

2. Конституція України Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.
<https://zakon.rada.gov.ua/laws/show/%D0%B2%D1%80#Text>

3. Науково-практичний коментар Кримінального кодексу України /Д.С. Азаров, В.К. Гришук, А.В. Савченко; за заг.ред. О.М. Джужі, А.В. Савченка, В.В. Чернея. 2-ге вид., перероб. і допов. Київ: Юрінком Інтер, 2018. 1104 с.

4. Про авторське право і суміжні права: Закон України від 1 грудня 2022 року № 2811-IX
<https://zakon.rada.gov.ua/laws/show/2811-20#n855>

5. Про охорону прав на промислові зразки: Закон України від 15 грудня 1993 року № 3688-III
<https://zakon.rada.gov.ua/laws/show/3688-12#Text>

6. Филь Р. С. Кримінально-правова охорона прав на об'єкти промислової власності в Україні : дис... канд. юрид. наук: 12.00.08. Київ, 2018. 268 с.

*Збаржевська О.,
здобувач ступеня вищої освіти магістра
Національної академії внутрішніх справ
Консультант з мови: Богуцький В.*

THE ROLE OF ARTIFICIAL INTELLIGENCE IN DIGITAL FORENSICS: INTERNATIONAL PRACTICE

Digital forensics is undergoing a fundamental transformation driven by the exponential growth in data volume and complexity. Traditional digital forensic techniques are fundamentally labor-intensive, time-consuming, and prove ineffective when confronted with large-scale and sophisticated cyber incidents. Human investigators often struggle with the sheer volume and variety of digital evidence encountered in contemporary investigations. [1]

Despite technological advantages, the widespread implementation of AI is constrained by the need to overcome ethical (bias), legal (admissibility of evidence), and technical (the “black box” problem – XAI) challenges. This necessitates the unification of approaches and the development of international standards.

The aim of the study is to analyze international practices of AI application in digital forensics, identify key directions of its use (triage, deep learning), and outline the main challenges faced by leading global jurisdictions (the USA, the United Kingdom, the EU).

Artificial intelligence is becoming a key tool in digital forensics, as it provides the automation of triage, analysis of multimedia evidence, and processing of large data arrays, which significantly increases the efficiency of investigators' work. Traditional forensic methods – often relying on manual triage, keyword searches, and investigator intuition, struggle to cope with this scale and complexity [2]. Machine learning algorithms have significantly improved the process of forensic triage, allowing investigators to quickly classify and categorize large numbers of digital files based on their relevance to an investigation [3]. Deep learning models demonstrate high accuracy in face recognition, audio transcription, and detection of manipulated media including deepfakes.

In the United States, law enforcement agencies are actively integrating AI into digital forensics to increase the efficiency and speed of investigations. AI is revolutionizing digital forensics, enabling the police to uncover critical evidence more quickly, solve cases with greater precision, and potentially shield investigators from the toll of repeatedly viewing disturbing content [4]. For example, the analysis of large volumes of data – text messages, logs, videos, or audio – using AI allows for “unburdening” human resources and reducing data processing time, which could previously take weeks or months. Integrating machine learning into digital forensics enhances the ability to detect anomalies and improve the efficiency of investigations [5]. At the same time, this implementation of AI in the US is accompanied by organizational challenges: a recent study emphasizes that the rise of “AI-driven cybercrime and deepfake fraud” requires agencies – particularly the Federal Bureau of Investigation (FBI) – to modernize their structure, improve interagency cooperation, and ethical regulation to use AI effectively and responsibly [6]. Thus, the US experience demonstrates that AI can significantly enhance the capabilities of digital forensics – provided adequate resources, legal procedures, and control.

In the United Kingdom, the use of AI in criminal justice covers almost all stages of the investigation and judicial process – from the analysis of digital evidence to case management, indicating a systemic approach to the integration of new technologies. At every stage of the

criminal process, at least one actor is using AI in some form [7]. For example, the police in England and Wales use AI for operational support, automating requests and editing documents, which significantly accelerates routine procedures (one implementation reduced authorization time from several hours to a minute). Machine learning and automated evidence review systems are applied to analyze and sort large data arrays – logs, images, videos, documents – for selecting relevant content, allowing for a substantial reduction in the workload on investigators and lawyers. However, although formal legislative regulations concerning AI in the criminal process are still absent, professional bodies have already issued directives and principles (for police, judges, lawyers) that establish standards for the responsible, transparent, and controlled application of AI. Thus, the British experience demonstrates that AI can be implemented systematically, bringing digital forensics closer to modern realities, but only under the condition of appropriate procedures, institutional control, and adherence to ethical standards.

In EU countries, the development of the legal and institutional environment allows for the integration of AI into criminal proceedings and digital forensics, establishing a base for coordinated, regulated use of such technologies. As noted, Eurojust – the EU Agency for Criminal Justice Cooperation – established a special AI group within its Cybercrime Working Group to “monitor legislative developments” and facilitate the implementation of AI by law enforcement and judicial authorities. On the one hand, AI tools can significantly enhance the capabilities for analyzing digital evidence, processing large volumes of data, and international information exchange within the EU – which is crucial for cross-border cases and cybercrime. On the other hand, the EU has adopted a regulatory framework: specifically the Artificial Intelligence Act, which classifies types of AI applications by risk level, establishes mandatory requirements for “high-risk” systems (transparency, human rights impact assessment, control, and audits), and prohibits certain applications, particularly real-time biometric recognition in public spaces without strict conditions. At the same time, experts note that the regulation of AI in the criminal process in the EU remains fragmented, and further harmonization of norms, clear standards for the evidentiary value of AI-analytics, and guarantees of human rights protection are needed.

The use of AI in digital forensics generates serious ethical and legal challenges, particularly concerning the admissibility of evidence, algorithm transparency, and the protection of the rights of participants in the process. While AI can substantially enhance forensic analysis, there are significant concerns about the accuracy and reliability of AI-generated results [8]. Additionally, many AI models function as “black-boxes”, and it is unclear how exactly they arrived at their conclusions, which complicates the substantiation of digital evidence in court – the decision-making processes are often opaque, making it difficult for forensic experts to explain how a conclusion was reached [2]. Furthermore, publications emphasize the risks of violating fundamental rights – privacy, fair trial, the right to defense – if there are no clear standards and regulations. The absence of a proper regulatory framework for the use of AI in criminal justice creates a threat to the violation of the rights of participants in the process [8]. Thus, although AI has the potential to significantly increase the effectiveness of digital forensics, its application remains ethically and legally sensitive, requiring the development of transparent, standardized, and legally enshrined procedures and guarantees.

Artificial intelligence is transforming digital forensics by automating triage, analyzing multimedia evidence, and processing large datasets efficiently. Experiences from the USA, the UK, and the EU show its potential to enhance investigations, while highlighting organizational, ethical, and legal challenges. Effective AI adoption requires standardized procedures, regulatory frameworks, and safeguards to ensure transparency, fairness, and the protection of fundamental rights. Properly managed, AI can make digital forensics faster, more accurate, and more reliable.

References:

1. Rajni R. The Role of Artificial Intelligence in Digital Forensics: Balancing Efficiency and Privacy, 2025. URL: <https://ijrpr.com/uploads/V6ISSUE11/IJRPR55542.pdf> (date of access: 23.11.2025).
2. Vasileva T. Artificial Intelligence and the Transformation of Digital Forensic Investigations, 2025. URL: <https://medium.com/@tedislava.vasileva/artificial-intelligence-and->

the-transformation-of-digital-forensic-investigations-732ee28c7653
(date of access: 23.11.2025).

3. Mandayam R. The Impact of Artificial Intelligence on Digital Forensics, 2024. URL: <https://www.onlinescientificsresearch.com/articles/the-impact-of-artificial-intelligence-on-digital-forensic.pdf> (date of access: 23.11.2025).

4. Amick T. Justin Fitzsimmons, How AI is revolutionizing digital forensics, 2025. URL: <https://www.policechiefmagazine.org/ai-is-revolutionizing-digital-forensics-magnet/> (date of access: 23.11.2025).

5. Collins A., Oye E., Moore J. Integration of Machine Learning in Digital Forensics for Anomaly Detection, 2021. URL: https://www.researchgate.net/publication/389847636_Integration_of_Machine_Learning_in_Digital_Forensics_for_Anomaly_Detection (date of access: 23.11.2025).

6. Leo S. F. Lin. Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud, 2025. URL: <https://www.mdpi.com/2075-471X/14/4/46> (date of access: 23.11.2025).

7. Oxford Institute of Technology & Justice, <https://www.techandjustice.bsg.ox.ac.uk/research/united-kingdom> (date of access: 23.11.2025).

8. Курман О. В., Переваги та проблемні питання використання штучного інтелекту при дослідженні цифрових слідів, 2025. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/44-3.pdf> (дата звернення: 23.11.2025).