джерел, аналізу соціальних мереж і OSINT-платформ. Цифрові матеріали повинні відповідати вимогам Протоколу Берклі щодо цифрових відкритих джерел розслідувань [2], який регламентує процедури фіксації часу, місця, джерела походження та збереження первинного файлу. У межах спільних слідчих груп, створених за підтримки Євроюсту [14], результати контррозвідувального документування передаються до Офісу Генерального прокурора та Міжнародного кримінального суду відповідно до Меморандуму про взаєморозуміння щодо співробітництва і обміну доказами [10].

Оперативно-розшукове документування виконує функцію з'єднання між фактичними даними та процесуальним доказом. Його результатом є формування масиву інформації, що після перевірки може бути використаний як доказ у міжнародному судочинстві. Водночас така діяльність вимагає дотримання принципів законності, пропорційності та захисту прав людини. Практика Європейського суду з прав людини у справах *Roman Zakharov v. Russia* [5] та *Big Brother Watch and Others v. the United Kingdom* [6] визначає межі допустимого втручання державних органів у приватне життя громадян навіть за умов загрози національній безпеці. Тому контррозвідувальні підрозділи СБУ повинні діяти в межах чітко регламентованих повноважень, із гарантіями незалежного контролю за законністю проведення негласних заходів.

Особливістю сучасного етапу є широке впровадження штучного інтелекту у сфері аналітики та перевірки цифрових доказів. Алгоритми машинного навчання (*machine learning algorithms*) дозволяють автоматично розпізнавати місця подій, фіксувати збіги осіб чи об'єктів на фото- і відеоматеріалах, аналізувати часові послідовності та зв'язки між учасниками злочину. Проте такі технології можуть застосовуватись лише в межах принципів, визначених Європейською етичною хартією щодо використання штучного інте-

лекту в судових системах (*European Ethical Charter on AI in Judicial Systems*) [7], – прозорості, підконтрольності людині та забезпечення права на справедливий суд. Практичні аспекти використання алгоритмів штучного інтелекту для цілей доказування детально аналізуються у науковій праці Лігеті К. (*Ligeti K.*) «CRIM_AI – Розкриття (аналіз) доказів, отриманих із використанням штучного інтелекту» [9] і в аналітичному звіті Європолу «Штучний інтелект і поліцейська діяльність (AI and Policing)» [8], які визначають ризики автоматизованих рішень та акцентують на необхідності людського підтвердження результатів. В українському правовому полі ефективність документування злочинів проти людяності залежить від належної взаємодії СБУ з іншими правоохоронними структурами – Державним бюро розслідувань, Національною поліцією та Офісом Генерального прокурора. Їхні повноваження визначені відповідними законами [16; 17; 18; 19]. В умовах воєнного стану важливою є єдність інформаційного простору: матеріали оперативно-розшукової діяльності СБУ повинні узгоджуватись із процесуальними діями слідчих ДБР та поліції, щоб забезпечити послідовний ланцюг від фіксації факту до його кваліфікації та передачі в Міжнародний кримінальний суд.

Контррозвідувальні й оперативні підрозділи СБУ створюють основу національної доказової архітектури, що поєднує методи розвідки, контррозвідки, оперативно-розшукової діяльності й цифрової криміналістики (*цифрової форензіки – digital forensics*). Їх діяльність є ключовою для наповнення Державного хабу збору доказів воєнних злочинів Офісу Генерального прокурора[3] (портал «Warcrimes») [2], яка узгоджується зі стандартами ENFS [4] та Протокол Берклі [2]. У такій моделі документування забезпечується комплексна доказова безперервність – від первинного спостереження й фіксації до міжнародної судової оцінки.

Отже, контррозвідувальна та оперативно-розшукова, аналітична, спеціальна військова та процесуально-криміналістична ді-

[3] Державний хаб збору доказів воєнних злочинів Офісу Генерального прокурора запущено 6 березня 2022 року як ініціативу ОГП у співпраці з партнерами. Окремі медіа-аналітики та правники інколи неформально називають його «Українським (національним) центром цифрових доказів» – як державну платформу акумулювання цифрових доказів злочинів держави-агресора. Саме через цей портал громадяни та організації подають цифрові матеріали щодо воєнних злочинів і злочинів проти людяності. Водночас офіційно **Український національний центр цифрових доказів** як окремий державний реєстр/установа **не створений** і наразі існує лише як пропозиція, що обговорюється в наукових і професійних колах.

яльність Служби безпеки України становить основу практичного механізму документування злочинів проти людяності. Вона поєднує державну функцію захисту національної безпеки з міжнародно-правовими зобов'язаннями щодо збору й передачі доказів, сприяючи досягненню стратегічної мети – притягненню керівництва рф до відповідальності за масові злочини проти цивільного населення.

У теорії доказування предмет доказування визначає межі пізнання, коло обставин, що мають значення для правильного вирішення справи, та напрями, за якими здійснюється збирання фактичних даних. У справах про злочини проти людяності предмет доказування має розширене значення, оскільки охоплює не лише окремі факти, а й *контекст системного нападу* на цивільне населення, наявність державної політики переслідувань, зв'язок між діями виконавців і рішеннями керівництва рф, а також соціально-політичні наслідки таких дій [11].

Злочини проти людяності мають ознаки масовості, організованості й плановості, тому їх доказування потребує інтеграції різних джерел інформації – від матеріальних слідів до електронних і цифрових даних. У міжнародному правосудді предмет доказування формується на основі норм *Римського статуту* (стаття 7) [11], який встановлює перелік актів, що можуть кваліфікуватися як злочини проти людяності: убивство, поневолення, депортація, тортури, сексуальне насильство, переслідування, насильницьке зникнення, знищення та інші нелюдські дії тощо. Для кожного з цих діянь доказуванню підлягають як матеріальні елементи (дія, наслідок, причинний зв'язок), так і суб'єктивні – намір, обізнаність про контекст системного нападу.

Документування злочинів проти людяності підрозділами СБУ спрямоване на забезпечення повноти такого предмета доказування. На практиці це означає виявлення, фіксацію та перевірку обставин, які підтверджують існування державної політики рф, спрямованої на вчинення таких злочинів, визначення структури підпорядкування, засобів координації, характеру та масштабу насильства, а також ідентифікацію осіб, що приймали рішення або виконували накази. У цьому контексті предмет доказування визначає напрям оперативно-розшукових і контррозвідувальних заходів, зокрема встановлення комунікацій між органами влади рф, окупаційними адміністраціями та виконавцями злочинів [18; 19].

Важливою складовою є контекстуальна доказовість – підтвердження того, що конкретні діяння вчинені не ізольовано, а як частина планомірної політики держави. Для цього застосовується аналіз документів, наказів, протоколів нарад, публічних виступів та інформаційних кампаній, які розкривають наміри й усвідомлення організаторів злочинів. Подібний підхід використовувався у рішенні Міжнародного трибуналу щодо Руанди (International Criminal Tribunal for Rwanda) у справі Акайесу (Akayesu) [1], де контекст державної політики геноциду був доведений через аналіз промов і документів влади. У межах національного кримінального процесу предмет доказування конкретизується положеннями статей 91–92 КПК України [20], які визначають, що доказуванню підлягають подія злочину, винуватість особи, форма вини, мотиви, наслідки та інші обставини, що мають значення для провадження. Для злочинів проти людяності ці обставини охоплюють додатково: факти координації злочинних дій між військовими й політичними структурами рф; наявність системної пропаганди, спрямованої на дегуманізацію українського населення; наслідки для окремих категорій жертв – цивільних, військовополонених, депортованих дітей.

Формування предмета доказування безпосередньо впливає на структуру доказової бази, визначаючи, які саме матеріали мають збиратись і яким критеріям вони повинні відповідати. Цифрові докази – відео, аудіо, метадані, супутникові знімки – набувають центрального значення у предметі доказування, коли вони підтверджують масовий або систематичний характер дій. Для засвідчення їх автентичності застосовують Настанови належної практики Європейської мережі судово-експертних установ (ENFSI) [4] та Берклійський протокол [2], які вимагають фіксації походження файлів, часу створення, геолокації, технічних параметрів і (за наявності) цифрових підписів. У контексті злочинів проти людяності підрозділи СБУ визначають предмет доказування не лише через правову норму, а й через аналітичну оцінку безпекового середовища. Контррозвідувальні підрозділи аналізують зміст і наслідки дій рф, які утворюють елементи злочину: примусові депортації, створення фільтраційних таборів, катування, організацію інформаційно-психологічного тиску. Оперативні матеріали при цьому оформлюються у протоколи спостереження, аналітичні довідки, схеми структур взаємодії між військовими частинами та цивільними адміністраці-

ями. У подальшому ці документи передаються до Офісу Генерального прокурора для легалізації та використання як доказів [10; 14].

Міжнародний досвід показує, що належне визначення предмета доказування у справах проти людяності полегшує процес оцінки доказів у суді. Рішення Міжнародного кримінального суду (*International Criminal Court*) у справі Прокурор проти Боско Нтаганда (*The Prosecutor v. Bosco Ntaganda*) [12] і практика ЄСПЛ у справах Роман Захаров проти Росії (*Roman Zakharov v. Russia*) [5] та Біг Бразер Вотч та інші проти Сполученого Королівства (*Big Brother Watch and Others v. the United Kingdom*) [6] свідчать, що системність доказів і наявність логічного зв'язку між елементами обвинувачення забезпечують їх прийнятність навіть за умови використання складних цифрових джерел. Саме предмет доказування визначає, які факти є релевантними, і таким чином формує методологічну рамку всього процесу документування.

Отже, предмет доказування у справах про злочини проти людяності є ключовою методологічною категорією, що поєднує кримінально-процесуальний, контррозвідувальний та криміналістичний виміри. Його належне визначення дозволяє забезпечити цілеспрямоване збирання даних, їх системну перевірку та ефективну інтеграцію у міжнародний доказовий процес. Для Служби безпеки України це означає перехід від епізодичного документування фактів до створення комплексної доказової системи, здатної витримати стандарти допустимості Міжнародного кримінального суду й майбутнього спеціального трибуналу, що розглядатиме злочини агресора проти українського народу.

Результати документування злочинів проти людяності, отримані Службою безпеки України та іншими правоохоронними органами, становлять основу національної доказової бази для міжнародного кримінального переслідування осіб, причетних до злочинів рф. Від моменту їх фіксації до подання у суд вони проходять багаторівневу систему перевірки, легалізації та оцінки, що забезпечує автентичність, належність і допустимість доказів відповідно до вимог Римського статуту [11] і правил доказування Міжнародного кримінального суду.

Відповідно до Меморандуму про взаєморозуміння між Офісом прокурора Міжнародного кримінального суду та Офісом Генерального прокурора України [10], Україна забезпечує передачу

до МКС матеріалів, отриманих у ході контррозвідувального, оперативно-розшукового та слідчого документування. Передача здійснюється через узгоджений канал співробітництва із гарантією дотримання вимог конфіденційності та безпеки джерел. При цьому збереження автентичності даних забезпечується шляхом використання цифрових підписів, контрольних хеш-сум і ланцюга збереження (*chain of custody*), регламентованого стандартами «Цифрової криміналістики Європейської мережі судово-експертних установ (*ENFSI Digital Forensics*)» [4] та Протоколу Берклі [2].

Згідно з міжнародною практикою, результати документування поділяються на три групи: прямі докази, які безпосередньо підтверджують факт злочину (відео-, аудіоматеріали, свідчення очевидців, супутникові знімки); непрямі (контекстуальні) докази, що відображають системність і організований характер злочину (накази, звіти, листування, політичні директиви); аналітичні докази, отримані в результаті контррозвідувального аналізу, які демонструють зв'язки між виконавцями, командуванням і політичними центрами ухвалення рішень [18; 19].

На етапі міжнародного оцінювання такі докази повинні відповідати критеріям, встановленим у рішеннях Міжнародного трибуналу щодо Руанди (International Criminal Tribunal for Rwanda) у справі Акайесу (Akayesu, 1998) [1] та МКС у справі Нтаганда (Ntaganda, 2019) [12]: достовірність джерела, перевірюваність, релевантність і відсутність процесуальних порушень під час отримання. МКС не вимагає абсолютної форми національного процесуального акту, однак наполягає на можливості незалежної перевірки походження кожного доказу. Національний етап перевірки та легалізації результатів документування здійснюється під процесуальним керівництвом Офісу Генерального прокурора, який формує доказові пакети для подання у міжнародні інстанції, зокрема до спільних слідчих груп (Joint Investigation Teams) під егідою Євроюсту [14].

Взаємодія між СБУ, Державним бюро розслідувань, Національною поліцією та прокурорами має уніфікований формат: кожен матеріал супроводжується протоколом походження, цифровим хеш-кодом і довідкою про ланцюг осіб, які мали доступ до доказу. У процесі передачі доказів важливу роль відіграє координація з міжнародними експертними структурами, такими як Європол [8] та Європейська мережа судово-експертних установ (ENFSI) [4],

які здійснюють технічну оцінку автентичності цифрових матеріалів. Перевірка включає ідентифікацію метаданих, встановлення часу створення файлу, GPS-координат, використаних пристроїв і програмного забезпечення, що гарантує прийнятність матеріалів у міжнародному суді, де кожен доказ оцінюється з точки зору його достовірності, незалежності джерела і відповідності процедурним стандартам.

Значне місце у доказуванні займають результати контррозвідувальних операцій, що підтверджують ланцюг підпорядкування між військово-політичним керівництвом рф і виконавцями злочинів. Такі матеріали, як перехоплення телефонних розмов, відеоспостереження, внутрішні документи окупаційних адміністрацій, після належної легалізації мають статус доказів непрямої участі у злочині. Вони дозволяють довести усвідомленість керівництва агресора щодо наслідків своїх дій, що є важливим елементом суб'єктивної сторони злочину проти людяності [19; 25].

У системі міжнародного правосуддя особливу роль відіграє баланс між доказовою ефективністю та дотриманням прав людини. Рішення ЄСПЛ у справах Роман Захаров проти Росії (*Roman Zakharov v. Russia*) [5] та Біг Бразер Вотч та інші проти Сполученого Королівства (*Big Brother Watch and Others v. the United Kingdom*) [6] сформували критерії пропорційності при збиранні та використанні електронних даних: втручання у приватність допускається лише за умов, коли це є необхідним для досягнення легітимної мети та супроводжується ефективними гарантіями контролю. Дотримання цих стандартів забезпечує легітимність доказів і запобігає їх відхиленню у суді через порушення правових процедур.

Використання доказів, отриманих за допомогою технологій штучного інтелекту (*artificial intelligence, AI*), регулюється положеннями Європейської етичної хартії щодо використання штучного інтелекту в судових системах (European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems) [7], яка встановлює принципи надійності (*reliability*), пояснюваності (*explainability*) та збереження суддівського контролю (*judicial oversight*). Аналітичні системи Служби безпеки України, створені на основі методології CRIM_AI – Розкриття доказів, отриманих за допомогою штучного інтелекту (*CRIM_AI – Unpacking AI Evidence*) [9], застосовуються для класифікації цифрових матеріалів і виявлення взаємозв'язків

між епізодами злочинів, однак остаточна оцінка їх доказової сили залишається за людиною.

Таким чином, результати документування злочинів проти людяності виконують подвійну функцію: на національному рівні вони формують підґрунтя кримінального переслідування, а на міжнародному – забезпечують виконання Україною зобов'язань щодо співпраці з Міжнародним кримінальним судом і спеціальним трибуналом. Вони є доказовим інструментом, що поєднує технологічну точність, процесуальну законність і гуманістичну мету – притягнення до відповідальності осіб, причетних до масових порушень прав людини. Забезпечення належного ланцюга збереження, автентичності й верифікації матеріалів документування є запорукою їхньої прийнятності у міжнародних судових процесах.

Практика документування злочинів проти людяності в умовах повномасштабної агресії рф проти України виявила низку проблем, що мають як нормативний, так і організаційно-технічний характер. Ці проблеми стосуються не лише внутрішньої координації між органами сектору безпеки, а й узгодження національних процедур із міжнародними стандартами доказування. Їх системне осмислення необхідне для формування єдиної доказової політики держави, здатної забезпечити використання зібраних матеріалів у міжнародному правосудді без втрати доказової сили.

Однією з ключових проблем є фрагментарність законодавчого регулювання процедур документування. Хоча Кримінальний процесуальний кодекс України [20], закони України «Про Службу безпеки України» [19] та «Про оперативно-розшукову діяльність» [18] передбачають можливість використання матеріалів негласних заходів як доказів, відсутня деталізація щодо критеріїв їх цифрової автентичності та допустимості в міжнародних судових інстанціях. Це створює ризик втрати доказової сили матеріалів через невідповідність формальним вимогам Римського статуту [11] та практиці МКС [12]. Необхідним є розроблення єдиного нормативного акту, який регламентував би процес цифрової фіксації, верифікації та зберігання матеріалів у справах про злочини міжнародного характеру.

Другою проблемою є недостатня технологічна уніфікація процесу фіксації та обробки цифрових доказів. Попри використання СБУ, ДБР і Національною поліцією сучасних засобів збору інформації, різниця у форматах файлів, методах хешування, системах марку-

вання та протоколах передачі даних часто ускладнює об'єднання матеріалів у єдиний доказовий масив. Вирішення цього питання можливе через впровадження технічних стандартів, розроблених Європейською мережею судово-експертних установ *(ENFSI BPM – Digital Forensics)* [4], які передбачають обов'язкове створення контрольних копій, протоколів ланцюга збереження (*chain of custody*) та цифрових підписів. Для СБУ це означає необхідність запровадження національного реєстру цифрових доказів, який забезпечить ідентифікацію, збереження та контроль за кожним файлом, отриманим у межах документування злочинів.

Третій блок проблем пов'язаний із кадровими та аналітичними викликами. Документування злочинів проти людяності вимагає залучення спеціалістів з цифрової криміналістики, OSINT-розвідки, аналізу великих масивів даних та міжнародного права. Водночас у правоохоронних органах відчувається дефіцит експертів, здатних поєднувати технічну компетенцію з процесуальним мисленням. Розв'язання цього питання потребує створення міжвідомчої навчальної програми на базі Академії СБУ, Національної академії прокуратури та університетів, де готують фахівців у сфері міжнародного кримінального права. Особливу увагу слід приділити підготовці аналітиків, які зможуть інтегрувати цифрові дані у процес доказування відповідно до міжнародних правил [2; 9].

Четвертий блок проблем – ризики маніпуляцій і дезінформації. В умовах гібридної війни рф активно використовує фальсифіковані матеріали, діпфейки, підроблені фото- і відеозаписи, що імітують воєнні злочини українських військових. Такі дії спрямовані на дискредитацію офіційних доказів і зниження довіри до національних розслідувань. У цьому аспекті особливого значення набуває застосування міжнародних алгоритмів перевірки, передбачених Протоколом Берклі [2] і аналітичних інструментів Інтерполу [8], які дозволяють встановлювати походження файлу, його метадані, дату створення та можливі ознаки редагування. Для мінімізації ризиків підробки СБУ запроваджує практику багаторівневої верифікації: первинна перевірка на рівні оперативного підрозділу, повторна – технічними лабораторіями, третинна – спільними аналітичними групами з представниками ОГП та міжнародних експертів.

П'ята блок проблем стосується недостатньої інституційної взаємодії між органами досудового розслідування, СБУ та МКС. По-

при існування спільних слідчих груп (*Joint Investigation Teams*) [14], потребує вдосконалення процес обміну доказами, зокрема щодо захисту конфіденційних даних і забезпечення сумісності технічних систем зберігання. Окрему увагу слід приділити етико-правовим аспектам використання штучного інтелекту та автоматизованих систем аналізу. Технології машинного навчання, які нині застосовуються для сортування доказів, створюють ризики порушення принципу пояснюваності судового рішення. Відповідно до Європейської етичної хартії щодо використання штучного інтелекту в судових системах [7], кожне рішення, прийняте з використанням алгоритмів, повинно залишатись під контролем людини, а застосовані системи – проходити незалежну перевірку на прозорість і відсутність дискримінації. У майбутньому Службі безпеки України доцільно створити національну платформу штучного інтелекту для судової експертизи (AI-Forensics), сертифіковану за міжнародними стандартами, яка забезпечуватиме експертну перевірку результатів роботи алгоритмів та їх процесуальну легалізацію.

Шостим блоком проблем є потреба у закріпленні міжнародно-правових гарантій визнання доказів, отриманих українськими органами, у юрисдикціях інших держав і міжнародних трибуналів. Вирішення цього питання передбачає активну участь України у формуванні нових норм міжнародного кримінального права, що регулюють обіг цифрових доказів, і укладання двосторонніх угод про взаємне визнання результатів криміналістичних експертиз.

Отже, подальший розвиток системи документування злочинів проти людяності вимагає одночасного зміцнення правового регулювання, технологічної модернізації, кадрового забезпечення та міжнародної інтеграції. Необхідно перейти від фрагментарної моделі реагування до системної – побудованої на стандартах Римського статуту [11], Протоколу Берклі [2], Європейська мережа судово-експертних установ (ENFSI) [4], практиці ЄСПЛ [5; 6] та етичних принципах використання технологій [7; 9]. Це дозволить Україні створити стійку, самодостатню доказову інфраструктуру, яка забезпечить належне документування злочинів рф, їх ефективну перевірку й представлення у Міжнародному кримінальному суді та майбутньому спеціальному трибуналі.

Документування злочинів проти людяності в діяльності Служби безпеки України є складовою національної системи забезпечен-

ня справедливості, безпеки та дотримання міжнародного права. Воно поєднує процесуально-криміналістичні, контррозвідувальні, оперативно-технічні та цифрові аспекти, що утворюють єдину доказову модель, сумісну з міжнародними стандартами доказування. Ця модель ґрунтується на принципах законності, достовірності, автентичності, пропорційності, відтворюваності й захисту прав людини – тих засадах, які закладені у Римському статуті [11], практиці Міжнародного кримінального суду [12], рішеннях Європейського суду з прав людини [5; 6] та протоколах міжнародних організацій [2; 4; 7].

Сучасний етап розвитку контррозвідувальної діяльності СБУ характеризується зростанням ролі цифрових технологій і алгоритмів аналітичної обробки даних. Використання штучного інтелекту, машинного навчання та систем OSINT істотно підвищує ефективність виявлення, фіксації й перевірки доказів, однак вимагає суворого дотримання етичних і правових меж [7; 9]. Мета цих технологій – не заміна людського судження, а підсилення спроможності контррозвідника, оперативного працівника, аналітика, слідчого та відповідних керівників контррозвідувальних, оперативно-технічних, аналітичних, слідчих та інших спеціальних підрозділів СБУ забезпечити об'єктивність і глибину доказування відповідно до своїх повноважень. З огляду на це доцільно нормативно передбачити створення у Центральному управлінні СБУ, його структурних підрозділах і регіональних органах спеціальних аналітичних підрозділів (або інтеграцію відповідних цифрових технологій та AI-алгоритмів у вже існуючі аналітичні підрозділи) з чітким розмежуванням функцій, доступів і відповідальності, обов'язковими журналами аудиту, підтриманням ланцюга збереження та відтворюваністю результатів.

Служба безпеки України є центральним структурним елементом у національній доказовій архітектоніці – як суб'єкт контррозвідувального документування, який забезпечує отримання первинних фактичних даних, і як партнер міжнародних слідчих органів, що бере участь у створенні спільних доказових баз. Її діяльність інтегрована з роботою Державного бюро розслідувань, Національної поліції, Офісу Генерального прокурора та Міжнародного кримінального суду через систему спільних слідчих груп (*Joint Investigation Teams*) [14] і угоди про співпрацю [10]. Такий формат

взаємодії дозволяє перетворювати національні доказові матеріали на докази, придатні для міжнародного судового розгляду, і забезпечує дотримання вимог до автентичності та ланцюга збереження доказів (*chain of custody*) [4].

Розвиток системи документування злочинів проти людяності потребує подальшої інституційної та технологічної модернізації всіх органів правопорядку й спецслужб України, зокрема Служби безпеки України, та створення єдиної інтегрованої платформи – «Українського центру цифрових доказів» (Ukrainian Evidence Hub), що забезпечуватиме централізоване збирання, маркування, верифікацію, хешування й архівацію матеріалів, отриманих СБУ, ДБР, Нацполіцією, військовими структурами та міжнародними партнерами, із функціонуванням за принципами відкритої взаємодії, застосуванням стандартизованих технічних протоколів Європейської мережі судово-експертних установ (ENFSI) [4] і процедур перевірки, визначених Берклійським протоколом [2], а також із безперервним веденням ланцюга збереження; на практиці це передбачає нормативне закріплення відповідальності за весь цикл оброблення з чітким визначенням компетенції уповноваженого координатора – доцільно покласти такі повноваження на Офіс Генерального прокурора [10], тоді як СБУ має виступати ключовим виробником і первинним верифікатором цифрових доказів (OSINT/SIGINT/документування місця події), інтегруючи власні сховища з Хабом через захищені шлюзи, проводячи попередню технічну атестацію артефактів і забезпечуючи відтворюваність процедур; на мою думку, саме така модель – «координуюча роль ОГП + операційно-аналітична роль СБУ з уніфікованими протоколами ENFSI/Berkeley» – мінімізує фрагментацію, унеможливлює дублювання, гарантує цілісність і відтворюваність доказів та створює передумови для ефективного міжнародного переслідування воєнних злочинів і злочинів проти людяності.

У практичному вимірі документування злочинів проти людяності є не лише складовою слідчої, розвідувальної, контррозвідувальної, оперативно-технічної та іншої спеціалізованої діяльності з фіксації злочинів рф, а й дієвим інструментом відновлення історичної правди, справедливості та міжнародного правопорядку, заснованого на верховенстві права і цивілізованому співіснуванні держав. Кожен задокументований факт – це свідчення про злочини, скоєні

проти українського народу, проти людяності і водночас доказ, який наближає момент міжнародного визнання відповідальності рф. за ці злочини. Зібрані матеріали вже сьогодні формують доказову базу для проваджень у Міжнародному кримінальному суді та національних юрисдикціях інших держав, що здійснюють переслідування за принципом універсальної юрисдикції. Значну увагу слід приділити удосконаленню нормативної бази, зокрема оновленню Закону України «Про Службу безпеки України» [19] у частині, що стосується документування міжнародних злочинів, і розробленню спеціального міжвідомчого положення про порядок цифрової фіксації, зберігання та передачі доказів до міжнародних судових інституцій. Запровадження єдиних стандартів відповідальності, контролю та звітності сприятиме зростанню довіри міжнародних партнерів до української доказової системи.

Важливим напрямом розвитку цифрових технологій і алгоритмів аналітичної обробки даних із використанням штучного інтелекту є *також кадрова спеціалізація в СБУ*. Необхідно розширювати підготовку аналітиків цифрових доказів, експертів з OSINT, фахівців із міжнародного кримінального права та технічних консультантів, які забезпечують перевірку даних. Такі кадри повинні володіти навичками роботи з великими масивами інформації, застосовувати криміналістичні засоби дослідження електронних доказів (інструментами кіберфорензіки) та методи відновлення знищених або прихованих даних. Підготовку кадрів з цифрових технологій і алгоритмів аналітичної обробки даних із використанням штучного інтелекту слід покласти на навчальні заклади СБУ, які мають забезпечити базові й поглиблені програми, а також системні курси підвищення кваліфікації для слідчих, оперативних працівників, аналітиків і керівників усіх рівнів, із повним охопленням викладацького складу. Головним центром такої підготовки та розробником наукових і навчально-методичних кейсів має стати *Національна академія Служби безпеки України*. До підготовки та перепідготовки таких фахівців в навчальних закладах СБУ, слід долучати практичних працівників різних відповідних підрозділів СБУ, які мають практичний досвід роботи з цифровими технологіями і алгоритмами аналітичної обробки даних із використанням штучного інтелекту, а також провідних науковців інших ЗВО МОН та МВС. Системна підготовка таких фахівців має проводитися у співпраці

з Національною академією внутрішніх справ, з Тренінговим центром прокурорів України[4], а також з міжнародними навчальними центрами Міжнародного кримінального суду (МКС) та Агентства ЄС з питань співробітництва у сфері кримінального правосуддя (Євроюст), з яким СБУ має укласти відповідні угоди. Доцільним є також запровадження стажувань для викладачів та відповідних менеджерів навчальних закладів СБУ, задіяних у підготовці фахівців із цифрових технологій та алгоритмів аналітичної обробки даних із використанням штучного інтелекту, у навчальних центрах МКС та Євроюсту.

Таким чином, система документування злочинів проти людяності в діяльності Служби безпеки України виконує стратегічну функцію – вона є ланкою, що поєднує оперативно-службову (контррозвідувальну, оперативно-технічну, аналітичну, кримінально-процесуальну та ін.) діяльність СБУ у взаємодії з іншими органами правопорядку (Державне бюро розслідувань, Національна поліція, органи прокуратури), кримінальне правосуддя й міжнародне право. Подальший розвиток цієї системи має відбуватись за трьома взаємопов'язаними векторами: *нормативним* – через удосконалення законодавства та процесуальних стандартів; *технологічним* – через розбудову цифрової інфраструктури та використання штучного інтелекту; *міжнародним* – через посилення співпраці з Міжнародним кримінальним судом (МКС), Євроюстом, Європолом і Європейською мережею судово-експертних установ (ENFSI). Комплексна реалізація цих напрямів забезпечить створення сталої системи доказового забезпечення процесу розслідування та судового розгляду злочинів агресії, воєнних злочинів і злочинів проти людяності, перетворюючи результати документування на належні й допустимі докази у національних та міжнародних судових інституціях, що є інструментом реалізації принципів справедливості, юридичної відповідальності та міжнародного правового відновлення порушених прав людини, суверенітету й територіальної цілісності України, а також відшкодування завданих матеріальних збитків і компенсації шкоди жертвам війни та їхнім родинам.

[4] Тренінговий центр прокурорів України (*Prosecutor's Training Center of Ukraine*) зареєстровано 10.03.2020. Офіційний сайт: ptcu.gp.gov.ua. До цього в системі прокуратури України функціонувала Національна академія прокуратури України, яку було ліквідовано у 2020 році.

Список використаних джерел:

1. Akayesu, J. Judgment. Prosecutor v. Jean-Paul Akayesu (ICTR-96–4-T). International Criminal Tribunal for Rwanda, 2 September 1998. URL: https://www.ictrcaselaw.org/documents/akayesu/. (Дата звернення 1.09.2025).

2. Berkeley Protocol on Digital Open Source Investigations. OHCHR & UC Berkeley Human Rights Center. Geneva, 2020. URL: https://www.ohchr.org/sites/default/files/Documents/Publications/BerkeleyProtocol.pdf. (Дата звернення 1.09.2025).

3. Court of Justice of the European Union. *Case C-670/22 (M.N.) – EncroChat.* Judgment of 30 April 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0670. (Дата звернення 1.09.2025).

4. ENFSI. Best Practice Manuals – Digital Forensics. European Network of Forensic Science Institutes, 2025. URL: https://enfsi.eu/documents/best-practice-manuals. (Дата звернення 1.09.2025).

5. European Court of Human Rights (Grand Chamber). *Roman Zakharov v. Russia,* no. 47143/06. Judgment of 4 December 2015. URL: https://hudoc.echr.coe.int/eng?i=001–159324. (Дата звернення 1.09.2025).

6. European Court of Human Rights (Grand Chamber). *Big Brother Watch and Others v. the United Kingdom,* nos. 58170/13, 62322/14, 24960/15. Judgment of 25 May 2021. URL: https://hudoc.echr.coe.int/eng?i=001–203614. (Дата звернення 1.09.2025).

7. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Council of Europe, 2018. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. (Дата звернення 1.09.2025).

8. Europol. *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement.* The Hague, 2023. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf. (Дата звернення 1.09.2025).

9. Ligeti, K. et al. *CRIM_AI – Unpacking AI Evidence and (Re-) Defining Authentication in Criminal Justice.* University of Luxembourg, 2024. URL: https://aiandcriminaljustice.uni.lu/wp-content/uploads/sites/260/2024/11/Unpacking-AI-Evidence_Ligeti.pdf. (Дата звернення 1.09.2025).

10. Office of the Prosecutor of the International Criminal Court & Office of the Prosecutor General of Ukraine. *Memorandum of Understanding on Cooperation and Evidence Sharing.* The Hague–Kyiv, March 2023. URL: https://www.icc-cpi.int/news/ukraine-memorandum-of-understanding-signed. (Дата звернення 1.09.2025).

11. Rome Statute of the International Criminal Court. 17 July 1998. URL: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf

12. The Prosecutor v. Bosco Ntaganda. Judgment, ICC-01/04–02/06–2666. International Criminal Court, 8 July 2019. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2019_03568.PDF. (Дата звернення 1.09.2025).

13. Pohoretskyi, M., Cherniak, A., Serhieieva, D., Chernysh, R., & Toporetska, Z. *Detection and proof of cybercrime. Amazonia Investiga.* 2022. 11(53), 259–269. **DOI**: https://doi.org/10.34069/AI/2022.53.05.26 URL: https://amazoniainvestiga.info/index.php/amazonia/issue/archive. (Дата звернення 1.09.2025).

14. Євроюст / Офіс Генерального прокурора України. *Joint Investigation Teams (JIT) for Core International Crimes in Ukraine.* Brussels–Kyiv, 2023. URL: https://www.eurojust.europa.eu/joint-investigation-team-support. (Дата звернення 1.09.2025).

15. Верховний Суд. Постанова Касаційного кримінального суду від 26 січня 2023 р. у справі № 183/3452/19. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/108686155. (Дата звернення 1.09.2025).

16. Закон України «Про Державне бюро розслідувань». URL: https://zakon.rada.gov.ua/laws/show/794–19#Text. (Дата звернення 1.09.2025).

17. Закон України «Про Національну поліцію». URL: https://zakon.rada.gov.ua/laws/show/580–19#Text. (Дата звернення 1.09.2025).

18. Закон України «Про оперативно-розшукову діяльність». URL: https://zakon.rada.gov.ua/laws/show/2135–12#Text. (Дата звернення 1.09.2025).

19. Закон України «Про Службу безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2229–12#Text. (Дата звернення 1.09.2025).

20. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI (із змінами). URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text. (Дата звернення 1.09.2025).

21. Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави: наук. – практ. журнал.* Київ: НАСБУ, 2009. № 2 (2). С. 77–81.

22. Погорецький М.А., Шеломенцев В.П. Кіберзлочини: до визначення поняття. *Вісник прокуратури.* 2012. № 8. С. 89–96.

23. Погорецький М.А., Сергєєва Д.Б. Криміналістична тактика: щодо визначення поняття. *Часопис Національного університету «Острозька академія». Серія «Право».* 2012. № 1 (5). URL: https://lj.oa.edu.ua/articles/2012/n1/12pmasvp.pdf. (Дата звернення 1.09.2025).

24. Погорецький М.А., Сергєєва Д.Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2 (33). С. 137–141. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_34. (Дата звернення 1.09.2025).

25. Погорецький М.А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства України.* 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf. (Дата звернення 1.09.2025).

26. 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. (Дата звернення 1.09.2025).

27. Погорецький М.А. Використання даних EncroChat у кримінальному провадженні: порівняльно-правовий та процесуальний аналіз. *Юридичний науковий електронний журнал.* 2025. № 8. С. 223–229. DOI: https://doi.org/10.32782/2524–0374/2025–8 URL: http://lsej.org.ua/8_2025/48.pdf. (Дата звернення 1.09.2025).

28. Погорецький М.А., Меленті Є.О. Документування атак держави-агресора на об'єкти критичної інфраструктури України: методика інтелектуального аналізу мультисенсорних даних та використання його результатів у кримінальному процесуальному доказуванні. *Право і суспільство.* 2025. № 4. С. 251–274. DOI: https://doi.org/10.32842/2078–3736/2025.4.1.36 URL: http://pravoisuspilstvo.org.ua/archive/2025/4_2025/part_1/. (Дата звернення 1.09.2025).

29. Погорецький М.А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. *Аналітично-порівняльне правознавство*. 2025. № 5. Ч. 3. С. 239–256. DOI https://doi.org/10.24144/2788–6018.2025.05.3.37. URL: https://app-journal.in.ua/wp-content/uploads/2025/10/APP_05_2025_part-3–2.pdf. (Дата звернення 1.09.2025).

30. Погорецький М.А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство.* 2025. № 4. ч. 3. С. 269–279. DOI https://doi.org/10.24144/2788–6018.2025.04.3.40. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42–2.pdf. (Дата звернення 1.09.2025).

31. Погорецький М.А. Верховенство права у кримінальному процесуальному доказуванні: методологія та практика застосування. *Вісник Національної академії правових наук України*. 2025. Т. 32. № 3. С. 275–299 DOI: https://doi.org/10.31359/1993–0909–2025–32–3–275. URL: https://visnyk.kh.ua/uk/journals/visnik-naprnu-3–2025-r/verkhovenstvo-prava-u-kriminalnomu-protsesualnomu-dokazuvanni-metodologiya-ta-praktika-zastosuvannya. (Дата звернення 1.09.2025).

32. Державний хаб збору доказів воєнних злочинів Офісу Генерального прокурора (портал «Warcrimes»). URL: https://warcrimes.gov.ua/en?utm_. (Дата звернення 1.09.2025).