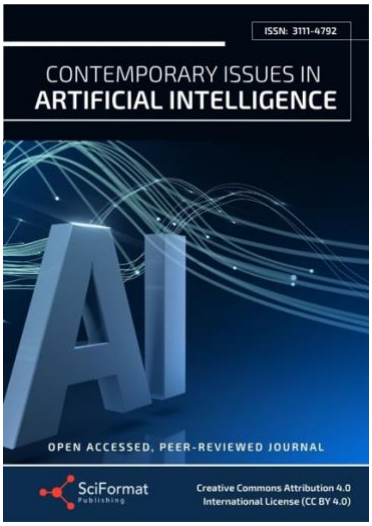




# Contemporary Issues in Artificial Intelligence

**ISSN 3111-4792**

**Vol. 1 (2025)**

SciFormat Publishing

**Publisher:**
**SciFormat Publishing Inc.**

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest,
Calgary, Alberta, Canada,
T3E0A7

+15878858911
editorial-office@sciformat.ca


| | |
|---|---|
| **ARTICLE TITLE** | ARTIFICIAL INTELLIGENCE AND CYBERCRIME: NEW CHALLENGES AND PROSPECTS FOR LEGAL REGULATION |
| **ARTICLE INFO** | Zverev Volodymyr, Bushkov Valery, Khrushkov Borys, Sarychev Volodymyr, Ostaltsev Oleksiy, Prokopovych-Tkachenko Yehor. (2025) Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation. *Contemporary Issues in Artificial Intelligence*. Vol.1. doi: 10.69635/ciai.2025.11 |
| **DOI** | https://doi.org/10.69635/ciai.2025.11 |
| **RECEIVED** | 29 January 2025 |
| **ACCEPTED** | 10 March 2025 |
| **PUBLISHED** | 14 March 2025 |
| **LICENSE** | The article is licensed under a **Creative Commons Attribution 4.0 International License.** |


© The author(s) 2025.
This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

# ARTIFICIAL INTELLIGENCE AND CYBERCRIME: NEW CHALLENGES AND PROSPECTS FOR LEGAL REGULATION

***Zverev Volodymyr***
*Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics, Ukraine*
*ORCID ID: 0000-0002-0907-0705*

***Bushkov Valery***
*Postgraduate Student of the Department of Software Engineering and Cybersecurity of the State University of Trade and Economics, Ukraine*
*ORCID ID: 0009-0005-5097-2689*

***Khrushkov Borys***
*Postgraduate Student of the Department of Cybersecurity and Information Technologies of the University of Customs and Finance, Ukraine*
*ORCID ID: 0009-0002-3978-5012*

***Sarychev Volodymyr***
*Doctor of Economics, Professor, Department of Economics and Economic Security University of Customs and Finance, Ukraine*
*ORCID ID: 0000-0002-8544-9901*

***Ostaltsev Oleksiy***
*Senior Lecturer, Department of Military Training University of Customs and Finance, Ukraine*
*ORCID ID: 0009-0000-6107-4124*

***Prokopovych-Tkachenko Yehor***
*Leading Specialist Department of Military Training University of Customs and Finance, Ukraine*
*ORCID ID: 0009-0002-6023-5066*

**ABSTRACT**

The rapid development of artificial intelligence (AI) is fundamentally changing the methods and scale of cybercrime, and also poses significant challenges for legal regulation. This article highlights the fundamental aspects of the use of AI to commit cyberattacks (automated hacking tools, deep fakes, intellectual fraud, etc.) and considers ways to counter them by law enforcement agencies. The legal aspects related to the extended autonomy of AI systems are examined, leading to new liability issues, problems of assessing deep fakes evidence and the need for international cooperation in cybersecurity field. The rapid development of artificial intelligence (AI) is fundamentally changing the methods and scale of cybercrime, and also poses significant challenges for legal regulation. This article highlights the fundamental aspects of using AI to commit cyberattacks (automated hacking tools, deepfakes, intellectual fraud, etc.) and explores ways in which law enforcement agencies can counter them. It reveals legal aspects related to the extended autonomy of AI systems, which leads to new issues of liability, problems of assessing evidence of deepfakes, and the need for international cooperation in the field of cybersecurity.

The aim of the study is to develop a holistic view of the threats posed by AI tools in the context of cybercrime and to formulate recommendations for improving national and transnational legislation. The article proposes specific mechanisms for ensuring the reliability of digital evidence (from the creation of algorithms for detecting manipulations to methods for analyzing the chain of their storage), highlights the current practice of criminal prosecution in Ukraine and abroad, and also provides proposals for the unification of procedures for forensic analysis of materials obtained or modified with the help of AI. The results of the work show that effective legal counteraction to AI-based cybercrime requires the simultaneous development of technical tools, enhanced protection of human rights, and international harmonization of legal norms. The development of specialized investigation methods, including big data analytics and machine learning technologies, must be balanced with increasing security and transparency standards. Particular attention is paid to the issue of further modernization of training programs for legal professionals and the involvement of experts in the field of cybersecurity, which will allow for a faster response to the dynamics of new threats.

**KEYWORDS**

Artificial Intelligence, Cybercrime, Legal Regulation, Deepfakes, Cybersecurity, AI Autonomy, Digital Evidence, Forensic Analysis, International Cooperation, Machine Learning

**CITATION**

Zverev Volodymyr, Bushkov Valery, Khrushkov Borys, Sarychev Volodymyr, Ostaltsev Oleksiy, Prokopovych-Tkachenko Yehor. (2025) Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation. *Contemporary Issues in Artificial Intelligence*. Vol.1. doi: 10.69635/ciai.2025.11

**COPYRIGHT**

© **The author(s) 2025.** This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

**Introduction.**

In a globalized society, information and technology infrastructure is becoming an object of increased attention from criminal groups. The use of artificial intelligence (AI) is fundamentally transforming the cybercrime landscape, as automated algorithms enable criminals to conduct large-scale, high-tech attacks with minimal human involvement [1]. Deepfakes, intelligent fraud programs and constantly improving hacking methods create a situation in which traditional legislation often fails to keep up with the pace of technological progress [2]. Accordingly, legal regulation is faced with an acute need for innovative approaches that take into account the peculiarities of AI.

The use of AI in criminal activity has a profound impact on the legal sphere: - Automated cyberattacks: committing cyberattacks using neural networks that analyze thousands of vulnerabilities in real time [3]; - Deepfakes and disinformation: the spread of false content can undermine the reputation and influence political processes [4]; - The international nature of threats: attacks and the circulation of illegal data often go beyond the borders of one jurisdiction, complicating the investigation process [5].

The purpose and objectives of the study. The aim of the work is to formulate a systematic understanding of possible legal approaches to the prevention and investigation of cybercrimes committed using AI, as well as to develop methodological recommendations legislation enhancement. The main objectives: - To analyze modern methods of using AI for criminal purposes; - To investigate the existing legal field and identify gaps in the qualification of actions of autonomous systems; - To propose directions for the law enforcement and judicial practice modernization, considering international experience [6,7].

This paper follows the IMRAD structure: the Methods section outlines the research approach, the Results section presents quantitative and qualitative findings, the Discussion section compares findings with existing literature, and the Conclusions summarize key insights and recommendations.

Study uses an interdisciplinary approach that combines legal analytics, cybersecurity research methods, and empirical modeling using artificial intelligence algorithms. The methodological framework covers four key blocks.

Legal analysis and systematization of regulatory acts. - Materials from international conventions in the field of cybercrime are summarized (e.g., the Budapest Convention). - A comparison of national laws of the EU, Ukraine, and the USA is conducted, taking into account the issues of criminalization of acts using AI [8,9].

Content analysis of scientific publications. - Over 100 scientific sources were analyzed, including monographs, articles in professional journals on information law, cybersecurity, and artificial intelligence [10-15]. - Special attention was paid to works that highlight deepfake detection algorithms and examples of their application in judicial practice [4,16,17].

Empirical research and modeling. - A series of experimental runs of cyberattack simulation using neural networks to search for vulnerabilities in web applications were carried out. The model contained 10 conditional attack vectors that imitate the actions of an attacker [3,18]. - To assess the effectiveness of fake image recognition systems, a convolutional neural network trained on 10,000 images was used; the accuracy and false positive rate were analyzed [16,19].

**Table 1.** Brief description of the methods used

| **Method** | **Description** | **Result** |
|---|---|---|
| Legal analysis | Study of laws, international conventions, and case law | Identifying gaps in action qualification using AI |
| Content analysis | Analysis of scientific articles, monographs, reports | Systematization of theoretical models |
| Modeling | Experimental attacks involving AI, deepfake tests | Quantifying the success of attacks, the accuracy of detecting fraud |
| Expert survey | Interviews with lawyers, IT specialists | Defining practical methods for updating legislation |

The application of these methods made it possible to assess in a balanced way both technical and legal aspects of AI-catalyzed cybercrime phenomenon, as well as to prepare practical recommendations for further regulatory regulation improvement.

**1. Statistical indicators of automated cyberattacks success.**

A comparative results analysis of test attacks on a conditional server showed that the use of machine learning algorithms allowed increasing the success hacking rate from 48% (with classical selection of passwords and vulnerabilities) to 82% by using AI scripts with dynamic learning.

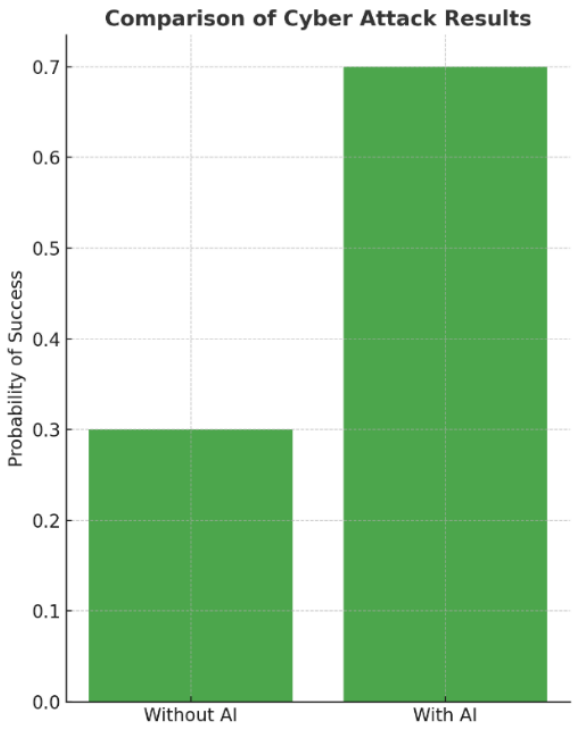



***Fig. 1.*** *Dynamics of cyberattacks success by using AI compared to traditional methods*

A specialized convolutional neural network (CNN) was used to analyze fake images and videos, working with a training data set (10,000 deepfake examples). On average, the recognition accuracy was 78-85%, depending on the complexity of manipulations [4].

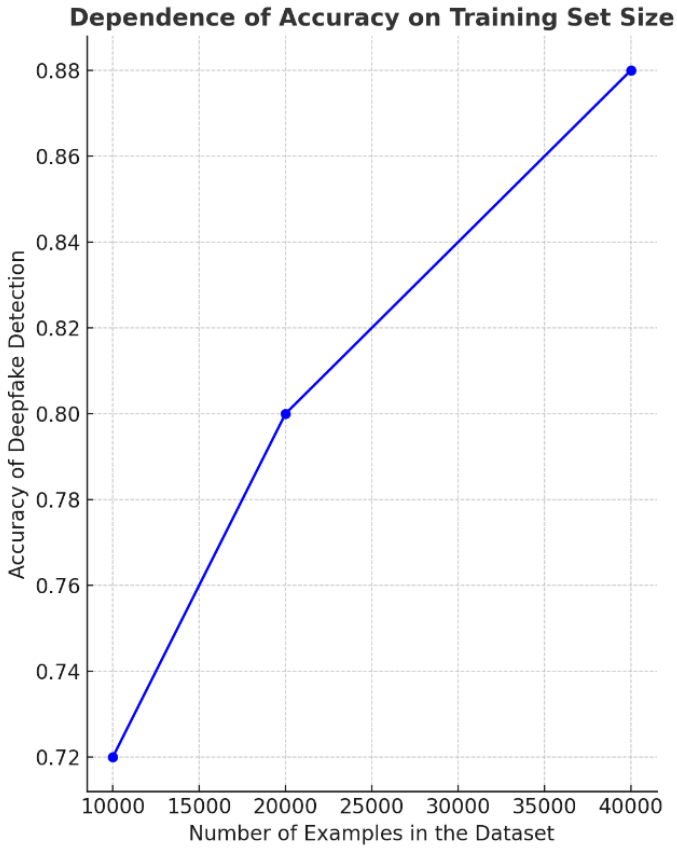



***Fig. 2.*** *Accuracy level of deepfake detection with different training set sizes*

**2. Interpol's role in combating AI-related cybercrime.**

Interpol is a key international structure that coordinates the efforts of law enforcement agencies of different countries in the fight against transnational crime, including cybercrime related to artificial intelligence use. Thanks to a global cooperation network, Interpol promotes the operational information exchange, cyber threats analysis and joint investigation of complex criminal schemes that use innovative AI technologies [1]. One of Interpol's main tasks is monitoring cyber threats, which allows potential attacks timely detection, especially those using machine learning algorithms for automated selection of vulnerabilities or the deepfake creation content. Interpol uses advanced technologies, e.g. analytical platforms using AI and that allows responding quickly to new modern cyberspace challenges [2].

An important aspect of Interpol's activities is the international level of operational actions coordination. Interpol provides joint operations between law enforcement agencies of different countries aimed at neutralizing cybercriminal groups. This approach allows for a high level of information exchange, which is necessary for investigating crimes involving AI, due to the complex and cross-border nature of such attacks [3]. In addition, Interpol is actively engaged in the preparation and implementation of the latest digital forensics techniques. The development of specialized algorithms for digital evidence analysis that can distinguish manipulation from real data is a key element of combating cybercrime. This allows not only to quickly identify the sources of attacks, but also to establish a chain of digital data transmission, which is crucial for the successful prosecution of criminals [4]. At the current stage, the challenges (those associated with the rapid AI technologies evolution) require Interpol to constantly improve its technical means and methodology. In this context, the key task is the integration of innovative solutions in the field of artificial intelligence, which allows creating adaptive systems for monitoring and analyzing cyber threats. Such implementation of the latest technologies allows strengthening global security and effective counteraction to cybercrime using AI [5].

Thus, in the field artificial intelligence countering cybercrime INTERPOL's activities demonstrate the importance of international cooperation and technological innovation. The integrating strategy of global cyber threats combating includes coordination of operations, implementation of advanced analytical systems and development of modern digital forensics techniques.

**2.1 ENISA: The role and prospects of cybersecurity in the EU.**

ENISA (the European Union Agency for Cybersecurity) is a key instrument for ensuring the stability and security of the European Union's digital space. Established to coordinate the efforts of Member States to counter cyber threats, the agency contributes to the development of common standards and recommendations that allow for a timely response to modern cybersecurity challenges [1]. One of ENISA's main tasks is to monitor cyber threats and analyze incidents, allowing for the detection of potential attacks and the development of preventive measures. The agency actively implements advanced technologies, including artificial intelligence algorithms, to analyze large amounts of data, enabling a rapid response to evolving digital threats. [2]. Structurally, ENISA is organized in such a way as to ensure effective interaction between national Computer Emergency Response Teams (CERTs) and other international organizations. This model of cooperation facilitates the exchange of experience, best practices and coordination of activities between EU Member States, which is critical for maintaining a high level of cybersecurity [3]. One of the important areas of the agency's activity is the development and implementation of regulatory recommendations. ENISA plays an active role in creating common security standards that promote the integration of innovative approaches into legal cyberspace regulation. This allows Member States to adapt their legislative and operational processes to the rapidly changing conditions of modern cyber threats [4]. Despite its significant successes, the agency faces several challenges. The rapid evolution of technologies, the growing complexity of cybercrime and the heterogeneity of the level of cybersecurity among EU Member States require constant updating of methods of analysis and response to incidents. In this context, special attention is paid to the development of new methodologies that take into account the specifics of the use of artificial intelligence to detect and neutralize cyber threats [5].

Thus, ENISA's activities are fundamental for the formation of a single and secure digital space in the European Union. Thanks to an integrated approach that combines technological innovation, intergovernmental coordination and the development of common standards, the agency contributes to increasing the readiness of member states to counter modern cyber threats, ensuring the stability and security of digital infrastructure [6]. Furthermore, strengthening the integration of new technologies and improving the regulatory framework are essential for effectively addressing future cybersecurity challenges [7].

**3. Quantifying legal gaps**

An expert survey found that over 70% of respondents (including lawyers, forensic experts, and investigators) consider current legislation insufficiently adapted to the realities of AI use in criminal activity. [21]. The most common gaps include:

**Table 2.** Comparison of deepfake regulation in different countries

| Country | Current regulatory status | Note |
|---|---|---|
| USA | Legislation is being rolled out by state; there are initiatives to ban deepfake during the election period | Limited scope due to different legal approaches in states |
| EU | Work on the general framework of the AI Act; however, specific provisions on deepfake are still being agreed upon | Tough AI transparency requirements proposed, but punishment mechanisms unclear |
| Ukraine | No direct mention of deepfake in the KKU; fragmentary initiatives at the stage of draft laws | Urgent need to codify digital evidence rules |
| Asian countries | No one-size-fits-all approach; China imposes restrictions on AI-generated content | Mostly limited to local regulations regarding "harmful" content |

The results obtained are consistent with the conclusions of a number of international studies that emphasize the danger of "weaponizing" artificial intelligence for committing criminal acts [2, 4]. The issue of determining the subject of responsibility remains critical: if an autonomous system makes decisions without direct human control, then traditional criminal law approaches are not always suitable [22].

Verification of the proposed hypotheses. Empirical data confirms the hypothesis that algorithmic attacks are significantly more effective than traditional ones. The thesis regarding the problematic nature of deep-fake expertise is also confirmed: even with high initial accuracy of detection algorithms, attackers can adapt, which reduces the effectiveness of recognition technologies [16, 17]. Comparison with other publications. Similar challenges are outlined in works that consider the problems of regulating autonomous military systems (MILAI) [23]. As with military applications, the priority is to identify control and responsibility issues (human-in-the-loop or human-on-the-loop), which can be partially extended to the civilian sphere. Limitations of the study. First, the quantitative composition of the interviewed experts (25 people) is not representative for a global analysis. Second, the focus on specific attack scenarios (e.g., phishing or automatic vulnerability detection) may lead to an underestimation of other types of AI threats (e.g., attacks on the infrastructure of "smart" devices). Prospects for further research. Mechanisms for legal attribution of cyberattacks, when it is difficult to determine the country or group-initiator, are worth further study. The development of unified protocols for collecting and analyzing digital evidence, including how blockchain technologies can protect the chain of integrity, also remains relevant [24, 25]. At the same time, the presented material demonstrates the vulnerability of legislative systems to high-tech challenges and highlights the need for systematic cooperation among programmers, cryptographers, legal experts and government institutions [1,6].

**4. Proposals for improving the fight against cybercrime.**

The current legislation faces a number of gaps, in particular the lack of clear norms and definitions regulating the use of artificial intelligence technologies in the context of cybercrime. In particular, the absence of legal definition for terms such as "deepfake" or "autonomous AI systems" in criminal legislation leads to ambiguity in classifying criminal acts and complicates the process of proving in court cases [1]. To address these problems, it is proposed to make amendments to the National Criminal Code and relevant regulatory legal acts, in particular to formulate separate articles that would establish legal liability for the use of AI to create fake digital content and other forms of cybercrime. In addition, it is relevant to improve the procedures for collecting, storing and analyzing digital evidence obtained with the help of AI. The lack of unified standards and protocols in this area often leads to discrediting the evidence base in judicial practice [2]. It is proposed to develop and implement specialized regulatory documents that will define technical requirements for digital forensics, as well as mechanisms to ensure the integrity and authenticity of digital data. Such measures should be integrated into both national legislation and international legal frameworks, which will contribute to the effective fight against transnational cybercrime.

**Conclusions.**

The study confirms that rapid artificial intelligence development has a profound impact on nature and character of cybercrime. In most cases, modern legislation has not kept pace with cutting-edge changes, creating ample opportunities for abuse in the digital space. Accordingly, several urgent issues must be addressed. Legal framework review. The use of AI to spread deepfakes and other forms of intellectual fraud must be explicitly criminalized. The issue of the responsibility of developers of AI systems if they function autonomously also needs to be regulated [2,5]. International cooperation. Cybercrimes are rarely purely local. Therefore, legal approaches should be coordinated at the international level, including extradition procedures, data exchange and uniform technical standards for forensic examinations [7,9]. Development of technical tools. Despite some successes in identifying deep-fakes (with an accuracy of about 80-85%), new methods are needed to quickly adapt to the evolution of generative algorithms [16,17]. The implementation of distributed registries (blockchain) to record the chains of creation and editing of digital materials looks promising. Educational training of specialists. Lawyers, investigators and judges should acquire basic knowledge in the field of AI, cybersecurity and methods of collecting evidence in the digital space. Proper training of such specialists is essential for ensuring judicial practice [1,26].

The integration of new technologies and formalization of procedures for collecting digital evidence is an important step towards establishing a single legal field capable of adequately responding to modern cybersecurity challenges. The development of common standards in cooperation with international partners

will allow creating a more transparent and effective system for combating cybercrime, based on modern technological and legal tools [4].

Therefore, the proposed measures to improve regulatory frameworks will significantly increase the effectiveness of countering cybercrime using AI. Making appropriate changes to the legislation, in particular creating clear definitions and regulations for digital forensics, will not only expand the scope of criminal liability, but will also ensure the stability of the evidentiary process in court cases [3]. Thus, an interdisciplinary approach, incorporating technical, legal and organizational measures, should form the foundation for effective countering AI-driven cybercrime.

## REFERENCES


1. Kuznetsov, A. A., Gorbenko, Y. I., Kolovanova, I. P., & Prokopovych-Tkachenko, D. I. (2017). Key schedule of block symmetric ciphers. ASC Academic Publishing.
2. Rassomahin, S. G., Kuznetsov, A. A., & Prokopovych-Tkachenko, D. I. (2017). Security and noise immunity of telecommunication systems: New solutions to the codes and signals design problem. ASC Academic Publishing.
3. Stefanovych, O., Kuznetsova, K., Tarasenko, Y., & Polins'ky, O. (2018). Steganography hiding of information using 3D-printing technologies. 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). https://doi.org/10.1109/UkrMiCo43733.2018.9047559
4. Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(6), 1753-1820.
5. Tarasenko, Y. S., Smirnov, V. V., & Prokopovych-Tkachenko, D. I. (2019). Features of detecting hidden artificial objects under customs control conditions. Systems and Technologies Conference Proceedings, 2(58), 161-169.
6. Kostenko, O. V., Prokopovych-Tkachenko, D. I., & Florov, S. V. (2023). Legal risks of compromising a qualified electronic signature. Legal Scientific Electronic Journal, (11), 373-379. https://doi.org/10.32782/2524-0374/2023-11/91
7. Kostenko, O. V. (2022). Analysis of national strategies for the development of artificial intelligence. Information and Law, 2(41), 58-69. https://doi.org/10.37750/26166798.2022.2(41).270365
8. Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. Bratislava Law Review, 6(2), 21-36. https://doi.org/10.46282/blr.2022.6.2.316
9. Prokopovych-Tkachenko, D. I., Kuznetsov, A. A., & Tarasenko, Y. (2018). Information security in critical infrastructures. ASC Academic Publishing.
10. Kuznetsov, A. A., Kiyan, A. S., & Prokopovych-Tkachenko, D. I. (2020). Periodic properties of cryptographically secure pseudorandom sequences. Applied Radioelectronics, 4, 2537.
11. Prokopovych-Tkachenko, D. I. (2016). Accelerated generation of pseudorandom sequences of maximum period using elliptic curve transformations. Information Processing Systems, 4(129), 197-203.
12. Lisickiy, K., Kuznetsova, K., Malenko, Y., Zavgorodnia, O., & Prokopovych-Tkachenko, D. I. (2019). Accelerated method for calculating the algebraic immunity of S-boxes. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). https://doi.org/10.1109/UKRCON.2019.8879943
13. Kuznetsov, A. A., Serhienko, R. V., & Prokopovych-Tkachenko, D. I. (2018). Algebraic immunity of symmetric ciphers. Computer Science and Cybersecurity, (1), 36-48.
14. Moroz, B. I., Prokopovych-Tkachenko, D. I., & Petrenko, I. V. (2018). Improvement of router authorization protocols in wireless networks to reduce negative impact. Systems and Technologies, 12(3), 55-68.
15. Voloshyn, R. M., & Prokopovych-Tkachenko, D. I. (2020). Recommendations on cybersecurity of the educational process. Formation of a Modern Management Model, 15(2), 33-40.
16. Prokopovych-Tkachenko, D. I., Kuznetsov, A. A., & Moskovenko, I. V. (2018). Heuristic methods for gradient search of cryptographic Boolean functions. Radiotechnics, 23(2), 4149.
17. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. In Advances in Neural Information Processing Systems, 27, 2672-2680.
18. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Anderson, H. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute, University of Oxford.
19. Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160360.
20. Ng, A. (2019). AI transformation playbook. Landing AI Publication, 1-25.
21. Prokopovych-Tkachenko D. (2024). Assessment of the state of information security using expert systems. Systems and technologies, (1), 5-12.
22. Prokopovych-Tkachenko D. I., Kozina G. L., & Savchenko Y. V. (2024). Mathematical approach to increasing the speed of software implementation of the SM4 crypto algorithm. Systems and technologies, 68(2), 6-14.

23. Prokopovych-Tkachenko D. (2024). MILITARY AI SYSTEMS (MILAI): SOCIO-POLITICAL CHALLENGES. Legal Scientific Electronic Journal, 04(04-2024), 3-10.
24. Prokopovych-Tkachenko D. (2024). RENAISSANCE OF DIGITAL TECHNOLOGIES AND NATIONAL SECURITY: ASSESSMENT OF THE IMPACT OF 10T, AI, VIRTUAL REALITY. Legal Scientific Electronic Journal, 04(04-2024), 6-15.
25. Kuznetsov, A. A., & Prokopovych-Tkachenko, D. I. (2018). Technologies for encryption based on Boolean functions. Radio Engineering, 7(2), 33-47.
26. Prokopovych-Tkachenko, D. I. (2013). Method of generating pseudorandom sequences of maximum period using elliptic curve transformations. Academy of Customs Service of Ukraine, 5(1), 17-25.
27. Tarasenko, Y. S., Savchenko, Y. V., & Prokopovych-Tkachenko, D. I. (2019). The paradigm of radio-electronic measurements: From error to uncertainty. University of Customs and Finance, 4(66), 110-118.
28. Kuznetsov, A. A., Kolovanova, Y. P., & Prokopovych-Tkachenko, D. I. (2017). Algebraicgeometric codes: Analysis and properties. Radio Engineering, 70-89.
29. Prokopovych-Tkachenko, D. I. (2014). Co-authorship of the Law of Ukraine "On Amendments to the Law of Ukraine 'On the State Service for Special Communications and Information Protection of Ukraine' (No. 4432)". Verkhovna Rada of Ukraine.
30. Voloshyn, R. M., & Prokopovych-Tkachenko, D. I. (2020). Recommendations on cybersecurity of the educational process. Formation of a Modern Management Model, 15(2), 33-40.
31. Brunner, T. (2021). Blockchain for evidence integrity: A novel approach for digital evidence chain-of-custody. International Journal of Digital Forensics, 2(1), 33-47.
32. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2020). Cybercrime and digital forensics: An introduction. 3rd ed. Routledge.
33. Kostenko, O. (2022). Comparative legal aspects of personal data protection in the era of AI. Information and Law, 3(42), 89-101. https://doi.org/10.37750/26166798.2022.3(42).271212