Latest Criminalistic Tools and Technologies in the Investigation of Cybercrimes: International and Ukrainian Experience

Submitted: 13 October 2024
Reviewed: 2 May 2025
Revised: 20 May 2025
Accepted: 21 May 2025

Viktor Shevchuk[*]
https://orcid.org/0000-0001-8058-3071
Oleg Bululukov[**]
https://orcid.org/0000-0003-1598-0542
Hennadii Chornyi[***]
https://orcid.org/0000-0003-1649-6437
Olha Tyshchenko[****]
https://orcid.org/0000-0003-1551-1367
Vasyl Baranchuk[*****]
https://orcid.org/0000-0002-3643-2484

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i2.55927

Abstract

[Purpose] The purpose of this study was to examine promising technologies for investigating cybercrime based on international experience.

[Methodology/approach/design] The study employed comparative legal analysis to assess various legal systems and practices, focusing on the integration of specialized knowledge in cybercrime investigations, with particular attention to European countries.

[Findings] The findings highlight the growing role of automation, digitalization, and artificial intelligence (AI) in enhancing the efficiency of criminal investigations. These technologies are increasingly used in the pre-trial and court processes, improving the

[*]Full Doctor, Professor at the Department of Criminalistics, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine. Email: viktorshevchuk994@gmail.com.

[**]PhD, Associate Professor at the Department of Criminalistics, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine. Email: olegbululukov@outlook.com.

[***]PhD, Associate Professor at the Department of Criminalistics, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine. Email: hechornyi@hotmail.com.

[****]Full Doctor, Associate Professor at the Department of Criminal Process, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine. Email: olha_tyshchenko@outlook.com.

[*****]PhD, Assistant at the Department of Criminalistics, Yaroslav Mudryi National Law University, 61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine. Email: vasyl.baranchuk@hotmail.com.

effectiveness of detecting, investigating, and preventing cybercrimes. The study emphasizes the transnational nature of cybercrime and the importance of international cooperation in addressing the challenges posed by the digital environment. The use of criminalistic tools, such as EnCase™ Forensic, AccessData FTK Imager, and IBM i2 Analyst's Notebook, has proven critical in advancing forensic science, particularly in the collection and analysis of digital evidence. Despite challenges, including martial law and limited resources in Ukraine, the study advocates for the adaptation of international best practices to improve the country's cybersecurity framework.
[Practical implications] Such a comprehensive approach to these issues ensures the efficiency and effectiveness of criminal justice tasks, considering international standards and the Ukrainian reality of the current military situation.

Keywords: Martial Law. Digital Environment. Special Knowledge. Artificial Intelligence. Forensic Examination. Digital Technologies. Criminalistic Innovations. Criminal Proceedings. Digital Traces. Digital Forensics. Criminalistic Methodics. Cyber Forensics.

INTRODUCTION

The task of modern criminalistics is to combat crime through the use of innovative criminalistic tools, methods, and technologies aimed at effective investigation of crimes and collection of evidence. One of the key aspects is to provide law enforcement agencies with the necessary criminalistic resources to effectively detect, investigate, prevent, and prosecute crimes. To achieve these goals, it is necessary to use the latest scientific developments and put them into practice. In the current reality of the Russian invasion of Ukraine and the subsequent implementation of martial law, it is essential to consider the processes of informatisation, digitalisation, and globalisation, as well as their impact on crime, social development, and the emergence of international and global threats.

The Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part (2014) emphasises that countering cybercrime is a vital element of gradual integration in the field of foreign and security policy, which requires comprehensive measures at the legislative, organisational, personnel, and educational levels. The significance of these issues is reflected in the Cybersecurity Strategy of Ukraine (Decree of the..., 2021), which states that to ensure effective counteraction to cybercrime, strategic goals must be achieved. It is planned to strengthen capacities in this area by improving the professional level and material and technical base of forensic experts working in the field of digital technologies to ensure effective combating of cybercrime. Particular attention is paid to improving the professional level of training and qualifications of employees of operational units, pre-trial investigation bodies, prosecutors, and

judges in the field of digital technologies and cybersecurity, specifically in the collection, analysis, and examination of digital evidence.

The forensic training of specialists in digital forensic science is essential, as is the necessity to enhance the development of forensic pedagogy for cybercrime investigations. The implementation of modern technology encounters substantial obstacles due to martial law and constrained resources, impeding the delivery of essential support. Addressing these challenges necessitates the formulation of effective strategies, including the harmonisation of Ukrainian and international legislation with European norms. A thorough criminalistic approach for the investigation of organised, international, and latent cybercrimes is urgently required. Studying the methodologies of prominent nations such as the United States and Poland can bolster Ukraine's initiatives in addressing cybercrime. Notwithstanding the existence of contemporary instruments, the necessity for cohesive methodologies in cybercrime investigations and professional training persists. The implementation and utilisation of modern criminalistic advancements are essential priority for forensic science to enhance efficiency and optimise law enforcement processes (BEKISHEV et al., 2019).

This issue has been the subject of research by various researchers. O. Ukhno (2021) and M. Dumchykov et al. (2020) focused on the investigation of the historical development and current state of criminalistic, procedural, and organisational aspects related to the selection, licensing, use, and adaptation of modern information, digital, and telecommunications technologies.

V. Shevchuk et al. (2023a) investigated the specific features of using modern criminalistic tools and technologies to optimise and increase the effectiveness of combating iatrogenic crimes. The researchers identify the prospects, vectors, and possible potential for improving such activities in the current conditions and for the future. The researchers also focused on and analysed conventional and innovative means, methods, and technologies of forensic support for successful investigation of this category of criminal offences, considering international experience and Ukrainian reality. The study identified the circumstances and factors which necessitate the creation of a modern information system for registration and analysis of cases of improper provision of medical care with a view to taking preventive measures using legal, criminal procedural, and criminalistic means. All this is also important for the investigation of cybercrime.

The development, implementation, and use of innovative approaches, tools, and technologies in criminalistics and forensic examination are key areas of research, which are the focus of studies by M. Martineau et al. (2023), M. Bada and J. Nurse (2021), A. Rakha (2024). The studies found that European practices in the development of forensic science focus on the integration of advanced

institutions and the introduction of the most effective methods and modern technologies.

W. Fahmy (2024), R. Vella and J. Farrugia (2024), M. Dweikat et al. (2021) focus on the current issues of using the latest technologies in crime investigations. Attention is focused on the significance of integrating these technologies to improve the accuracy and speed of investigations, ensure greater transparency in proof procedures and reduce human error.

Research devoted to the study and analysis of the current state and trends in the development of new promising areas in forensic science is of scientific and practical interest (BORYSENKO et al., 2021). The organisation and conduct of such research are crucial for studying the problems of investigating cybercrime, as the use of specialised knowledge, among which forensic expertise is of particular importance, is a valuable tool for improving the effectiveness of combating such complex crimes in the context of their successful detection, investigation, solving, and prevention.

Enhancing the efficacy of criminal investigations, particularly in cybercrime, involves a focus on innovative organisational and tactical methods, such as tactical operations (SHEVCHUK et al., 2023b), which are essential for the collection of digital evidence and the optimisation of pre-trial investigations. Despite advancements in the integration of new technologies into worldwide cybercrime investigations, deficiencies persist in tailoring these tools to the Ukrainian setting. Critical difficulties encompass the absence of methodological guidance for the use of international experience, legal disputes stemming from the incorporation of international standards into Ukrainian law, and the inadequacy of cyber criminalistics tools inside law enforcement agencies. There is an imperative necessity to formulate a criminalistic methodology for the investigation of cybercrimes (SHEVCHUK et al., 2022a) and to enhance international collaboration, with Ukraine requiring further integration into global exchange programs for optimal practices and technologies.

The purpose of this study was to identify promising criminalistic tools and technologies for combating cybercrime, considering the experience of the USA, Poland, Spain, and analysis of the current state of criminalistic support in Ukraine. The principal objectives of the study were as follows:

1. To investigate the specific features of implementation and adaptation of modern technologies (EnCase™ Forensic, AccessData FTK Imager, ASR SMART, IBM i2 Analyst's Notebook, Autopsy, Rifiuti2, Oracle Solaris) in the legal system of Ukraine.

2. To assess the effectiveness of available criminalistic tools in the investigation of cybercrime in Ukraine.

MATERIALS AND METHODS

The methodological approach of the study included the use of a comprehensive approach integrating general scientific and specialised methods to analyse modern criminalistic tools and technologies. Logic diagrams and tables were used to systematise the data and highlight various aspects and stages of their application in investigation of cybercrimes. The methodology included a dialectical approach to analysing criminogenic phenomena emerging in social and global cyberspace and helped to explore the interconnections and contradictions between the physical and virtual environment, which contributes to understanding the structure and nature of cybercrime.

Using the formal legal method, the study analysed the regulations governing the investigation of cybercrime in Ukraine, as well as in the United States, Poland, and Spain. Specifically, laws and regulations that define the procedure for the use of innovative technologies in the criminalistic process and empirical data were examined, including Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part (2014), Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 'On the Cybersecurity Strategy of Ukraine'" (2021), Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), Order of the Prosecutor General's Office No. 298 "On Approval of the Regulation on the Unified Register of Pre-trial Investigations, Procedure for its Formation and Maintenance" (2020), as well as Report on the work of the Cyber Incident Response Centre "Systems for detecting vulnerabilities and responding to cyber incidents and cyber-attacks" (2023).

A synthesis method was employed to integrate information on cybercrime and related phenomena into a unified knowledge system, covering a variety of factors affecting cybercrime. The classification method was used to structure and systematise the data on these factors according to certain criteria, including sources, content, timeframe, research areas, scope, and geographical distribution. Comparative legal and statistical methods were used to compare official statistics with the results of empirical studies, ratings, and reports provided by non-governmental organisations. The comparative legal method allowed for a detailed analysis of the legislative and legal frameworks in different countries, such as the United States, Poland, Spain, and Ukraine, in the context of combating cybercrime. This approach helped to compare the level of legal regulation, identify gaps and advantages of national systems in the context of combating cybercrime.

The statistical method was used to analyse quantitative data on the number of registered cybercrimes, the frequency of their investigations, and successful prosecutions in these countries. This included analysing official data from government agencies and comparing it with ratings and reports from non-governmental organisations that provided a broader understanding of cybercrime. This approach helped to verify the data for objectivity, completeness, and reliability, as well as helped to identify potential discrepancies between official reports and independent research.

Using the formal logical method, the study analysed and compared international and Ukrainian approaches to the use of criminalistic tools. This included comparing the effectiveness of different technologies and tools in the context of the specific requirements and conditions of investigation of cybercrimes in various jurisdictions. This method helped to identify logical connections between factors and circumstances affecting the use of criminalistic technologies, as well as to investigate the cause-and-effect relationship between innovations in forensic science and their impact on the effectiveness of cybercrime investigations. In addition, this method ensured the formulation of reasonable conclusions and recommendations to improve criminalistic tools and technologies based on a logical analysis of the data obtained and the findings of the comparison.

RESULTS

According to the provisions of the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), cybercrime is defined as a set of socially dangerous actions committed in or using cyberspace and for which criminal liability is provided. Such acts include cyber incidents, cyberattacks, and cyberthreats, which are covered by the concept of a computer crime and may also be recognised as crimes under international treaties of Ukraine. The legislative definition emphasises that the specifics of cybercrime are determined by the environment in which they are committed, namely cyberspace. In Ukraine, crimes of this type are classified according to Reference No. 9 to the Regulation on the Unified Register of Pre-trial Investigations, the procedure for its formation and maintenance as those committed using high information technologies and telecommunication networks, which indicates the significance of the means of their commission (Order of the..., 2020). The analysis of the provisions of the Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017) shows the crucial role of cyberspace in the formation and classification of cybercrime. The law clearly defines cybercrime as the result of socially dangerous acts committed in or using the virtual environment and provides for criminal liability for such acts. This includes

cyber incidents, cyberattacks, and cyberthreats, which are recognised as crimes both at the national level and according to international agreements of Ukraine. The legislative definition emphasises that the specificity of cybercrime is determined by the environment of its implementation, namely cyberspace.

The specificity of cybercrime is determined by the nature of the cyberspace in which it occurs. Cyberspace is a virtual environment where crimes are committed digitally, without physical boundaries, and exist within electronic systems, networks, and data (SHCHERBIAK et al., 2024). This allows criminals to operate anonymously and remotely, making it much more difficult to detect and prosecute them. Furthermore, cyberspace is globally accessible through the Internet and telecommunications networks, which allow criminals to operate across state borders and hide their activities using technology. The technical sophistication of cybercrime is conditioned by the use of modern information technologies, such as computer programs and data management systems, used to create malware, attack information systems, and manipulate data (KULLOLLI, 2024). The dynamism of cyberspace is also an important feature, as the development of latest technologies and threats increases the need to update methods of combating cybercrime, as well as to improve legislative and law enforcement approaches.

The investigation process becomes even more complicated when such crimes become cross-border and are committed by organised criminal groups (ORLOVSKYI et al., 2023). Thus, the specificity of cybercrime is determined by such aspects of cyberspace as its virtual, global nature, technological complexity, and constant evolution, which shapes the specific features of legal regulation and requires the use of specialised tools to effectively combat these crimes by means of forensic science. In this context, it is vital to take account of methodological principles in the formation of the terminology for studying this issue and official statistics in the fight against cybercrime in Ukraine, Europe, and the world, considering the impact of military threats in the current environment (SHEVCHUK, 2020). According to statistics from the State Service for Special Communications and Information Protection of Ukraine, the number of cyber incidents increased by 62.5% in 2023 compared to 2022 (Figure 1).

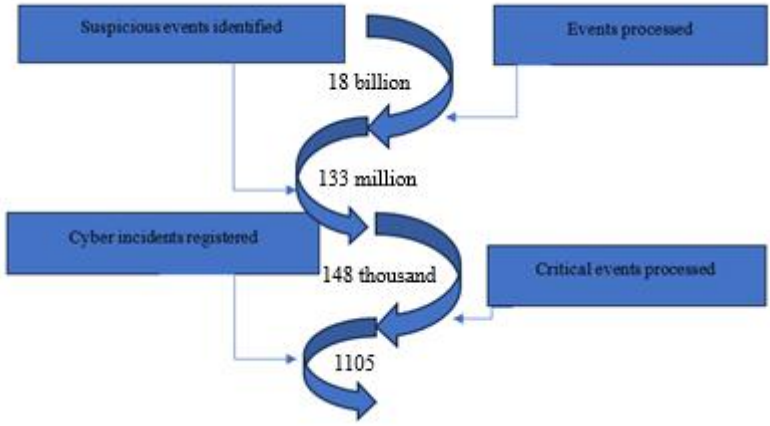

Chart 1 – State of cybersecurity as of 2023

Source: compiled by the authors based on the Report on the work of the Cyber Incident Response Centre "Systems for detecting vulnerabilities and responding to cyber incidents and cyberattacks" (2023).

The increase in cybercrime on the Internet is largely caused by Russia's military aggression against Ukraine, which has led to a dramatical increase in the number of cybercrimes, much of which is of Russian origin (APAKHAYEV et al., 2017). During a joint press briefing of the National Security and Defence Council of Ukraine, the National Bank of Ukraine, and Kyivstar JSC on 15 February 2023, the aggressor actively used various tools to inflict maximum damage on Ukraine, including hybrid forms of warfare such as cyberfraud (BABENKO, 2023). However, this data does not reflect the full extent of cybercrime due to the elevated level of latency, the use of advanced technologies, modern hardware and software, as well as complex organisation and international connections. Cybercrime is often transnational in nature, using resources located in different countries, which makes it difficult to counteract and accurately determine its scale (KRAVCHUK et al., 2024). Under these circumstances, there is an urgent need to develop a criminalistic methodology for investigating cybercrime committed by transnational criminal groups (ORLOVSKYI et al., 2022).

In the context of forensic science, the current paradigm of crimes committed in cyberspace is characterised by complexity. It is not merely a set of crimes or a technology of criminal activity. Criminals can use computer technologies to achieve various criminal outcomes or combine them in a typical way to fulfil a particular purpose, which is actively used by organised criminal groups. The development of a modern comprehensive criminalistic investigation

methodology is a key factor in the fight against cybercrime, as it allows for the adaptation of conventional and innovative criminalistic approaches to the changing conditions of cyberspace and ensures the effective detection, investigation, and solution of crimes in this category by modern criminalistic means, considering the latest advances in science and technology, the needs of practice and international experience, and European standards in the collection of digital evidence.

Modern forensic science is facing new challenges and tasks due to the expansion of cybercrime, which requires the introduction of high-tech tools for the effective investigation of offences in the digital environment. The development of digital technologies and the increase in the amount of information stored and transmitted through computer systems set new requirements for criminalistic tools that must meet current conditions and provide accurate and detailed analysis.

For instance, EnCase™ Forensic is one of the most recognised and trusted tools developed for complex digital criminalistic investigations. The tool provides powerful data processing capabilities and integrates different stages of an investigation, allowing investigators to customise reports to meet their needs. Another example is the AccessData FTK Imager, which specialises in previewing data for recovery from various storage media. This tool also allows creating exact copies of the data, called forensic images. An important feature of the program is its free access. This software can be used to make forensic copies of individual files, folders, or even entire storage devices such as local hard drives, floppy disks, Zip drives, CDs, and DVDs.

ASR SMART software provides a user-friendly data collection and analysis platform that allows previewing, evaluating, extracting, authenticating, and analysing storage devices (AVTALION et al., 2024). Its capabilities include searching for and recovering lost files, performing comprehensive file system searches, and efficiently collecting and analysing various metadata. ASR SMART enables more efficient storage device management and forensic analysis, providing critical information and solutions to numerous investigative challenges. Additionally, it enables secure remote data collection and collaboration, documenting findings, sharing results, and searching and retrieving data from unallocated space.

The IBM i2 Analyst's Notebook tool creates a sophisticated visual data analysis environment that allows quickly building a single picture of intelligence. The software product includes a universal data model and a wide range of visual analysis tools that facilitate the identification of key people, connections, interactions, events, patterns, and trends. Built-in social network analysis

functions offer a better insight into social relations and the internal structure of the networks under study.

The graphical user interface of Autopsy makes it easy to analyse both mobile devices and hard drives, contributing to the efficient conduct of computer forensic science. Within the framework of this process, the Rifiuti2 tool is used to examine the data from the Windows Recycle Bin in detail, helping to establish when the files were deleted, their original location and size. Additionally, the Oracle Solaris Fingerprint Database provides integrity checks for files distributed through the Solaris operating system.

Thus, the digital investigation process involves the integrated use of specialised digital forensic science tools and techniques to ensure the effective detection and seizure of digital evidence to support judicial investigations. The use of software products such as EnCase™ Forensic, AccessData FTK Imager, ASR SMART, IBM i2 Analyst's Notebook, Autopsy, Rifiuti2, and the Oracle Solaris fingerprint database allows for high accuracy and reliability in the collection, analysis, and storage of digital data. These tools and technologies represent modern approaches to cybercrime investigations, enabling professionals to provide comprehensive and detailed data analysis in a rapidly changing digital environment.

In modern reality, automation and digitalisation technologies are being actively implemented in the field of pre-trial investigation, which can considerably increase the efficiency of detecting signs of a crime (TOKARIEVA et al., 2024). This is especially useful when conducting online investigations, as automated systems can accelerate the process of finding the necessary information and help create reports summarising the data found. Although automation is not a recent technology, its impact on the field of investigations is becoming increasingly visible, changing the way tasks are approached. This creates new challenges related to the legal aspects of automation (POLIAK, 2022). Questions arise as to the legal basis for decisions prepared by automated systems, specifically in the context of court decisions. Machine learning can be used both at the stage of committing a crime and during its investigation (Figure 2). Criminals can use artificial intelligence to harm victims' systems, potentially resulting in significant losses. Furthermore, AI can be used to develop more sophisticated attacks that are carried out with great speed and accuracy beyond the capabilities of individuals.

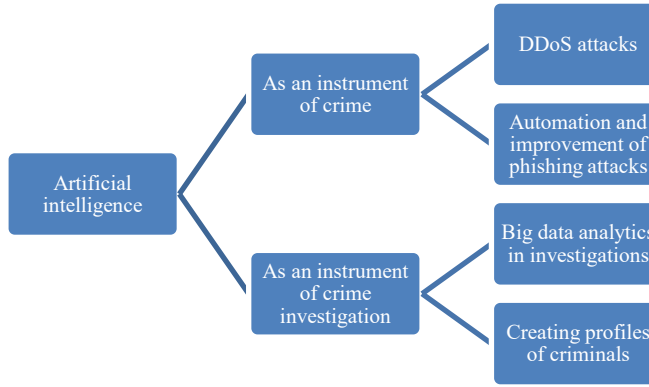

Chart 2 – The use of artificial intelligence in the commission of crimes and their investigation

Source: created by the authors.

An example of the use of AI to develop sophisticated attacks is the use of machine learning to create phishing campaigns. Such attacks typically involve fake emails or websites designed to mislead users and illegally obtain their confidential information. Thanks to AI, such attacks can be made much more difficult. Thus, in 2020, a phishing campaign was detected where attackers used AI to generate personalised emails aimed at stealing the credentials of corporate network users. Attackers used machine learning algorithms to collect information about company employees through open sources such as social media. Based on this information, AI created emails that imitated communication from high-profile employees or partners of the company, which increased the probability that victims would open attachments or click on fake links (DEWEY and PATEL, 2024).

This example illustrates how artificial intelligence can be used to conduct sophisticated and effective attacks that go beyond the capabilities of conventional criminal methods. The use of AI allows attackers to develop attacks that are faster, more precise, and more adaptive, which requires original approaches to cybersecurity from defence systems. Considering the possibility of such methods being used by criminals, investigators need to have the knowledge to recognise them and respond appropriately during the investigation. Due to the potential for advanced techniques such as AI to be used to commit sophisticated cybercrime, investigators must have a prominent level of competence in recognising and responding to such threats during investigations.

Knowledge of the latest technological innovations is an essential aspect of investigating cybercrime. Investigators should be familiar with advances in technology that can be used to commit crimes (ZILE et al., 2023). This involves understanding the principles of machine learning algorithms, automated data

collection methods, and the latest approaches to cyberattacks, such as phishing, malware, or attacks on information systems. Furthermore, new threats emerging in cyberspace should be constantly monitored and analysed. This includes monitoring new techniques and tactics used by criminals and assessing their impact on investigations. It is important to understand how these threats can be modified or evolve to ensure an effective investigation.

For example, Deepfake technology, which uses AI to create incredibly realistic but completely fictionalized movies, audio recordings or images, raises serious ethical and privacy concerns, especially in the field of criminal investigations. The ability to create credible but misleading images of people performing actions or uttering statements they never made has serious implications for their reputations, privacy and personal safety. Deepfakes are used to spread misinformation, defame people, or commit fraud (APAKHAYEV et al., 2024). As technology becomes more accessible, its potential for harm increases, forcing law enforcement to tackle new types of cybercrime. Investigators are faced with the question of how to distinguish genuine content from altered content, especially in cases involving defamation, political interference or extortion.

Existing forensic technologies may not be able to cope with the growing threat of deepfake technology. Conventional digital forensics, which emphasizes the identification and preservation of digital evidence such as file integrity and metadata, may need to be adapted to address the unique challenges posed by deepfake detection. For example, forensic scientists must develop and implement new artificial intelligence-based techniques capable of detecting small inconsistencies in movies or audio files, such as unusual blinks, inconsistent lip movements, or anomalies in vocal tone. In addition, as deepfake technology advances, existing tools will need constant updating to stay ahead of increasingly sophisticated manipulations. This emerging challenge highlights the need to incorporate specialized deepfake detection techniques into forensic methodology, as well as ethical standards to prevent the use of such technologies and protect individual rights in the digital age.

One also needs to have specialised skills in using digital forensic science tools. For example, knowing how to use software such as EnCase™ and AccessData FTK Imager is essential for data collection and analysis. The ability to use such tools allows not only identifying and collecting evidence, but also ensuring its integrity and reliability throughout the investigation process. If new or more sophisticated attacks are discovered, investigators should be prepared to adapt their investigation strategies. This may involve the use of new methods of evidence collection, adjustments to data analysis tactics, or changes to information gathering and processing procedures. Interdisciplinary cooperation is

also important, as investigating cybercrime often requires interaction with experts in information technology, cybersecurity, and law. Investigators need to be able to communicate and collaborate effectively with such specialists to maximise results.

Professional development and training are vital parts of an investigator's work (ALIMBEKOVA et al., 2019). Regular updating of knowledge and skills on latest technologies and methods of modern cybercrime is essential to maintain a prominent level of competence and efficiency in investigations (KHAMZIN et al., 2022). A promising area for improving the fight against cybercrime is to consider the psychological aspects of combating such crimes, special psychological training of such specialists, and it is advisable to factor in the existing research on this issue (FILIPENKO et al., 2024). Overall, improving the knowledge and skills of investigators in these areas is a key factor in the successful investigation of cybercrime, which allows effectively combating modern threats and ensuring fairness in law enforcement.

In the current environment of rapid advancement in digital technologies and integration of the information space, cybersecurity issues are becoming critical for Ukraine. Cybercrime, characterised by its dynamism and complexity, requires the introduction of advanced criminalistic tools and technologies for effective investigation. In this context, the international practices are of particular significance, as leading countries already have accumulated knowledge and successful practices in combating cybercrime. The integration and adaptation of innovative investigative methods and technologies in Ukraine will not only contribute to the effectiveness of the fight against cybercrime but will also help strengthen national cybersecurity at the global level.

Thus, in the United States of America, modern criminalistic tools and technologies are used to investigate cybercrime, which are constantly being improved to meet new challenges in the field of cybersecurity (DEWEY and PATEL, 2024). One of the key technologies is digital forensic science, which involves the use of tools to analyse large amounts of data that can be collected from digital devices, networks, and cloud services. For instance, blockchain technologies are used to ensure the integrity of collected data, which helps to maintain an unbroken chain of custody of evidence. Another important technology is AI systems that help investigators automatically analyse large amounts of information, such as images, emails, or chats. Artificial intelligence can considerably reduce the time required to find the necessary evidence, which is particularly useful in cybercrime investigations (KAPLINA et al., 2023). The latest methods are also actively used to investigate attacks on critical infrastructure. For example, tools that analyse the control logic in industrial systems help to detect traces of cyberattacks on facilities such as nuclear power

plants or hydroelectric power stations. These tools are designed to investigate the ways in which attackers can manipulate management software.

Poland employs the latest criminalistic tools and technologies in the investigation of cybercrime, including AI, quantum technologies, and specialised methods of big data processing. Polish law enforcement agencies are integrating these technologies to counter growing cyberthreats, especially in the context of new European regulations such as NIS Directive 2 (n.d.) and AI ACT (Negotiations on the..., 2023). Specifically, AI is used to analyse cyberthreats and automate investigation processes, allowing for faster and more efficient detection of potential crimes (SHEVCHUK et al., 2022b). Quantum technologies, albeit still in the early stages of implementation, are also considered a promising means of enhancing the security of cryptographic systems and preventing cybercrime. Polish experts are also focusing on the legislative regulation of these recent technologies, considering their potential and risks for national and European cybersecurity. These aspects are actively discussed at specialised forums, such as CYBERSEC CEE EXPO & FORUM 2024, where experts from Poland and other countries share their experience and strategies for implementing the latest technologies in cyber defence.

The experience of Spain in combating cybercrime using modern digital technologies is of considerable interest (Directive of the..., 2016; Code for the..., 2015). In response to the rapid growth of cybercrime in the context of technological advance, the government has introduced a series of measures aimed at protecting the population from threats arising in the digital environment through the adoption of relevant legislation. Spanish cyber law was developed by integrating three key areas of law: computer science, media, and telecommunications. The public part of cyber law covers issues related to cybercrime, data protection, and consumer privacy, while the private sector regulates electronic contracts, intellectual property, and e-commerce (AVIV et al., 2023). These legislative acts are aimed at ensuring that citizens are held accountable for their activities in the digital space and at regulating interaction on the Internet. Thus, Spain has regulated the aspects of combating cybercrime and protecting information using relevant digital technologies at the legislative level.

In Ukraine, protection against cyberthreats is carried out through a comprehensive approach that includes various technological, organisational, and legal measures (Smart Grid in..., 2023). Key aspects include the development and implementation of cybersecurity software, the use of cyber analytics to detect suspicious activity, the improvement of cryptographic technologies to protect confidential data, as well as the ongoing training of cybersecurity specialists and regular updates of security systems. In the context of martial law, cooperation with international law enforcement agencies and partners from other countries

plays a special role in exchanging information and coordinating efforts to counter cyberthreats, specifically in cases of transnational cybercrime.

Grid network technologies play a key role in the fight against cybercrime. These technologies allow executing program codes on one or more remote computers, providing access to both structured data (databases) and unstructured information (files), as well as to data sources such as sensors and observation instruments. Grid technology is based on the concept of integrating various resources to create an infrastructure that combines information and computing capabilities on a global scale. This infrastructure extends the boundaries of conventional computer systems by enabling interaction between different types of resources, such as computing power, server clusters, information storage, and networks. Thanks to the use of network technologies, specialised middleware, and standardised services, the grid allows unhindered access to distributed resources, which ensures high reliability and efficiency in data exchange and processing.

This creates a new computing ecosystem that can meet the needs of both scientific research and industrial applications, combining resources into a single integrated structure. This model of cyber defence is aimed at preventing cyberattacks on important targets, such as critical infrastructure, government resources, and banking systems. In 2021, the National Coordination Centre for Cybersecurity at the National Security and Defence Council of Ukraine, together with the United States Agency for International Development's Cybersecurity of Ukraine's Critical Infrastructure project, conducted cyber defence measures for critical facilities called Grid NetWars, based on the use of a grid network to collect and process information. Mastering the NetWars Grid technique allows specialists to acquire best practices in detecting and countering cyberattacks on critical infrastructure, increasing their readiness to respond to cyberattacks of any complexity (Ukraine's first Grid..., 2021). Thus, effective counteraction to cybercrime requires the regulation of a wide range of issues, including those related to electronic evidence, software for analysing, processing, and storing information, and data protection.

The issue of ensuring cybersecurity and protection of critical infrastructure in Ukraine is becoming increasingly important, especially in the face of growing threats from network attacks. To properly counter cybercrime, especially in times of war, it is necessary to develop and implement effective algorithms for protecting information systems, as well as to strengthen measures to counter such offences (SHEVCHUK et al., 2023c). Recent legislative innovations in the field of cybersecurity regulation indicate the need to expand the powers of law enforcement agencies to more effectively counter cyberthreats. At the same time, strengthening criminal liability for cybercrime, especially those committed during martial law, is a necessary step to reduce the risk of new crimes. The introduction

of harsher penalties for offenders acting in the context of armed conflict is a justified and prompt measure that will contribute to strengthening national security.

The use of modern technology in criminal investigations, especially cybercrime, involves significant ethical implications and confidentiality issues. Technologies such as digital forensics, AI and automated systems can greatly enhance investigations by facilitating the rapid detection and solving of crimes. However, the widespread use of these technologies poses challenges related to potential privacy violations. Surveillance technologies may inadvertently lead to the surveillance of those who are not committing illegal acts, thereby violating their right to privacy. In addition, the comprehensive collection and examination of personal data, often done without explicit authorization, can lead to misappropriation or inadvertent disclosure of sensitive information, leaving individuals vulnerable to privacy violations. When incorporating sophisticated technologies into investigative techniques, the balance between public safety and privacy must be carefully evaluated.

In addition, the ethical use of these technologies requires transparency, accountability, and robust oversight procedures. In the absence of these protections, there is the potential for misuse of technology, such as mass surveillance or racial profiling, which can lead to prejudice. Ethical implications also include the potential for bias in AI systems that could affect the fairness of criminal investigations. AI systems are often trained on historical data that may embody prevailing cultural biases, which can lead to unfair outcomes for specific populations. Consequently, there is a need for legislation and ethical standards that ensure the appropriate use of new technologies, build trust and protect the rights of individuals, enabling law enforcement agencies to effectively combat cybercrime.

To effectively combat cybercrime, Ukraine should continue to develop a comprehensive cybersecurity system, focusing on critical infrastructure protection and information security. It is essential to implement the latest technologies and AI to protect the information space, encrypt data, and prevent cyber threats. In the context of martial law, strengthening cybersecurity is particularly relevant as cybercriminals attempt to attack military facilities. This requires close cooperation between government agencies, the public, IT professionals, military units, and the private sector to improve mechanisms for countering cybercrime. One of the key aspects is training and professional development of specialists from various services. Higher education institutions should update their curricula to include courses on cyber defence and information security to reduce the risk of sensitive information leakage.

The fight against cybercrime under martial law requires compliance with international standards and national legislation, with an emphasis on the protection of human rights and fundamental freedoms (SHEVCHENKO et al., 2024). The key is to bring national regulations in line with international legal norms and current cybersecurity requirements. In this context, combating cybercrime is becoming a priority for both the state and the international community. The integration of modern technologies and the latest methods in this area helps to increase the effectiveness of cybercrime countermeasures and reduce the negative consequences of cyber incidents, which is especially significant during military conflicts. The introduction of the latest scientific and technical advances into investigative practice is essential to improve the effectiveness of investigations.

Integrating modern scientific and technical developments, forensic science provides law enforcement agencies with innovative tools, methods, and techniques that meet the challenges of modern crime. The key purpose of using criminalistic tools is to identify and analyse traces of criminal acts, as well as to obtain evidence from these traces. The skilled use of modern criminalistic tools ensures the completeness, accuracy, and efficiency of investigations and trials, optimising these processes and contributing to the achievement of the main objectives and goals of criminal proceedings.

DISCUSSION

Law enforcement agencies are increasingly focusing on cybercrime investigations, which is reflected in the growing number of specialised units and personnel focused on cybercrime. However, the role of computer systems in shaping these investigations has not been sufficiently addressed. In this regard, it is worth supporting the opinion expressed by F. Greco and G. Greco (2020), B. Jerome (2020) and A. Ndope (2024) that modern forensic science and its various sectors are facing new challenges and theoretical and methodological problems. In this context, it is important to consider modern scientific and technological trends and threats arising in the field of modern crime, as well as their impact on the formation of criminalistic knowledge. As noted earlier, the rapid development of information, telecommunication, and biometric technologies, as well as their widespread use in criminal activities, requires specialised research into the latest digital and electronic technologies. This allows for the identification, recording, and seizure of electronic (digital) traces generated when preparing, committing, and concealing crimes, as well as for detailed investigation to establish all the circumstances surrounding a particular crime.

G. Sarkara and S. Shuklaa (2023), N. Hamad and D. Eleyan (2022) note that in the field of cybercrime, digital artefacts are important sources of critical information. This suggests that the effective use of digital investigative technologies to accurately collect evidence can substantially affect the outcome of investigations. Computers have a significant impact on cybercrime investigations, increasing the complexity of existing problems or introducing new challenges. The technologies used in modern investigations provide major benefits to investigators, including facilitating confidential investigations, providing access to global networks and databases, and allowing them to collect large amounts of evidence necessary for justice (MAKHAMBETSALIYEV et al., 2024; SAPARBEKOVA et al., 2024). However, these aspects have not yet received sufficient attention in scientific research.

The analysis of forensic investigations of cybercrime in the United States, Poland, Spain, and Ukraine revealed certain trends that can be compared with other studies in this context. In European countries, such as Germany and the UK, the emphasis is on integrating advanced technologies into criminalistic processes, particularly in the areas of AI and investigation automation. A. Cassidya et al. (2024), M. Singh et al. (2021), and A. Nicolás-Sánchez and F. Castro-Toledo (2024) highlight the considerable impact of artificial intelligence and machine learning algorithms on cybersecurity. Specifically, these algorithms play a vital role in threat detection due to their ability to analyse large amounts of data in depth and identify patterns that might otherwise go unnoticed by conventional methods. Anomaly detection has become another key aspect, as AI allows for quick and accurate recognition of deviations from the normal functioning of systems, which may indicate potential cyberthreats or attacks. Furthermore, the automation of decision-making processes through machine learning algorithms considerably improves the efficiency of incident response, allowing systems to adapt more quickly to new threats and minimise human intervention in the cyberdefence process (HALTSOVA et al., 2021).

According to Sarafatma and R. Singrore (2024), J. Gruber et al. (2022), F. Gordon et al. (2024), computer forensic science uses specialised techniques to identify and preserve evidence stored on computer devices. This discipline is important for identifying evidence that is legally valid in a court of law and contributes to the achievement of justice. The systematic application of criminalistic methodologies by professionals in the field is crucial, according to C. Horan and H. Saiedian (2021), N. AllahRakha (2024), A. Shah and D. Chudasama (2021); cloud forensic science is one of the principal areas of development in digital forensic science, as services are increasingly moving to cloud environments. Although open-source intelligence and online investigations have long been used in practice, investigators are constantly integrating the latest

technologies into these methods. However, natural language processing is not a universal solution to all problems. Specifically, it may not be effective due to limitations in the accuracy of context analysis, possible data quality issues, and variations in language constructions. Therefore, while natural language processing is a powerful tool in digital forensic science, its use should be combined with other methods to ensure a comprehensive approach to investigations and increase the efficiency of evidence discovery and analysis.

According to L. Sikos (2020), S. Grigaliunas and J. Toldinas (2020), B. Payne and L. Hadzhidimova (2020), automation and machine learning are essential aspects of the development of modern technologies that affect cybercrime investigations. Automation helps to accelerate the collection of evidence, while machine learning helps to identify and classify it. However, automation also raises new legal issues and challenges for law enforcement agencies. Despite the obvious benefits of automation in the face of growing data volumes and complexity, there is a limited amount of research offering solutions to related problems such as knowledge representation. In this context, AI plays a significant role. Specialised knowledge organisation systems and digital criminalistic ontologies ensure formalisation of concepts and properties in the field of forensic investigations. These systems can be focused on both investigation processes and concrete digital artefacts. There is immense potential for further research in this area as automation and machine learning continue to improve.

The analysis of criminalistic sources and investigative practice revealed a series of substantial difficulties encountered in the application of criminalistic techniques and methods. It was found that these difficulties are mainly related to the insufficient level of criminalistic support, specifically due to the limited qualifications of specialists and the lack of knowledge and skills in the use of the latest scientific and technical means and techniques. Such shortcomings negatively affect the effectiveness of detection, investigation, and prevention of modern crimes. According to K. Steinmetz et al. (2023), to improve the situation, it is necessary to focus on the practical aspect of forensic science. This involves the development and implementation of scientifically sound methodological recommendations for the effective use of criminalistic tools and methods, as well as the organisation of their integration into the practical activities of law enforcement agencies. Modern trends in criminalistic technology focus on the search for and implementation of innovative solutions aimed at optimising the process of crime investigation and trial. Such innovations include new or adapted criminalistic techniques, including modern information technology and electronic databases. Furthermore, it is important to introduce new methods of recording, analysing, and evaluating evidence. Therefore, it is worth agreeing with the

opinion that the integration of these innovations into investigative practice can increase the efficiency of criminal investigations and ensure a more accurate and reliable assessment of the evidence obtained.

In cybercrime investigation, law enforcement agencies are focusing their efforts on forming specialised units and improving the skills of personnel handling these issues. The development of information and biometric technologies requires the introduction of specialised techniques to effectively detect, record, and recover digital traces of crimes.

Thus, modern technologies, specifically natural language processing, can substantially improve the efficiency of investigations, but their use has certain limitations. In this context, it is important to continue to improve criminalistic practice by developing new techniques and integrating innovative technologies that meet modern requirements. This includes the development of new procedures for the collection, analysis, and evaluation of evidence, adapted to the specifics of digital crime and the latest technologies. It is necessary to introduce advanced technologies such as AI and machine learning into criminalistic practice. These tools can greatly facilitate the investigation process by automating routine tasks and increasing the accuracy of data analysis. For instance, AI algorithms can detect anomalies in large amounts of data or automate the process of classifying evidence. A comprehensive approach to developing new techniques and integrating innovative technologies is essential to improving the efficiency of forensic investigations. Continuous professional development and effective cooperation between various stakeholders are also key factors in ensuring fairness and improving the effectiveness of criminal investigations.

Current trends in forensic science point to the need for a comprehensive approach to the introduction of the latest technologies, including AI and automation, to improve the efficiency of investigations and ensure justice. Ukraine and other European countries should focus on further integration of these technologies and continuous training of forensic science specialists.

CONCLUSION

Cybercrime is one of the biggest threats that can destabilise both public life and government activities. The urgency of this problem has increased due to Russia's war against Ukraine, which has prompted an intensified search for new forms and methods of combating cybercrime. This also raised the issue of legislative regulation of aspects of combating this phenomenon. The current conditions require criminalistics to intensify its scientific potential and use the latest opportunities for effective prevention and fight against organised crime. Since criminals actively use cyberspace to commit offences, it is important to note that it is in this environment that traces of their activities are preserved. To

strengthen the fight against cybercrime, law enforcement agencies must develop and implement new operational and investigative measures and methods that accommodate the specifics of cyberspace.

The global community of digital experts, together with law enforcement agencies, is constantly looking for effective methods to protect network systems from compromise. The study identified the most popular security tools available to organisations fighting cyberthreats. Combining these tools with regular software updates can considerably improve cybersecurity and prevent numerous cyberattacks. The digital investigation process involves the use of specialised digital criminalistics tools and techniques to effectively identify and recover digital evidence necessary for judicial investigations. The use of software products such as EnCase™ Forensic, AccessData FTK Imager, ASR SMART, IBM i2 Analyst's Notebook, Autopsy, Rifiuti2, and Oracle Solaris fingerprint databases allows for high accuracy and reliability in the collection, analysis, and storage of digital data. These tools reflect modern approaches to investigating cybercrime, enabling specialists to provide comprehensive and detailed data analysis in a dynamically changing digital environment.

The experience of Poland and Spain in the field of the latest criminalistic technologies and the fight against cybercrime can be usefully implemented in Ukraine through the introduction of advanced tools and methods for investigating cybercrime. Poland's practices in integrating the latest technologies and legislative initiatives, such as NIS Directive 2 and AI ACT, provide valuable lessons for adapting and implementing analogous approaches in Ukraine. Spain has demonstrated the successful integration of legislative initiatives in the field of cybersecurity, combining computer science, media, and telecommunications into a single legal system to combat cybercrime. Legislation covering data protection, privacy, and e-commerce could serve as a model for the development of analogous regulations in Ukraine. The Spanish experience in this area can be used to develop a set of legal and technological measures aimed at improving the fight against cybercrime in the Ukrainian context.

The analysis was limited to specific geographical regions, such as individual countries or territories, which may reduce the extent to which international experience is considered in the overall global context.

Practice shows that a prominent area of scientific development is the investigation of new areas of criminalistic technology that determine the innovative vectors of modern forensic research. The relevance of studying new areas of criminalistic technology is especially growing in the context of global threats, information influences, and epidemiological crises such as pandemics, which emphasises the need to adapt criminalistic practices to new challenges and requirements.

REFERENCES

ALIMBEKOVA, M.A., IBRAYEVA, A.S., ICHSHANOVA, G.T., USEINOVA, K.R., & IBRAYEV, N.S. (2019). Legal culture of public servants: The comparative legal analysis of the formation practices of various countries. *Journal of Advanced Research in Law and Economics*, 10(7), 1956-1967. https://doi.org/10.14505/jarle.v10.7(45).02

ALLAHRAKHA, N. (2024). Transformation of crimes (cybercrimes) in digital age. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.156.

APAKHAYEV, N., ADILOVA, K., BUGYBAY, D., MUKALDYEVA, G., MUKHAMADIYEVA, G.N., & KOSHPENBETOV, B.M. (2017). Childhood legal protection in Kazakhstan. *Journal of Advanced Research in Law and Economics,* 8(3), 714-721. https://doi.org/10.14505/jarle.v8.3(25).03

APAKHAYEV, N., ADILOVA, K., BUGYBAY, D., TOKTYBAEV, A., & KOPBAYEV, D. (2024). The problem of protecting the rights and legitimate interests of the child in the family and outside IT. *Danube,* 15(3), 221-236. https://doi.org/10.2478/danb-2024-0013

Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part. (2014). https://zakon.rada.gov.ua/laws/show/984_011#Text.

AVIV, I., GAFNI, R., SHERMAN, S., AVIV, B., STERKIN, A., & BEGA, E. (2023). Cloud infrastructure from python code–breaking the barriers of cloud deployment. In B. Tekinerdogan, C. Trubiani, C. Tibermacine, P. Scandurra, C.E. Cuesta (Eds.), *European Conference on Software Architecture, ECSA* (pp. 1-8). https://www.researchgate.net/profile/Itzhak-Aviv/publication/373897534_Cloud_Infrastructure_from_Python_Code_-breaking_the_Barriers_of_Cloud_Deployment/links/6501edd2808f9268d573dea5/Cloud-Infrastructure-from-Python-Code-breaking-the-Barriers-of-Cloud-Deployment.pdf

AVTALION, Z., AVIV, I., HADAR, I., LURIA, G., & BAR-GIL, O. (2024). Digital Infrastructure as a New Organizational Digital Climate Dimension. *Applied Sciences (Switzerland),* 14(19), 8592. https://doi.org/10.3390/app14198592

BABENKO, M. (2023). Fakes, phishing, stealing money from cards: cyber fraud in Ukraine has Russian roots. https://focus.ua/uk/economics/550155-feyki-fishing-kraza-deneg-s-kart-u-kibermoshennichestva-v-ukraine-rossiyskie-korni.

BADA, M., & NURSE, J. (2021). Profiling the cybercriminal: A systematic review of research. https://doi.org/10.48550/arXiv.2105.02930.

BEKISHEV, A.K., IBRAYEVA, A., SMANOVA, A., NUSSIPOVA, L., & KAN, A.G. (2019). Challenges in contract murder investigations. *Journal of Advanced Research in Law and Economics,* 10(3), 725-733. https://doi.org/10.14505/jarle.v10.3(41).05

BORYSENKO, I.V., BULULUKOV, O.Y., PCHOLKIN, V.D., BARANCHUK, V.V., & PRYKHODKO, V.O. (2021). The modern development of new promising fields in forensic examinations. *Journal of Forensic Science and Medicine*, 7(4), 137-144. https://doi.org/10.4103/jfsm.jfsm_66_21.

CASSIDYA, A., FUADB, A., & SHOFY, M. (2024). Emerging trends and challenges in digital crime: A study of cyber criminal tactics and countermeasures. *Journal of Computer Science and Technology*, 1(1), 38-45. https://doi.org/10.70063/techcompinnovations.v1i1.25.

Code for the Cybersecurity Law of Spain. (2015). https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&tipo=C&modo=2.

Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 'On the Cybersecurity Strategy of Ukraine'". (2021). https://zakon.rada.gov.ua/laws/show/447/2021#Text.

DEWEY, J.N., & PATEL, S. (2024). Blockchain & cryptocurrency laws and regulations 2024. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa/.

Directive of the European Parliament and of the Council No. EU 2016/1148 "Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union". (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

DUMCHYKOV, M., PAKHOMOV, V., & BONDARENKO, O. (2020). Forensic problematic aspects of combating crimes in cyberspace. *Criminalistics and Forensics*, 65, 283-290. https://doi.org/10.33994/kndise.2020.65.27.

DWEIKAT, M., ELEYAN, D., & ELEYAN, A. (2021). Digital forensic tools used in analyzing cybercrime. *Journal of University of Shanghai for Science and Technology*, 23(3), 367-379. http://doi.org/10.51201/Jusst12621.

FAHMY, W. (2024). The cybercrime acts and the electronic transaction in international law. *Economics, Law and Policy*, 7(1), 18-41. http://doi.org/10.22158/elp.v7n1p18.

FILIPENKO, N., SHEVCHUK, V., LUKASHEVYCH, S., YAZAN, N., & SLIPETS, O. (2024). Legal and psychological principles of preventing sexual violence against children: International experience and realities of Ukraine. In M. Nechyporuk, V. Pavlikov, D. Krytskyi (Eds.), *Integrated Computer Technologies in Mechanical Engineering – 2023* (pp. 271-300). Cham: Springer. https://doi.org/10.1007/978-3-031-60549-9_21.

GORDON, F., MCGOVERN, A., THOMPSON, C., & WOOD, M. (2024). Beyond cybercrime: New perspectives on crime, harm and digital technologies. *International Journal for Crime, Justice and Social Democracy*, 11(1).

GRECO, F., & GRECO, G. (2020). Investigate techniques in the digital age: cybercrime and criminal profiling. *European Journal of Social Sciences Studies*, 5(3). https://doi.org/10.5281/zenodo.3877668.

GRIGALIUNAS, S., & TOLDINAS, J. (2020). Habits attribution and digital evidence object models based tool for cybercrime investigation. *Baltic Journal of Modern Computing*, 8(2), 275-292. https://doi.org/10.22364/bjmc.2020.8.2.05.

GRUBER, J., VOIGT, L., BENENSON, Z., & FREILING, F. (2022). Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. *Forensic Science International: Digital Investigation*, 43, 301438. https://doi.org/10.1016/j.fsidi.2022.301438.

HALTSOVA, V.V., KHARYTONOV, S.O., KHRAMTSOV, O.M., ZHYTNYI, O.O., & VASYLIEV, A.A. (2021). Criminal law as a means of protecting human rights and freedoms in the modern world. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(3), 248-256. https://doi.org/10.37635/jnalsu.28(3).2021.248-256.

HAMAD, N., & ELEYAN, D. (2022). Digital forensics tools used in cybercrime investigation – Comparative analysis. *Journal of Xi'an University of Architecture & Technology*, 4, 113-127.

HORAN, C., & SAIEDIAN, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, 1(4), 580-596. https://doi.org/10.3390/jcp1040029.

JEROME, B. (2020). Criminal investigation and criminal intelligence: Example of adaptation in the prevention and repression of cybercrime. *Risks*, 8(3), 99. https://doi.org/10.3390/risks8030099.

KAPLINA, O., TUMANYANTS, A., KRYTSKA, I., & VERHOGLYAD-GERASYMENKO, O. (2023). Application of artificial intelligence systems in criminal procedure: Key areas, basic legal principles and problems of correlation with fundamental human rights. *Access to Justice in Eastern Europe*, 6(3), 147-166. https://doi.org/10.33327/AJEE-18-6.3-a000314.

KHAMZIN, A., BURIBAYEV, Y., & SARTAYEVA, K. (2022). Prevention of Human Trafficking Crime: A View from Kazakhstan and Central Asian Countries. *International Journal of Criminal Justice Sciences,* 17(1), 34-53. https://doi.org/10.5281/zenodo.4756088

KRAVCHUK, M., KRAVCHUK, V., HRUBINKO, A., PODKOVENKO, T., & UKHACH, V. (2024). Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security,* 2(2), 28-38. https://doi.org/10.62566/lps/2.2024.28

KULLOLLI, B. (2024). Legal liability for plagiarism of scientific works: How do major publishers protect their content. *Social and Legal Studios,* 7(3), 36-43. https://doi.org/10.32518/sals3.2024.36

Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine". (2017). https://zakon.rada.gov.ua/laws/show/2163-19#Text.

MAKHAMBETSALIYEV, D., ALIMOVA, E., UTEGENOV, C., SAGYNBEKOVA, G., & SMANOVA, A. (2024). The main directions of the judicial activity of the Supreme Court of the United States in the field of civil rights and freedoms. *Scientific Herald of Uzhhorod University. Series Physics,* 55, 1532-1542. https://doi.org/10.54919/physics/55.2024.153ol2

MARTINEAU, M., SPIRIDON, L., & AIKEN, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. *Forensic Sciences*, 3(3), 452-477. https://doi.org/10.3390/forensicsci3030032.

NDOPE, A. (2024). *Implementation of digital forensic tools in white-collar cybercrimes: A qualitative study about implementation of digital forensic tools when it comes to investigation of white-collar cybercrimes*. Malmö: Malmö University.

Negotiations on the EU AI Act are over. We will know the final content in a month. (2023). https://publicystyka.ngo.pl/koniec-negocjacji-w-sprawie-unijnego-ai-act-ostateczna-tresc-poznamy-za-miesiac?gad_source=1&gclid=CjwKCAjw8fu1BhBsEiwAwDrsjFkuYiTyhTWCt4shadOnoBtLaaMEsrkpP82Z5ZQgLWeT0JwF7EmIphoCQyUQAvD_BwE.

NICOLÁS-SÁNCHEZ, A., & CASTRO-TOLEDO, F. (2024). Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: A European Union perspective. *Crime Science*, 13, 11. https://doi.org/10.1186/s40163-024-00209-7.

NIS Directive 2. (n.d.). https://infonet-projekt.com.pl/uslugi-it/audyt-nis2/?utm_source=googleads&utm_medium=cpc&utm_campaign=Oxari-Dyrektywa_NIS_2&utm_content=search&gad_source=1.

Order of the Prosecutor General's Office No. 298 "On Approval of the Regulation on the Unified Register of Pre-trial Investigations, Procedure for its Formation and Maintenance". (2020). https://zakon.rada.gov.ua/laws/show/v0298905-20#Text.

ORLOVSKYI, R., US, O., & SHEVCHUK, V. (2022). Committing a criminal offence by an organized criminal group. *Pakistan Journal of Criminology*, 14(2), 33-46.

ORLOVSKYI, R., US, O., & SHEVCHUK, V. (2023). Human trafficking committed by transnational organised groups: criminal law and criminalistic means combating. *Pakistan Journal of Criminology*, 15(4), 119-136.

PAYNE, B., & HADZHIDIMOVA, L. (2020). Disciplinary and Interdisciplinary Cybercrime Research: An examination. *International Journal of Cyber Criminology*, 14(1), 81-105. https://doi.org/10.5281/zenodo.3741131.

POLIAK, Y. (2022). *Use of technical means in conducting investigative (detective), covert investigative (detective) actions and use of its results during pre-trial investigation*. Lviv: Lviv State University of Internal Affairs.

RAKHA, A. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2), 23-54. https://doi.org/10.22201/iij.24485306e.2024.2.18892.

Report on the work of the Cyber Incident Response Centre "Systems for detecting vulnerabilities and responding to cyber incidents and cyber-attacks". (2023). https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a.

SAPARBEKOVA, E.K., SMANOVA, A.B., MAKHAMBETSALIYEV, D.B., NESSIPBAEVA, I.S., & NUSSIPOVA, L.B. (2024). Comparative Analysis of the Concept of Constitutional Judicial Law-Making in the United States of America and Kazakhstan. *International Journal for the Semiotics of Law,* 38(2), 603-617. https://doi.org/10.1007/s11196-024-10138-y

SARAFATMA, & SINGRORE, R. (2024). Study to examine forensic cybercrime and the role of computer forensics. *International Journal of Innovative Research in Technology and Science*, 12(2), 17-23.

SARKARA, G., & SHUKLAA, S. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminilogy,* 2, 100034. https://doi.org/10.1016/j.jeconc.2023.100034.

SHAH, A., & CHUDASAMA, D. (2021). Investigating various approaches and ways to detect cybercrime. *Journal of Network Security*, 9(2), 12-20. https://doi.org/10.37591/JoNS.

SHCHERBIAK, I., BINYTSKA, K., KOSTENKO, D., KRUPKO, S., KOLESNIKOV, A., & GERCHAKIVSKY, S. (2024). The Conceptual Information Model for Enhancing Social Mobility among Students through the Digitalization of the University's Educational Space. In *Proceedings - International Conference on Advanced Computer Information Technologies, ACIT*, (pp. 842-847). Ceske Budejovice: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ACIT62333.2024.10712543

SHEVCHENKO, S., YUNIN, O., BOBRISHOVA, L., KATORKIN, R., & TSYHULSKYI, S. (2024). Sources of Criminal Law on Domestic Violence Prevention. *Pakistan Journal of Criminology,* 16(2), 157-168. https://doi.org/10.62271/pjc.16.2.157.168

SHEVCHUK, O., SHEVCHUK, V., KOMPANIIETS, I., LUKASHEVYCH, S., & TKACHOVA, O. (2022a). Features of ensuring the rights of drug addicts for rehabilitation in Ukraine and the European Union: comparative legal aspect. *Juridical Tribune*, 12(2), 263-282. https://doi.org/10.24818/TBJ/2022/12/2.07.

SHEVCHUK, V., KAPUSTINA, M., ZATENATSKYI, D., KOSTENKO, M., & KOLESNIKOVA, I. (2023a). Criminalistic support of combating iatrogenic criminal offenses: Information system prospects. *Social and Legal Studios,* 6(4), 208-216. https://doi.org/10.32518/sals4.2023.208.

SHEVCHUK, V., KOSTENKO, M., MYSHKOV, Y., PAPUSHA, I., & HRYSHKO, I. (2023b). Functional purpose of tactical operations in the development of criminalistic methodics of crime investigation. *Pakistan Journal of Criminology*, 15(2), 61-78.

SHEVCHUK, V., VAPNIARCHUK, V., BORYSENKO, I., ZATENATSKYI, D., & SEMENOGOV, V. (2022b). Criminalistic methodics of crime investigation: Current problems and promising research areas. *Revista Juridica Portucalense*, 32, 320-341. https://doi.org/10.34625/issn.2183-2705(32)2022.ic-14.

SHEVCHUK, V.M. (2020). Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine*, 27(2), 170-183. https://doi.org/10.37635/jnalsu.27(2).2020.170-183.

SHEVCHUK, V.M., MUSIIENKO, O.L., & SOKOLENKO, M.O. (2023c). Criminal offences related to illicit trafficking in falsified medicines: investigation problems. *Wiadomosci Lekarskie*, 76(5), 992-1000. https://doi.org/10.36740/WLek202305116.

SIKOS, L. (2020). AI in digital forensics: Ontology engineering for cybercrime investigations. *WIREs Forensic Science*, 3(3), e1394. https://doi.org/10.1002/wfs2.1394.

SINGH, M., FRANK, R., & ZAINON, W. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, 10(3), 1658-1668. https://doi.org/10.11591/eei.v10i3.3028.

Smart Grid in Ukraine: What is it, why is it needed, and when will it be introduced? (2023). https://dia.dp.gov.ua/smart-grid-v-ukra%D1%97ni-shho-ce-take-navishho-potribne-i-koli-zyavitsya/.

STEINMETZ, K., SCHAEFER, B., BREWER, C., & KURTZ, D. (2023). The role of computer technologies in structuring evidence gathering in cybercrime investigations: A qualitative analysis. *Criminal Justice Review*. https://doi.org/10.1177/07340168231161091.

TOKARIEVA, K.S., KOVALCHUK, O.Y., KOLESNIKOV, A.P., DZYURBEL, A.D., BODNAR-PETROVSKA, O.B., & PREDMESTNIKOV, O.G. (2024). The use of ai-language models in judicial proceedings: information and legal aspects. *Revista Juridica*, 2(78), 520-538. https://doi.org/10.26668/revistajur.2316-753X.v2i78.6928

UKHNO, O. (2021). Genesis and issues of using latest technologies and artificial intelligence in criminalistics, forensic expert activity and pre-trial investigation. *Theory and Practice of Forensic Science and Criminalistics*, 25(3), 40-59. https://doi.org/10.32353/khrife.3.2021.04.

Ukraine's first Grid NetWars cyber training has started in Kyiv. (2021). https://www.rnbo.gov.ua/ua/Diialnist/5170.html.

VELLA, R., & FARRUGIA, J. (2024). Criminal profiling and its use in crime solving. Applicable for Malta? *European Journal of Theoretical and Applied Sciences*, 2(2), 672-685. https://doi.org/10.59324/ejtas.2024.2(2).58.

ZILE, A., PALKOVA, K., & VILKS, A. (2023). Study of the Influence of External Conditions and Materials on the Preservation of Hidden Prints under Water. *Pakistan Journal of Criminology,* 15(2), 305-322.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET