

FORENSIC ARTIFICIAL INTELLIGENCE: INNOVATIVE APPROACHES AND INFORMATION TECHNOLOGIES

Natalia Filipenko

Department of Law Faculty of Humanities and Law
National Aerospace University Kharkiv, Ukraine
n.filipenko@khai.edu, <https://orcid.org/0000-0001-9469-3650>

Aleksandar Ivanović

University od Novi Pazar
Novi Pazar, Serbia
aleksandar@t-com.me, <https://orcid.org/0000-0002-8186-0883>

Ergin Hakić

University od Novi Pazar
Novi Pazar, Serbia
e.hakic@uninp.edu.rs, <https://orcid.org/0000-0002-2983-4346>

Abstract

Crime prevention has become one of the most important tasks for public authorities in Ukraine, especially in the context of digitalization and the rapid development of information technologies. The purpose of this article is to enhance crime prevention measures by integrating innovative approaches and digital tools. The article aims to determine the current state and prospects of forensic institutions' activities in crime prevention through the use of information technologies. Forensic institutions occupy a special position among crime prevention actors in Ukraine due to their professional competence and procedural independence. Their preventive activities, carried out either at the request of authorized bodies during criminal proceedings or on their own initiative under relevant legal acts, represent a crucial element of crime prevention. The article identifies key areas of artificial intelligence application in law enforcement and forensic practice, including: satellite image analysis to detect landscape changes related to war crimes and illegal burials; video and photo analysis for object and suspect recognition; audio processing for voice identification and geolocation; social network analysis to establish links between suspects and witnesses; medical data analysis to determine causes of death and identify prisoners of war; and textual information processing to automate evidence search. The authors emphasize that the most promising direction for preventive forensic activities in Ukraine and globally is the introduction of Forensic Artificial Intelligence (FAI). By integrating AI technologies, forensic institutions can increase the efficiency of investigations, reduce the risk of subjective errors, and strengthen the inevitability of punishment. This aligns with Ukraine's Cybersecurity Strategy, updated by the Decree of the President of Ukraine in 2025, and the Concept for the Development of Artificial Intelligence (2020), which remain the main policy documents regulating AI and digital security. Although Ukraine continues the stage-by-stage implementation of the Roadmap for AI Regulation, ongoing legislative initiatives aim to fully harmonize national regulation with the EU Artificial Intelligence Act (2024), ensuring compliance with international standards.

Keywords: criminology, crime prevention, forensic examination, information technologies, innovation, artificial intelligence, cybersecurity, Forensic Artificial Intelligence (FAI).



FORENZIČKA VEŠTAČKA INTELEGENCIJA: INOVATIVNI PRISTUPI I INFORMACIONE TEHNOLOGIJE

Apstrakt

Prevenција kriminaliteta postala je jedan od primarnih zadataka državnih organa u Ukrajini, naročito u svetlu digitalizacije i ubrzanog razvoja informacionih tehnologija. Cilj ovog rada je unapređenje mera za sprečavanje kriminaliteta putem integracije inovativnih pristupa i digitalnih alata. Rad teži da utvrdi trenutno stanje i perspektive delovanja forenzičkih institucija u domenu prevencije kriminaliteta kroz primenu informacionih tehnologija. Forenzičke institucije zauzimaju specifičan položaj među akterima prevencije kriminaliteta u Ukrajini zahvaljujući svojoj profesionalnoj kompetentnosti i procesnoj nezavisnosti. Njihove preventivne aktivnosti, koje se sprovode na zahtev nadležnih organa tokom krivičnog postupka ili na sopstvenu inicijativu u skladu sa relevantnim zakonskim aktima, predstavljaju ključni element sistema suzbijanja kriminaliteta. U radu su identifikovane ključne oblasti primene veštačke inteligencije u sprovođenju zakona i forenzičkoj praksi, što obuhvata: analizu satelitskih snimaka radi detekcije promena u pejzažu povezanih sa ratnim zločinima i ilegalnim grobnicama; analizu video-materijala i fotografija u svrhu identifikacije objekata i osumnjičenih lica; audio-obradu radi identifikacije glasa i geolociranja; analizu društvenih mreža radi utvrđivanja povezanosti između osumnjičenih i svedoka; analizu medicinskih podataka radi utvrđivanja uzroka smrti i identifikacije ratnih zarobljenika; kao i obradu tekstualnih informacija u cilju automatizacije pretrage dokaza. Autori naglašavaju da najperspektivniji pravac preventivnog forenzičkog delovanja, kako u Ukrajini tako i na globalnom nivou, predstavlja uvođenje forenzičke veštačke inteligencije (FVI). Integracijom tehnologija veštačke inteligencije, forenzičke institucije mogu značajno povećati efikasnost istraga, minimizirati rizik od subjektivnih grešaka i osnažiti princip neizbežnosti kazne. Ovakav pristup je u potpunosti usklađen sa Strategijom sajber-bezbednosti Ukrajine (ažuriranom Ukazom predsednika Ukrajine 2025. godine) i Konceptom razvoja veštačke inteligencije (2020), koji predstavljaju temeljne strateške dokumente u regulaciji veštačke inteligencije i digitalne bezbednosti. Iako Ukrajina sprovodi faznu implementaciju Mape puta za regulaciju veštačke inteligencije, aktuelne zakonodavne inicijative usmerene su ka potpunoj harmonizaciji nacionalne regulative sa Aktom o veštačkoj inteligenciji EU (2024), čime se osigurava usklađenost sa međunarodnim standardima.

Ključne reči: kriminologija, prevencija kriminaliteta, forenzičko veštačenje, informacione tehnologije, inovacije, veštačka inteligencija, sajber-bezbednost, forenzička veštačka inteligencija (FVI).

STATEMENT OF THE PROBLEM

Crime remains one of the most critical challenges to human security, affecting all dimensions of public life in the digital age. Its contemporary development is conditioned not only by traditional socio-economic factors but also by the rapid virtualization of criminal activities and the emergence of hybrid threats. Today, crime poses a systemic risk to the integrity of digital infrastructures, the stability of state institutions, and the overall resilience of public structures. As criminal actors increasingly leverage exponential technologies and cross-border digital platforms, their capacity for harm has escalated. This shift necessitates a transition from reactive law enforcement to proactive, technology-driven preventive strategies. In the current environment, effective crime prevention demands a comprehensive state-

level ecosystem that integrates legal safeguards with advanced forensic innovations to address both physical and cyber-physical threats.

From an object-functional perspective, the system of combating crime encompasses three interconnected areas of social relations:

1. General Organisation – a comprehensive set of organizational, managerial, and control actions by various institutions that leverage inter-departmental digital integration to achieve strategic results in crime prevention.
2. Law Enforcement Activity – specific measures implemented by state bodies, public organizations, or citizens to enforce the law, maintain order, and ensure digital justice through the use of verified forensic instruments.
3. Preventive Intervention and Monitoring – a proactive layer of activity focused on the early detection of criminogenic factors through forensic intelligence and automated threat assessment, aimed at neutralizing criminal intent before it materializes.

Crime prevention – actions by specialised subjects, provided for by law, aimed at preventing the development of unlawful intent at the preliminary stages of a criminal offence and identifying the causes and conditions of criminal activity [1, p. 158].

As noted by scholars, crime prevention in the modern legal framework can no longer be viewed as the exclusive prerogative of law enforcement agencies; instead, it constitutes a multi-layered and coordinated ecosystem encompassing all components of the state and social system. This comprehensive approach is based on the involvement of a wide range of actors – from representative bodies and executive authorities to the judiciary, private enterprises, public associations, and individual citizens. Within the contemporary legal landscape, the crime prevention system is defined by the activities of institutions that perform four key strategic functions: (1) defining the strategic directions, tasks, and evidence-based methods of crime prevention rooted in scientific forecasting; (2) providing comprehensive information and analytical support, necessitating the active implementation of Big Data and Artificial Intelligence to process vast arrays of unstructured data; (3) identifying and signaling latent criminogenic factors that often remain invisible to traditional monitoring but can be detected through predictive analytics; and (4) implementing targeted measures to neutralize criminogenic conditions, including the digital and social rehabilitation of individuals aimed at correcting behavioral patterns within the modern information society. Such a functional model facilitates the transformation of the legal order from a reactive to a proactive stance, ensuring a high level of security across both physical and digital environments [2; 3, p. 83].

Depending on their goals and responsibilities, actors can be divided into two groups: those operating at the general social level and specialised actors. The latter include state bodies specifically created to counteract crime, as well as institutions functioning outside the criminal justice system.

A special place in this system is occupied by forensic institutions of Ukraine, which play a decisive role in preventive measures. A forensic expert is a neutral participant in procedural relations, possessing specialised knowledge and skills necessary to solve forensic tasks. Their role is to assist the court in objectively investigating

circumstances and thereby ensuring the protection of violated or disputed rights [4, p. 2].

Forensic science units (FSUs) and certified specialists are increasingly integrated into the proactive prevention framework, equipped with mandates that extend beyond traditional post-factum examinations. Their role has evolved to include preventive intervention at the earliest stages of criminal activity, such as the formation of intent or preparation, particularly within the digital domain. In this contemporary context, forensic activities are intrinsically preventive: the application of predictive analytical models and advanced research allows for the identification of latent threats and criminal patterns before they escalate into realised offences.

Consequently, forensic experts have become strategic partners in the crime prevention ecosystem. They do not merely strengthen the evidence base but provide high-tech monitoring mechanisms to ensure compliance with the law in complex socio-technical environments. The integration of forensic intelligence into a holistic national security strategy is a decisive step toward reinforcing the rule of law and ensuring public resilience against modern, technology-driven threats.

ANALYSIS OF RESEARCH AND PUBLICATIONS

Karchevskiy M. V., Fedchak I. A., Babenko A. M., Korystin O. E., Obolentsev V. F., and other scholars have examined the theoretical foundations of applying information methods in crime research and prevention [5]. In his work, Fedorov O. V. [7] proposed approaches to the use of information methods for criminological forecasting.

Filipenko N., Lukashevych S., Andreeva O., and Salaeva K. [8] investigated the social and ethical requirements for the use of information and communication technologies and artificial intelligence in modern society. They emphasised that the application of artificial intelligence requires special legal regulation, since it directly affects human life and health, even when used for innovative approaches to crime prevention and detection.

Strukov V. M. and Hnusov Y. V. analysed software products («analytical tools») for data retrieval, analysis, and visualisation based on artificial intelligence, including RICAS [10], ShotSpotter [11], and Palantir Gotham [12] [9, p. 64]. Scholars such as S. Matuilen, V. Shevchuk, and J. Baltrunene studied the challenges of applying AI technologies in law enforcement under martial law, identifying both prospects and gaps in legal regulation within the digital technology sector [13].

In our earlier works [14; 15], we also addressed theoretical and practical aspects of criminological activities of forensic institutions in Ukraine. Using phenomenological, praxeological, historical, functional, and structural methods of analysis, we examined the system of expert institutions and highlighted current problems related to the implementation of advanced technologies in their activities.

The aim of this article is to analyse and identify the most effective areas of artificial intelligence application in law enforcement activities involving forensic experts, based on the latest research of modern Ukrainian and foreign scholars. Particular attention is paid to the integration of AI into forensic practice in line with Ukraine's

National Cybersecurity Strategy (updated for 2025-2026 implementation phase) and the Concept for the Development of Artificial Intelligence (2020), as well as the evolving requirements of the EU Artificial Intelligence Act (2024). These documents, supported by recent national roadmaps for AI regulation, establish the framework for ensuring transparency, accountability, and the procedural admissibility of AI-based methods in criminal proceedings.

Results and Discussion

Criminologists emphasize that the object of preventive influence is a complex phenomenon of both material and intangible nature which, interacting with personality traits, leads to the emergence of criminal motivation, intent, and the commission of an offence. In recent decades, the rapid evolution of the digital landscape has shifted the focus toward «virtual» and hybrid objects of preventive influence. These include digital assets, information flows, and algorithmic environments, which now play a decisive role in the formation of criminal intent and requires specialized forensic monitoring to prevent the escalation of cyber-physical threats. Their identification and clarification through expert research require further study at theoretical, procedural, and applied levels. Such an approach enriches not only forensic activity itself but also the theory and practice of crime prevention and control at all levels – general social, special criminological, and individual [14, p. 231].

Crime prevention is defined in scientific and educational literature as «activities aimed at overcoming criminogenic and harmful contradictions in social relations in order to resolve them and gradually eliminate them (general social prevention), as well as counteracting the implementation of criminal manifestations at different stages (special criminological prevention)» [16, p. 16]. It is also described as «a set of various activities and measures undertaken by the state to improve social relations, eliminate negative phenomena and processes that generate or contribute to crime, and prevent offences at different stages of criminal behavior» [17, p. 156].

General social measures of crime prevention involve «overcoming or limiting criminogenically dangerous contradictions in society and gradually eradicating negative phenomena created by political, economic, psychological, ideological, international, and other factors of criminogenic potential» [16, p. 19]. The objects of such measures include unemployment, decline in morality, prostitution, drug addiction, alcoholism, homelessness, criminal attitudes within the population, shortcomings in regulatory frameworks, and social conflict.

Special criminological crime prevention is defined as «the practice of implementing methods of active influence on phenomena and processes that cause or may cause activation of the criminogenic potential of society in the form of criminal manifestations, as well as anticipation of their implementation at different stages of criminal behavior» [16, p. 21].

The object of special criminological crime prevention in the contemporary legal landscape includes two key components: firstly, criminogenic phenomena and processes that manifest at the pre-criminal stage or during criminal activity, and

secondly, the fundamental social values and digital assets threatened by such acts. The effectiveness of prevention measures depends on a synergy of factors: (1) a deep understanding of the preventive influence object, accounting for the nature of criminogenic processes and the specifics of protected values; (2) the competence of preventive actors, requiring a clear definition of powers and coordinated interaction among institutions; and (3) scientifically grounded methods, including modern digital instruments that reflect the capacities of the actors involved. Thus, a systematic approach must be based on a robust relationship between the object, subject, and methods of preventive influence to ensure maximum efficiency in combating crime.

In recent decades, the rapid evolution of information technologies has fundamentally transformed this preventive framework. New «virtual» and hybrid objects of preventive influence have emerged, particularly within the sphere of complex cybercrime. This encompasses unauthorized access to information systems, data theft, the distribution of malicious software, and sophisticated forms of digital fraud. These offences do not merely cause material damage; they violate fundamental digital rights, including the right to privacy, data sovereignty, and overall cybersecurity. Consequently, the integration of forensic intelligence into the monitoring of these virtual objects is now a decisive factor in ensuring the resilience of modern public structures.

Consequently, information as an object of preventive influence requires a special approach to protection, based on innovative technological, organisational, and legal mechanisms. At the state level, particular attention is devoted to cybersecurity, which ensures the protection of vital interests of individuals, society, and the state in cyberspace. This includes sustainable development of the information society, timely detection, prevention, and neutralisation of threats to national security, and safeguarding digital communication environments [18]

It is noteworthy that Ukraine is implementing the Implementation Plan of the Cybersecurity Strategy (updated 2025) [19], which provides for the development of a system of cybersecurity indicators, the creation of specialised units authorised to conduct defensive operations in cyberspace, effective counteraction to intelligence and subversive activities, cyberterrorism, and the strengthening of technological and human resources of law enforcement agencies to prevent and investigate cybercrime. The plan also ensures the security of digital services and aligns national policy with European standards.

The subjects of crime prevention include «state bodies, public organisations, private institutions, social groups, officials, and individuals who direct their activities towards the development and implementation of measures related to the prevention, limitation, and elimination of criminogenic phenomena and processes that generate crimes, as well as their prevention at various stages of criminal behavior» [16, p. 62].

As N. Filipenko notes, «among the domestic subjects of crime prevention, forensic institutions of Ukraine have always stood out for their special competence» [2, p. 87]. She emphasises that expert activity in relation to crime prevention can be defined as the preventive work of employees of expert institutions during civil,

administrative, or criminal proceedings, or on their own initiative under relevant regulations [3, p. 180]. The main tasks of expert prevention include: developing and improving methods for identifying the causes and conditions of criminal offences; studying typical results of expert research and providing recommendations for crime prevention; determining measures to protect objects from criminal attacks; designing preventive strategies against criminal offences [3, p. 100].

Experts also highlight that «almost every branch of science has acquired its forensic dimension. In judicial proceedings, there is a need to engage forensic experts of various specialisations, who apply modern, specific, and sophisticated methods in their work» [20, p. 26].

Due to the rapid digitalisation of criminal offences, the preventive activities of forensic institutions in Ukraine have acquired a strategic dimension, particularly in counteracting complex cyber-threats. Their role has expanded to encompass four critical pillars: (1) advanced digital forensics, involving the deep-layer investigation of digital traces and documentation of unauthorised access; (2) the development of innovative forensic methods for real-time analysis of malicious software and information flows; (3) comprehensive legal support to ensure the procedural admissibility of digital evidence under the latest legislative standards; and (4) specialised education, focusing on the training of experts capable of addressing emerging cyber-threats. Consequently, the detection and evaluation of digital traces are no longer merely technical tasks but have become the core components of a proactive crime prevention strategy adapted to the requirements of a high-tech society.

In this context, Computer and Technical Expertise (CTE) has become increasingly vital. The primary task of experts within the CTE framework is to apply specialised knowledge in computer forensics to the systematic search, securing, and examination of digital evidence. Modern CTE enables the formation of a holistic evidence base by addressing both diagnostic and identification challenges, including the forensic recovery and analysis of information contained within complex, often encrypted, computer systems. By integrating these high-tech examinations into the investigative process, forensic institutions provide the necessary mechanisms to identify digital footprints and establish the factual circumstances of cyber-dependent and cyber-enabled crimes. As a result, CTE conducted during investigations of information security breaches generates valuable insights into vulnerabilities within information processing systems [21, p. 171].

In preventive activities of forensic institutions, information methods based on artificial intelligence (AI) are increasingly applied. Scholars note that “artificial intelligence in forensic science can be used to process and analyse large amounts of data, with emphasis on interpretation. AI helps overcome shortcomings of forensic investigation and human error, primarily by improving, accelerating, and facilitating investigations” [22; 23].

The Concept for the Development of Artificial Intelligence in Ukraine (2020) [24] defines AI as «an organised set of information technologies used to perform complex tasks through scientific research methods and algorithms for processing

information, creating and using knowledge bases, decision-making models, and algorithms for achieving defined objectives».

Artificial intelligence technologies are increasingly influencing public life, shaping both opportunities and the degree of protection of social values [25, p. 1085]. Functionally, AI is a software-based information processing system formed by interconnected computing nodes, capable of accumulating knowledge, generalising it, and presenting it in a form convenient for interpretation and decision-making [26].

Modern research highlights the extensive capabilities of Artificial Intelligence (AI) in law enforcement and preventive forensics. The most critical areas of its application currently include: (1) automated satellite imagery analysis for detecting landscape changes indicative of war crimes, such as mass graves or destruction of infrastructure; (2) multimodal biometric identification, including facial recognition and behavioral analysis in video and photo materials; (3) advanced acoustic processing for voice recognition and geolocation based on ambient sound data; (4) OSINT and social media analytics to uncover hidden connections within criminal networks; (5) automated medical and forensic data processing to identify victims or perpetrators and determine causes of death; and (6) natural language processing (NLP) for the rapid analysis of vast volumes of textual evidence and communications. The integration of these technologies significantly enhances the precision and velocity of investigations while mitigating the risks associated with human cognitive biases.

A pivotal advancement in this field is the introduction of Forensic Artificial Intelligence (FAI), conceptualised as an intellectual decision-support system (IDSS). FAI is designed to accelerate forensic data processing and provide structured, data-driven insights to judges, prosecutors, and legal counsel. However, within the current legal framework of 2026, the application of FAI must strictly adhere to the «human-in-the-loop» principle. This ensures that every AI-generated analytical output remains subject to mandatory validation and interpretation by certified forensic specialists who retain procedural accountability. Such a safeguard is indispensable for maintaining the legal admissibility of evidence, ensuring transparency, and upholding the standards of a fair trial in the digital age.

At the same time, researchers underline that the integration of FAI inevitably raises ethical and legal challenges. These include the protection of sensitive personal data (DNA profiles, fingerprints, digital traces), the risk of technological malfunctions or cyberattacks, and the unresolved issue of responsibility in case of errors. As noted in recent scholarship, «the most important aspect of FAI's work is ethics, followed by security, transparency, impartiality, and privacy protection» [27, p. 20]. International standards, such as the EU Artificial Intelligence Act (2024), further stress that AI systems cannot be recognised as independent legal subjects but must remain tools under human control.

Practical applications of FAI include automated fingerprint and DNA analysis, forensic ballistics, toxicology, and digital forensics. By automating routine tasks, FAI enables human experts to concentrate on interpretive and evaluative aspects of investigations, thereby enhancing both efficiency and fairness in judicial decision

making. The hardware component of FAI would consist of electronic and mechanical parts enabling AI operations, while the software would include programmes for managing the system and processing forensic data. FAI could also collect information from scientific and professional networks across specific forensic disciplines, making relevant data available to all participants in court proceedings in real time.

Additionally, FAI may conduct meta analyses of data extracted from monographs, textbooks, journals, and studies, transforming metadata into simplified and useful information for legal practitioners. By storing and analysing vast amounts of forensic data, FAI would significantly reduce the time required for evidence collection and verification, thereby enhancing the reliability of judicial decisions by confirming or refuting evidence more efficiently [27, p. 19].

CONCLUSION

Summarising the results of applying innovative approaches and information technologies in forensic expert activity for crime prevention and detection, the following points can be highlighted:

1. The primary tasks of forensic institutions in Ukraine encompass a comprehensive analysis of the systemic causes and conditions contributing to criminal offences, including those emerging in the digital environment. This involves the development of advanced high-tech methods for crime detection and the formulation of practical recommendations aimed at eliminating these factors through evidence-based preventive measures and digital forensics.
2. The results of forensic research provide law enforcement agencies with high-precision analytical tools that significantly enhance operational efficiency. This ensures more effective investigation of complex crimes and reinforces the principle of the inevitability of punishment through irrefutable digital and physical evidence. The successful implementation of these tasks strengthens the resilience and protection of critical infrastructure, maintains public order, and systematically reduces crime rates. Consequently, forensic institutions evolve beyond traditional research roles, performing proactive preventive functions that are vital for the development of a modern, technology-driven national crime prevention strategy.
3. Artificial intelligence techniques have evolved into fundamental technological tools for forensic experts, enabling the multimodal analysis of vast and heterogeneous datasets. These technologies automate the detection of complex criminal patterns and provide high-accuracy predictive analytics for forecasting potential security threats. Advanced AI algorithms facilitate in-depth research through the automated processing of unstructured data – including text, video, and audio – allowing for the identification of latent connections between participants in criminal networks and the discovery of digital evidence that would remain inaccessible through traditional manual methods.
4. The implementation of Forensic Artificial Intelligence (FAI) represents a promising direction for the preventive activities of forensic institutions in Ukraine and globally. Conceptualised as an intellectual decision-support system (IDSS), FAI

significantly accelerates the processing of complex datasets and minimises the risk of subjective cognitive biases. Its practical applications encompass AI-driven satellite imagery analysis for detecting and documenting war crimes in accordance with international protocols (e.g., the Berkeley Protocol), as well as the automation of fingerprint, DNA, ballistic, toxicological, and digital forensic examinations. However, current legal doctrine and EU-aligned regulations strictly mandate that FAI applications follow the "human-in-the-loop" principle. This ensures that every AI-generated analytical output is rigorously validated and interpreted by certified forensic specialists who bear procedural responsibility. Such a safeguard is essential to guarantee compliance with national criminal procedural law and to preserve the transparency, reliability, and accountability of evidence in judicial proceedings.

5. At the same time, the integration of FAI raises critical ethical and legal challenges that require constant regulatory monitoring. These include ensuring the high-level protection of sensitive personal data, mitigating the risks of algorithmic bias, and addressing technological vulnerabilities to cyberattacks. Under current legal frameworks, including the fully implemented EU Artificial Intelligence Act (2024) and harmonised national legislation, the legal liability for errors remains with the human operator or the institution using the system, rejecting any notion of AI as an independent legal subject. International standards explicitly mandate that AI systems must remain socio-technical tools under meaningful human control, ensuring that accountability and transparency are maintained throughout the entire forensic lifecycle.

6. Balancing technological innovation with ethical responsibility remains the foundational condition for the legal admissibility and legitimacy of FAI-generated outputs in criminal justice. Only through the implementation of robust human oversight mechanisms and clearly defined ethical filters can FAI effectively contribute to enhancing both the operational efficiency and the procedural fairness of judicial decision-making. Adherence to these principles ensures that the integration of artificial intelligence serves to uphold the rule of law rather than undermining the fundamental rights of participants in the trial.

REFERENCES

1. Ahmed Alaa El-Din, E. (2022) Artificial intelligence in Forensic Science: invasion or revolution? *Egyptian Society of Clinical Toxicology Journal*, 10(2), 20-32. [in English].
2. Aleksandar Ivanović, Natalia Filipenko (2024) Proposal for Introducing the Institution of Forensic Artificial Intelligence. *Aktual'ni pytannya sudovoyi ekspertyzy i kryminalistyky : zb. mat-liv Mizhnar. nauk.-prakt. konf., prysvyachenoyi pam"yati vydatnoho vchenoho Vladyslava Fedorenka («Fedorenkivs'ki chytannya»)* (Kharkiv, 15.10.2024). Kharkiv : NNTS «ISE im. Zasl. prof. M. S. Bokariusa», 2024. C. 16-20.
3. Aleksandar Ivanović, Nataliia Filipenko. Acceptance of Forensic Evidence — Are There Standards? (2023). *Aktualjni pytannja sudovoji ekspertyzy i kryminalistyky: zb. mat-liv mizhnar. nauk.-prakt. konf. z naghody 100-richchja Nacionaljnogho naukovogho centru «Instytut sudovykh ekspertyz im. Zasl. prof. M. S. Bokariusa»*

- (Kharkiv, 10.11.2023). Kharkiv : NNC «ISE im. Zasl. prof. M.S. Bokarius», 2023. S. 22-27. <http://www.ndekc.lviv.ua/pdf/c05122023.pdf> [in English].
4. Budić, M. Š. (2023) Etičke dileme i stavovi prema primeni veštačke inteligencije 1. Kritika: časopis za filozofiju i teoriju društva, 4(1), 49-65. [in English].
 5. Fedorov, O.V. (2023). Zastosuvannya sistemnogo pidhodu u rozrobci ta vikoristanni informacijnih metodik vivchennya zlochinnosti [Application of a systematic approach in the development and use of information methods for the study of crime]. Analitichno-porivnyalne pravoznavstvo - Analytical and comparative jurisprudence, 04, 425-429. DOI <https://doi.org/10.24144/2788-6018.2023.04.68> [in Ukrainian].
 6. Filipenko N. Ye., Obolyentseva-Krasyvs'ka O. S. (2021) Sudovo-ekspertni ustanovy Ukrainy yak sub'yekt protydyi zlochynnosti. Aktual'ni problemy kryminalistychnoho ta ekspertnoho zabezpechennya diyal'nosti pravookhoronnykh orhaniv ta sudu v Ukraini. NDI publichnoyi polityky i sotsial'nykh nauk. Kharkiv, 2021. P. 52-56. [in Ukrainian].
 7. Filipenko N.Y., Lukashevych S.Y. (2023) Informatsiyni metodyky doslidzhennya kryminal'nykh pravoporushen', vchynenykh z vykorystannyam tekhnolohiy shtuchnoho intelektu. Naukovi perspektyvy (Seriya «Derzhavne upravlinnya», Seriya «Pravo», Seriya «Ekonomika», Seriya «Medytsyna», Seriya «Pedahohika», Seriya «Psykholohiya») Vypusk № 11(41)2023. Kyiv. 2023. № 1(7) C.1084-1096. [in Ukrainian].
 8. Filipenko, N. Ye. (2020). Kriminologichna diyalnist sudovo-ekspertnih ustanov Ukrainy [Criminological activity of forensic institutions of Ukraine]. Kharkiv : Collegium [in Ukrainian].
 9. Filipenko, N. Ye., Snigerov, O.P., Bublikov, A.V. (2020). Zastosuvannya specialnih znan pid chas viyavlennya, profilaktiki j rozsliduvannya zlochiniv u sferi komp'yuternoyi informaciyi ta vysokih tehnologij (oglyadova stattya) [Application of special knowledge during detection, prevention and investigation of crimes in the field of computer information and high technologies (review article)]. Teoriya ta praktika sudovoyi ekspertizi i kriminalistiki - Theory and practice of forensic examination and criminology, 22, 162 - 178. Retrieved from <https://khrife-journal.org/index.php/journal/article/download/373/388> [in Ukrainian].
 10. Filipenko, N., Lukashevych, S., Andreyeva, O. i Salayeva, K. (2024). Sotsial'no-pravovi ta moral'no-etychni problemy zastosuvannya shtuchnoho intelektu ta informatsiyno-komunikatsiynykh tekhnolohiy. Visnyk Penitentsiarnoyi asotsiatsiyi Ukrainy. 4 (Sich 2024), 95-103. DOI:<https://doi.org/https://doi.org/10.34015/2523-4552.2023.4.10>. [in Ukrainian].
 11. Golina, V.V. (2011). Zapobigannya zlochinnosti (teoriya i praktika) [Crime prevention (theory and practice)]. Harkiv: Nac. yurid. akad. Ukrainy [in Ukrainian].
 12. Golovkin, B.M., Holina, V.V., Lysodyed, O.V. (2020). Kryminolohiya : pidruchnyk [Criminology: textbook] Holovkin B.M. (Ed.). Kharkiv : Pravo. [in Ukrainian].
 13. Implementaciya ILP modeli v Ukraini [Implementation of the ILP model in Ukraine]. ospace.oduvs.edu.ua Retrieved from <https://ospace.oduvs.edu.ua/server/api/core/bitstreams/c517baeb-f95d-4c77-a0e8-97f808399412/content> [in Ukrainian].
 14. Kryminolohiya. Akademichnyy kurs/kol. avtoriv; za zah. red. O. M. Lytvynova. Kyiv: Kondor, 2018. 588 c. [in Ukrainian].

15. Lemyk L. YA. (2014) Praktyka zastosuvannya spetsial'nykh znan' v tsyvil'nomu protsesi v krayinakh YES (na prykladi Nimechchyny, Frantsiyi ta Velykobrytaniyi). Chasopys Natsional'noho universytetu «Ostroz'ka akademiya». Seriya Pravo. 2014. № 1 (9). С. 1–13. [in Ukrainian].
16. Lukashevich S.Yu., Salayeva K.A. (2023). Ekspertno-kryminalistychni zasady vyznachennya ob'yektiv zapobizhnoho vplyvu [Expert and forensic principles of determining objects of preventive influence]. Aktual'ni pytannya sudovoyi ekspertyzy i kryminalistyky - Current issues of forensic examination and forensics: Proceedings of the 100th anniversary of the National Scientific Center "Institute of Forensic Expertise named after Ex. Prof. M. S. Bokarius" (Kharkiv, November 10, 2023) Kharkiv: NSC "ISE named after Ex. Prof. M. S. Bokarius". (p.p. 229-231). Retrieved from URL: <https://nncise.org.ua/diyalnist/naukova> [in Ukrainian].
17. Matulyene, S., Shevchuk, V., Baltrunene, Yu. (2023). Shtuchnij intelekt v diyalnosti organiv pravoporyadku ta yusticiyi: ukrayinskij ta yevropejskij dosvid [Artificial intelligence in the activities of law enforcement and justice bodies: Ukrainian and European experience]. Teoriya ta praktika sudovoyi ekspertizi i kriminalistiki - Theory and practice of forensic examination and criminology, 4 (29), 12-46. DOI: 10.32353/khrife.4.2022.02. <https://khrife-journal.org/index.php/journal/issue/view/18/4-22> [in Ukrainian].
18. Nataliia Filipenko, Serhii Lukashevych, Olena Andrieieva, Aleksandar Ivanović (2024) Application of Artificial Intelligence and Information and Communication Technologies: Socio-Ethical Problems (Review Article). Теорія та практика судової експертизи і криміналістики. 2024. Випуск 1 (34). DOI: <https://doi.org/10.32353/khrife.1.2024.02> URL: <https://khrife-journal.org/index.php/journal> [in English].
19. Obolentsev, V. F. (2021). Bazovi zasady systemnoho analizu ta modelyuvannya systemy zapobihannya zlochynnosti v Ukraini [Basic principles of system analysis and modeling of the crime prevention system in Ukraine]. Kharkiv, Jurayt, 192 p. Retrieved from: <https://dspace.nlu.edu.ua/handle/123456789/19459> [in Ukrainian].
20. Palantir Gotham www.palantir.com Retrieved from <https://www.palantir.com/platforms/gotham/> [in English].
21. Plan realizatsiyi Stratehiyi kiberbezpeky Ukrainy Vvedeno v diyu Ukazom Prezydenta Ukrainy vid 1 lyutoho 2022 p. № 37/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text> [in Ukrainian].
22. RICAS. Intelktualna platforma analizu informaciyi [Intelligent information analysis platform]. ricas.org Retrieved from <https://ricas.org/uk/> [in Ukrainian].
23. Rozporyadzhennya Kabinetu Ministriv Ukrainy "Pro shvalennya Konceptiyi rozvitku shtuchnoho intelektu v Ukraini" [The Order of the Cabinet of Ministers of Ukraine "On the approval of the Concept of the Development of Artificial Intelligence in Ukraine"]. (n.d). [zakon.rada.gov.ua](https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text) Retrieved from <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>. [in Ukrainian].
24. Rudenko, O. G., Bodyanskij, Ye.V. (2006). Shtuchni nejronni merezhi [Artificial neural networks]. Harkiv : TOV «Kompaniya SMIT» [in Ukrainian].
25. SafetySmart. www.soundthinking.com Retrieved from <https://www.soundthinking.com/safetysmart-platform/> [in English].
26. Strukov, V.M., Gnusov, Y. V. (2021). Instrumental intelligent platforms for criminal analysis. Law and Safety, 83, 4, 64–65 [in English].
27. Zakon Ukrainy «Pro osnovni zasady zabezpechennya kiberbezpeki Ukrainy» [The Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine"]. (n.d).

zakon.rada.gov.ua Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].

REZIME

Prevenција kriminaliteta postala je jedan od primarnih zadataka državnih organa u Ukrajini, naročito u svetlu ubrzane digitalizacije društva i intenzivnog razvoja informacionih i komunikacionih tehnologija. Savremeni oblici kriminaliteta, uključujući sajber-kriminal, transnacionalni organizovani kriminal i krivična dela povezana sa oružanim sukobima, zahtevaju primenu inovativnih, tehnološki zasnovanih pristupa u njihovom suzbijanju i prevenciji. Cilj ovog rada jeste unapređenje postojećih mera prevencije kriminaliteta kroz integraciju savremenih digitalnih alata i metoda, sa posebnim fokusom na primenu veštačke inteligencije u forenzičkoj praksi. Rad nastoji da utvrdi trenutno stanje, izazove i perspektive delovanja forenzičkih institucija u oblasti prevencije kriminaliteta u Ukrajini, analizirajući njihov institucionalni položaj, normativni okvir i operativne kapacitete. Forenzičke institucije zauzimaju specifično mesto među akterima prevencije kriminaliteta zahvaljujući visokom nivou stručnosti, tehničkoj opremljenosti i procesnoj nezavisnosti. Njihove aktivnosti, koje se realizuju kako na zahtev nadležnih organa u okviru krivičnog postupka, tako i proaktivno – na osnovu sopstvenih inicijativa u skladu sa zakonom – predstavljaju važan segment celokupnog sistema suzbijanja kriminaliteta. Posebna pažnja u radu posvećena je identifikaciji ključnih oblasti primene veštačke inteligencije u sprovođenju zakona i forenzičkoj delatnosti. U tom kontekstu analiziraju se mogućnosti primene AI tehnologija u obradi velikih količina podataka, uključujući analizu satelitskih snimaka radi otkrivanja promena u prostoru koje mogu ukazivati na postojanje ilegalnih grobnica ili mesta izvršenja ratnih zločina; obradu video i foto materijala u cilju identifikacije lica, objekata i događaja; naprednu audio-analizu za potrebe identifikacije govornika i određivanja geolokacije; kao i analizu sadržaja društvenih mreža radi mapiranja odnosa između osumnjičenih, svedoka i drugih relevantnih aktera. Dodatno, razmatra se primena AI u analizi medicinskih i biometrijskih podataka radi utvrđivanja uzroka smrti i identifikacije žrtava i ratnih zarobljenika, kao i u obradi tekstualnih podataka kroz automatizaciju pretrage i klasifikacije dokaza. Autori posebno ističu značaj razvoja i implementacije forenzičke veštačke inteligencije (FVI) kao najperspektivnijeg pravca unapređenja preventivnog delovanja. Integracijom ovih tehnologija moguće je značajno povećati efikasnost i brzinu istraga, unaprediti kvalitet prikupljenih dokaza, smanjiti uticaj ljudskog faktora i subjektivnih grešaka, te ojačati princip pravne sigurnosti i neizbežnosti sankcije. Istovremeno, ukazuje se na potrebu uspostavljanja jasnih etičkih i pravnih okvira za primenu AI, kako bi se obezbedila zaštita ljudskih prava, privatnosti i procesnih garancija. Rad takođe analizira strateški i normativni okvir Ukrajine u oblasti digitalne bezbednosti i regulacije veštačke inteligencije. Posebno se razmatra usklađenost predloženih mera sa ključnim nacionalnim dokumentima, uključujući Strategiju sajber-bezbednosti Ukrajine (ažuriranu 2025. godine) i Koncept razvoja

veštačke inteligencije (2020), kao i sa savremenim međunarodnim standardima. U tom smislu, razmatra se proces harmonizacije nacionalnog zakonodavstva sa pravnim tekovinama Evropske unije, naročito sa Aktom o veštačkoj inteligenciji EU (2024), koji postavlja sveobuhvatan regulatorni okvir za bezbednu i odgovornu upotrebu AI tehnologija. Zaključno, rad ukazuje da će systemska i odgovorna implementacija savremenih digitalnih rešenja, uz jačanje institucionalnih kapaciteta i međunarodne saradnje, značajno doprineti unapređenju prevencije kriminaliteta u Ukrajini. Takav pristup ne samo da povećava efikasnost rada nadležnih organa, već i doprinosi jačanju vladavine prava, poverenja građana u institucije i ukupne bezbednosti društva u uslovima digitalne transformacije.