

Стратонов В.М.

Херсонський державний університет

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ВИЯВЛЕННІ ТА ДОКУМЕНТУВАННІ ФАКТІВ ЕКСПЛУАТАЦІЇ ЛЮДИНИ ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ: ДОКАЗОВА БАЗА В МІЖНАРОДНИХ СУДАХ

У зв'язку з ескалацією збройних конфліктів у світі та зростанням кількості злочинів, пов'язаних з експлуатацією цивільного населення, зокрема жінок і дітей, особливої уваги набуває питання ефективного виявлення, фіксації та доказування таких фактів. Ускладненість доступу до місць подій, латентність фактів експлуатації людини вимагають використання новітніх технологій для їх виявлення, документування та подальшої кримінально-правової оцінки. У світлі практики Міжнародного кримінального суду, Європейського суду з прав людини зростає значення цифрових доказів, отриманих з відкритих джерел, супутникових знімків, відеозаписів, даних мобільних пристроїв, блокчейн-технологій тощо.

У статті проаналізовано стандарти допустимості цифрових доказів у справах про експлуатацію людини в умовах збройного конфлікту та обґрунтовано шляхи імплементації відповідних міжнародних практик у кримінальний процес України.

У дослідженні використано порівняльно-правовий, формально-юридичний та структурно-функціональний методи. Аналізувалися норми міжнародного права, стандарти Міжнародного кримінального суду, судової практики Міжнародного трибуналу щодо колишньої Югославії, та положення Кримінального процесуального кодексу України.

У роботі обґрунтовано, що цифрові докази, отримані з відкритих джерел (OSINT), супутникових знімків, відео, метаданих, можуть бути допустимими у міжнародному правосудді за умови дотримання визначених стандартів автентичності, верифікації та збереження. Виявлено відсутність аналогічного механізму в українському процесуальному законодавстві, що унеможливорює належне документування експлуатаційних кримінальних правопорушень.

Узагальнено, що цифрові докази є критичним інструментом у розслідуванні кримінальних правопорушень у сфері експлуатації людини в умовах збройного конфлікту. Досвід Міжнародного кримінального суду підтверджує їх допустимість за умови дотримання міжнародних стандартів – автентичності, цілісності та верифікації. Україна має внести до кримінального процесуального законодавства поняття цифрового доказу, процедури технічної експертизи та перевірки, а також імплементувати стандарти по типу протоколу Берклі для формування доказової бази, визнаної міжнародним правосуддям.

Ключові слова: цифрові докази, електронні докази, супутниковий моніторинг, експлуатація людини, міжнародне гуманітарне право, збройний конфлікт, експертиза, автентичність.

Постановка проблеми. У сучасних умовах збройних конфліктів питання документування порушень міжнародного гуманітарного права, зокрема фактів експлуатації людини, набуло особливого значення в контексті забезпечення ефективного міжнародного кримінального правосуддя. Новизна теми полягає у системному аналізі інтеграції технологічних інструментів – таких як OSINT (Open source intelligence – відкриті джерела розвідки), супутниковий моніторинг, цифрова верифікація доказів, штучний інтелект – у механізми виявлення, фіксації та процесуального доведення випадків примусової праці, сексуального

рабства, залучення дітей до воєнних дій тощо. З огляду на транснаціональний характер таких порушень, застосування технологій є необхідною умовою формування достовірної та прийнятної доказової бази у справах, що розглядаються Міжнародним кримінальним судом, спеціалізованими трибуналами чи регіональними судами.

Аналіз останніх досліджень і публікацій. Стан наукової розробки проблематики застосування цифрових технологій у документуванні фактів експлуатації людини під час збройних конфліктів в українській юридичній доктрині поступово розширюється завдяки працям дослідників,

які досліджують як процесуальні, так і криміналістичні аспекти відповідних правопорушень, серед них зокрема Г.К. Авдєєва, І.В. Гора, Є.В. Діденко, В.А. Колесник, М.І. Пашковський, І.І. Попович, В. М. Стратонов та ін.

Постановка завдання. Мета дослідження полягає в аналізі стандартів допустимості цифрових доказів у справах про експлуатацію людини в умовах збройного конфлікту та обґрунтування шляхів імплементації відповідних міжнародних практик у кримінальний процес України.

Виклад основного матеріалу. У міжнародному кримінальному правосудді цифрові докази стали невід’ємною складовою процесу документування порушень, пов’язаних із експлуатацією людини під час збройних конфліктів. Йдеться насамперед про примусову працю, сексуальне поневолення, торгівлю людьми, використання дітей у збройних формуваннях, які становлять окремі складові злочинів проти людяності та воєнних злочинів. Застосування супутникових знімків, відеоматеріалів, записів з мобільних пристроїв, метаданих та OSINT-технологій суттєво розширило доказову базу у справах, що стосуються експлуатаційного насильства, зокрема в умовах окупації території [3].

У практиці Міжнародного кримінального трибуналу щодо колишньої Югославії цифрові джерела відігравали ключову роль у доведенні системної експлуатації. Так, у справі Прокурор проти Радована Караджича супутникові знімки були використані для підтвердження переміщення населення, руйнування селищ та місць масового утримання цивільних осіб, що, зокрема, включало експлуатацію жінок і дітей [6].

У справі Прокурор проти Душко Тадича були прийняті аудіо- та радіозаписи, що засвідчували координацію дій, пов’язаних із утриманням та примусовим залученням цивільного населення [7].

Міжнародний кримінальний суд (далі – МКС) визнає допустимими цифрові докази про сексуальну експлуатацію, вербування дітей у збройні формування, примусову працю та інші форми поневолення. Ці докази – відео з місця подій, знімки з дронів, дані мобільного трафіку, комунікації в месенджерах – застосовуються у поєднанні з протоколами захисту ланцюга збереження доказів (chain of custody), верифікації метаданих і принципами, викладеними у протоколі Берклі (англ. Berkeley Protocol on Digital Open Source Investigations) [8].

На підставі порівняльного аналізу стандартів оцінки цифрових доказів у практиці МКС та кримінального процесуального законодавства України виявлено суттєві відмінності у нормативному та процесуальному підході до визначення, збирання, верифікації та допустимості такого типу доказів.

Міжнародний кримінальний суд застосовує розгорнуту систему внутрішніх керівництв та процедур, які регламентують використання цифрових доказів у справах про геноцид, злочини проти людяності та воєнні злочини. Зокрема, у практиці Суду визнаються як допустимі цифрові матеріали, отримані з OSINT-джерел, супутникових платформ, соціальних мереж, відеозаписів з мобільних пристроїв, за умови дотримання низки критеріїв. Ключовими серед них є вимоги до автентичності, які забезпечуються шляхом фіксації ланцюга зберігання доказів (chain of custody), верифікації метаданих, використання таких інструментів, як протокол Берклі. Докази визнаються допустимими лише за умови дотримання цих технічних та юридичних гарантій, а також проходження спеціалізованої процедури оцінки достовірності. До розгляду доказів залучаються цифрові аналітики, експерти з верифікації та спеціалісти з інформаційної безпеки. Водночас сторони мають можливість оскаржувати не лише зміст, але й спосіб отримання цифрового доказу, що забезпечує високий рівень процесуального балансу.

На відміну від цього, Кримінальний процесуальний кодекс України не містить ані визначення цифрового доказу, ані спеціалізованої процедури його обробки. Хоча стаття 84 КПК дозволяє використання «інших джерел» доказової інформації, у тому числі технічного характеру [2], чинне законодавство не деталізує стандарти автентичності, не передбачає механізмів перевірки метаданих, не закріплює обов’язкового залучення експертів, а також не визначає спеціального порядку для оскарження таких доказів. У результаті суди в Україні вимушені покладатися на загальні правила допустимості, що не відповідає специфіці цифрових джерел у справах про експлуатацію людини під час збройних конфліктів.

У національному контексті Україна поки не має чіткого правового механізму, який дозволяв би надійно фіксувати та використовувати цифрові докази у справах, що стосуються експлуатації людини в умовах війни. Закон України «Про основні засади забезпечення кібербезпеки України» лише побічно регулює обіг цифрової інформації.

ції [1]. Натомість Кримінальний процесуальний кодекс України не містить визначення «цифрового доказу» та не передбачає спеціальної процедури з його верифікації. Попри те, що стаття 84 КПК визнає допустимість «інших джерел» доказів, відсутність нормативної конкретизації створює складнощі у справах, пов'язаних із використанням супутникових знімків, відеозаписів або OSINT для документування злочинів, пов'язаних з експлуатацією людини.

Судова практика України у цій сфері залишається розрізною. У деяких випадках цифрові матеріали визнаються доказами, але суди не мають чітких критеріїв щодо їхньої автентичності чи допустимості. Це знижує ефективність переслідування експлуатаційних правопорушень у реаліях воєнного стану.

Водночас у національному кримінальному процесуальному законодавстві України зберігається традиційна модель централізованого збору доказів, згідно з якою процес доказування є винятковою компетенцією слідчого або прокурора в межах офіційно відкритого кримінального провадження. Такий підхід закріплений у статтях 93, 223, 224 та інших положеннях Кримінального процесуального кодексу України [2], де чітко визначено процесуальні суб'єкти, уповноважені здійснювати збір доказів, їх фіксацію, вилучення та долучення до матеріалів справи.

Це принципово відрізняється від підходу, що застосовується в міжнародному кримінальному правосудді, зокрема в діяльності Міжнародного кримінального суду, де допустимими визнаються цифрові докази, зібрані не лише процесуальними суб'єктами, а й незалежними організаціями, журналістами, правозахисниками або навіть самими постраждалими, за умови дотримання певних критеріїв автентичності, ланцюга збереження (chain of custody) та технічної верифікації. У зв'язку з цим відкривається ширше поле для збору доказової інформації форс-мажорних обставинах – наприклад, під час окупації територій або в умовах бойових дій, де доступ офіційних слідчих органів України є фізично унеможливленим.

Міжнародна судова практика останніх десятиліть підтверджує: цифрові докази відіграють ключову роль у викритті та доказуванні експлуатації цивільного населення під час збройних конфліктів. Ці докази визнаються допустимими у міжнародних кримінальних провадженнях за умови дотримання встановлених процедур. На рівні доказового аналізу такі матеріали оцінюються за спеціальними стандартами, які охоплю-

ють: достовірність джерела (chain of custody), технічну цілісність (відсутність редагування), автентичність (експертиза метаданих), релевантність до обставин справи та відповідність принципу справедливого судового розгляду. Наприклад, у справі Онгвена Суд визнав, що GPS-файли й відеодокази мали незалежне значення для встановлення як самого факту злочинів, так і контексту примусової участі дітей у бойових діях, що кваліфікується як експлуатація у формі залучення до збройного конфлікту [5]. Інституційна практика МКС також демонструє можливість використання цифрових доказів, отриманих за допомогою OSINT. Наприклад, дані з Twitter, TikTok, YouTube, Google Earth можуть застосовуватись як джерела інформації про місцезнаходження військових об'єктів, рух військових колон або присутність цивільних у районах конфлікту. Але лише за умови дотримання процесуальних гарантій автентифікації.

Для України важливо враховувати зазначені стандарти та механізми під час адаптації національного кримінального процесу до вимог МКС, оскільки цифрові свідчення експлуатації – єдиний реальний механізм документування таких кримінальних правопорушень у зонах, що перебувають під окупацією або в активній фазі бойових дій. Наприклад, у випадках примусової праці цивільного населення на тимчасово окупованих територіях, відеозаписи робіт із символікою російської федерації, фотографії умов проживання, свідчення у соцмережах можуть бути цінними джерелами доказування. Аналогічно – при фіксації використання неповнолітніх для інформаційних кампаній, збройних дій чи побутових завдань у тилу окупаційних сил.

Таким чином, доказова база в міжнародних судах щодо експлуатації під час збройних конфліктів все більше ґрунтується на цифрових доказах, а їх правова оцінка стає одним з найважливіших напрямів судової практики. Це вимагає не лише вдосконалення кримінального процесуального законодавства України, а й формування нових інструментів співпраці з міжнародними інституціями, включаючи механізми фіксації, експертизи та передачі цифрових матеріалів у межах універсальної юрисдикції чи спільних розслідувань.

З урахуванням того, що Україна вже ініціювала розгляд ситуації на своїй території в Міжнародному кримінальному суді у зв'язку з воєнними злочинами та злочинами проти людяності, у тому числі – у сфері експлуатації цивільного населення, особливо актуальним є забезпечення належної

доказової бази, яка відповідатиме міжнародним стандартам допустимості цифрових доказів.

Міжнародна практика демонструє визнання допустимості цифрових матеріалів, отриманих з відкритих джерел – включно з відеозаписами, метаданими, координатами тощо – за умови забезпечення ланцюга збереження (chain of custody), технічної верифікації та експертної оцінки. Аналогічно – докази отримані з OSINT-джерел або мобільних пристроїв, визнаються МКС у справах про залучення дітей до бойових дій, трудову експлуатацію або примусову депортацію.

Отже, першим кроком у напрямі гармонізації українського кримінального процесуального законодавства із міжнародними стандартами є закріплення на рівні КПК: поняття «цифровий доказ» з переліком джерел (OSINT, відео, супутникові знімки, соціальні мережі); стандарти автентичності, релевантності, цілісності, верифікованості та законності походження; обов'язкову участь технічного експерта для аналізу цифрових матеріалів та метаданих; право сторін процесу оскаржувати спосіб отримання цифрових доказів.

Але вагомою зміною має стати впровадження положень, аналогічних протоколу Берклі [8]. Цей Протокол, розроблений за участю Організації Об'єднаних Націй та провідних міжнародних експертів, визначає універсальні стандарти збору, верифікації, збереження та оцінки цифрових доказів, отриманих з відкритих джерел. Його головною метою є забезпечення належної доказової сили таких матеріалів у міжнародному правосудді, з урахуванням принципів автентичності, цілісності, перевіряємості, релевантності та процесуальної доброчесності. Для України імплементація ключових положень цього протоколу могла б стати основою для розробки національних інструкцій, методичних рекомендацій та процесуальних норм щодо роботи з цифровими доказами у справах, пов'язаних із експлуатацією людини під час збройного конфлікту.

Такі зміни дозволять українським органам документувати експлуатацію цивільного населення, зокрема використання дітей у бойових діях, примусову працю, сексуальне поневолення – в умовах окупації, де традиційні докази недоступні. У такому випадку цифрові докази можуть стати ключовим інструментом у розкритті та доведенні фактів експлуатації людини на тимчасово окупованих територіях України, особливо в умовах, коли класичні механізми збирання свідчень – зокрема огляди місця події чи фізичне вилучення речових доказів – є обмеженими або повністю

неможливими. Наприклад, на окупованій території Запорізької або Херсонської областей можуть існувати факти примусового залучення місцевих жителів до роботи на об'єктах російської армії – облаштування окопів, перевезення боєприпасів, прибирання територій, будівництво укріплень – без належної оплати, під загрозою насильства або репресій. Такі випадки необхідно фіксувати: на відео, записаному очевидцем або навіть самими окупантами (що поширюється у відкритому доступі в соціальних мережах: Telegram, TikTok, VK, тощо), де видно цивільних осіб у робочому одязі з символікою російської федерації, які виконують завдання на лінії фронту чи в тилу; за допомогою супутникових знімків, які підтверджують наявність нових об'єктів, що будуються у короткі строки, у поєднанні з геолокаційною інформацією та свідченнями про людський ресурс без офіційної логістики; через метадані мобільних пристроїв, які фіксують пересування осіб у конкретній місцевості в аномальному ритмі (наприклад, регулярне повернення до військових об'єктів), що може вказувати на виконання робіт під примусом; у вигляді дописів у соцмережах з коментарями про побутові умови примусової праці, описами погроз, втратою зв'язку з рідними, що створює елемент психологічної експлуатації.

Інший приклад – залучення неповнолітніх до інформаційної діяльності, зокрема через участь у мітингах або вуличних акціях з пропагандистською метою. Відео таких подій, що містять зображення дітей у формі з російською символікою, з примусовим декламуванням ідеологічних гасел, можуть бути кваліфіковані як залучення до діяльності, яка не відповідає віковим особливостям і порушує право на розвиток і гідність дитини. У разі доведення факту системного характеру таких дій – це може вважатися формою експлуатації. Указані цифрові докази, за умови правильного збирання, верифікації (згідно з протоколами типу Берклі) та забезпечення ланцюга збереження (chain of custody), можуть бути використані у Міжнародному кримінальному суді як докази злочинів проти людяності або воєнних злочинів з елементом експлуатації. Такі матеріали мають потенціал не лише для міжнародних трибуналів, а й для національних проваджень, які ведуться в рамках універсальної юрисдикції іншими державами, що підтримують розслідування злочинів, скоєних на території України.

Висновки. Застосування цифрових технологій у виявленні, фіксації та доказуванні кримінальних правопорушень у сфері експлуатації людини

під час збройних конфліктів є не лише технічним, але й концептуальним зрушенням у системі міжнародного кримінального правосуддя. Досвід Міжнародного кримінального суду та трибуналів свідчить, що у справах про сексуальне рабство, примусову працю, вербування дітей, примусові шлюби та інші форми експлуатаційного насильства саме цифрові докази часто є єдиним засобом встановлення обставин злочину. Їх доказова сила зростає за умови дотримання міжнародно визнаних стандартів автентичності, цілісності, релевантності та законності походження, викладених, зокрема у протоколі Берклі.

Для України, яка фактично стала полем масових порушень прав людини в умовах агресії, особливо важливо адаптувати кримінальне процесуальне законодавство до цих міжнародних стандартів. Визначення дефініції цифрового доказу, унормування chain of custody, запрова-

дження процесуальної участі технічного експерта та створення механізмів верифікації – це базові умови, які забезпечать належне документування злочинів експлуатації на тимчасово окупованих територіях.

Інтеграція сучасних цифрових технологій у кримінальне переслідування експлуатації в умовах збройного конфлікту – це не просто модернізація процесу, а створення нової парадигми доказування, в якій цифрова істина, обґрунтована технічними й правовими процедурами, здатна забезпечити притягнення до відповідальності за найтяжчі злочини проти людяності. Для України це означає можливість ефективної участі у міжнародному правосудді, визнання цифрових матеріалів на рівні Міжнародного кримінального суду та інших міжнародних органів, а також побудову суверенної системи захисту прав людини навіть в умовах війни.

Список літератури:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 09.04.2025).
2. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. – URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 09.04.2025).
3. Матвієнко О. OSINT для журналістів: із чого почати та чим користуватися. НакупілоОсвіта: офіційний сайт. URL: <https://osvita.nakupilo.ua/osint-dlya-zhurnalistiv-iz-chogo-pochaty-ta-chym-korystuvatysya> (дата звернення: 07.04.2025).
4. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. Jurfem: офіційний сайт. – URL: <https://jurfem.com.ua/protokol-berkli-schodo-rozsliduvannia-iz-vykorystanniam-zyfrovych-danych> (дата звернення: 07.04.2025).
5. Decision on the confirmation of charges against Dominic Ongwen (ICC-02/04-01/15-422-Red) від 23 березня 2016 р. Pre-Trial Chamber II, International Criminal Court. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2016_02331.PDF (дата звернення: 09.04.2025).
6. Judgement: Prosecutor v. Radovan Karadžić. Case No. IT-95-5/18-T. 24 March 2016. International Criminal Tribunal for the former Yugoslavia (ICTY). URL: https://www.icty.org/x/cases/karadzic/tjug/en/160324_judgement.pdf (дата звернення: 07.04.2025).
7. Tadić (IT-94-1). Case information. International Criminal Tribunal for the former Yugoslavia : official website. URL: <https://www.icty.org/case/tadic/4> (дата звернення: 07.04.2025).
8. The Berkeley Protocol on Digital Open Source Investigations: A Practical Guide to Human Rights and Criminal Accountability Investigations. Office of the United Nations High Commissioner for Human Rights (OHCHR). 2022. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 07.04.2025).

Stratonov V.M. THE USE OF DIGITAL TECHNOLOGIES IN DETECTING AND DOCUMENTING HUMAN EXPLOITATION DURING ARMED CONFLICTS: EVIDENTIARY BASIS IN INTERNATIONAL COURTS

In light of the escalation of armed conflicts worldwide and the growing number of crimes involving the exploitation of civilians, particularly women and children, the issue of effective detection, documentation, and evidentiary substantiation of such facts has gained critical importance. The limited access to sites of violations and the latent nature of human exploitation necessitate the use of advanced technologies for identification, documentation, and subsequent legal qualification. In the context of the practices of the International Criminal Court and the European Court of Human Rights, the role of digital evidence obtained from open sources, satellite imagery, video recordings, mobile device data, and blockchain technologies is increasingly significant.

The purpose of this research is to analyze the standards for the admissibility of digital evidence in cases of human exploitation during armed conflict and to substantiate pathways for implementing relevant international practices into Ukraine's criminal procedure.

The study employs comparative legal, formal legal, and structural-functional methods. It analyzes norms of international law, standards developed by the International Criminal Court, jurisprudence of the International Criminal Tribunal for the former Yugoslavia, and provisions of the Criminal Procedure Code of Ukraine.

The study substantiates that digital evidence obtained from open sources (OSINT), satellite imagery, video recordings, and metadata may be admissible in international criminal proceedings, provided that authenticity, verification, and preservation standards are met. It identifies the absence of a comparable mechanism in Ukrainian procedural legislation, which prevents comprehensive documentation of exploitation-related criminal offenses.

Digital evidence is a critical tool for investigating criminal offenses related to human exploitation during armed conflict. The experience of the International Criminal Court confirms its admissibility, subject to compliance with international standards of authenticity, integrity, and verification. Ukraine must incorporate the concept of digital evidence into its criminal procedural legislation, including procedures for technical expertise and validation, and adopt standards similar to the Berkeley Protocol to establish an evidentiary framework recognized by international justice.

Key words: *digital evidence; electronic evidence, satellite monitoring; human exploitation; international humanitarian law; armed conflict, expertise, authenticity.*