УДК 35:004.9:343.3/7
DOI https://doi.org/10.32782/2521-6473.2026-1.20

Ю. В. Цуркан-Сайфуліна, докторка юридичних наук,
професорка кафедри загальнотеоретичної юриспруденції
та прав людини Чернівецького навчально-наукового
юридичного інституту Національного університету
«Одеська юридична академія»
ORCID: 0000-0003-3125-4655

В. В. Грисюк, доктор філософії в галузі 081 «Право»,
викладач Чернівецького фахового коледжу
Київського університету інтелектуальної власності та права
ORCID: 0009-0005-9036-0222

ПРАВОВА РЕГЛАМЕНТАЦІЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ МЕТОДІВ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

У статті проаналізовано правові засади цифрової трансформації методів документування воєнних злочинів у контексті сучасних збройних конфліктів та розвитку інформаційних технологій. Здійснено комплексне осмислення змін у підходах до фіксації, збирання, збереження та перевірки відомостей про грубі порушення норм міжнародного гуманітарного права, що відбуваються під впливом цифровізації доказової діяльності. Визначено, що в умовах обмеженого фізичного доступу до місць подій, масштабних руйнувань та високої динаміки бойових дій цифрові методи набувають системного значення й формують нову модель створення доказової бази, здатної забезпечити процесуальну стійкість і надійність зібраних матеріалів.

У межах дослідження здійснено аналіз механізмів, які дозволяють трансформувати інформацію технічного походження у юридично значущі докази за умови дотримання вимог автентичності, цілісності та простежуваності. Визначено роль процедур контролю за обігом цифрових матеріалів як ключового чинника забезпечення довіри до результатів документування та недопущення втрати або спотворення інформації. Окрему увагу приділено взаємозв'язку між національними підходами та міжнародними стандартами, що сприяють уніфікації практик цифрового документування та підвищенню ефективності правозастосування.

Також здійснено узагальнену характеристику використання відкритих інформаційних ресурсів і спеціалізованих цифрових систем у процесі фіксації воєнних злочинів. Визначено, що такі інструменти розширюють можливості встановлення обставин подій, ідентифікації причетних осіб і відтворення просторово-часових параметрів злочинних дій без безпосередньої присутності на місці події. Зроблено висновок, що ефективність цифрової трансформації методів документування безпосередньо залежить від рівня нормативної узгодженості, методологічної визначеності та інтегрованості цифрових рішень у загальну систему кримінального правосуддя. Такий підхід створює передумови для посилення спроможності правових механізмів реагувати на виклики сучасних конфліктів і забезпечувати невідворотність відповідальності за воєнні злочини.

Ключові слова: *документування, воєнні злочини, електронні документи, документальна інформація, верифікація документальної інформації, міжнародне правосуддя, відкриті джерела інформації, нформаційно-документаційні системи.*

Yu. V. Tsurkan-Saifulina, V. V. Hrysyuk. Legal regulation of digital transformation of war crimes documentation methods

The article analyzes the legal principles of the digital transformation of the methods of documenting war crimes in the context of modern armed conflicts and the development of information technologies. A comprehensive understanding of changes in approaches to recording, collecting, preserving, and verifying information on gross violations of international humanitarian law norms that occur under the influence of digitization of evidentiary activities has been carried out. It was determined that in the conditions of limited physical access to the places of events, large-scale destruction and high dynamics of hostilities, digital methods acquire systemic importance and form a new model of creating an evidence base capable of ensuring the procedural stability and reliability of the collected materials.

Within the framework of the study, an analysis of the mechanisms that allow transforming information of technical origin into legally significant evidence, provided that the requirements of authenticity, integrity and traceability are met. The role of control procedures for the circulation of digital materials is defined as a key factor in ensuring trust in the results of documentation and preventing the loss or distortion of information. Particular attention is paid to the relationship between national approaches and international standards, which contribute to the unification of digital documentation practices and increase the effectiveness of law enforcement.

A generalized characterization of the use of open information resources and specialized digital systems in the process of recording war crimes was also carried out.It was determined that such tools expand the possibilities of establishing the

circumstances of the events, identifying the persons involved and reproducing the spatio-temporal parameters of criminal acts without being directly present at the scene. It was concluded that the effectiveness of the digital transformation of documentation methods directly depends on the level of regulatory coherence, methodological certainty and integration of digital solutions into the general system of criminal justice. This approach creates prerequisites for strengthening the capacity of legal mechanisms to respond to the challenges of modern conflicts and ensure the inevitability of responsibility for war crimes.

Key words: *documentation, war crimes, electronic documents, documentary information, verification of documentary information, international justice, open sources of information, information and documentation systems.*

Постановка проблеми. Актуальність дослідження зумовлена суттєвими трансформаціями, що відбуваються у сфері документування воєнних злочинів під впливом стрімкого розвитку цифрових технологій та ускладнення характеру сучасних збройних конфліктів. Традиційні методи фіксації та збирання доказів дедалі частіше виявляються недостатніми для забезпечення повноти, об'єктивності й оперативності розслідувань, особливо в умовах обмеженого доступу до територій, високої динаміки бойових дій та активного використання інформаційних маніпуляцій. За таких обставин цифрові засоби документування набувають визначального значення, оскільки дозволяють акумулювати значні масиви інформації з різних джерел, забезпечувати їх збереження та подальшу процесуальну обробку. Водночас ефективне застосування таких інструментів потребує належного правового врегулювання, здатного гарантувати трансформацію технологічних даних у юридично значущі та допустимі докази.

Додаткову актуальність дослідження зумовлює необхідність узгодження національних підходів до цифрового документування воєнних злочинів із загальновизнаними міжнародними стандартами правосуддя. В умовах зростання ролі цифрових доказів у кримінальному переслідуванні за найтяжчі міжнародні злочини особливої ваги набувають питання правової визначеності, дотримання процесуальних гарантій, забезпечення автентичності та цілісності інформації. Відсутність системного наукового осмислення правової регламентації цифрової трансформації методів документування може призвести до фрагментарності правозастосовної практики та зниження ефективності розслідувань. У зв'язку з цим виникає об'єктивна потреба у комплексному дослідженні правових засад використання цифрових технологій у процесі фіксації воєнних злочинів як необхідної умови забезпечення принципу невідворотності відповідальності.

Мета статті полягає у дослідженні правової регламентації цифрової трансформації методів документування воєнних злочинів, визначенні її ключових принципів та напрямів розвитку, а також у з'ясуванні ролі цифрових технологій у формуванні процесуально придатної доказової бази в національному та міжнародному кримінальному судочинстві.

Виклад основного матеріалу. Цифрова трансформація методів документування воєнних злочинів у сучасних збройних конфліктах постає як фундаментальний зсув у парадигмі міжнародного кримінального правосуддя, який безпосередньо впливає на ефективність реалізації принципу невідворотності кримінальної відповідальності за найтяжчі порушення норм міжнародного гуманітарного права та міжнародного кримінального права. В умовах збройної агресії рф проти України, а також у контексті інших сучасних конфліктів, традиційні засоби збирання доказів, що ґрунтуються переважно на показаннях свідків, матеріалах огляду місця події та судово-медичних експертизах, дедалі частіше виявляються недостатніми з огляду на масштабність руйнувань, обмежений доступ до окупованих територій та зони бойових дій, систематичне знищення матеріальних слідів злочинів та динамічність бойових дій, інформаційних атак ворога і поширення рейкових повідомлень та ін. За таких умов цифровізація процесу документування воєнних злочинів набуває не допоміжного, а системоутворювального значення, трансформуючи його у високотехнологічну, багаторівневу та юридично верифіковану модель формування доказової бази.

Основним фундаментом реалізації концепції цифрової трансформації у сфері міжнародного правосуддя є розбудова чіткої та несуперечливої правової регламентації, яка б дозволяла трансформувати технологічні дані у юридично значимі докази. В умовах повномасштабної агресії, яку здійснює росія, правове регулювання документування воєнних злочинів в Україні зазнало суттєвої еволюції, що відображається у гармонізації національного законодавства із міжнародними стандартами.

Правову основу цього процесу складають положення ст.ст. 9 та 99 Кримінального процесуального кодексу України, які у своїй сукупності легітимізують використання інноваційних технологій у кримінальному судочинстві. Зокрема, ст. 9 КПК України встановлює обов'язок всебічного та неупередженого дослідження обставин провадження, що в сучасних реаліях вимагає залучення супутникового спостереження, аналізу відкритих джерел інформації та тривимірного моделювання місць руйнувань для забезпечення повноти доказової бази. Важливим елементом є визнання пріоритету міжнародних договорів та практики Європейського суду з прав людини, що дозволяє інтегрувати передові світові стандарти цифрової криміналістики, такі як Берклійський протокол, у національну юридичну практику [1]. В свою чергу, процесуальне закріплення цифрових даних реалізується через ст. 99 КПК України, яка визначає комп'ютерні дані, матеріали фотозйомки та відеозапису як повноцінні доказові документи [1]. Ключовою новелою у законодавстві є прирівнювання відображення електронного документа до його оригіналу та визнання копій комп'ютерних даних, виготовлених із залученням спеціалістів, автентичними доказами, що дозволяє ефективно

використовувати технологію блокчейн для захисту метаданих та гарантувати незмінність цифрового ланцюга збереження доказів від моменту фіксації до винесення судового вироку. Таким чином, інституціоналізація цифрових методів документування згідно зі ст.ст. 9 та 99 КПК України створює стійку правову модель, яка забезпечує невідворотність покарання за найтяжчі міжнародні злочини шляхом формування неспростовної та верифікованої доказової бази.

Важливо підкреслити, що правова регламентація охоплює не лише факт фіксації даних, але й суворий порядок їх збереження та верифікації. У теорії права такий порядок отримав назву «ланцюг збереження доказів» (chain of custody), що передбачає обов'язкову фіксацію кожного етапу поводження з цифровим об'єктом – від моменту його виявлення на електронному носії або у мережі Інтернет до представлення у судовому засіданні. Як підкреслює М. Пашковський ланцюг зберігання є «методом забезпечення хронологічної нерозривності законного володіння (збирання, збереження, подальшого поводження, зокрема переміщення та розпорядження) уповноваженими особами доказами у кримінальному провадженні з моменту їх (як потенційних доказів) виявлення або отримання до їх (доказів) поточного статусу і місцеперебування» [2, с. 159].

Правова регламентація використання цифрових методів базується на положеннях Берклійського протоколу (Протокол Берклі) щодо розслідувань у відкритих джерелах, який, хоч і не є нормативно-правовим актом у класичному розумінні, фактично став універсальним стандартом для українських правоохоронних органів та міжнародних інституцій в сфері фіксації воєнних злочинів в ході російсько-української війни. Протокол Берклі щодо розслідувань із використанням відкритих цифрових даних є першим універсальним міжнародним стандартом, спрямованим на врегулювання процесів використання інформації з відкритих джерел як доказів у розслідуваннях порушень прав людини та міжнародного гуманітарного права, і встановлює комплексні вимоги до пошуку, збирання, збереження, перевірки та аналізу цифрового контенту, зокрема фотографій, відеозаписів, матеріалів соціальних мереж і супутникових знімків, з урахуванням професійних, правових та етичних принципів. Його значення полягає у формуванні єдиних підходів до онлайн-розслідувань без прив'язки до конкретних технологічних інструментів, що забезпечує адаптивність до стрімкого розвитку цифрових технологій та сприяє процесуальній придатності таких доказів у міжнародному кримінальному судочинстві. Практична ефективність стандартів Протоколу підтверджується досвідом їх застосування у діяльності міжнародних слідчих механізмів, зокрема при документуванні мови ненависті у М'янмі та фіксації ймовірних злочинів проти людяності в Південному Судані за допомогою супутникових знімків, що свідчить про зростаючу роль відкритих цифрових даних у подоланні інформаційної ізоляції зон конфлікту [3]. Особливого значення Протокол Берклі набуває в контексті збройної агресії рф проти України, оскільки дозволяє широкому колу суб'єктів, включаючи правозахисників, юристів, правоохоронців та журналістів, здійснювати фіксацію воєнних злочинів із дотриманням міжнародних стандартів безпеки та достовірності, сприяючи формуванню стійкої доказової бази для притягнення винних до відповідальності, що концептуально перегукується з історичною традицією використання новітніх технологій у кримінальному процесі, започаткованою ще під час Нюрнберзького трибуналу, де вперше було визнано відеозапис як допустимий доказ.

Крім того, правова регламентація цифрової трансформації методів документування воєнних злочинів включає використання спеціалізованих реєстрів, таких як Інформаційно-аналітична система «Злочини, вчинені в умовах збройного конфлікту», яка дозволяє акумулювати дані з різних джерел у єдиному захищеному цифровому просторі. Наприклад, Офіс Генерального прокурора разом з українськими та міжнародними партнерами створили ресурс WarCrimes.gov.ua для належного документування воєнних злочинів та злочинів проти людяності, скоєних російською армією в Україні [4]. WarCrimes.gov.ua є інституційно оформленим механізмом збору та збереження доказів злочинів проти людяності й воєнних злочинів, що функціонує відповідно до міжнародних стандартів кримінального правосуддя та спрямований на забезпечення належної доказової бази як для національних судів, так і для Міжнародного кримінального суду та майбутнього спеціального трибуналу. Даний інструмент поєднує в собі елементи цифрового приймання, верифікації та захисту інформації і свідків, забезпечуючи можливість для громадян передавати фото-, відеоматеріали та інші відомості про факти вбивств і поранень цивільного населення, катувань, сексуального насильства, незаконних депортацій, використання «живих щитів», знищення цивільної, культурної та релігійної інфраструктури, нападів на медичний і гуманітарний персонал, а також інші грубі порушення норм міжнародного гуманітарного права. Передбачена ресурсом структурована форма подання інформації, що включає дані про час, місце, характер події, потерпілих, свідків та можливих виконавців, а також відомості щодо засобів ведення війни, сприяє уніфікації процесу фіксації злочинів і підвищує процесуальну придатність зібраних матеріалів, інтегруючи цифрові механізми документування у загальну систему кримінального переслідування та формуючи важливу складову сучасної моделі подолання безкарності за найтяжчі міжнародні злочини [4].

Правова регламентація документування воєнних злочинів на міжнародному рівні в т.ч. базується на положеннях Римського статуту Міжнародного кримінального суду (далі – Римський статут), який створює гнучку та технологічно адаптивну правову рамку для збору доказів. Зокрема, ст. 54 Римського статуту, яка визначає обов'язки та повноваження прокурора під час проведення розслідування, у відповідності до яких прокурор зобов'язаний поширювати розслідування на всі факти і докази, що мають відношення до

визначення кримінальної відповідальності, що в умовах сучасних конфліктів безпосередньо передбачає залучення цифрових доказів. Наприклад, положення ч.3 ст. 54 надає прокурору право укладати спеціальні угоди або домовленості, що не суперечать Статуту, для полегшення збору інформації, що дозволяє залучати технологічні ресурси приватних компаній (як-от Maxar Technologies або Planet Labs) та неурядових організацій, які спеціалізуються на цифровій розвідці.

Отже, узагальнюючи викладене, слід констатувати, що цифрова трансформація методів документування воєнних злочинів, легітимізована синергією національного законодавства та міжнародно-правових норм, формує принципово нову архітектуру правосуддя. Інституціоналізація цифрових стандартів забезпечують процесуальну трансформацію технологічних даних у неспростовну доказову базу через механізм суворого дотримання «ланцюга збереження доказів». Такий комплексний підхід гарантує об'єктивність розслідувань у зонах конфлікту та становить дієвий інструмент подолання стратегій заперечення фактів, створюючи передумови для невідворотного притягнення винних до відповідальності в національних та міжнародних судових інстанціях.

У контексті цифрової трансформації методів документування воєнних злочинів розвідка на основі відкритих джерел (Open Source Intelligence, далі – OSINT), як приклад практичного застосування сучасних технологій, посідає особливе місце. Вона демонструє механізм, за допомогою якого інформація, що формально перебуває у публічному доступі, трансформується у юридично значущий доказ у кримінальному провадженні щодо найтяжчих міжнародних злочинів. Сутність OSINT полягає у системному, цілеспрямованому та методологічно вивіреному збиранні, перевірці та аналізі даних із загальнодоступних інформаційних ресурсів з метою встановлення фактичних обставин подій, ідентифікації осіб, визначення часу, місця та способу вчинення злочину. На відміну від класичних розвідувальних практик, цей метод не пов'язаний із таємним проникненням у інформаційні системи чи використанням прихованих засобів отримання інформації, а ґрунтується виключно на легальних джерелах: матеріалах соціальних мереж, супутникових знімках, відкритих державних реєстрах, публікаціях у медіа та повідомленнях локальних спільнот. Саме ця обставина зумовлює особливу цінність OSINT для правозастосовної діяльності, оскільки мінімізує ризики визнання доказів недопустимими з процесуальних підстав.

Практичне значення OSINT у документуванні воєнних злочинів проявляється передусім у можливості здійснення прецизійної геолокації та хронолокації подій, що дозволяє з високим ступенем точності встановлювати просторово-часові параметри злочинних дій. Аналіз відеозаписів, розміщених у соціальних мережах, із урахуванням архітектурних особливостей будівель, розташування дорожніх знаків, характеру ландшафту або напряму падіння тіней, дає змогу співвіднести зафіксовані події з конкретною місцевістю та моментом часу, що, зокрема, має вирішальне значення для доведення факту присутності певних осіб або підрозділів збройних сил росії у місці вчинення злочину. У цьому аспекті технологія OSINT фактично розширює інструментарій сучасної криміналістики, інтегруючи її класичні методи з цифровою аналітикою та геоінформаційними системами.

Окрему роль відіграє ідентифікація осіб, причетних до воєнних злочинів, яка здійснюється шляхом зіставлення зображень, оприлюднених у відкритих джерелах, із профілями у соціальних мережах та іншими цифровими слідами. У контексті збройної агресії росії проти України саме методи OSINT неодноразово дозволяли встановлювати персональні дані військовослужбовців, які брали участь у розстрілах цивільного населення, катуваннях або депортаціях, навіть за відсутності їхнього фізичного затримання. Аналіз типів озброєння за фрагментами, зафіксованими на фото, дозволяє не лише встановити характер застосованої сили, але й визначити напрямок обстрілу та тип підрозділу, що має безпосереднє значення для доведення причинно-наслідкового зв'язку між діями конкретних військових формувань росії та заподіяною шкодою.

Показовими є практичні кейси, які отримали міжнародне визнання та суттєво вплинули на формування стандартів використання цифрових доказів. Зокрема, міжнародна дослідницька група Bellingcat («незалежний міжнародний колектив дослідників, слідчих і громадянських журналістів, які використовують відкриті джерела та соціальні мережі для розслідування» [5]), спираючись на інструментарій OSINT, змогла реконструювати маршрут пересування зенітно-ракетного комплексу, за допомогою якого було збито літак рейсу MH17. Аналогічно, під час розслідування масових убивств у місті Буча супутникові знімки та записи з камер відеоспостереження були використані журналіста The New York Times для спростування дезінформації росії про інсценування злочинів. Такі приклади свідчать, що розвідка на основі відкритих джерел здатна не лише доповнювати традиційні слідчі дії, але й заміщати їх у ситуаціях, коли фізичний доступ до місця події є неможливим.

Висновки. Цифрова трансформація методів документування воєнних злочинів сформувала якісно новий підхід до фіксації та опрацювання відомостей про порушення норм міжнародного гуманітарного права. Поєднання сучасних інформаційних технологій із правовими механізмами забезпечує можливість оперативного збирання, збереження та перевірки даних у ситуаціях, коли традиційні інструменти виявляються обмеженими або недоступними. Сформована правова рамка дозволяє інтегрувати цифрову інформацію з різних джерел у кримінально-процесуальну діяльність за умови дотримання вимог автентичності, цілісності та простежуваності, що є необхідною передумовою її процесуальної придатності. У цьому

контексті цифрові методи перестають виконувати допоміжну функцію й набувають системного значення у формуванні доказової бази щодо найтяжчих міжнародних злочинів.

Сучасна модель правового регулювання цифрового документування орієнтована на узгодження національних підходів із міжнародними стандартами та практиками, що сприяє уніфікації процедур і підвищенню рівня довіри до зібраних матеріалів. Використання відкритих цифрових джерел, спеціалізованих інформаційних систем і аналітичних інструментів розширює можливості встановлення обставин подій, ідентифікації причетних осіб та подолання інформаційної ізоляції зон конфлікту. Такий підхід створює передумови для ефективного кримінального переслідування та реалізації принципу невідворотності відповідальності, водночас актуалізуючи потребу подальшого розвитку цілісного й послідовного правового забезпечення цифрових процесів у сфері міжнародного правосуддя.

Список використаних джерел:

1. Кримінальник процесуальний кодекс України від 13.04.2012 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n1140 (дата звернення: 15.01.26).

2. Пашковський М. Ланцюг зберігання доказів (chain of custody): процесуальна форма. *Інноваційна наука: пошук відповідей на виклики сучасності* : матеріали конференцій МЦНД, (06.12.2024; Могилів-Подільський, Україна), С. 157–161. URL: https://archives.mcnd.org.ua/index.php/conference-proceeding/article/view/385 (дата звернення: 03.01.26).

3. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. *ЮрФем*. URL: https://jurfem.com.ua/protokol-berkli-schodo-rozsliduvannia-iz-vykorystannyam-zyfrovych-danych/ (дата звернення: 08.01.26).

4. Документуємо воєнні злочини російської федерації в Україні. *Офіс Генерального прокурора*. URL: https://warcrimes.gov.ua/ (дата звернення: 20.01.26).

5. Офіційна веб сторінка Bellingcat. URL: https://www.bellingcat.com/ (дата звернення: 11.01.26).

Дата першого надходження статті до видання: 19.01.2026
Дата прийняття статті до друку після рецензування: 20.02.2026
Дата публікації (оприлюднення) статті: 23.03.2026