DOI: https://doi.org/10.54477/LH.25192353.2026.1.pp.62-71

CURRENT ISSUES IN LEGAL PREVENTION AND COUNTERACTION OF CRIME IN THE FIELD OF INFORMATION TECHNOLOGIES

Viktoriia Sydor
Department of State and Legal Disciplines
«KROK» University
03113, 30-32, Tabirna Str., Kyiv, Ukraine
e-mail: victoriasd@krok.edu.ua
https://orcid.org/0000-0002-1794-2577

Kostiantyn Perepadin
«KROK» University
03113, 30-32, Tabirna Str., Kyiv, Ukraine
e-mail: perepadinkv@krok.edu.ua
https://orcid.org/0009-0009-5205-5824

Recieved: 20 December 2025
Accepted: 17 January 2026

Abstract

The article analyses contemporary challenges in the legal prevention and combating of cybercrime amid rapid digitalisation, expansion of cyberspace, and advances in telecommunications. Cybercrime is characterised as a dynamic and transnational phenomenon encompassing offences such as unauthorised interference with computer systems, illegal collection of personal data, distribution of malicious software, phishing, social engineering, and violations of intellectual property rights. Key factors hindering effective counteraction are identified, including the high latency of cybercrime, its cross-border nature, and the use of advanced technologies by offenders, such as anonymisation tools, cryptocurrencies, blockchain, artificial intelligence, and automated systems. The study examines legal, institutional, and organisational mechanisms for combating cybercrime in Ukraine and internationally, with particular attention to international legal standards, including the Council of Europe Convention on Cybercrime, EU legal instruments, and recommendations of international organisations. The article highlights the growing importance of integrating innovative technologies into law enforcement practice, including digital forensics, artificial intelligence for big data analysis, automated threat detection systems, and advanced monitoring tools. It is emphasised that digital forensics as an emerging scientific field significantly enhances pre-trial investigation, evidence collection, and the administration of justice in cybercrime cases. The author argues that effective counteraction to cybercrime requires a comprehensive, interdisciplinary approach combining legal reform, technological innovation, professional training, cybersecurity awareness, and strengthened international cooperation. Special attention is given to the need to adapt criminal justice mechanisms under martial law, where cyber threats to critical infrastructure intensify. Strengthening cybercrime prevention is essential for ensuring national and information securityKeywords: cybercrime, digitalization, artificial intelligence, forensics, digital forensics, information technology, cyberattacks.

Keywords: cybercrime; cybersecurity; digital forensics; information technology crime; transnational crime;

1. Introduction

The rapid advancement of digital technologies, the globalisation of the information space, and the growing scale and sophistication of cyber threats have created a fundamentally new security environment in which traditional mechanisms for combating crime are increasingly inadequate. In this transformed landscape, cybercrime has emerged as one of the most serious challenges to both national and international security. It encompasses a wide spectrum of offences, ranging from cyber fraud and unauthorised access to computer systems to large-scale attacks on critical infrastructure, state institutions, and information resources. As societies become more dependent on digital systems, the potential consequences of such offences intensify, affecting not only economic stability but also public safety, democratic governance, and the protection of fundamental rights (Halushko, 2025).

This issue acquires particular urgency under conditions of martial law, where cyberspace becomes a crucial domain of confrontation. In such circumstances, cyberattacks are often integrated into broader hybrid warfare strategies and may target energy systems, communication networks, financial institutions, and governmental databases. The digital environment thus transforms into both a tool and a battlefield, requiring states to ensure not only conventional security but also resilience in the cyber domain. Consequently, the effectiveness of criminal justice systems in responding to cyber threats becomes a key determinant of national security (Helzhynska and Kravchyk, 2025). The complexity of combating cybercrime is обусловлена several interrelated factors. First, cyber offences are characterised by a high level of latency, as many incidents remain undetected or unreported due to technical difficulties, lack of awareness, or reputational concerns of victims. Second, the transnational nature of cybercrime significantly complicates jurisdictional issues, evidence gathering, and international cooperation. Offenders can operate across multiple jurisdictions simultaneously, exploiting legal inconsistencies and gaps in regulatory frameworks. Third, the rapid evolution of digital technologies continuously expands the arsenal of tools available to criminals. These include anonymisation services, cryptocurrencies, blockchain technologies, artificial intelligence systems, and automated attack mechanisms, all of which enhance the sophistication and concealment of criminal activities. In this context, it becomes evident that existing national legal systems often lag behind technological developments. Normative frameworks designed for traditional forms of crime are not always capable of adequately addressing the specific digital offences, particularly with regard to the identification, collection, and admissibility of electronic evidence (Lysko et al., 2022) The need to ensure procedural safeguards while maintaining investigative efficiency further complicates this task. As a result, the development of effective mechanisms for the legal prevention, detection, and investigation of cybercrime represents an urgent priority for modern states.

A promising direction in addressing these challenges lies in the integration of innovative technologies into law enforcement practice. In particular, the use of artificial intelligence systems offers significant potential for enhancing the analysis of large datasets, detecting patterns of criminal behaviour, and predicting cyber threats. Similarly, advances in digital forensics enable more efficient identification, preservation, and examination of electronic evidence, thereby strengthening the evidentiary basis in criminal proceedings. These technological tools, however, must be accompanied by appropriate legal regulation to ensure their lawful and ethical application (Maras, 2016).

The issues of combating cybercrime and ensuring information security have attracted considerable attention from both domestic and foreign scholars and practitioners. The theoretical foundation of this study is based on research addressing general trends in the development of cybercrime, as well as the legal and organisational mechanisms for countering it. In particular, scholarly works have examined the evolution

DOI: https://doi.org/10.54477/LH.25192353.2026.1.pp.62-71

of criminal liability for cyber offences in the context of digitalisation, as well as the conceptual and socio-legal nature of cybercrime. Significant attention has also been devoted to international legal aspects, including the provisions of the Council of Europe Convention on Cybercrime and relevant European Union directives, which establish key standards in the field of cybersecurity and digital criminal justice (Verizon, 2024).

Despite the substantial body of academic research and the existence of numerous international initiatives, several important aspects of legal prevention and counteraction to cybercrime remain insufficiently developed (Wall, 2007). Among the most pressing unresolved issues is the need for comprehensive adaptation of national legislation to the rapid pace of technological change. Legal norms must be flexible enough to respond to emerging forms of cyber threats while maintaining legal certainty and the protection of individual rights. Furthermore, challenges persist in ensuring the proper collection, authentication, and admissibility of digital evidence in judicial proceedings, particularly in cross-border contexts.

Another significant issue concerns the effective use of artificial intelligence in criminalistics. While AI technologies offer considerable advantages, their implementation raises complex legal and ethical questions related to transparency, accountability, and potential biases in algorithmic decision-making. In addition, the harmonisation of national mechanisms for combating cybercrime with international standards remains a critical task, requiring enhanced cooperation between states, international organisations, and private sector actors. Equally important is the problem of professional capacity-building in the field of cybersecurity and digital forensics (Luhivska et al., 2024). The growing complexity of cyber threats necessitates the training of highly qualified specialists capable of operating at the intersection of law, information technology, and criminology. However, existing educational and training programmes often fail to meet the demands of this rapidly evolving field, highlighting the need for comprehensive reforms in legal and technical education.

The purpose of this study is to provide a comprehensive analysis of contemporary challenges in the legal prevention and combating of crime in the field of information technology. It aims to identify the key threats facing the national criminal justice system and to develop proposals for improving legal, organisational, and technological mechanisms for countering cybercrime. Particular attention is paid to the integration of international experience and best practices, as well as to the adaptation of criminal justice systems to the realities of digital transformation and martial law.

The study seeks to contribute to the development of an effective and resilient system for combating cybercrime, capable of responding to current and future challenges in the digital environment.

2. Materials and Methods

In the course of the study on the legal prevention and counteraction of crime in the field of information technologies, a complex of interrelated general scientific and special legal methods was employed, ensuring the systematic nature, objectivity, and reliability of the results obtained. The methodological framework of the research is grounded in the provisions of contemporary legal theory, criminology, criminalistics, and information law, which make it possible to consider cybercrime as a complex socio-legal phenomenon emerging under conditions of digitalisation and the transformation of the security environment.

The study applies general scientific methods, in particular analysis and synthesis, which made it possible to generalise scholarly approaches to defining the essence of cybercrime, its key features, and current development trends. The methods of induction and deduction were used to formulate theoretical generalisations and conclusions based on individual empirical and scholarly data. The system approach enabled the examination of cybercrime as a multi-level phenomenon encompassing

legal, organisational, and technological components, as well as the identification of interconnections between them. Comparative analysis was employed to contrast the national legislation of Ukraine with international standards in the field of cybersecurity and the counteraction of cybercrime.

Among the special legal methods, particular importance was attached to the formal-legal method, which was used to analyse the norms of national and international law, including the provisions of the Council of Europe Convention on Cybercrime, European Union directives, and other нормативно-правових acts in the field of information security. The comparative legal method made it possible to examine the experience of foreign countries in combating cybercrime and to determine the prospects for its implementation within the domestic legal system. The method of legal modelling was applied to develop proposals for improving legal and organisational mechanisms for countering cyber threats, while the method of legal interpretation was used to clarify the content of legal provisions and the specific features of their practical application.

The empirical basis of the study consists of scholarly works by domestic and foreign researchers, analytical materials of international organisations, national legal acts of Ukraine and international documents in the field of cybersecurity, as well as the findings of contemporary research on the application of digital forensics and artificial intelligence technologies in law enforcement activities. The combined application of these methods ensured a comprehensive approach to the study, enabling the formulation of scientifically substantiated conclusions and practical recommendations aimed at enhancing the effectiveness of legal prevention and counteraction to cybercrime in the context of digitalisation and martial law.

3. Result

The contemporary development of information technologies has significantly transformed the nature of criminal activity and generated new challenges for law enforcement agencies and the criminal justice system. Cybercrime today constitutes a complex socio-legal phenomenon encompassing a broad range of unlawful activities in the digital environment, including unauthorised access to information systems, data manipulation and falsification, cyber fraud, dissemination of malicious software and harmful content, as well as infringements of copyright and related rights.

The growth of cybercrime is driven by several interrelated factors, notably the widespread integration of digital technologies into all spheres of social life, the increasing interconnectedness of computer systems, and the globalisation of economic and social processes. In the context of armed conflict and heightened national security threats, the risk of cyberattacks targeting critical infrastructure, financial institutions, public authorities, and defence enterprises increases substantially. These threats are systemic in nature and affect not only specific sectors of public administration but national security as a whole (Council of Europe, 2001).

One of the key challenges is the high level of latency associated with cybercrime. Empirical studies indicate that a significant proportion of cyber offences remain undetected or are inadequately investigated. According to Krapyvin, more than 90% of cybercrimes in Ukraine are not promptly identified, which creates serious difficulties not only for law enforcement agencies but also for the judiciary, particularly in relation to the lawful collection, preservation, and admissibility of digital evidence (Yak v Ukraini rozsliduiut kiberzlochyny?, n.d.).

Another major challenge lies in the rapid technological sophistication of criminal activities. Offenders increasingly utilise advanced technologies widely available in civilian and commercial sectors, including blockchain, artificial intelligence, robotics, and unmanned systems. The deployment of such technologies enables perpetrators to minimise detection risks and maintain anonymity, thereby complicating identification and prosecution processes.

DOI: https://doi.org/10.54477/LH.25192353.2026.1.pp.62-71

Halushko (2025) also emphasises the socio-psychological dimension of cybercrime. Such offences may cause not only financial losses but also harm to individuals' mental well-being, while infringing upon rights to privacy and confidentiality. This creates additional challenges for the legal system, which must strike a balance between effective crime control and the protection of fundamental human rights.

In these circumstances, modern criminalistics and law enforcement in Ukraine require the integration of advanced digital technologies and innovative investigative methods. This includes the development of specialised approaches to detecting, recording, and analysing digital traces, the training of qualified professionals in digital forensics, and the implementation of comprehensive strategies to counter cybercrime, taking into account international experience and current technological trends.

The problem of cybercrime is not limited to the increasing number and complexity of offences but also involves the necessity of adapting national criminal justice systems to the realities of a digital society and wartime conditions. Both academic research and practical efforts must focus on a comprehensive response, combining legal, technical, and organisational mechanisms to protect society from digital threats. Cybercrime is inherently global and transcends national borders, necessitating international cooperation and the harmonisation of legal frameworks. At present, the development of effective countermeasures has become a priority for many states and international organisations, as traditional domestic approaches often prove insufficient in addressing transnational cyber threats (Lysko et al., 2022).

One of the fundamental international legal instruments in this field is the Convention on Cybercrime of 2001 (Budapest Convention), which establishes legal standards for criminalising offences such as illegal access to information systems, computer-related fraud, dissemination of malicious software, and copyright violations. It also provides mechanisms for international cooperation, including extradition, evidence sharing, and joint investigations, which are essential for effectively combating cybercrime (Council of Europe, 2001).

The European Union has actively developed its own cybersecurity strategies and legal responses to cyber threats. In particular, the NIS2 Directive establishes requirements for ensuring the security of critical information infrastructure, regulating the obligations of essential service operators and digital service providers in preventing cyber incidents and ensuring timely reporting. These mechanisms enhance transparency and coordination among Member States in the field of cybersecurity (European Union, 2022).

Practical approaches to combating cybercrime worldwide include the establishment of specialised institutions responsible for monitoring cyberspace and responding to cyber incidents. For example, as noted by Lysko, Melanich, and Slavita, the Federal Bureau of Investigation's Cyber Division in the United States coordinates cybercrime investigations at the national level and cooperates with international partners. In the United Kingdom, the National Cyber Security Centre plays a key role in protecting critical infrastructure and advising both public and private sectors on cyber threats (Lysk et al., 2022).

An important aspect of international practice is the integration of advanced technologies into cybercrime prevention and response. Many countries employ analytical platforms based on artificial intelligence, machine learning, and big data to predict cyber threats, detect attacks at early stages, and automate response processes. These technologies enable efficient processing of large volumes of information, identification of anomalous activities, and rapid mitigation of potential damage.

International cooperation also involves the standardisation of digital forensic procedures, exchange of expertise, and professional training. Organisations such as INTERPOL and Europol develop training programmes and practical frameworks that enhance the competencies of investigators, forensic experts, and analysts. This

contributes to the harmonisation of investigative methods, facilitates mutual legal assistance, and ensures efficient information exchange between states. International experience demonstrates that effective counteraction to cybercrime requires a comprehensive approach combining legal regulation, technological protection measures, and professional capacity-building. The incorporation of such practices into national criminal justice systems enhances the effectiveness of responses to digital threats, particularly in the context of global challenges associated with armed conflicts and rapid digitalisation.

Modern criminalistics, in the context of rapid digital transformation, increasingly integrates advanced technologies and artificial intelligence systems to improve the efficiency of pre-trial investigations and judicial proceedings. These technologies not only automate processes but fundamentally transform methods of evidence collection, processing, and analysis. A key area in this regard is digital forensics, which focuses on the identification and examination of digital traces of criminal activity. This includes the analysis of computer systems, mobile devices, network platforms, and other digital data sources. Digital forensic specialists conduct comprehensive examinations involving data extraction, recovery, analysis, and the formation of an evidentiary base for judicial proceedings.

According to V. Shevchuk, artificial intelligence in criminalistics is used to automate analytical processes and improve predictive accuracy. Machine learning algorithms enable the identification of behavioural patterns of offenders, forecasting of potential crime locations and timing, and detection of hidden correlations between events that may not be evident to investigators. Moreover, intelligent systems are capable of processing large datasets from diverse sources, including social media, surveillance systems, and law enforcement databases, significantly reducing the time required for analytical assessments (Shevchuk, 2023).

The use of unmanned technologies and sensor systems is also of considerable importance. Drones and autonomous devices facilitate the collection of evidence in inaccessible or hazardous environments, including the documentation of war crimes, traffic violations, and illicit arms trafficking. Intelligent sensors and networked systems are integrated into early warning frameworks, enabling law enforcement agencies to respond promptly to emerging threats. Beyond practical applications, the use of artificial intelligence in criminalistics also reshapes professional training requirements. Modern investigators, forensic experts, and analysts must possess competencies in digital technologies, understand AI algorithms, conduct technical forensic examinations, and assess the reliability of digital evidence. This gives rise to a new professional role the digital forensic specialist who combines traditional криміналістичні skills with expertise in information technologies (NABU, n.d.). At the same time, the application of digital technologies and artificial intelligence must comply with legal and ethical standards. These technologies should be used in a manner that safeguards human rights, ensures procedural transparency, and maintains objectivity in evidence collection and analysis. Artificial intelligence should be regarded not as a replacement for human expertise but as a supportive tool that enhances investigative efficiency and analytical accuracy.

The integration of digital technologies and AI systems into criminalistics is an essential component of modern legal practice, enabling more effective crime prevention, ускорення investigative processes, and strengthening the evidentiary basis in judicial proceedings. At the organisational level, such integration transforms law enforcement structures, enhances professional competencies, and fosters the development of digital forensics as an independent scientific discipline. The current state of criminalistics demonstrates that digital technologies and artificial intelligence are becoming indispensable elements of law enforcement and judicial processes. At the same time, they generate new research challenges and перспективи for further development and

DOI: https://doi.org/10.54477/LH.25192353.2026.1.pp.62-71

integration into the justice system. One of the key perspectives is the establishment of digital forensics as an autonomous scientific field. This involves the systematisation of knowledge on digital traces, the development of standardised methodologies for their identification, preservation, and analysis, and the establishment of unified criteria for evaluating digital evidence in court.

Another important task is the development of comprehensive methods for collecting and processing digital data under conditions of martial law and crisis situations. This requires the integration of multiple data sources, including cloud services, social networks, video surveillance systems, and Internet of Things devices, combined with AI-based analytical tools for automated evidence selection. There is also a growing need to enhance professional training in digital forensics. This involves the creation of advanced educational programmes for investigators, forensic experts, and analysts, combining knowledge of criminalistics with competencies in machine learning, digital modelling, and cybersecurity. The emergence of the digital forensic profession opens new opportunities for specialised education and international knowledge exchange.

Among priority areas is the improvement of legal and ethical frameworks governing the use of digital technologies and artificial intelligence. This includes ensuring data protection, safeguarding human rights, and preventing algorithmic bias. Scientific research should also focus on developing methods for assessing data quality and reliability in order to ensure the admissibility and credibility of digital evidence (Helzhynska and Kravchyk, 2025). Finally, strengthening international cooperation and standardisation in digital forensics remains a critical objective. Joint research initiatives and harmonised methodologies facilitate effective investigation of cybercrime, exchange of digital evidence, and application of advanced technologies across jurisdictions. This enhances the global capacity to combat cybercrime in an increasingly interconnected and digitalised world.

In addition, ongoing research into emerging forms of cybercrime and evolving cyber threats is essential. Continuous monitoring of technological developments and criminal behaviour patterns will enable the development of adaptive protection models and the early detection of potential threats, thereby ensuring a proactive approach to cybersecurity.

4. Discussion

The findings of this study corroborate the position that cybercrime has evolved into a complex and rapidly transforming socio-legal phenomenon, the development of which is closely linked to the processes of digitalisation and globalisation of the information environment. This conclusion is consistent with the views of contemporary scholars, who emphasise the transformation of criminal activity under the influence of digital technologies and the need to reconsider traditional approaches to criminal liability and prevention (Luhivska et al., 2024; Halushko, P2025). In this context, cybercrime should be understood not merely as a category of offences, but as a systemic challenge affecting legal regulation, institutional capacity, and societal security as a whole.

One of the key issues confirmed by this research is the high level of latency of cybercrime, which significantly complicates its detection and investigation. Empirical observations indicate that a substantial proportion of cyber offences remain outside official statistics, thereby undermining the effectiveness of criminal justice responses and limiting the development of evidence-based policy decisions (Yak v Ukraini rozsliduiut kiberzlochyny? (n.d.). This finding aligns with broader international assessments, which highlight the underreporting of cyber incidents as a global problem requiring improved reporting mechanisms and enhanced public awareness (Council of Europe, 2001; National Institute of Standards and Technology, 2018). Consequently, reducing latency should be regarded as a strategic priority in the development of national cybersecurity systems.

The study also contributes to the ongoing academic discourse regarding the role of advanced technologies, particularly artificial intelligence, in the field of criminal justice. The results confirm that AI technologies significantly enhance analytical capabilities, enabling the identification of behavioural patterns, the prediction of cyber threats, and the processing of large volumes of data (Helzhynska and Kravchyk, 2025). At the same time, the integration of such technologies raises complex legal and ethical issues, including concerns related to transparency, accountability, and the protection of personal data. These challenges are widely discussed in both national and international research, which emphasises the necessity of developing appropriate regulatory frameworks to govern the use of AI in law enforcement and judicial processes (Luhivska et al., 2024; Maras, 2016).

An important aspect of the discussion concerns the role of digital forensics as a ключовий component of modern criminalistics. The findings of this study support the view that digital forensics is gradually emerging as an independent scientific discipline with its own methodological foundations and practical significance. However, a number of unresolved issues remain, particularly regarding the standardisation of forensic procedures, the admissibility of digital evidence in court, and the training of specialised experts. These challenges are reflected in both academic literature and practical guidelines, which underline the importance of developing unified standards and strengthening professional competencies in this field (INTERPOL, 2023; Maras, 2016).

The transnational nature of cybercrime necessitates a high level of international cooperation, which is also confirmed by the results of this study. International legal instruments, such as the Convention on Cybercrime, as well as European Union directives, provide a foundational framework for harmonising legal approaches and facilitating cross-border investigations (Europol, 2023; ENISA, 2023). At the same time, practical implementation remains complicated by differences in legal systems, jurisdictional limitations, and varying levels of technological development among states. Reports of international organisations further emphasise the need for coordinated global responses, including information sharing, joint operations, and capacity-building initiatives (ENISA, 2023; Halushko, 2025; Helzhynska and Kravchyk, 2025).

Particular attention should be paid to the специфіка of cybercrime under conditions of martial law, where cyber threats become an integral element of hybrid warfare strategies. In such circumstances, cyberattacks increasingly target critical infrastructure, state institutions, and strategic communication systems, thereby amplifying risks to national security. This observation is consistent with recent analytical reports, which highlight the growing role of cyber operations in modern conflicts and the necessity of integrating cybersecurity into broader defence strategies (National Institute of Standards and Technology, 2018; NABU, n.d.). At the same time, this raises important questions regarding the balance between security measures and the protection of fundamental rights, which require further scholarly examination.

Despite the comprehensive nature of this study, certain limitations should be acknowledged. The research is primarily based on doctrinal analysis and secondary sources, which may not fully reflect the practical challenges faced by law enforcement agencies. In addition, the rapid evolution of digital technologies implies that some of the conclusions may require continuous revision in light of new developments. Future research should therefore focus on empirical investigations, including case studies and practitioner-based analyses, in order to deepen understanding of the operational aspects of combating cybercrime.

In summary, the discussion confirms that effective counteraction to cybercrime requires an integrated and interdisciplinary approach combining legal reform, technological innovation, institutional development, and international cooperation. The findings contribute to the broader academic discourse by identifying key challenges

DOI: https://doi.org/10.54477/LH.25192353.2026.1.pp.62-71

and перспективи in this field, while also outlining directions for further research aimed at enhancing the resilience and adaptability of criminal justice systems in the digital age.

Conclusions

The findings of the study demonstrate that, under contemporary conditions, cybercrime constitutes a complex, dynamic, and multidimensional socio-legal phenomenon that evolves in parallel with the processes of digitalisation and the globalisation of the information space. Its defining characteristics include a high level of latency, a transnational nature, technological sophistication, and the capacity for rapid adaptation to emerging digital tools. Taken together, these factors significantly complicate the activities of law enforcement agencies and necessitate a reconsideration of traditional approaches to crime prevention and control.

It is substantiated that the effectiveness of legal prevention and counteraction to cybercrime largely depends on the ability of the national legal system to respond promptly to technological developments. The study establishes that existing legislation requires further adaptation to the realities of the digital environment, particularly with regard to the regulation of the collection, recording, preservation, and evaluation of digital evidence, as well as the delineation of legal boundaries for the use of emerging technologies, including artificial intelligence.

The research demonstrates that a promising avenue for enhancing the effectiveness of counteracting cybercrime lies in the integration of innovative technologies into law enforcement practice. In particular, the application of digital forensics tools, big data analytics, and artificial intelligence algorithms significantly improves the detection, documentation, and investigation of cyber offences. At the same time, it is emphasised that the use of such technologies must be accompanied by appropriate legal regulation, ensuring compliance with the principles of legality, proportionality, transparency, and the protection of fundamental human rights.

It is further established that international cooperation represents a key prerequisite for effectively countering cybercrime, given its inherently cross-border nature. The harmonisation of national legislation with international standards, active participation in joint investigations, and the exchange of information and best practices contribute to increased effectiveness in this domain. In this context, particular importance is attached to the implementation of international legal instruments and the adoption of best practices from leading states and international organisations.

Special attention is devoted to the issue of human resource capacity, as effective counteraction to cyber threats requires the training of a new generation of specialists who combine legal expertise with competencies in information technology, digital forensics, and data analytics. Accordingly, there is a pressing need to modernise educational programmes and to introduce interdisciplinary approaches in the training of professionals for the criminal justice system.

In summary, the study concludes that effective counteraction to cybercrime is possible only through the implementation of a comprehensive approach that integrates the improvement of the legal framework, the deployment of advanced technologies, the development of digital forensics, the enhancement of professional competencies, and the strengthening of international cooperation. The implementation of these measures will contribute to the establishment of a resilient and effective cybersecurity system capable of responding adequately to current and future challenges of the digital environment, particularly under conditions of martial law and heightened threats to national security.

References

Council of Europe. (2001). Convention on cybercrime (Budapest Convention). https://

www.coe.int/en/web/cybercrime/the-budapest-convention
European Union. (2013). Directive 2013/40/EU on attacks against information systems. https://eur-lex.europa.eu/eli/dir/2013/40/oj
European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555
Europol. (2023). Internet organised crime threat assessment (IOCTA). https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment
ENISA. (2023). ENISA threat landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
Halushko, P. P. (2025). Cybercrime: Concept and socio-legal nature. *Visnyk Kryminolohichnoi Asotsiatsii Ukrainy, 34*(1), 808–817. https://doi.org/10.32631/vca.2025.1.66
Helzhynska, T. Ya., & Kravchyk, O. R. (2025). Legal regulation of the use of artificial intelligence in education: Ukrainian and European experience. *Akademichni vizii, 42*, 1–11. https://academy-vision.org/index.php/av/article/view/1897
INTERPOL. (2023). Global crime trend report. https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-Global-Crime-Trend-Report
Luhivska, L. R., Yatsyshyn, O. O., & Liubavina, V. P. (2024). Trends in the development of criminal liability for cybercrime in the context of digitalisation of society. *Dictum Factum, 2*(16), 258–264. https://df.duit.in.ua/index.php/dictum/article/view/363
Lysko, T. D., Melanich, V. V., & Slavita, Yu. V. (2022). Counteracting cybercrime: Current state of national legislation and foreign experience. *Aktualni problemy derzhavy i prava, 96,* 44–49. https://doi.org/10.32782/apdp.v96.2022.4
Maras, M.-H. (2016). *Cybercriminology*. Oxford University Press.
Microsoft. (2023). Microsoft digital defense report. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/cyberframework
NABU. (n.d.). Chief specialist of the digital forensics laboratory detective unit. https://nabu.gov.ua/robota-v-nabu/perelik-vakansiy/golovnyyi-spetcialist-pidrozdilu-detektiviv-tcyfrovo-kryminalistychno-laboratori/
Shevchuk, V. M. (2023). Use of artificial intelligence technologies and the process of digitalisation of criminalistics in wartime. In *Proceedings of the All-Ukrainian scientific and practical conference "Actual problems of combating crime and corruption"* (pp. 171–176).
United Nations Office on Drugs and Crime. (2021). Comprehensive study on cybercrime (updated materials). https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
Verizon. (2024). Data breach investigations report (DBIR). https://www.verizon.com/business/resources/reports/dbir/
Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
World Economic Forum. (2024). Global cybersecurity outlook 2024. https://www.weforum.org/reports/global-cybersecurity-outlook-2024
Yak v Ukraini rozsliduiut kiberzlochyny? (n.d.). Merezha UPLAN. https://uplan.org.ua/analytics/iak-v-ukraini-rozsliduiut-kiberzlochyny/