

УДК 343.98

DOI [https://doi.org/10.36919/3041-1149\(Print\)14.2026.290-297](https://doi.org/10.36919/3041-1149(Print)14.2026.290-297)

А. В. Лісіцький,
доктор філософії права (PhD),
доцент кафедри криміналістики та судової медицини,
Національна академія внутрішніх справ
email: andriilisitskij@gmail.com
ORCID 0000-0002-9908-6267

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ТА OSINT У КРИМІНАЛІСТИЧНОМУ ЗАБЕЗПЕЧЕННІ ДОКУМЕНТУВАННЯ Й РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

ARTIFICIAL INTELLIGENCE AND OSINT TECHNOLOGIES IN FORENSIC SUPPORT FOR DOCUMENTATION AND INVESTIGATION OF WAR CRIMES

У статті досліджено теоретичні та прикладні засади використання технологій штучного інтелекту (Artificial Intelligence, AI) і розвідки з відкритих джерел (Open Source Intelligence, OSINT) у криміналістичному забезпеченні документування й розслідування воєнних злочинів. Обґрунтовано, що цифровізація сучасних збройних конфліктів істотно трансформує механізми виникнення, виявлення, фіксації та дослідження криміналістично значущої інформації, що обумовлює потребу в розвитку нових підходів до криміналістичного забезпечення розслідування міжнародних злочинів.

Проаналізовано сучасні можливості використання технологій штучного інтелекту під час автоматизованого аналізу цифрових даних, ідентифікації об'єктів, геопросторової локалізації, аналізу супутникових знімків, виявлення змін цифрових зображень, реконструкції механізму події та обробки значних масивів інформації. Визначено особливості використання OSINT як криміналістичного інструменту пошуку, накопичення, систематизації та верифікації інформації з відкритих цифрових джерел.

Особливу увагу приділено дослідженню цифрових криміналістичних слідів воєнних злочинів як специфічної форми відображення кримінально релевантної інформації в цифровому середовищі. Запропоновано авторський підхід до визначення поняття цифрового криміналістичного сліду, розкрито його основні ознаки й запропоновано класифікацію залежно від джерела походження, способу виникнення та криміналістичного значення. Обґрунтовано, що ефективне використання цифрових слідів потребує застосування комплексної криміналістичної верифікації, яка поєднує технічні, інформаційно-аналітичні й тактичні засоби підтвердження автентичності, цілісності та походження цифрової інформації.

Зроблено висновок, що технології штучного інтелекту й OSINT доцільно розглядати як взаємодоповнювальні елементи сучасного криміналістичного забезпечення документування та розслідування воєнних злочинів. Їхнє використання сприяє підвищенню ефективності виявлення, аналізу й інтерпретації цифрових криміналістичних слідів, однак не замінює процесуальної діяльності слідчого, прокурора, експерта чи суду.

Ключові слова: воєнні злочини, криміналістика, криміналістичне забезпечення, штучний інтелект, OSINT, цифрові криміналістичні сліди, цифрові докази, документування воєнних злочинів, цифрова криміналістика, міжнародні злочини.



This article examines the theoretical and practical foundations for the use of artificial intelligence (AI) and open-source intelligence (OSINT) technologies in the forensic documentation and investigation of war crimes. It is argued that the digitization of modern armed conflicts is significantly transforming the mechanisms by which criminologically relevant information arises, is identified, recorded, and analyzed, which necessitates the development of new approaches to forensic support for the investigation of international crimes.

The study analyzes current possibilities for using artificial intelligence technologies in the automated analysis of digital data, object identification, geospatial localization, analysis of satellite imagery, detection of changes in digital images, reconstruction of event mechanisms, and processing of large data sets. The paper identifies the specific features of using OSINT as a forensic tool for searching for, collecting, organizing, and verifying information from open digital sources.

Particular attention is paid to the study of digital forensic traces of war crimes as a specific form of representation of criminally relevant information in the digital environment. An original approach to defining the concept of a digital forensic trace is proposed; its main characteristics are revealed, and a classification is suggested based on the source of origin, the manner of creation, and forensic significance. It is argued that the effective use of digital traces requires comprehensive forensic verification that combines technical, information-analytical, and tactical methods for confirming the authenticity, integrity, and origin of digital information.

It is concluded that artificial intelligence and OSINT technologies should be considered complementary elements of modern forensic support for the documentation and investigation of war crimes. Their use helps improve the effectiveness of identifying, analyzing, and interpreting digital forensic traces; however, it does not replace the procedural activities of an investigator, prosecutor, expert, or court.

Keywords: war crimes, forensic science, forensic support, artificial intelligence, OSINT, digital forensic traces, digital evidence, documentation of war crimes, digital forensics, international crimes.

Постановка проблеми. Повномасштабна збройна агресія Російської Федерації проти України істотно змінила не лише характер сучасних воєнних злочинів, а й способи їх документування та розслідування. Якщо під час збройних конфліктів другої половини XX століття основними джерелами доказової інформації були матеріальні сліди, показання очевидців і результати огляду місця події, то сучасна війна супроводжується безперервним формуванням значного масиву цифрової інформації, яка відображає обставини кримінально караних діянь практично в режимі реального часу. Цифрове середовище стало невід'ємною складовою сучасного збройного конфлікту. Використання мобільних пристроїв, безпілотних літальних апаратів, супутникових систем дистанційного зондування Землі, камер відеоспостереження, соціальних мереж, месенджерів, електронних картографічних сервісів та інших цифрових платформ приводить до формування значної кількості інформаційних слідів, які можуть містити відомості про час, місце, спосіб, механізм і наслідки вчинення воєнних злочинів. Значна частина такої інформації виникає незалежно від діяльності органів досудового розслідування, що принципово відрізняє сучасні міжнародні злочини від традиційних моделей криміналістичного слідоутворення.

За цих умов особливого значення набувають технології штучного інтелекту та розвідки з відкритих джерел (OSINT), які дають змогу здійснювати пошук, накопичення, автоматизовану обробку, систематизацію, геопросторову локалізацію та взаємну верифікацію значних масивів цифрової інформації. Саме завдяки цим технологіям стало можливим документування воєнних злочинів навіть за відсутності безпосереднього доступу до місця їхнього вчинення, що має принципове значення в умовах активних бойових дій або тимчасової окупації окремих територій.

Водночас розвиток цифрових технологій ставить перед криміналістикою низку нових теоретичних і прикладних завдань. Традиційні підходи до дослідження механізму слідоутворення були сформовані переважно щодо матеріальних слідів кримінального правопорушення. Натомість сучасне цифрове середовище продукує специфічні інформаційні об'єкти, які мають іншу природу виникнення, інші закономірності існування та потребують застосування спеціальних криміналістичних засобів їх виявлення, фіксації, дослідження й інтерпретації. У зв'язку з цим

виникає потреба в переосмисленні окремих положень криміналістичної техніки, тактики та методики розслідування з урахуванням особливостей цифрового середовища. Характерної актуальності ця проблема набуває в контексті міжнародного документування воєнних злочинів. Практика діяльності Офісу Генерального прокурора України, Міжнародного кримінального суду, Спільних слідчих груп (Joint Investigation Teams), міжнародних правозахисних організацій і незалежних OSINT-спільнот свідчить, що значна частина інформації про міжнародні злочини формується саме у відкритому цифровому просторі. Однак відсутність єдиних криміналістичних підходів до її використання ускладнює забезпечення належного рівня достовірності, відтворюваності й наукової обґрунтованості результатів цифрового документування.

У сучасній криміналістичній науці достатньо ґрунтовно досліджено питання використання цифрових доказів, електронної інформації та комп'ютерно-технічної експертизи. Водночас комплексне дослідження використання технологій штучного інтелекту й OSINT саме як складових криміналістичного забезпечення документування та розслідування воєнних злочинів фактично перебуває на початковому етапі формування. Недостатньо розробленими залишаються питання визначення поняття цифрового криміналістичного сліду, особливостей його виникнення, криміналістичної класифікації, методів верифікації та використання під час реконструкції механізму воєнного злочину.

Аналіз останніх досліджень і публікацій. Проблематика використання цифрових технологій під час документування та розслідування кримінальних правопорушень останніми роками набула особливої актуальності як у зарубіжній, так і у вітчизняній юридичній науці. Це обумовлено стрімкою цифровізацією суспільних відносин, розвитком технологій штучного інтелекту, поширенням відкритих інформаційних ресурсів і потребою в адаптації криміналістичних засобів і методів до нових умов формування криміналістично значущої інформації. Особливого значення вказані питання набули після початку повномасштабної збройної агресії Російської Федерації проти України, коли цифрові джерела інформації стали одним із ключових засобів документування воєнних злочинів.

Теоретичні засади криміналістичного забезпечення розслідування злочинів традиційно розроблялись у працях вітчизняних учених-криміналістів. Значний внесок у розвиток криміналістичної техніки, криміналістичної тактики, методики розслідування окремих видів кримінальних правопорушень і вчення про криміналістичні сліди зробили В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель, В. В. Тіщенко, М. В. Шепітько та інші дослідники [11, с. 16–133; 12, с. 39–46; 7, с. 357–370; 1].

Їхні праці сформуvalи методологічне підґрунтя сучасної криміналістики, однак були розроблені переважно щодо традиційних матеріальних джерел доказової інформації та неповною мірою враховують особливості цифрового середовища, що сформувалося в умовах сучасних збройних конфліктів.

Окремий напрям досліджень присвячено цифровим доказам, електронній інформації, інформаційно-комунікаційним технологіям та особливостям їхнього використання в кримінальному провадженні. В українській правовій науці ці питання досліджувалися переважно крізь призму кримінального процесу, допустимості електронних доказів, інформаційної безпеки й процесуального порядку використання цифрової інформації. Так, В. Шевчук ґрунтовно досліджує трансформацію криміналістики під впливом ШІ, зокрема використання нейромереж в OSINT для підвищення ефективності розслідування воєнних злочинів. Він зазначає, що ШІ здатен автоматично збирати інформацію, здійснювати розпізнавання облич, об'єктів і військової техніки на фото- / відео-, проводити геолокацію та аналізувати емоційну тональність текстів [10, с. 356–361].

У сфері інноваційних технологій боротьби зі злочинністю також зазначаються праці вчених, які оцінюють доцільність використання AI та OSINT у криміналістиці, пропонуючи способи вирішення можливих проблем [3; 9; 8; 4; 6; 5; 10; 13].

Водночас криміналістичні аспекти застосування сучасних цифрових технологій, особливо штучного інтелекту та OSINT, залишаються недостатньо систематизованими.

У зарубіжній науковій літературі використання цифрових технологій під час документування міжнародних злочинів отримало значно ширший розвиток. Суттєвий вплив на розвиток методології

документування міжнародних злочинів справив Berkeley Protocol on Digital Open Source Investigations [2], який вперше систематизував стандарти використання інформації з відкритих джерел під час документування порушень міжнародного гуманітарного права та міжнародного кримінального права.

Останніми роками в світовій науці активно досліджуються можливості використання штучного інтелекту у сфері кримінальної юстиції. Предметом наукової дискусії стали питання автоматизованого аналізу великих масивів даних, алгоритмічного розпізнавання об'єктів, геопросторової локалізації, цифрової реконструкції подій, виявлення синтетичних медіа (deepfake), а також забезпечення прозорості та надійності алгоритмічних систем. Водночас переважна більшість цих досліджень має технічний або процесуально-правовий характер і лише фрагментарно стосується криміналістичних аспектів використання технологій штучного інтелекту. Аналіз сучасної наукової літератури свідчить, що більшість наявних досліджень присвячена окремим питанням використання цифрових доказів, інформаційних технологій, електронних джерел інформації або процесуальним аспектам їхнього застосування. Значно менше уваги приділено комплексному дослідженню штучного інтелекту та OSINT саме як елементів криміналістичного забезпечення документування та розслідування воєнних злочинів. Недостатньо розробленими залишаються питання поняття цифрового криміналістичного сліду, особливостей його виникнення, криміналістичної класифікації, алгоритмів криміналістичної верифікації цифрової інформації та використання сучасних цифрових технологій під час реконструкції механізму воєнного злочину.

Отже, проведений аналіз свідчить про наявність наукової прогалини, яка полягає у відсутності комплексного криміналістичного дослідження використання технологій штучного інтелекту та OSINT у системі документування й розслідування воєнних злочинів. Саме потреба у формуванні сучасного теоретичного підходу до використання цифрових криміналістичних слідів, визначення місця III та OSINT у системі криміналістичного забезпечення, а також розроблення науково обґрунтованих рекомендацій щодо їхнього застосування обумовлює актуальність і спрямованість цього дослідження. Більшість наукових праць зосереджена або на процесуальних питаннях допустимості цифрової інформації, або на технічних аспектах функціонування алгоритмів штучного інтелекту та інструментів OSINT. Натомість недостатньо дослідженими залишаються закономірності виникнення цифрових криміналістичних слідів, їхнє місце в системі криміналістично значущої інформації, особливості криміналістичного дослідження, верифікації та використання під час реконструкції механізму воєнного злочину.

Метою статті є комплексне дослідження теоретичних і прикладних засад використання технологій штучного інтелекту й розвідки з відкритих джерел (OSINT) у криміналістичному забезпеченні документування та розслідування воєнних злочинів.

Виклад основного матеріалу дослідження. Потребують подальшого наукового осмислення питання визначення поняття цифрового криміналістичного сліду, розроблення його криміналістичної класифікації, встановлення співвідношення між цифровими криміналістичними слідами, цифровими доказами та інформацією, отриманою із застосуванням технологій штучного інтелекту й OSINT. Не менш важливим є дослідження можливостей використання алгоритмів штучного інтелекту під час криміналістичної реконструкції події воєнного злочину, аналізу цифрової обстановки місця події, встановлення просторово-часових зв'язків між окремими цифровими об'єктами та побудови інформаційної моделі механізму злочину.

Окремою науковою проблемою залишається відсутність у вітчизняній криміналістиці цілісної концепції криміналістичного забезпечення документування воєнних злочинів із використанням сучасних цифрових технологій. Наявні дослідження переважно висвітлюють окремі технічні або процесуальні аспекти їхнього застосування, однак не розкривають місця технологій штучного інтелекту та OSINT у системі криміналістичної техніки, криміналістичної тактики й методики розслідування міжнародних злочинів.

Вважаємо, що сучасна війна змінює не лише характер міжнародних злочинів, а й закономірності виникнення криміналістично значущої інформації. Варто показати, що цифрове середовище стало самостійним простором формування слідів злочинної діяльності, а використання мобільних пристроїв, безпілотних літальних апаратів, супутникових систем, соціальних мереж, месенджерів і

геоінформаційних сервісів створює нові можливості для документування воєнних злочинів. Пропонуємо таке визначення, що цифровізація збройних конфліктів трансформує закономірності слідоутворення, унаслідок чого поряд із традиційними матеріальними слідами формується самостійний масив цифрової криміналістично значущої інформації, що потребує застосування спеціальних криміналістичних засобів її виявлення, дослідження та інтерпретації.

Стрімкий розвиток інформаційно-комунікаційних технологій і цифровізація сучасних збройних конфліктів зумовили суттєву трансформацію підходів до документування воєнних злочинів. Якщо раніше основним джерелом криміналістично значущої інформації були результати огляду місця події, матеріальні сліди, речові докази та показання учасників кримінального провадження, то сьогодні значний масив відомостей формується в цифровому інформаційному просторі. Соціальні мережі, месенджери, супутникові знімки, відкриті державні реєстри, геоінформаційні сервіси, платформи обміну відеоконтентом і фотоматеріалами стали джерелами інформації, що дають змогу встановлювати обставини воєнних злочинів навіть за відсутності фізичного доступу до місця їхнього учинення. У цих умовах особливого значення набуває розвідка з відкритих джерел (Open Source Intelligence, OSINT), яка дедалі активніше використовується як міжнародними судовими інституціями, так і правоохоронними органами, спеціалізованими слідчими групами та правозахисними організаціями. Практика документування злочинів, учинених під час збройної агресії проти України, переконливо демонструє, що саме відкриті цифрові джерела нерідко стають першими носіями інформації про факти обстрілів цивільної інфраструктури, незаконного поводження з цивільним населенням, застосування заборонених засобів ведення війни, депортації населення та інших порушень міжнародного гуманітарного права.

У спеціальній літературі поняття OSINT традиційно визначається як процес пошуку, збирання, аналізу й інтерпретації інформації, отриманої із загальнодоступних джерел. Первісно зазначений підхід сформувався у сфері розвідувальної діяльності та національної безпеки, однак розвиток цифрових технологій суттєво розширив можливості його використання в криміналістиці. Сучасний OSINT уже не обмежується пошуком відкритої інформації. Його інструментарій охоплює геопросторовий аналіз, часову верифікацію цифрових матеріалів, дослідження метаданих, зіставлення різних інформаційних джерел, аналіз супутникових зображень, картографічних сервісів та інших цифрових ресурсів, що дає змогу реконструювати окремі елементи механізму злочину.

На нашу думку, розглядати OSINT виключно як інформаційно-аналітичну технологію є недостатнім. З позицій криміналістики його доцільно визначати як комплексний інструмент криміналістичного документування, що забезпечує виявлення, фіксацію, аналіз, перевірку та інтерпретацію цифрової інформації про кримінальне правопорушення. Тому пропонуємо визначення, що OSINT у криміналістичному забезпеченні документування воєнних злочинів – це система криміналістичних, інформаційно-аналітичних та цифрових методів і засобів, спрямованих на виявлення, збирання, фіксацію, верифікацію, аналіз та інтерпретацію інформації з відкритих джерел для встановлення обставин учинення воєнних злочинів, реконструкції їхнього механізму й формування доказової бази відповідно до вимог кримінального процесуального законодавства та міжнародних стандартів документування.

Запропонований підхід дає нагоду розглядати OSINT не як альтернативу традиційним криміналістичним засобам, а як їхнє логічне доповнення. Його застосування найбільш ефективно на початковому етапі документування воєнних злочинів, коли виникає потреба в оперативному отриманні інформації про місце події, характер руйнувань, можливих потерпілих, переміщення військової техніки, використання певних видів озброєння або інші обставини, що мають криміналістичне значення. Практика документування міжнародних злочинів свідчить, що можливості OSINT не обмежуються лише пошуком інформації. Використання сучасних цифрових сервісів дає змогу здійснювати багаторівневу перевірку відомостей через зіставлення різних відкритих джерел. Так, фотографії та відеозаписи можуть бути співвіднесені із супутниковими знімками, географічними координатами, цифровими картами, метеорологічними даними, архітектурними особливостями місцевості та іншими відкритими джерелами інформації. Саме поєднання різномірних цифрових даних забезпечує високий рівень достовірності криміналістичних висновків і мінімізує ризик використання сфальсифікованих або маніпульованих матеріалів.

Водночас використання OSINT у криміналістичній діяльності, на нашу думку, супроводжується низкою методичних проблем. Відкритий характер джерел інформації не гарантує їхньої достовірності, а розвиток генеративних технологій штучного інтелекту значно підвищив ризик поширення змінених або повністю синтетичних цифрових матеріалів. Це обумовлює потребу в застосуванні комплексної криміналістичної верифікації, яка повинна охоплювати перевірку походження цифрового об'єкта, аналіз його метаданих, встановлення часу й місця створення, дослідження ознак цифрового редагування, зіставлення із незалежними джерелами інформації та документування всіх етапів роботи з цифровими матеріалами. Особливого значення набуває інтеграція OSINT із технологіями штучного інтелекту. Алгоритми машинного навчання дають змогу автоматизувати пошук релевантної інформації, класифікувати великі масиви цифрових даних, ідентифікувати однакові об'єкти на різних зображеннях, встановлювати географічне положення місця події за сукупністю візуальних ознак і виявляти закономірності, які практично неможливо встановити за допомогою традиційного аналізу. У результаті формується новий рівень криміналістичного дослідження цифрової інформації, в якому можливості людини доповнюються алгоритмічними інструментами аналізу. Водночас результати, отримані із застосуванням OSINT, не можуть автоматично визнаватися достовірними або використовуватися як самодостатня підстава для формування висновків щодо обставин кримінального правопорушення. Вони повинні оцінюватися у взаємозв'язку з іншими джерелами криміналістично значущої інформації та проходити відповідну процесуальну перевірку. Саме тому OSINT потрібно розглядати як інструмент розширення інформаційних можливостей криміналістики, а не як заміну традиційним методам документування та розслідування.

Отже, сучасний розвиток цифрових технологій дає нагоду констатувати, що OSINT набув ознак самостійного елементу криміналістичного забезпечення документування воєнних злочинів. Його ефективність визначається не лише обсягом доступної цифрової інформації, а насамперед можливістю її комплексної криміналістичної перевірки, систематизації та інтеграції з іншими джерелами доказової інформації. Саме поєднання традиційних криміналістичних методів із сучасними цифровими технологіями створює передумови для підвищення ефективності документування міжнародних злочинів і забезпечення належної якості доказової бази в кримінальному провадженні.

Стрімкий розвиток технологій штучного інтелекту (Artificial Intelligence, AI) є одним із найбільш визначальних чинників цифрової трансформації сучасної криміналістики. Якщо ще донедавна застосування алгоритмів машинного навчання асоціювалося переважно з автоматизацією окремих інформаційно-аналітичних процесів, то сьогодні штучний інтелект поступово інтегрується практично в усі етапи криміналістичного забезпечення документування й розслідування воєнних злочинів – від первинного виявлення цифрових слідів до реконструкції механізму події та побудови версій щодо її розвитку. Особливості сучасних збройних конфліктів характеризуються безпрецедентними обсягами цифрової інформації, що формується в режимі реального часу. Фото- та відеоматеріали, записи камер спостереження, супутникові знімки, матеріали безпілотних літальних апаратів, повідомлення в соціальних мережах, геопросторові дані, телекомунікаційна інформація та інші цифрові ресурси створюють інформаційний масив, опрацювання якого традиційними методами нерідко є практично неможливим. Саме тому застосування алгоритмів штучного інтелекту стає не лише технічно доцільним, а й вагомим елементом сучасного криміналістичного забезпечення розслідування воєнних злочинів.

У сучасній юридичній літературі штучний інтелект здебільшого досліджується крізь призму автоматизації правосуддя, прогнозування судових рішень або процесуальної допустимості результатів алгоритмічного аналізу. Водночас вважаємо, що криміналістичний потенціал ШІ є значно ширшим. Його практичне значення полягає не в ухваленні процесуальних рішень, а в підвищенні ефективності виявлення, аналізу й інтерпретації криміналістично значущої інформації. Так, технології штучного інтелекту доцільно розглядати як сучасний елемент криміналістичної техніки, що розширює можливості пізнавальної діяльності слідчого, прокурора, експерта та інших суб'єктів документування воєнних злочинів. На нашу думку, штучний інтелект у криміналістиці варто визначати як сукупність алгоритмічних технологій, що забезпечують

автоматизований аналіз, класифікацію, зіставлення, моделювання та інтерпретацію криміналістично значущої інформації з метою виявлення закономірностей, встановлення взаємозв'язків між цифровими слідами й інформаційної підтримки процесу документування та розслідування кримінальних правопорушень. Запропоноване визначення акцентує увагу на тому, що об'єктом використання ШІ є не процесуальні рішення, а інформаційні процеси, які передують формуванню доказової бази. Саме такий підхід відповідає сучасним міжнародним тенденціям розвитку цифрової криміналістики.

Отже, використання технологій штучного інтелекту в криміналістичному забезпеченні документування та розслідування воєнних злочинів свідчить про формування нового етапу розвитку криміналістики, у межах якого цифрові технології стають невід'ємною складовою криміналістичної техніки. Водночас їхнє застосування не змінює фундаментальних закономірностей криміналістичного пізнання, а лише розширює інструментарій виявлення, аналізу й інтерпретації цифрових криміналістичних слідів. Саме поєднання можливостей штучного інтелекту з класичними криміналістичними методами створює передумови для підвищення ефективності документування воєнних злочинів, забезпечення повноти доказової інформації та зміцнення доказової бази в кримінальних провадженнях щодо міжнародних злочинів.

Висновки. Висловлені думки в цій статті є намаганням констатувати й осучаснити криміналістичне забезпечення документування та констатувати, що цифровізація сучасних збройних конфліктів суттєво трансформує криміналістичне забезпечення документування й розслідування воєнних злочинів. На відміну від традиційної моделі слідотворення сучасні міжнародні злочини супроводжуються формуванням значного масиву цифрової інформації, яка виникає внаслідок функціонування інформаційно-комунікаційних систем, цифрових платформ, супутникових технологій, безпілотних літальних апаратів, мобільних пристроїв та інших технічних засобів. Це зумовлює потребу в розвитку криміналістичної теорії з урахуванням особливостей цифрового середовища. Самі технології штучного інтелекту та OSINT доцільно розглядати як взаємопов'язані елементи сучасного криміналістичного забезпечення документування воєнних злочинів. Їхнє функціональне призначення полягає у виявленні, накопиченні, систематизації, аналізі, верифікації та інтерпретації криміналістично значущої інформації, отриманої з відкритих цифрових джерел та інших інформаційних ресурсів. Водночас використання алгоритмічних технологій не змінює фундаментальних засад криміналістичного пізнання, а розширює можливості криміналістичної техніки, тактики й методики розслідування. Отже, результати проведеного дослідження дають підстави стверджувати, що використання технологій штучного інтелекту та OSINT є одним із ключових напрямів розвитку сучасної криміналістики. Водночас їхня ефективність визначається не рівнем технологічної досконалості алгоритмів, а можливістю інтегрувати отримані результати в систему криміналістичного забезпечення документування та розслідування воєнних злочинів із безумовним дотриманням принципів законності, наукової обґрунтованості, об'єктивності й процесуальних гарантій кримінального провадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Konovalova V. O., Shevchuk V. M. (2023). Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries of modern science: experience, approaches and innovations* : collection of scientific papers III International Scientific and Theoretical Conference, January 20, 2023. Amsterdam : European Scientific Platform. Pp. 73–77.
2. Office of the United Nations High Commissioner for Human Rights, & Human Rights Center at the UC Berkeley School of Law. 2022. *Berkeley protocol on digital open source investigations*. United Nations. ohchr.org
3. Використання цифрових технологій у криміналістиці та судовій експертизі : матеріали Міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р. : електрон. наук. вид. / редкол. : В. Ю. Шепітько, Г. К. Авдєєва ; Нац. акад. прав. наук України, НДІ вивчення проблем злочинності імені акад. В. В. Сташиса, НАПрН України. Харків : Право, 2024. 144 с.
4. Мартинюк С. О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал*. 2021. № 9. С. 332–334.

5. Матулене С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 4 (29). С. 12–46.
6. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4 (6). С. 201–208.
7. Тіщенко В. В. Теоретичні і практичні проблеми формування основ воєнної криміналістики. *Вісник Національної академії правових наук України*. 2023. Том 30, № 3. С. 357–370. DOI 10.31359/1993-0909-2023-30-3-357
8. Тома М. Г., Василюва О. В. Інструменти OSINT: фіксація воєнних злочинів в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. Випуск 02. С. 905–909. URL : <https://app-journal.in.ua/wp-content/uploads/2025/04/136.pdf>
9. Філіпенко Н. Є., Лукашевич С. Ю. Діяльність судово-експертних установ щодо запобігання злочинності з використанням прогресивних інформаційних методик та технологій. *Наукові інновації та передові технології*. 2023. Вип. 14 (28). С. 487–495. URL : <http://perspectives.pp.ua/index.php/nauka/article/download/7907/7951/7950>
10. Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки і обороноздатності України. *Юридичний науковий електронний журнал*. 2024. № 6. С. 356–361.
11. Шепітько В. Ю. Місце цифрових доказів та інституту доказування в доктрині криміналістики та судової експертизи. Інформаційне забезпечення розслідування злочинів : матеріали IX Міжнародного круглого столу, 4 червня 2021 р. Одеса : Вид. дім «Гельветика», 2022. С. 126–133.
12. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю : зб. наук. праць*. Харків : Право, 2011. Вип. 21. С. 39–46.
13. Шрамко С. С. Використання технологій штучного інтелекту у протидії злочинності. Матеріали науково-практичного онлайн-семінару. Харків : Право, 2020. 112 с.

Дата надходження статті: 27.07.2026

Дата прийняття статті: 25.08.2026

Дата публікації статті: 14.09.2026