

УДК 343.98

DOI <https://doi.org/10.24144/2307-3322.2025.90.4.42>

ПЕРЕВАГИ ТА ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ДОСЛІДЖЕННІ ЦИФРОВИХ СЛІДІВ

Курман О.В.,
*кандидат юридичних наук, доцент,
доцент кафедри криміналістики,
Національний юридичний університет імені Ярослава Мудрого
ORCID: 0000-0002-5432-7215*

Курман О.В. Переваги та проблемні питання використання штучного інтелекту при дослідженні цифрових слідів.

У науковій статті здійснено комплексне дослідження проблемних питань, що виникають під час застосування технологій штучного інтелекту у процесі виявлення, фіксації, аналізу та оцінювання цифрових слідів у межах кримінального провадження. Обґрунтовано актуальність впровадження інтелектуальних технологій у практику діяльності правоохоронних органів і судово-експертних установ у контексті цифровізації злочинної діяльності та зростання обсягів інформації, що має цифровий формат. Наведено сучасні наукові підходи до тлумачення поняття «цифрові сліди», висвітлено їх типові ознаки та криміналістичну значущість у процесі досудового розслідування. Особливу увагу приділено можливостям застосування штучного інтелекту для автоматизованого виявлення, класифікації, аналізу та систематизації цифрових даних, що містяться в мобільних пристроях, на серверах, у хмарних сховищах, соціальних мережах і месенджерах.

У дослідженні охарактеризовано ключові функціональні можливості штучного інтелекту в контексті його використання у правозастосовній діяльності. Водночас обґрунтовано наявність низки викликів і загроз, пов'язаних із впровадженням штучного інтелекту у сферу кримінального провадження: обмежена прозорість і пояснюваність алгоритмів, вразливість до цілеспрямованих атак, імовірність хибних результатів, неможливість точного тлумачення складних контекстів тощо.

Проаналізовано відсутність належного нормативного регулювання використання штучного інтелекту в кримінальному судочинстві та звернено увагу на ризики порушення фундаментальних прав учасників процесу, зокрема права на захист і права на справедливий суд. Аргументовано необхідність формування правових, технічних та етичних стандартів застосування штучного інтелекту під час дослідження цифрових слідів. Зроблено висновок, що ефективне й безпечне впровадження штучного інтелекту в криміналістичну практику можливе лише за умови поєднання інноваційних технологічних рішень із чітким процесуальним регламентом, дотриманням принципів об'єктивності, науковості та захисту прав людини.

Ключові слова: штучний інтелект, цифрові сліди, розкриття злочину, розслідування кримінальних правопорушень, судові експертизи, криміналістична методика.

Kurman O.V. Advantages and challenges of using artificial intelligence in the examination of digital traces.

The scientific article presents a comprehensive study of the problematic issues arising from the application of artificial intelligence technologies in the process of detecting, documenting, analyzing, and evaluating digital traces within the framework of criminal proceedings. The relevance of implementing intelligent technologies into the practice of law enforcement agencies and forensic institutions is substantiated, particularly in the context of the digitalization of criminal activity and the growing volume of information in digital format.

The article outlines current scientific approaches to interpreting the concept of «digital traces», highlighting their typical characteristics and forensic significance during pre-trial investigation. Special

attention is paid to the potential use of artificial intelligence for the automated detection, classification, analysis, and systematization of digital data stored on mobile devices, servers, cloud platforms, social networks, and messaging services.

The study describes the key functional capabilities of artificial intelligence in the context of its application in law enforcement activities. At the same time, it identifies a range of challenges and threats associated with the introduction of artificial intelligence into the domain of criminal justice, including the limited transparency and explainability of algorithms, susceptibility to adversarial attacks, the likelihood of erroneous outcomes, and the inability to accurately interpret complex contextual information.

The lack of adequate regulatory frameworks governing the use of artificial intelligence in criminal proceedings is critically analyzed. Attention is drawn to the potential risks of violating fundamental rights of the parties involved in the process, particularly the right to defense and the right to a fair trial. The necessity of developing legal, technical, and ethical standards for the application of artificial intelligence in the examination of digital traces is substantiated.

The study concludes that the effective and safe integration of artificial intelligence into forensic practice is possible only under the condition of combining innovative technological solutions with clear procedural regulations and strict adherence to the principles of objectivity, scientific validity, and the protection of human rights.

Key words: artificial intelligence, digital traces, crime detection, criminal investigation, forensic examinations, criminalistic methodology.

Постановка проблеми. Сучасні технології відіграють важливу роль в оновленні та модернізації світового порядку. Вагоме місце серед них посідає галузь штучного інтелекту. Актуальність штучного інтелекту (далі – ШІ) у сучасних умовах є надзвичайно високою. Штучний інтелект активно впроваджується в різноманітні сфери людської діяльності, забезпечуючи автоматизацію процесів, оптимізацію прийняття управлінських рішень, підвищення ефективності й продуктивності, а також створення умов для інноваційного розвитку в таких галузях, як охорона здоров'я, фінансовий сектор, промисловість, транспорт, електронна комерція, освіта та інші.

Не залишилася осторонь і система кримінального судочинства, яка все активніше включається в процес використання потенціалу машинного навчання. З огляду на стрімкий розвиток науки й техніки, що є характерним для сучасного етапу, питання впровадження штучного інтелекту в професійну діяльність осіб, які здійснюють досудове розслідування кримінальних правопорушень, набуває особливої значущості. Це зумовлено, по-перше, зростанням зацікавленості представників так званого «кримінального середовища» у сфері інформаційних технологій, що передбачає використання відповідних наукових досягнень у протиправній діяльності; по-друге, наявністю позитивного досвіду застосування ШІ в протидії злочинності в ряді зарубіжних держав.

За таких умов особливої актуальності набувають проблеми активізації розроблення та впровадження інноваційних підходів у криміналістиці, новітніх технологій і криміналістичних засобів, а також їх активне застосування в слідчій (детективній), судовій та експертній діяльності у сфері протидії злочинності. Серед таких засобів найбільш перспективним у сучасних умовах глобальних загроз і воєнних викликів є використання технологій штучного інтелекту [1, с. 84].

Мета дослідження: визначення переваг та можливих проблем при використанні штучного інтелекту під час дослідження цифрових слідів.

Стан опрацювання проблематики. Проблематиці використання штучного інтелекту в судовій та правоохоронній діяльності приділяється значна увага з боку науковців-правознавців. Свої наукові праці цій тематиці присвятили такі дослідники, як Белова М.В., Белов Д.М., Рушак І.В. [2], Карчевський М.В., Куковинець Д.О. [3], Негребецький В.В. [4], Плахотнік О.В. [5], Червеко К.О. [6] та інші. Водночас, з огляду на стрімку динаміку розвитку штучного інтелекту, його активне впровадження у практику діяльності правоохоронних та експертних органів, а також пов'язані з цим виклики та проблеми, цей напрям наукових криміналістичних досліджень потребує постійного вивчення, оновлення та вдосконалення. В. Шевчук справедливо наголошує на необхідності активізації зусиль щодо застосування штучного інтелекту з метою розв'язання практичних завдань як у сфері правозастосування, так і в боротьбі зі злочинністю в умовах війни [7, с. 198].

Виклад основного матеріалу. Сучасні злочини дедалі частіше супроводжуються величезними обсягами цифрових даних – лог-файлів, повідомлень, зображень, відеозаписів, метаданих та

інформації з мобільних пристроїв. В умовах настільки масштабних і різноманітних цифрових слідів традиційні методи аналізу виявляються недостатньо ефективними та ресурсоємними. Застосування штучного інтелекту (ШІ) для аналізу цифрових слідів становить перспективний науково-практичний напрям, що здатен докорінно змінити як процес досудового розслідування, так і доказування у кримінальному провадженні.

На сьогодні категорія «цифрові сліди» не має однозначного тлумачення та усталеного розуміння. У межах теорії криміналістичної техніки тривають дискусії щодо природи цифрових слідів, їх ознак і класифікацій.

Так, І. Колеснікова наводить визначення цифрових слідів через сукупність їх характерних властивостей. Зокрема: 1) цифрові сліди – це інформація, що міститься на матеріальних цифрових пристроях; 2) для аналізу такої інформації необхідні спеціальні криміналістичні знання із застосуванням комп'ютерних технологій; 3) цифрові сліди як інформаційний ресурс містять відомості про вчинені кримінальні правопорушення. До основних властивостей цифрових слідів, за авторкою, належать: відсутність нерозривного зв'язку з матеріальним носієм; динамічність, тобто здатність до просторового переміщення; можливість їх миттєвого знищення, а також здатність створювати ідентичні копії без втрати змісту [8, с. 473].

Г. Авдєєва визначає цифрові сліди як матеріальні невидимі сліди, що містять криміналістично значущу інформацію (відомості, дані), зафіксовану в цифровій формі на матеріальних носіях, які можуть бути виявлені, зафіксовані та досліджені із застосуванням відповідних цифрових пристроїв [9, с. 91].

Є. Демидова подає визначення цифрових слідів через перелік їх ознак, а саме: 1) наявність цифрової форми існування (відсутність традиційної матеріальної форми); 2) виникнення внаслідок взаємодії певного об'єкта з цифровими пристроями, технологіями або інформаційними мережами; 3) локалізація в цифровому просторі (сервері, комп'ютері, смартфоні тощо); 4) можливість їх виявлення та дослідження з використанням відповідного обладнання та/або спеціалізованого програмного забезпечення; 5) здатність до копіювання (виготовлення дублікатів) без втрати якості, у тому числі дистанційно; 6) можливість дистанційного модифікування або знищення [10, с. 75].

В умовах цифровізації суспільних відносин і злочинної діяльності спостерігається стрімке зростання обсягів та форм цифрових слідів, що зумовлює необхідність застосування сучасних інтелектуальних технологій, здатних обробляти великі й неоднорідні масиви інформації в умовах обмеженого часу.

У розв'язанні таких завдань саме ШІ може відіграти ключову роль. Штучний інтелект може бути використаний для автоматизованого пошуку цифрових слідів у різних джерелах: мобільних пристроях, персональних комп'ютерах, хмарних сховищах, соціальних мережах і месенджерах. Із застосуванням методів інтелектуального пошуку та фільтрації системи на основі ШІ здатні ідентифікувати потенційно релевантні файли, повідомлення, зображення чи журнали подій, спираючись на ключові слова, часові мітки, геолокаційні дані та контекст використання.

Цифрові сліди, як правило, мають неструктурований характер і різноманітні форми (текстові файли, мультимедійні дані, системні логи тощо). За допомогою алгоритмів машинного навчання та технологій обробки природної мови (NLP) ШІ здатен класифікувати дані за категоріями, виявляти зв'язки між об'єктами (наприклад, IP-адресами, обліковими записами, діями користувачів) та формувати логічно послідовні структури, придатні для подальшого аналізу.

Технології ШІ, зокрема алгоритми часової аналітики, дозволяють відновити хронологію дій суб'єкта, виявити підозрілу активність і простежити ланцюг подій, наприклад: вхід у систему → копіювання файлів → спроба приховування слідів. Такий підхід є особливо важливим під час розслідування злочинів у сфері інформаційних технологій, витоків інформації або несанкціонованого доступу.

Завдяки технологіям комп'ютерного зору ШІ може здійснювати розпізнавання облич, номерних знаків транспортних засобів, предметів та дій на фото- й відеоматеріалах, вилучених під час розслідування. Це дозволяє точно встановити місцезнаходження та поведінку підозрюваного, зіставити його зовнішність із даними з інших джерел, а також виявити можливі фальсифікації відеоматеріалів шляхом виявлення цифрових маніпуляцій (аналіз deepfake).

Штучний інтелект може бути використаний для аналізу масивів текстових повідомлень, переписок у месенджерах, публікацій у соціальних мережах з метою виявлення ключових тем, намірів

та потенційних учасників злочинного угруповання. Технології семантичного аналізу дозволяють визначити емоційне забарвлення повідомлень, ідентифікувати умовні сигнали (кодові слова) та виявляти приховані загрози.

Штучний інтелект також може бути інтегрований з чинними криміналістичними базами даних (зокрема дактилоскопічними, генотипічними, відеоархівами, реєстрами викрадених транспортних засобів, зброї, мобільних телефонів тощо) з метою автоматизованого зіставлення цифрових слідів з наявною інформацією. Це сприяє оперативному встановленню особи підозрюваного, виявленню аналогічних злочинів і формуванню профілю правопорушника.

Під час використання штучного інтелекту у роботі з цифровими слідами виникає низка проблем і викликів, які можуть істотно вплинути на допустимість, достовірність та ефективність застосування таких технологій у кримінальному судочинстві і розслідуванні.

Сучасні системи штучного інтелекту, зокрема ті, що ґрунтуються на методах глибокого навчання, демонструють високу ефективність та точність при обробленні великих обсягів цифрової інформації. Водночас, ключовим викликом залишається їхня обмежена пояснюваність, що має критичне значення в умовах кримінального провадження. Низький рівень прозорості алгоритмів створює загрозу неможливості об'єктивного обґрунтування, чому саме алгоритм сформулював певний висновок або рішення, що ускладнює перевірку обґрунтованості висновків ШІ, що прямо впливає на допустимість і належність доказів у суді. Крім того, відсутність чітких критеріїв і механізмів перевірки відкриває простір для потенційних маніпуляцій, зокрема шляхом цілеспрямованого налаштування параметрів системи під заздалегідь визначений або бажаний результат, що суперечить засадам змагальності, об'єктивності й справедливості кримінального процесу.

Попри значний технічний потенціал, системи штучного інтелекту не позбавлені суттєвих обмежень, які можуть впливати на точність та достовірність аналізу цифрових слідів у межах кримінального провадження. Однією з основних загроз є ймовірність виникнення хибнопозитивних або хибнонегативних результатів, що виявляється, зокрема, у неправильній інтерпретації текстових повідомлень, помилковій ідентифікації облич або інших цифрових об'єктів. Така недостовірність здатна суттєво вплинути на висновки слідства та оцінку доказів у суді.

Окрему проблему становить нездатність ШІ враховувати контекст повідомлення, особливо у випадках використання неструктурованої лексики, професійного жаргону, іронії або двозначних висловлювань. Унаслідок цього зміст інформації, що аналізується, може бути істотно спотворений, що створює ризики неправомірних висновків.

Крім того, системи ШІ є вразливими до цілеспрямованих атак з боку сторонніх осіб. Зокрема, мова йде про так звані *adversarial examples* – штучно змінені вхідні дані, які при незначних, непомітних для людини змінах, здатні спричинити істотні помилки в результатах аналізу. Такі уразливості ставлять під сумнів надійність використання ШІ в роботі з цифровими слідами, особливо в умовах змагальності судового процесу.

Аналіз чинного законодавства України свідчить про відсутність належного нормативного врегулювання ключових аспектів застосування систем штучного інтелекту у сфері кримінального провадження. Аналогічна ситуація простежується і в інших галузях права, що обумовлює міждисциплінарний характер проблеми.

По-перше, не визначено правовий статус результатів, отриманих за допомогою ШІ. Це створює правову прогалину щодо можливості визнання таких результатів належними, допустимими, достовірними та достатніми доказами у кримінальному провадженні. Відсутність чітких критеріїв оцінки ставить під сумнів можливість процесуального використання інформації, яка була сформована або оброблена штучним інтелектом.

По-друге, законодавство не містить уніфікованих правил перевірки (верифікації) цифрових слідів, які були зібрані, ідентифіковані або проаналізовані автоматизованими засобами на основі ШІ. Це ускладнює оцінку їх достовірності, а також створює ризики використання доказів, що не відповідають критеріям наукової обґрунтованості, відтворюваності та об'єктивності.

По-третє, відсутні чіткі алгоритми розподілу відповідальності у разі помилок або збоїв під час прийняття рішень. Виникає питання: хто саме повинен нести юридичну відповідальність за наслідки використання ШІ – розробник програмного забезпечення, оператор системи, експерт, який застосовував інструмент ШІ, чи слідчий, що обґрунтовував прийняття процесуальних рішень на відповідних результатах? Така невизначеність має прямі наслідки для забезпечення га-

рантій справедливого судового розгляду, дотримання прав сторін, а також ефективного захисту від можливих технічних або процедурних зловживань.

Системи штучного інтелекту, за умов їх неналежного або неконтрольованого застосування у кримінальному провадженні, можуть стати джерелом серйозних порушень прав учасників процесу. Передусім ідеться про ризики, пов'язані з основоположними засадами кримінального судочинства та стандартами справедливого правосуддя. У випадках, коли сторона захисту не має доступу до архітектури алгоритму, параметрів його навчання або методики оброблення цифрових слідів, постає реальна загроза обмеження права на захист, зокрема права на ефективне заперечення доказів, які використовуються проти обвинуваченого. Також, використання алгоритмів, навчених на упереджених, нерепрезентативних даних, може призводити до формування дискримінаційних або стереотипних висновків. Такі ситуації вже фіксувалися в міжнародній практиці – коли штучний інтелект демонстрував статистичну схильність до обвинувальних висновків щодо представників окремих етнічних, соціальних або демографічних груп. Так, під час журналістського розслідування було виявлено щонайменше 8 випадків неправомірних арештів у різних штатах США, де алгоритми розпізнавання обличчя дали хибні збіги. Більшість постраждалих – афроамериканці, що підтверджує існування системної упередженості [11].

Штучний інтелект навчається на наявних даних, і у разі, якщо вихідні цифрові сліди були спотворені, підроблені або отримані з порушенням законодавства, висновки, сформовані на їх основі, також будуть недостовірними та такими, що не відповідають дійсності. Крім того, системи ШІ не завжди здатні розрізняти автентичні сліди від підроблених, особливо коли фальсифікація виконана з використанням сучасних, високотехнологічних методів того самого ШІ. Це створює суттєві ризики для точності, достовірності та допустимості доказів, що базуються на автоматизованому аналізі цифрових даних.

Висновки. Таким чином, системи штучного інтелекту дають змогу автоматизувати процеси виявлення, класифікації та інтерпретації цифрових слідів з високим рівнем точності. Вони здатні виявляти приховані взаємозв'язки між об'єктами, виявляти аномалії у поведінці окремих осіб, відновлювати ланцюги подій і формувати доказові гіпотези на основі комплексного аналізу цифрових даних. Крім того, технології штучного інтелекту можуть бути інтегровані в процедуру судових експертиз, істотно прискорюючи дослідження та інтерпретацію цифрових доказів. Одночасно, незважаючи на високу потенційну ефективність застосування штучного інтелекту під час роботи з цифровими слідами, його впровадження пов'язано з низкою суттєвих ризиків і проблем, які потребують комплексного нормативного врегулювання, розроблення етичних стандартів та підвищення цифрової грамотності всіх учасників кримінального провадження. Без належного вирішення цих питань широкомасштабне, необґрунтоване використання ШІ у сфері кримінального судочинства може поставити під загрозу засади кримінального судочинства, що є недопустимим апіорі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шевчук В. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. *Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія / В.Ю. Шенітько, Г.К. Авдєєва, В.М. Шевчук та ін.* Харків: Право, 2024. С. 83–106. URL: <https://ivpz.kh.ua/wp-content/uploads/2025/01/Монографія-Криміналістів-2024.pdf> (дата звернення: 20.07.2025).
2. Белова М.В., Белов Д.М., Рушак І.В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично порівняльне правознавство*. 2025. № 1. URL: <https://journal-app.uzhnu.edu.ua/article/view/324040> (дата звернення: 20.07.2025).
3. Карчевський М.В., Куковинець Д.О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. URL: <https://pbz.nlu.edu.ua/article/view/301290> (дата звернення: 20.07.2025).
4. Негребецький В.В. Використання систем штучного інтелекту у боротьбі зі злочинністю: огляд та перспективи. *Українська поліцейстика: теорія, законодавство, практика*. 2024. DOI: <https://doi.org/10.32782/2709-9261-2024-1-9-13> (дата звернення: 20.07.2025).

5. Плахотнік О.В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4 (опубліковано 24.01.2020). URL: <https://vkslaw.com.ua/index.php/journal/article/view/222> (дата звернення: 20.07.2025).
6. Червеко К.О. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. DOI: <https://vca.univd.edu.ua/index.php/vca/article/view/43> (дата звернення: 20.07.2025).
7. Shevchuk V.M. Development trends in criminalistics in the era of digitalization. *Modern knowledge: research and discoveries: I International Scientific and Practical Conference* (May 19–20, 2023; Vancouver, Canada). 2023. Pp. 198–219. URL: <https://archive.interconf.center/index.php/2709-4685/issue/view/19-20.05.2023/165> (дата звернення: 14.07.2025).
8. Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2023. № 10. С. 472–475. URL: http://lsei.org.ua/10_2023/114.pdf (дата звернення: 14.07.2025).
9. Авдєєва Г. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики*. 2018. С. 90–93. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf (дата звернення: 20.07.2025).
10. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. Вип. 85, ч. 4. С. 71–75. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/12-3.pdf> (дата звернення: 20.07.2025).
11. MacMillan D. Arrested by AI: Police ignore standards after facial recognition matches. *The Washington Post*. 13 січня 2025. URL: <https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/> (дата звернення: 20.07.2025).