*УДК 343.985:004.056.53:341.322.5*
*DOI https://doi.org/10.24144/2788-6018.2025.04.3.44*

# ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ЦИФРОВИХ ДОКАЗІВ ВОЄННИХ ЗЛОЧИНІВ: МЕХАНІЗМИ ПРОТИДІЇ COUNTER FORENSICS

**Ткачук Т.Ю.**,
*доктор юридичних наук, професор,*
*учений секретар наукової лабораторії (наукової установи)*
*Українського науково-дослідного інституту*
*спеціальної техніки та судових експертиз*

**Оніщенко В.Г.**,
*провідний науковий співробітник*
*наукової лабораторії (наукової установи)*
*Українського науково-дослідного інституту*
*спеціальної техніки та судових експертиз*

**Ткачук Т.Ю.**, **Оніщенко В.Г. Забезпечення достовірності цифрових доказів воєнних злочинів: механізми протидії counter forensics.**

Вказується, широкомасштабна агресія росії проти України, що розпочалася у 2022 році, спричинила безпрецедентну кількість воєнних злочинів. Щоденно накопичуються тисячі відеосвідчень, фотоматеріалів, аудіозаписів та інших документальних доказів потенційних порушень норм міжнародного гуманітарного права.

У статті здійснено комплексне дослідження проблематики забезпечення достовірності цифрових доказів у контексті документування та розслідування воєнних злочинів, скоєних у період збройної агресії рф проти України. Автор зосереджується на актуальній загрозі застосування технологій counter forensics — навмисних дій, спрямованих на фальсифікацію, маніпулювання або знищення цифрових слідів з метою перешкоджання правосуддю. Визначено ключові категорії цифрових доказів, що використовуються у справах про злочини проти людяності, геноцид, воєнні злочини та злочини агресії, а також їхнє процесуальне значення відповідно до міжнародних стандартів доказування.

Особливу увагу приділено судово-експертним механізмам виявлення та нейтралізації контрфорензичних впливів, включаючи застосування методів цифрової атрибуції, аналізу метаданих, встановлення ланцюга збереження (chain of custody) та використання спеціалізованого програмного забезпечення для судової експертизи. Висвітлено нормативно-правові та методологічні засади судової експертизи цифрових доказів в Україні, з урахуванням її ролі у національній та міжнародній юрисдикції. На основі аналізу практики Міжнародного кримінального суду, Національного центру документування воєнних злочинів, платформи EyeWitness to Atrocities та інших інституцій запропоновано модель комплексного експертного супроводу процесу розслідування з урахуванням викликів, пов'язаних з війною.

У статті обґрунтовано необхідність розроблення спеціалізованих методик цифрової судової експертизи, орієнтованих на встановлення автентичності, цілісності та допустимості цифрових матеріалів у судовому провадженні. Підкреслено важливість міжвідомчої координації, підвищення кваліфікації експертів, розвитку технічної спроможності судово-експертних установ, а також формування єдиної системи протидії інформаційно-аналітичним впливам, що мають ознаки counter forensics.

**Ключові слова:** воєнні злочини, цифрові докази, counter forensics, судова експертиза, інформаційна безпека, цифрова верифікація, міжнародне кримінальне правосуддя, експерт.

**Tkachuk T.Yu., Onishchenko V.G. Ensuring the authenticity of digital evidence of war crimes: forensic mechanisms to counteract counter forensics.**

It is stated that Russia's large-scale aggression against Ukraine, which began in 2022, has caused an unprecedented number of war crimes. Thousands of video testimonies, photographs, audio recordings and other documentary evidence of potential violations of international humanitarian law are accumulating daily.

The article provides a comprehensive study of the issues of ensuring the authenticity of digital evidence in the context of documenting and investigating war crimes committed during the period of

the armed aggression of the Russian Federation against Ukraine. The author focuses on the current threat of the use of counter forensics technologies - deliberate actions aimed at falsifying, manipulating or destroying digital traces in order to obstruct justice. The key categories of digital evidence used in cases of crimes against humanity, genocide, war crimes and crimes of aggression are identified, as well as their procedural significance in accordance with international standards of evidence.

Special attention is paid to forensic mechanisms for detecting and neutralizing counter-forensic influences, including the use of digital attribution methods, metadata analysis, establishing a chain of custody, and using specialized software for forensic examination. The regulatory and methodological principles of forensic examination of digital evidence in Ukraine are highlighted, taking into account its role in national and international jurisdiction. Based on an analysis of the practice of the International Criminal Court, the National War Crimes Documentation Center, the EyeWitness to Atrocities platform, and other institutions, a model of comprehensive expert support for the investigation process is proposed, taking into account the challenges associated with war. The article substantiates the need to develop specialized methods of digital forensic examination focused on establishing the authenticity, integrity, and admissibility of digital materials in judicial proceedings. The importance of interdepartmental coordination, improving the skills of experts, developing the technical capacity of forensic institutions, as well as the formation of a unified system for countering information and analytical influences that have signs of counter-forensics is emphasized.

**Key words:** war crimes, digital evidence, counter forensics, forensic examination, information security, digital verification, international criminal justice, expert.

**Постановка проблеми.** Повномасштабне вторгнення рф до України, що триває з 2022 року, призвела до небаченого обсягу воєнних злочинів. Тисячі відео, фото, аудіозаписів та інших даних щодня фіксують можливі порушення міжнародного гуманітарного права. За даними уповноваженого Верховної Ради з прав людини станом на травень 2025 року зареєстровано понад 167 тисяч воєнних злочинів і злочинів агресії, а обсяг зібраних цифрових матеріалів обчислюється мільйонами файлів [1]. Такі докази відіграють ключову роль у притягненні винних до відповідальності – особливо з огляду на те, що рф систематично заперечує свою вину та поширює дезінформацію, називаючи задокументовані звірства «фейками» чи «постановкою», про що наголошують міжнародні експерти [2]. Отже, питання належного збору, збереження та судового дослідження цифрових доказів набуває першорядної актуальності.

Міжнародна спільнота та Україна реагують на цей виклик впровадженням новітніх підходів до документування воєнних злочинів. Українські прокурори вже застосовують в роботі визнані міжнародні стандарти, зокрема Берклійський протокол цифрових розслідувань (Berkeley Protocol), який було неофіційно перекладено українською й впроваджено в Україні вже в перші тижні після вторгнення [3]. Активно залучаються технологічні інструменти і спеціальні додатки для фіксації доказів, а також об’єднуються зусилля державних органів та громадянського суспільства. У цих умовах зростає роль судових експертів із цифрової криміналістики та водночас виникають нові загрози так званої counter forensics – цілеспрямованого протидіяння судовому встановленню істини шляхом фальсифікації або приховування цифрових слідів. Далі у статті проаналізовано поняття і характеристики цифрових доказів, сучасні експертні підходи до їх дослідження, а також окреслено ризики і методи протидії навмисному спотворенню таких доказів в умовах збройного конфлікту.

**Метою статті** є комплексне дослідження механізмів забезпечення достовірності цифрових доказів у справах про воєнні злочини в умовах зростаючих загроз counter forensics, з акцентом на судово-експертну практику, міжнародні стандарти та виклики, що постають перед українською системою кримінального правосуддя в контексті збройної агресії. Для реалізації визначеної мети передбачається вирішення таких наукових завдань: з’ясувати сутність і специфіку цифрових доказів у справах про воєнні злочини; проаналізувати сучасні загрози контрфорензіки; запропонувати науково обґрунтовані шляхи вдосконалення нормативного регулювання, експертної методики та кібербезпеки для посилення довіри до цифрових доказів у справах про воєнні злочини.

**Аналіз сучасного стану досліджень.** Останні роки позначені активним розвитком досліджень у сфері цифрових доказів воєнних злочинів, зокрема в умовах повномасштабної агресії рф проти України. R. Neilsen (2024) показує, як контрфорензичні дії з боку рф підривають процес міжнародного правосуддя. Про загрозу маніпуляцій deepfake та метаданими також пише J. Lay, наголошуючи на необхідності удосконалення цифрової автентифікації. Українські дослідники (Фігурський, 2023; Зінич, 2025) аналізують допустимість та методологію судової експертизи електронних доказів, а судді Верховного Суду уточнюють правові позиції щодо їх здобуття в міжнародній правовій допомозі. У сфері цифрової криміналістики заслуговує уваги звіт NATO CCDCOE про battlefield forensics, що знайшов відображення і в OSINT-аналізі злочинів (Ricci & Crawford). Ініціативи Eurojust та

проект CyberUA спрямовані на зміцнення спроможності України щодо документування злочинів у цифровому середовищі. Зрештою, як зазначає О. Головіна (2024), штучний інтелект стає перспективним інструментом попереднього аналізу цифрових доказів. Таким чином, сучасна наукова думка сходиться на необхідності інтегрованого підходу до захисту цифрових доказів від counter forensics – із залученням експертизи, міжнародних стандартів і новітніх технологій, що й актуалізує перспективність подальших наукових розвідок за цією тематикою.

**Виклад основного матеріалу.** У правничій доктрині терміни **«цифрові докази»** та **«електронні докази»** часто вживаються як синоніми [4]. Утім деякі дослідники наголошують, що поняття *цифрових* доказів є ширшим, оскільки охоплює всі дані, представлені у числовому (бінарному) форматі, тоді як *електронні* докази фактично означають будь-які докази, отримані з використанням електронних засобів, і за змістом збігаються з цифровими [5]. З урахуванням термінологічних підходів, які використовуються у Berkeley Protocol on Digital Open Source Investigations, документах Міжнародного кримінального суду (МКС), а також рекомендацій НАТО щодо доказової діяльності в умовах спеціальних операцій [6], пропонується системно використовувати саме термін «цифрові докази». Такий підхід дозволяє не лише акцентувати на технологічній природі цих джерел інформації, але й забезпечити узгодженість із міжнародною практикою розслідування міжнародних злочинів.

Узагальнено, цифрові докази слід визначати як будь-які відомості, зафіксовані у цифровій формі, які містять значущу інформацію про обставини вчинення правопорушення та можуть бути використані у кримінальному провадженні в межах доказування. Це охоплює широкий спектр даних, зокрема: електронні документи (тексти, таблиці, електронні листи); фото- та відеоматеріали; аудіофайли; записи камер спостереження; дані з мобільних пристроїв, соціальних мереж, месенджерів; файли журналів систем (log-файли); метадані, геолокаційні мітки, хеши тощо.

Серед основних ознак цифрових доказів виділяють: нематеріальність (існування у вигляді цифрового коду, а не фізичного об’єкта); залежність від спеціальних пристроїв і програмного забезпечення для ідентифікації, перегляду чи зчитування; високу варіативність та тиражованість (копіювання, передавання без втрати змісту); вразливість до змін, де навіть незначне редагування може зруйнувати цілісність або автентичність доказу.

Саме тому критичне значення мають питання забезпечення автентичності, цілісності та простежуваності цифрового доказу (chain of custody), які визначають його допустимість у судовому процесі, зокрема в контексті розслідування воєнних злочинів згідно з вимогами МКС та сучасними рекомендаціями Ради Європи, НАТО і Євроюсту.

Роль цифрових доказів у механізмах міжнародного гуманітарного права та міжнародного кримінального правосуддя неухильно зростає. Якщо традиційно розслідування воєнних злочинів спиралися переважно на свідчення очевидців, речові докази та документи, то в XXI столітті все більшого значення набувають саме цифрові **свідчення злочинів**. Так, фото- і відеоматеріали стали важливими доказами ще в ході Нюрнберзького трибуналу (де демонструвалися кінокадри звірств нацистів), а у 1990-х роках записи зі ЗМІ і супутникові знімки використовувалися Міжнародними трибуналами щодо Югославії та Руанди [7]. Нині ж завдяки соціальним мережам і повсюдному поширенню смартфонів практично кожен інцидент на кшталт удару по цивільному об’єкту майже одразу потрапляє в інтернет. Організації на кшталт **Bellingcat** та **Human Rights Watch** проводять онлайн-розслідування, опрацьовуючи загальнодоступний контент (принцип *OSINT* – розвідка за відкритими джерелами). Натомість спеціалізовані підрозділи, як-от **Evidence Lab** Amnesty International, фокусуються на верифікації відео атак на цивільні об’єкти (лікарні, школи) та фактів застосування забороненої зброї. Вже в найближчому майбутньому відкриті цифрові докази становитимуть ядро розслідувань найбільш тяжких злочинів, про що свідчить і стратегія Міжнародного кримінального суду: за оцінками експертів, відкриті джерела формуватимуть суттєву частину доказової бази майже в усіх провадженнях МКС у найближчі роки [8].

Разом з тим, активне залучення цифрових доказів породжує нові виклики. На відміну від фізичних речових доказів, цифрові дані легко копіюються, можуть бути викривлені через технічні збої чи навмисну фальсифікацію, потребують спеціальних методів зберігання (резервування, захист від несанкціонованого доступу). Міжнародне право станом на сьогодні не містить окремих матеріальних норм щодо «цифрових доказів», однак процесуальні режими поступово адаптуються. Приміром, Комітет міністрів Ради Європи ще у 2022 р. прийняв рекомендації для держав щодо посилення можливостей правоохоронних органів у збиранні та збереженні електронних доказів воєнних злочинів, наголосивши на важливості їх автентифікації та належного документування (щоб відповідали стандартам судочинства). В Україні законодавство також розвивається у цьому напрямку: внесено зміни до процесуальних кодексів, якими врегульовано порядок подання електронних доказів у суді, забезпечено можливість їх дослідження в електронній формі тощо. Таким

чином, теоретичні напрацювання та міжнародний досвід задають вектор: цифрові докази повинні розглядатися як рівноправні із традиційними, але до них слід застосовувати спеціальні заходи для гарантування достовірності та збереження.

У кримінальних провадженнях щодо воєнних злочинів цифрові докази піддаються оцінці як на етапі досудового слідства, так і безпосередньо в суді. Для встановлення автентичності, джерела походження та інших обставин, пов'язаних із цифровими даними, можуть призначатися спеціальні комп'ютерно-технічні експертизи.

Предметом комп'ютерно-технічних експертиз є дослідження змісту та властивостей електронних носіїв інформації – скажімо, вилучених телефонів, ноутбуків, жорстких дисків, серверів тощо – а також конкретних файлів або записів. Експерт може встановлювати, чи зазнавав файл змін, коли і яким пристроєм було зроблено фото або відео, чи відповідає вміст метаданим, чи певний обліковий запис (профіль) створював той чи інший допис у соцмережі, чи співпадають два зображення (наприклад, з різних джерел) як оригінал і копія, і багато інших питань. Методичне забезпечення таких експертиз перебуває в стані розвитку: українські фахівці переймають міжнародний досвід, створюються нові методики перевірки відеомонтажу, оцінки достовірності скриншотів і т.д. Проте наразі все ще бракує уніфікованих стандартів – багато в чому експерти керуються загальними принципами криміналістики та власним досвідом.

Сама можливість використання електронних доказів у судових процесах закріплена у процесуальному законодавстві України. Наприклад, Кримінальний процесуальний кодекс (ч. 2 ст. 99) відносить до доказів «*будь-які відомості… незалежно від носія*», а останніми змінами уточнено, що електронні носії інформації можуть розглядатися як речові докази. У цивільному та адміністративному судочинстві прямо визначено поняття електронних доказів. Втім, не врегульованим до кінця залишається процес перевірки автентичності цифрових матеріалів. На практиці нерідко сторони кримінального провадження заявляють клопотання про проведення експертизи електронних доказів – наприклад, фототехнічної (для встановлення факту монтажу зображення) чи портретної (для ідентифікації особи на відео). Водночас Верховний Суд вже висловив позицію, що **призначення експертизи не є обов'язковим, якщо особу на відеозаписі й так можна чітко ідентифікувати** [9]. Такий підхід спрощує використання цифрових доказів, коли їх зміст є очевидним і не викликає сумнівів.

У світовій практиці питання допустимості цифрових (електронних) доказів у суді також вирішується шляхом підтвердження їх автентичності через експертні висновки або сертифіковані технологічні рішення. Так, у багатьох країнах діють керівництва для правоохоронців щодо збору й зберігання електронних доказів (наприклад, стандарти SWGDE у США [10], рекомендації Європолу тощо). Створено міжнародні протоколи, як-от вже згаданий Berkeley Protocol on Digital Open Source Investigations – перший глобальний звід професійних стандартів поводження з відкритими цифровими доказами. Цей документ визначає мінімальні вимоги до ідентифікації, збору, верифікації та збереження відкритої інформації з прицілом на її використання у міжнародних кримінальних розслідуваннях. Виконання таких стандартів підвищує шанси, що суд визнає цифрові матеріали допустимими. Показово, що Верховний Суд України у 2024 році прямо послався на Берклійський протокол як на **«міжнародний еталон архівації цифрової інформації»**, вимагаючи його дотримання при отриманні доказів у співпраці з іноземними юрисдикціями [11].

На міжнародному рівні напрацьовано також механізми спільного розслідування воєнних злочинів із активним використанням цифрових доказів. Яскравий приклад – спільна слідча група (Joint Investigation Team, JIT) за участі України, кількох держав ЄС та Міжнародного кримінального суду, створена за підтримки *Eurojust* через три тижні після початку вторгнення рф [12]. У рамках цієї співпраці в лютому 2023 року Eurojust запустив центральну базу даних доказів основних міжнародних злочинів (CICED) – спеціалізований захищений реєстр для зберігання і аналізу доказів воєнних злочинів [13]. CICED дозволяє правоохоронцям різних країн обмінюватися доказовою інформацією та перевіряти, чи є потрібні дані в розпорядженні партнерів. Протягом першого року роботи до CICED було подано понад 3700 файлів доказів з 16 країн. Схожі ініціативи демонструють міжнародний підхід: замість ізольованого зберігання даних у кожної юрисдикції – створення спільних просторів і застосування єдиних експертних підходів.

Окрім цього, в 2023 р. *Europol* створив спеціальну **OSINT Task Force** для допомоги в розслідуванні воєнних злочинів в Україні, а Рада Європи реалізує проект **CyberUA** щодо підсилення спроможності українських органів працювати з електронними доказами воєнних злочинів [14]. Отже, міжнародний досвід рухається в напрямку стандартизації, співпраці та впровадження високих технологій у експертизу цифрових доказів. Для України важливо переймати ці найкращі практики, щоб забезпечити належний рівень доказування у справах про злочини проти людяності та воєнні злочини.

Зі зростанням значення цифрових доказів з'являються і нові способи протидії їх ефективному використанню – так звана **контрфорензіка** (counter-forensics). Це сукупність навмисних дій, спрямованих на знищення, спотворення або дискредитацію цифрових слідів злочинів з метою уникнення відповідальності. Розглянемо ключові загрози: (1) підробка або фальсифікація цифрових доказів, (2) маніпулювання метаданими, (3) інші технічні засоби протидії фіксації та розслідуванню.

Сучасні досягнення в галузі штучного інтелекту дозволяють відносно легко створювати *«діпфейки»* – синтетичні зображення, відео чи аудіо, що імітують реальні і подекуди майже непомітні для нефахівця. Якщо раніше виготовлення переконливого фальшивого відео вимагало значних зусиль, то тепер існують загальнодоступні інструменти, що спрощують такі маніпуляції [15]. У контексті воєнних злочинів цифрові технології створюють нові виклики для розслідування, зокрема можливість інформаційних операцій із фальсифікації доказів. Російські спецслужби потенційно можуть впроваджувати штучно згенеровані фото та відео, які або дискредитують українських військових, або виправдовують дії агресора. Використання технологій штучного інтелекту для створення аудіо- та відеодіпфейків може поставити під сумнів автентичність доказової бази, ускладнюючи процес притягнення винних до відповідальності.

Окрім маніпуляції візуальними даними, загрозою є зміни метаданих цифрових файлів – важливих атрибутів, що містять інформацію про час і місце створення, технічні параметри та історію редагування. Кіберзлочинці застосовують тактику timestomping, переписуючи часові мітки, щоб дезорієнтувати слідство. Водночас цифрова криміналістика здатна виявляти невідповідності та аномалії, що підтверджують факт втручання.

Додаткові ризики пов'язані з хакерськими атаками на сховища цифрових доказів. У 2023 році російські групи, пов'язані з ФСБ і ГРУ, намагалися проникнути в інформаційні системи Офісу Генпрокурора України та Міжнародного кримінального суду, що могло дозволити їм знищити, викрасти або сфальсифікувати дані. Успішний злам бази доказів підриває її довіру в суді, створюючи юридичні підстави для оскарження автентичності матеріалів.

Окрім цифрових атак, використовуються методи фізичного блокування збору доказів: знищення камер спостереження, глушіння мобільного зв'язку перед скоєнням злочинів, застосування месенджерів із самознищенням повідомлень. Попри ці складнощі, міжнародні слідчі та правозахисники розробляють нові технології виявлення та відновлення доказів, зокрема шляхом аналізу супутникових знімків і трофейних пристроїв.

Протидія counter forensics вимагає постійного вдосконалення цифрової криміналістики та кібербезпекових заходів для гарантування достовірності доказів воєнних злочинів. Саме тому цифровий доказ слід розглядати не лише як файл, а як комплексний процес його здобуття, обробки та правомірного використання. Цифровий доказ – це перш за все процес його легального здобуття, оброблення та правомірного використання. Ця теза підкреслює, що ключовим аспектом є не тільки зміст доказу, а й забезпечення його автентичності та допустимості через чітке дотримання процедурних стандартів.

Відповідно, цифрові докази набувають статусу повноцінного доказового матеріалу лише за умови їх коректного збору, належної реєстрації та збереження. Будь-які відхилення від процедури – невідоме або сумнівне джерело, відсутність оригінального файлу, ознаки редагування або маніпуляції – можуть поставити під сумнів їхню доказову цінність. Особливо критичним є питання достовірності цифрового контенту у справах про воєнні злочини, де інформаційні операції та counter forensics можуть бути використані для дискредитації автентичних доказів чи створення фальсифікованих матеріалів.

У цьому контексті важливу роль відіграє міжнародна практика цифрової криміналістики та експертної оцінки. Зокрема, стандарти обробки цифрових доказів, що застосовуються Міжнародним кримінальним судом, Європейським судом з прав людини та іншими юрисдикціями, визначають чіткі механізми перевірки автентичності, цифрової атрибуції та верифікації джерела отримання даних. Саме відповідність цим стандартам забезпечує правомірне використання цифрових доказів у судових процесах та їхню інтеграцію в міжнародну систему правосуддя.

Таким чином, питання судової експертизи цифрових доказів виходить за межі суто технічного аналізу та включає комплекс процедурних гарантій, спрямованих на захист їхньої доказової сили. Подальший розвиток методів цифрової криміналістики, удосконалення нормативного регулювання та міжнародної співпраці є критично важливими для забезпечення ефективного розслідування складних злочинів, зокрема у воєнних конфліктах.

Зростаючий обсяг та складність доказової бази у справах про воєнні злочини вимагають активного залучення новітніх технологій та спеціальних знань для їх обробки. Серед перспективних напрямів – ширше використання штучного інтелекту (ШІ) для автоматизації аналізу, впровадження блокчейн-технологій для гарантування цілісності даних та розвиток інструментів незалежної верифікації цифрових доказів.

AI-алгоритми вже допомагають українським правоохоронцям у фільтрації великих масивів даних, зокрема через машинне навчання для класифікації відеозаписів, розпізнавання обличчя і озброєння, а також автоматичне перетворення аудіо на текст. Хоча повна автоматизація розслідувань неможлива, технології можуть значно прискорити первинний аналіз та сортування доказів [16]. Особливо актуальним є використання AI для виявлення діпфейків та маніпуляцій з цифровими файлами: новітні алгоритми аналізують піксельні аномалії, відблиски, частотні характеристики голосу, проте їхня ефективність залежить від безперервного вдосконалення.

Ще одним важливим напрямом є блокчейн та криптографія для захисту доказів. Блокчейн, як розподілений реєстр, забезпечує незмінність інформації, що може бути використано для збереження цифрових доказів воєнних злочинів. Наприклад, проєкт Starling Lab хешує фото та відео, записуючи їх у блокчейн-мережі, унеможливлюючи непомітну зміну даних. Водночас ця технологія має обмеження: якщо у блокчейн занесено сумнівний файл, сам факт його захисту не гарантує достовірність.

Попри технічні виклики, тенденція до інтеграції AI та блокчейну в судову експертизу набирає обертів. У перспективі ці інструменти можуть стати стандартом для правозахисних організацій та міжнародних судів у боротьбі з маніпуляціями та знищенням цифрових доказів.

Перспективним напрямом розвитку ~~цифрової судової експертизи~~ є створення єдиних стандартів оцінки цифрових доказів та інтегрованих платформ для їхньої верифікації. Наразі перевірка автентичності матеріалів здебільшого здійснюється вручну або в межах окремих OSINT-спільнот, що обмежує масштабованість процесу. У зв'язку з цим виникає потреба у централізованій системі, яка забезпечувала б одночасну перевірку сумнівних матеріалів кількома незалежними модулями—AI-алгоритмами, сертифікованими судовими експертами та волонтерськими аналітичними мережами для геолокації та технічного аналізу. Подібні ініціативи, як-от EyeWitness, Mnemonic та Bellingcat, уже функціонують, проте бракує єдиного механізму, який акумулював би процес підтвердження достовірності доказів.

Цікавим концептом є створення глобального реєстру **підтверджених воєнних злочинів**, де кожен задокументований епізод отримував би унікальний цифровий ідентифікатор із відповідними маркерами автентичності доказів: «не перевірено», «підтверджено експертом», «верифіковано судом» тощо. Такий реєстр міг би стати важливим ресурсом для прокурорів, істориків та громадськості, забезпечуючи цілісну картину воєнних злочинів у цифровому форматі, що слугуватиме як доказова база для міжнародних судових процесів, так і меморіальний запис для майбутніх поколінь.

Реалізація подібних проєктів потребує значних ресурсів, часу та міжнародної співпраці. Сучасний підхід до документування воєнних злочинів в Україні залишається фрагментованим: різні платформи та архіви працюють автономно, бракує координації та уніфікованих стандартів оцінки доказів. Подолати ці виклики можливо шляхом інтеграції сучасних технологій та стандартизації процесів. Україна, яка вимушено стала полігоном для апробації новітніх методів документування злочинів, водночас має шанс створити прецедент технологічно підкріпленого правосуддя, що унеможливить уникнення відповідальності воєнними злочинцями.

**Висновки.** Документування воєнних злочинів у цифрову еру складний та багатоаспектний процес, що потребує злагодженої співпраці юристів, технічних експертів і міжнародної спільноти. Аналіз сучасних практик дозволяє окреслити кілька ключових висновків:

**Цифрові докази як невід'ємний елемент судових проваджень** В умовах війни в Україні цифрові матеріали набули особливого значення через масову фіксацію злочинів на камери та мобільні пристрої. Держава та суспільство адаптуються до нових викликів: впроваджено онлайн-платформи для збору доказів, налагоджено співпрацю з волонтерами, узгоджено процесуальні норми, що дозволяють використовувати електронні матеріали як повноцінні докази. Верховний Суд підтвердив, що цифрові докази мають оцінюватися за загальними принципами належності, допустимості та достовірності, без дискримінації порівняно з традиційними видами доказів.

**Counter forensics як новий виклик.** Держава-агресор не лише вчиняє воєнні злочини, а й намагається приховати або викривити інформацію про них—від класичних методів пропаганди до кібератак на сховища доказів та створення високотехнологічних фейків. Це вимагає посилення заходів кібербезпеки, зокрема захисту реєстрів цифрових доказів, резервування даних та розробки методів виявлення маніпуляцій. Перевірка автентичності цифрових доказів має бути комплексною—поєднувати технічну експертизу з аналітичним аналізом змісту.

**Інновації та міжнародна координація як основа розвитку** Штучний інтелект, великі дані та блокчейн-технології набувають прикладного значення в судовій експертизі. Їх впровадження потребує інституційної підтримки: створення навчальних програм для слідчих, спеціалізованих лабораторій та єдиної моделі архівування доказів. Як наголошують фахівці, наразі бракує центра-

лізованої системи управління доказами, що гармонізує зусилля різних гравців. Формування такої моделі є питанням найближчого майбутнього, яке сприятиме не лише ефективному розслідуванню воєнних злочинів, а й збереженню історичної пам'яті – створенню цифрового меморіалу страждань українського народу.

Міжнародні стандарти, зокрема Берклійський протокол, уже застосовуються на практиці та довели свою ефективність. Розвивається міжнародна координація: створюються спільні слідчі групи, централізовані бази даних (CICED), OSINT-коаліції, що стають новими інструментами правосуддя. Україна активно інтегрується в ці процеси та водночас продукує власні інновації, зокрема масштабне залучення громадських доказів і проведення дистанційних експертиз.

На завершення слід зазначити, що цифрові докази є не лише потужним інструментом, а й великою відповідальністю. Вони дають змогу викривати злочини та демонструвати правду світові, проте їхнє юридичне значення залежить від ретельного процесу збору, обробки та верифікації. Україна вже активно розвиває механізми судової експертизи цифрових доказів, закладаючи фундамент для майбутньої системи правосуддя, яка унеможливить безкарність воєнних злочинців. Використовуючи найкращі міжнародні практики та технологічні рішення, ми наближаємо день, коли цифрові докази стануть невідворотним вироком агресору.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**


1. Лубінець розповів, скільки воєнних злочинів зареєстровано з початку війни. КореспонденТ net. 18.-5.2025р. URL: https://ua.korrespondent.net/ukraine/4782590-lubinets-rozpoviv-skilky-voiennykh-zlochyniv-zareiestrovano-z-pochatku-viiny.
2. Rhiannon Neilsen File Not Found: Russia Is Hacking Evidence of Its War Crimes. War on the rocks. May 14, 2024 URL: https://warontherocks.com/2024/05/file-not-found-russia-is-hacking-evidence-of-its-war-crimes/#:~:text=Even%20breaching%20the%20database%20without,altogether%20due%20to%20insufficient%2C%20unclear.
3. Developing the Berkeley Protocol. Berkeley Human Rights Center URL: https://humanrights.berkeley.edu/projects/developing-the-berkeley-protocol-on-digital-open-source-investigations/#:~:text=The%20Berkeley%20Protocol%20is%20actively,foundation%20of%20our%20%2010.
4. Фігурський В.М. Докази в електронній формі у кримінальному провадженні. Галицькі студії: Юридичні науки. № 4. 2023. URL: https://journals.gi.ternopil.ua/ index.php/law/article/view/50.
5. Зінич Л.В. Судова експертиза цифрових доказів у справах про плагіат: методологія та проблеми доказування. Науковий вісник Ужгородського Національного Університету, 2025Серія ПРАВО. Випуск 88: частина 3 URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/05/40-2.pdf.
6. Väisänen, T., Braccini, C., Sadloň, M., Bahşi, H., Panico, A., van der Meij, K., & Huis in 't veld, M. (2016). *Battlefield Digital Forensics: Digital Intelligence and Evidence Collection in Special Operations*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/sites/default/files/multimedia/pdf/BDF_Battlefield_Digital_Forensics_final.pdf.
7. Andrea Ricci Jack Crawford Puzzling Pieces: OSINT and War Crime Accountability in Ukraine. RUSI URL: https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine#:~:text=Since%20the%20aftermath%20of%20the,2001%20and%20Lebanon%20in%202009.
8. Jay D. Aronson, Enrique Piracés To what extent can cyber evidence repositories, and digital and open—source evidence, facilitate the work of the OTP, and the ICC more generally? ICC forum (is an online legal journal and world-wide discussion forum) URL: https://iccforum.com/cyber-evidence#:~:text=How%20Can%20Cyber%20Evidence%20Help,undertakes%20in%20the%20near%20future.
9. Суддя ВС проаналізувала критерії допустимості й достовірності електронних доказів у кримінальному процесі. Юридична газета. 07 лютого 2025 URL: https://yur-gazeta.com/golovna/suddya-vs-proanalizuvala-kriteriyi-dopustimosti-y-dostovirnosti-elektronnih-dokaziv-u-kriminalnomu-p.html.
10. Scientific Working Group on Digital Evidence. SWGDE URL: https://www.swgde.org.
11. Суддя ВС у ККС окреслила правові позиції ВС щодо процесуальних особливостей здобуття електронних доказів у межах міжнародної правової допомоги та їх використання у кримінальному провадженні. Судово-психологічна експертиза. Застосування поліграфа і спеціальних знань в юридичній практиці. Он-лайн журнал. 29.05.2025. URL: https://expertize-journal.org.ua/zovnishni-novyny/15465-suddya-vs-u-kks-okreslila-pravovi-poziciyi-vs-shodo-

procesualnih-osoblivostej-zdobuttya-elektronnih-dokaziv-u-mezhah-mizhnarodnoyi-pravovoyi-dopomogi-ta-yih-vikoristannya-u-kriminalnomu-provadzhenni.
12. Three years since the full-scale invasion of Ukraine: Concrete steps supported by Eurojust on the road to accountability. European Union Agency for Criminal Justice Cooperation. 24.02.2025 URL: https://www.eurojust.europa.eu/news/three-years-full-scale-invasion-ukraine-concrete-steps-supported-eurojust-road-accountability#:~:text=Since%20the%20outbreak%20of%20the,Understanding%20with%20the%20United%20States.
13. Core International Crimes Evidence Database. European Union Agency for Criminal Justice Cooperation. URL: https://www.eurojust.europa.eu/core-international-crimes-evidence-database.
14. CyberUA: Посилення спроможності щодо електронних доказів воєнних злочинів та грубих порушень прав людини в Україні. Офіс Ради Європи в Україні URL: https://www.coe.int/uk/web/kyiv/cyberua.
15. Jerry Lay Evidence Tampering, Deepfakes, Image Manipulation and the Impact on Digital Forensic Authentication. URL: https://www.fticonsulting.com/insights/articles/deepfakes-evidence-tampering-digital-forensics#:~:text=Legal%20teams%20and%20digital%20forensics,facts%20and%20reaching%20fair%20resolutions.
16. Golovina O. Artificial Intelligence and War Crimes Investigations. Institute for war & peace reporting. 30 January, 2024. URL: https://iwpr.net/global-voices/artificial-intelligence-and-war-crimes-investigations#:~:text=Although%20only%20in%20its%20early,they%20are%20being%20presented%20with.