

Запровадження штучного інтелекту у процес проведення судових експертиз в Україні

Денис Паршин

науковий співробітник лабораторії інформаційно-аналітичного забезпечення судово-експертної діяльності, сертифікації та контролю якості досліджень, Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м. Харків, Україна, e-mail: parshyn.denys@hniise.gov.ua

Андрій Медвідь

науковий співробітник відділу підвищення кваліфікації судових експертів, Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м. Харків, Україна, e-mail: mad.grizzlee@gmail.com

Олександр Романь

науковий співробітник лабораторії інформаційно-аналітичного забезпечення судово-експертної діяльності, сертифікації та контролю якості досліджень, Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м. Харків, Україна, e-mail: roman.oleksandr@nncise.org.ua

Проаналізовано можливості впровадження штучного інтелекту у процес проведення судових експертиз в Україні. Розглянуто переваги застосування інтелектуальних систем для опрацювання даних, пришвидшення аналізу матеріалів справ і підвищення об'єктивності висновків. Виокремлено основні виклики, із якими стикається впровадження штучного інтелекту в судово-експертну діяльність, поміж яких правові обмеження, етичні аспекти й технічні труднощі. Окреслено перспективи розвитку цього напрямку та можливі шляхи подолання наявних бар'єрів.

Ключові слова: *судова експертиза; штучний інтелект; інтелектуальний асистент; цифрові технології.*

Introduction of Artificial Intelligence Into the Forensic Examination Process in Ukraine

Denys Parshyn, Andrii Medvid,

Oleksandr Roman

The article analyzes the possibilities of introducing artificial intelligence into the forensic examination process in Ukraine. The benefits of using intelligent systems to process data, speed up the analysis of case files, and increase the objectivity of expert opinions were considered. The authors highlight the main challenges facing the introduction of artificial intelligence in forensic activities, including legal restrictions, ethical aspects, and technical difficulties. The prospects for the development of this area and possible ways to overcome the existing barriers were outlined.

Keywords: *forensic examination; artificial intelligence; intelligent assistant; digital technologies.*

Штучний інтелект (далі — ШІ) здатний допомогти експертам в опрацюванні відео-, аудіозаписів, зображень і текстових документів [1—3]. Алгоритми можуть знаходити обличчя, номерні знаки автомобілів або певні предмети. У разі аудіоаналізу можливе попереднє визначення емоційного стану мовця або розпізнавання ключових слів, після чого експерт перевіряє та підтверджує результати. Алгоритми розпізнавання рукописного тексту здатні аналізувати особливості почерку, допомагаючи виявляти підробки. Робота з великими масивами даних дає змогу ШІ більш точно виявляти певні закономірності під час аналізування почерку. Біоінформатичні алгоритми значно прискорюють аналіз генетичного матеріалу. Вони автоматично порівнюють ДНК-профілі, допомагаючи експертам швидше знаходити збіги й відповідності. ШІ може посприяти створенню 3D-реконструкцій місця злочину на основі фотографій або сканування місцевості. Такі моделі дають змогу експертам точніше аналізувати траєкторії пострілів, сліди крові або розташування об'єктів. Голосові аналізатори здатні допомогти експертам у попередній ідентифікації особи за тембром голосу або виявленні маніпуляцій у записах. За допомогою спектрального аналізу ШІ здатний швидко визначити хімічний склад, походження та можливий вплив будь-якої речовини [4].

Різні країни проводять дослідження та експерименти щодо впровадження ШІ в судову експертизу. Сполучені Штати Америки є одним із лідерів у застосуванні цифрових технологій

у правоохоронній діяльності. ФБР активно послуговується автоматизованими системами аналізу, поміж яких система ідентифікації відбитків пальців *IAFIS* [5]. Програми аналізу цифрових доказів застосовують для розшифрування й інтерпретації даних із мобільних пристроїв, комп'ютерів та інших електронних носіїв [6, 7]. Жоден висновок у кримінальних справах не базується лише на висновках ШІ — усі результати проходять перевірку експертами.

У країнах ЄС триває активна наукова робота щодо впровадження ШІ у сферу цифрової криміналістики [8]. Наприклад, у Франції розробляють системи аналізу відео з камер спостереження, у Німеччині тестують алгоритми для швидкого розпізнавання фальшивих документів, у Великій Британії впроваджують технології ідентифікації маніпуляцій із цифровими файлами. Водночас на законодавчому рівні застосування ШІ як основного інструмента експертизи не дозволено.

Китай широко застосовує алгоритми розпізнавання обличчя та автоматизованого аналізу доказів, наприклад за допомогою системи *Skynet* [9]. Незважаючи на це, остаточні рішення залишаються за людиною.

В Індії активно впроваджують цифрові технології для автоматизації аналізу почерку й виявлення аномалій у цифрових доказах [10], проте ці технології поки що не мають офіційного статусу в судовій практиці. Розвиток ШІ у сфері судових експертиз в Україні відкриває нові можливості для підвищення ефективності роботи експертів. Очікується поглиблена інтеграція

ШІ в аналітичні платформи, розвиток адаптивних навчальних алгоритмів, автоматизована перевірка достовірності доказів, співпраця з міжнародними організаціями, автоматизація виявлення аномалій у доказах і розвиток гібридних експертних систем [11]. Важливо пам'ятати, що ШІ не замінює експертів, а є інтелектуальним асистентом.

Запровадження ШІ у процес проведення судових експертиз сприятиме підвищенню точності та швидкості аналізу доказів [4, 6, 11]. Для успішної інтеграції необхідно створювати відповідні технічні рішення та правові й етичні механізми.

Перелік джерел посилання

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Elsevier, 2011. 26 p. URL: https://booksite.elsevier.com/samplechapters/9780123742681/Front_Matter.pdf (дата звернення: 28.03.2025).
2. Garfinkel S. L. Digital forensics research: The next 10 years. *Digital Investigation*. 2010. Vol. 7. Suppl. Pp. S64—S73. DOI: 10.1016/j.diin.2010.05.009 (дата звернення: 28.03.2025).
3. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology. NIST SP 800-86, Aug 2006. DOI: 10.6028/NIST.SP.800-86 (дата звернення: 28.03.2025).
4. AI Uses in Forensic Science: Challenges and Opportunities / SIFS: web. Aug 25, 2024. URL: <https://www.sifs.in/events/blog-details/ai-uses-forensic-science-challenges-opportunities-mark-anthony> (дата звернення: 28.03.2025).
5. The Integrated Automated Fingerprint Identification System. U. S. Department of Justice ; FBI / FBI : web. URL: https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/iafis_0808_one-pager825 (дата звернення: 28.03.2025).
6. Lillis D., Becker B., O'Sullivan T., & Scanlon M. Current Challenges and Future Research Areas for Digital Forensic Investigation. *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*. Daytona Beach, FL, USA; May 2016. 11 p. DOI: 10.13140/RG.2.2.34898.76489 (дата звернення: 28.03.2025).
7. Khindre M., Monga D. The Role of Artificial Intelligence (AI) in Digital Forensic. *International Journal of Law, Policy and Social Review*. 2023. Vol. 5. Is. 4. Pp. 121—123. URL: <https://www.law-journals.net/assets/archives/2023/vol5issue4/5130-1701684595237.pdf> (дата звернення: 28.03.2025).
8. Artificial Intelligence (AI) in Criminal Justice. Dublin & Online, 13—14 June 2024 / ERA — Academy of European Law : web. URL: https://www.era.int/cgi-bin/cms?_SID=NEW&_sprache=en&_bereich=artikel&_aktion=detail&idartikel=132557 (дата звернення: 28.03.2025).
9. Sehyeon Baek D. Skynet Project in China – The Rise of Ubiquitous Surveillance / Medium : web. Nov 1, 2024. URL: <https://medium.com/@davidsehyeonbaek/skynet-project-in-china-the-rise-of-ubiquitous-surveillance-33fee53c350e> (дата звернення: 28.03.2025).
10. NIST : web. URL: <https://www.nist.gov/> (дата звернення: 28.03.2025).
11. Ministry of Justice of Ukraine : web. URL: <https://minjust.gov.ua/> (дата звернення: 28.03.2025).