http://dx.doi.org/10.18623/rvd.v23.6764

CHALLENGES OF INVESTIGATING FRAUDULENT ACTIVITIES IN CYBERSPACE

DESAFIOS NA INVESTIGAÇÃO DE ATIVIDADES FRAUDULENTAS NO CIBERESPAÇO

Article received on: 01/26/2026
Article accepted on: 4/26/2026

Hanna Foros*
***Odesa State University of Internal Affairs, Odesa, Ukraine
Orcid: https://orcid.org/0000-0002-9504-3681

Olena Hrezina*
***Odesa State University of Internal Affairs, Odesa, Ukraine
Orcid: https://orcid.org/0000-0002-2491-6529

Viktor Nikitenko**
****State University of Trade and Economics, Kyiv, Ukraine
Orcid: https://orcid.org/0000-0002-2798-1668

Olena Kofanova***
*****National Academy of Internal Affairs, Kyiv, Ukraine
Orcid: https://orcid.org/0000-0002-0919-7570

Yevgeniya Svoboda***
*****National Academy of Internal Affairs, Kyiv, Ukraine
Orcid: https://orcid.org/0000-0002-8639-8333

Kostiantyn Kochman*
***Odesa State University of Internal Affairs, Odesa, Ukraine
Orcid: https://orcid.org/0009-0001-3194-1220

The authors declare that there is no conflict of interest

Abstract
The rapid digitalization of social relations, development of financial technologies, and expansion of electronic communications have led to the emergence of new forms of fraudulent conduct in cyberspace and significantly complicated the mechanisms for their detection and suppression. Unlike traditional fraud, cyber fraud is characterized by transnationality, technological adaptability, remote influence on victims, and the active use of digital infrastructure, which creates additional challenges for investigation, proving, and ensuring cybersecurity. Under such conditions, countering fraudulent activities in cyberspace requires not only procedural responses but also the integration of criminal justice mechanisms with cyber defense and cybersecurity systems. The article presents a comprehensive study of the problems of investigating fraudulent acts in cyberspace and focuses on theoretical, procedural, and organizational aspects of this activity. A theoretical and legal characterization

Resumo
A rápida digitalização das relações sociais, o desenvolvimento das tecnologias financeiras e a expansão das comunicações eletrónicas conduziram ao surgimento de novas formas de conduta fraudulenta no ciberespaço e complicaram significativamente os mecanismos para a sua deteção e repressão. Ao contrário da fraude tradicional, a fraude cibernética caracteriza-se pela transnacionalidade, pela adaptabilidade tecnológica, pela influência à distância sobre as vítimas e pela utilização ativa da infraestrutura digital, o que cria desafios adicionais para a investigação, a prova e a garantia da cibersegurança. Nestas condições, o combate às atividades fraudulentas no ciberespaço requer não só respostas processuais, mas também a integração dos mecanismos de justiça penal com os sistemas de defesa cibernética e de cibersegurança. O artigo apresenta um estudo abrangente dos problemas da investigação de atos fraudulentos no ciberespaço e centra-se nos aspetos teóricos,

of cyber fraud is proposed, and a multi-level classification model is developed based on the method of fraudulent influence, object of encroachment, technological environment, degree of automation, and jurisdictional structure. It is substantiated that such classification has practical significance because it determines the structure of digital traces, affects the organization of investigation, and influences the methods of collecting and evaluating digital evidence. Particular attention is devoted to the analysis of legal, technical, and procedural barriers that complicate the coordination of national investigations of cyber fraud. The study identifies fragmented regulation, differences in approaches to digital evidence, jurisdictional uncertainty, technological asymmetry, and insufficient standardization of interagency cooperation as key factors reducing investigative effectiveness. It is argued that growing cyber threats require stronger institutional coordination and more advanced mechanisms of cybersecurity governance. The article also examines the main methodologies for collecting and preserving digital evidence and highlights the importance of maintaining authenticity, integrity, and chain of custody. It is demonstrated that the evidentiary value of digital information depends on compliance with procedural requirements and the use of forensic methods adapted to the digital environment. Based on the results obtained, recommendations are proposed to improve cooperation among public authorities, private entities, and international digital platforms through standardization, information exchange, professional training, and strengthening cybersecurity and cyber defense capacities.

Keywords: Fraudulent Acts in Cyberspace. Investigation. Digital Evidence. Proving. Cybersecurity. Cyber Threats. Cyber Defense.

processuais e organizacionais desta atividade. É proposta uma caracterização teórica e jurídica da fraude cibernética e é desenvolvido um modelo de classificação em vários níveis com base no método de influência fraudulenta, objeto da violação, ambiente tecnológico, grau de automatização e estrutura jurisdicional. É demonstrado que tal classificação tem significado prático, pois determina a estrutura dos vestígios digitais, afeta a organização da investigação e influencia os métodos de recolha e avaliação de provas digitais. É dedicada especial atenção à análise das barreiras jurídicas, técnicas e processuais que complicam a coordenação das investigações nacionais de fraude cibernética. O estudo identifica a regulamentação fragmentada, as diferenças nas abordagens às provas digitais, a incerteza jurisdicional, a assimetria tecnológica e a padronização insuficiente da cooperação interagências como fatores-chave que reduzem a eficácia investigativa. Argumenta-se que as crescentes ameaças cibernéticas exigem uma coordenação institucional mais forte e mecanismos mais avançados de governança da segurança cibernética. O artigo examina também as principais metodologias para a recolha e preservação de provas digitais e destaca a importância de manter a autenticidade, a integridade e a cadeia de custódia. Demonstra-se que o valor probatório da informação digital depende do cumprimento dos requisitos processuais e da utilização de métodos forenses adaptados ao ambiente digital. Com base nos resultados obtidos, são propostas recomendações para melhorar a cooperação entre autoridades públicas, entidades privadas e plataformas digitais internacionais através da normalização, do intercâmbio de informações, da formação profissional e do reforço das capacidades de cibersegurança e de ciberdefesa.

***Palavras-chave**: Atos Fraudulentos no Ciberespaço. Investigação. Provas Digitais. Prova. Cibersegurança. Ameaças Cibernéticas. Defesa Cibernética.*

1 INTRODUCTION

The rapid digitalization of social relations, the development of electronic

communications, the spread of financial technologies and the integration of digital platforms into everyday economic activity have led to a significant increase in the number of fraudulent actions in cyberspace. Unlike traditional forms of fraud, modern digital fraudulent models are characterized by a high level of technological adaptability, scalability and cross-border nature of implementation. The use of information and communication technologies creates the possibility for offenders to remotely influence victims, hide digital traces and use complex anonymization mechanisms. As a result, cyber fraud is gradually transforming from a local criminal and legal problem into a complex interdisciplinary phenomenon that directly affects the state of cybersecurity of the state and the stability of the digital environment.

The relevance of the study is due to the fact that traditional procedural and forensic investigation mechanisms are increasingly proving to be insufficiently effective in responding to modern cyber threats and ensuring proper evidence in criminal proceedings regarding fraudulent actions in cyberspace. Of particular difficulty are the issues of establishing jurisdiction, coordinating cross-border investigations, collecting and evaluating digital evidence, ensuring its authenticity and maintaining an uninterrupted chain of custody. Additional risk factors are the fragmentation of international cooperation mechanisms, the heterogeneity of cyber security standards, dependence on digital platforms and limited procedures for quick access to electronic information. In such conditions, the effectiveness of countering fraud is increasingly determined by the level of development of cybersecurity systems, digital forensics and inter-institutional interaction.

The purpose of the study is to theoretically substantiate and practically improve approaches to investigating fraudulent actions in cyberspace by forming a comprehensive model of their criminal-legal characteristics, classification, organization of evidence and ensuring proper work with digital evidence in the context of modern cyber threats and the development of cybersecurity systems. To achieve this goal, the following tasks are solved: carrying out a theoretical and legal characteristic and classification of fraudulent actions in cyberspace; analyzing legal, technical and procedural barriers to coordinating national investigations; studying the main methodologies for collecting, preserving and evaluating digital evidence, taking into account the requirements of reliability and the chain of custody; developing recommendations for increasing the effectiveness of

interaction between government agencies, the private sector and international platforms in the field of cybersecurity and cyber protection.

2 LITERATURE REVIEW

In modern scientific literature, the issue of fraudulent actions in cyberspace is studied mainly through the prism of the development of cybersecurity, digital forensics and the transformation of criminal procedural mechanisms of evidence. Along with this, modern scientific discourse in the field of criminal process, digital forensics and cybersecurity increasingly focuses on the issues of obtaining, verifying, admissibility and evaluation of digital evidence in criminal proceedings, as well as on the problems of international coordination of investigations in the digital environment and ensuring the reliability of electronic information (Casino *et al.*, 2022; Stoykova, 2021). Modern researchers pay special attention to the formation of procedural and technical guarantees of the authenticity of digital evidence, the improvement of digital forensics methodologies and the standardization of procedures for working with electronic data in the context of the growth of cross-border cyber threats (Stoykova, 2021; Dunsin *et al.*, 2023).

Modern studies also emphasize the need to ensure a continuous chain of custody of digital evidence, increase the transparency of procedures for their documentation and implement tools for controlling the integrity of electronic information at all stages of investigation and evidence (Nath *et al.*, 2024). At the same time, a separate direction of development is the integration of cyber protection mechanisms for critical digital infrastructure and the implementation of interdisciplinary approaches that combine criminal justice, digital forensics and institutional cybersecurity mechanisms (Dunsin *et al.*, 2023; Casino *et al.*, 2022).

At the same time, an analysis of existing research indicates insufficient integration of criminal law, procedural and cybersecurity approaches within a single model of investigating fraudulent actions in cyberspace. The issues of the relationship between the classification of fraudulent schemes, methods of proof, the specifics of working with digital evidence and mechanisms for ensuring cybersecurity in the context of the growth of cross-border cyber threats remain insufficiently researched.

3 METHODOLOGY

The methodological basis of the study is a comprehensive interdisciplinary approach that combines the provisions of criminology, criminal procedure, theory of evidence, cybersecurity and digital forensics to form a holistic model of investigating fraudulent actions in cyberspace. The work uses general scientific methods of cognition: analysis and synthesis - to generalize scientific approaches to determining the nature of cyber fraud and mechanisms for ensuring cyber protection; induction and deduction - to form a classification of fraudulent actions in cyberspace and establish patterns of their investigation; system-structural method - to study the relationship between cyber threats, mechanisms of evidence and institutional models for ensuring cybersecurity; comparative law method - to analyze approaches to organizing international cooperation and regulating access to digital evidence.

The empirical basis of the study is the results of the analysis of scientific publications, regulatory legal acts, international documents in the field of cybersecurity and cyber protection, as well as modern approaches to organizing the investigation of digital offenses. Special research methods include forensic modeling of typical mechanisms of fraudulent actions in cyberspace, analysis of the digital trail and processes of forming digital evidence, as well as structural analysis of procedures for ensuring the reliability of electronic information and maintaining the chain of custody. The research methodology is focused on ensuring scientific validity, reproducibility of results and the possibility of practical application of the formulated recommendations for improving the processes of investigation, evidence and organization of cybersecurity systems in the field of combating fraud.

4 RESULTS AND DISCUSSION

4.1. Theoretical and legal characteristics and classification of fraudulent actions in cyberspace

In the modern conditions of digital transformation of social relations, fraudulent actions in cyberspace have acquired the features of an independent criminogenic

phenomenon, which is characterized by a combination of traditional mechanisms of deception with the use of information and communication technologies. Unlike classical forms of fraud, where direct contact between subjects of legal relations is decisive, in cyberspace deception is implemented through the digital environment, automated tools, network platforms and algorithmic mechanisms of influence on user behavior. This necessitates the revision of established approaches to understanding the method of committing fraud, its objective side and the process of proving it.

The scientific understanding of this phenomenon is complicated by the lack of a universal definition of fraudulent actions in cyberspace in both international and national law. Most regulatory acts use a functional approach, where the legal assessment depends on the method of access to information, the form of seizure of property, or the nature of interference with information systems. At the same time, in the forensic aspect, cyber fraud is not limited to illegal access to computer systems, but covers a wide range of actions aimed at obtaining illegal benefits through the use of digital tools and information asymmetry between the offender and the victim (Bryzhko & Pylypchuk, 2021, p. 23). In view of this, fraudulent actions in cyberspace should be understood as intentional unlawful actions carried out using information and communication technologies, digital infrastructure, or electronic services and aimed at misleading a person, group of persons, or automated system in order to illegally obtain property benefits, access to digital assets, confidential information, or other economic benefits. This definition allows us to take into account not only the classic element of deception, but also the peculiarities of the digital environment, in which improper behavior is often implemented through automated or remote mechanisms.

The key feature of fraudulent actions in cyberspace is a specific way of forming a criminal result. Unlike traditional encroachments, here between the actions of the offender and obtaining a benefit there is usually an intermediate digital infrastructure – a platform, network, software product, electronic payment system or information service. This means that the digital environment ceases to be just a tool and actually turns into a separate structural element of the mechanism of committing an offense. In our opinion, to ensure systemic analysis and further formation of investigation methods, it is advisable to apply a multi-level classification of fraudulent actions in cyberspace. The first classification criterion should be to determine the method of implementing fraudulent

influence. According to this feature, socio-technical, technically mediated and platform forms of fraud can be distinguished. Socio-technical forms are based mainly on psychological influence and the use of social engineering mechanisms – phishing, impersonation, manipulative messages, telephone or text fraud. Technically mediated models involve the use of malware, compromised accounts, or automated means of obtaining illegal benefits. Platform fraud is implemented through electronic trading platforms, social networks, and other digital ecosystems.

The second classification criterion is to determine the subject of the criminal offense. According to this criterion, fraud aimed at the appropriation of financial resources, personal data, digital identity, cryptoassets, or access to information systems can be distinguished. This approach is of practical importance, since each category involves a different nature of evidentiary information, the specifics of procedural documentation, and different mechanisms for restoring violated rights.

The next classification criterion is the technological environment in which fraudulent actions are implemented. In this case, web-based fraud, mobile fraud, cloud fraud, social network fraud, and fraud using artificial intelligence technologies can be distinguished. The latter category is becoming particularly relevant due to the spread of generative models, synthetic content technologies, and automated mechanisms for creating false digital identities. The use of artificial intelligence technologies creates a qualitatively new level of scalability and adaptability of fraudulent schemes in the digital environment.

Also important for forensic analysis is the classification by the degree of automation of criminal activity. On this basis, manual, partially automated and fully automated forms of fraud can be distinguished. If manual models involve the direct participation of a person in interaction with the victim, then automated schemes use botnets, mass messaging scenarios, personal data collection algorithms and software tools for analyzing user behavior. A high level of automation significantly complicates the identification of the subject of the offense and requires the use of more complex digital forensics mechanisms. Of particular scientific interest is the classification by the jurisdictional structure of fraudulent activity. On this basis, domestic, cross-border and multi-jurisdictional forms of fraud can be distinguished. Their feature is the simultaneous operation of various elements of criminal activity in several countries: server hosting, use

of international payment systems, involvement of foreign digital platforms and the occurrence of consequences in different legal spaces. This category is the most difficult for the organization of the investigation and international cooperation.

It should also be taken into account that the classification of fraudulent actions in cyberspace has not only theoretical, but also applied significance. The type of fraudulent scheme determines the structure of the digital trail, the list of potential sources of evidence, the methods of their extraction, the features of maintaining the chain of custody of digital evidence and the range of subjects that should be involved in the investigation. Accordingly, the correct definition of the type of fraudulent actions at the initial stage of criminal proceedings significantly affects the effectiveness of proof and the further judicial perspective of the case.

Thus, fraudulent actions in cyberspace constitute a complex criminal-legal and forensic phenomenon that combines the traditional mechanism of deception with new technological methods of implementing criminal intent. Their theoretical and legal characteristics must take into account the features of the digital environment, multi-subject interaction, the dynamism of technologies and the specificity of proof. The proposed multi-level classification allows creating a conceptual basis for further analysis of the problems of coordinating investigations, collecting digital evidence and forming mechanisms of inter-institutional cooperation in the field of countering cyber fraud.

To ensure a systematic analysis of the subject of research and the formation of a methodological basis for further consideration of the problems of coordinating investigations, collecting digital evidence and inter-institutional interaction, it is advisable to apply a multi-level classification of fraudulent actions in cyberspace (Table 1). The proposed approach allows linking the criminal-legal characteristics of the relevant acts with the features of their proof and organization of the investigation.

Table 1

Classification of fraudulent acts in cyberspace and its significance for the organization of investigation

Classification Criterion	Type of Fraudulent Acts in Cyberspace	Substantive Characteristics	Typical Digital Trace (Sources of Evidence)	Practical Significance for Investigation
By the method of implementing fraudulent influence	**Socio-technical fraud**	Acquisition of property or information through deception using digital communications and social engineering mechanisms	Electronic messages, call records, communication history, login logs, communication metadata	Determines the need for prompt recording of communications and identification of the offender's digital identity
	Technically mediated fraud	Obtaining unlawful benefit through the use of software or network-based tools	System logs, network traffic, traces of software activity, access logs	Requires the application of digital forensics and technical infrastructure analysis
	Platform-based fraud	Use of digital platforms as an environment for implementing fraudulent schemes	Account data, transaction information, user activity logs	Requires cooperation with private platforms and international service providers
By the object of encroachment	**Financial fraud**	Unlawful acquisition of funds or economic benefit	Banking logs, payment records, electronic transactions	Directs investigation toward financial monitoring and asset tracing
	Personal data fraud	Unlawful acquisition or use of identifying information	Registration data, access logs, digital profiles	Necessitates identification of the source of data compromise
	Digital identity fraud	Use of another person's digital authentication or representation tools	Authentication history, digital certificates, login records	Requires verification of user authenticity and access methods
	Digital asset fraud	Acquisition of crypto-assets or other intangible digital valuables	Blockchain records, crypto wallets, transaction history	Requires international cooperation and specialized analytical methods
By technological environment	**Web-based fraud**	Use of websites, online interfaces, and web services	Domain records, server logs, web archives	Focuses investigation on web infrastructure analysis
	Mobile fraud	Use of mobile applications and mobile communication technologies	Device data, SIM identifiers, mobile logs	Requires seizure and analysis of mobile artifacts
	Cloud-based fraud	Commission of fraudulent acts through cloud environments and remote services	Provider data, synchronization logs, backup records	Requires consideration of the extraterritorial nature of data storage

Classification Criterion	Type of Fraudulent Acts in Cyberspace	Substantive Characteristics	Typical Digital Trace (Sources of Evidence)	Practical Significance for Investigation
	AI-oriented fraud	Use of artificial intelligence systems to automate deception	Traces of automated actions, content generation patterns	Requires analysis of indicators of algorithmic behavior
By degree of automation	**Manual fraud**	Direct participation of the offender in interaction with the victim	Communication records, digital behavioral traces	Aims at establishing individual involvement
	Partially automated fraud	Combination of human participation and software tools	Combined activity logs	Requires comprehensive technical and procedural assessment
	Fully automated fraud	Implementation of fraudulent schemes without direct human participation	Botnet data, automated scenarios	Requires large-scale digital analysis
By jurisdictional structure	**Domestic fraud**	All elements of the offense are connected to one state	National registries and local digital resources	Allows the use of standard procedural mechanisms
	Cross-border fraud	Certain elements of the offense are located in different jurisdictions	Data from foreign providers and international digital services	Requires international legal assistance
	Multi-jurisdictional fraud	Criminal activity simultaneously covers multiple states	Distributed digital infrastructure	Requires international coordination and complex management of digital evidence

4.2 Review of legal, technical and procedural barriers to the coordination of national investigations of fraudulent actions in cyberspace

Coordination of national investigations of fraudulent actions in cyberspace in the current conditions of transformation of the digital environment is gaining strategic importance for ensuring the effectiveness of criminal justice. Unlike traditional forms of property crimes, cyberfraud is characterized by a high speed of implementation of criminal intent, the possibility of remote influence on victims and the use of distributed digital infrastructure, which simultaneously covers several state jurisdictions. This creates the need to transition from a purely national approach to a model of integrated investigation based on international coordination, operational exchange of information and unified procedural standards.

One of the defining legal barriers remains the heterogeneity of regulatory

approaches to the qualification of fraudulent actions in cyberspace and to determining the procedural status of digital evidence. In different countries, electronic data can be considered as an independent means of evidence or as a type of documentary information, which affects the procedure for obtaining them and their admissibility in court. Differences also concern the grounds for conducting a search of information systems, procedures for temporary access to data, and conditions for applying special investigative measures.

Of particular importance in this context is the issue of international legal assistance in criminal proceedings. Traditional mechanisms for interstate cooperation were created mainly for material evidence and did not take into account the peculiarities of the fast-moving digital environment. Practice shows that the procedure for preparing, sending, and executing international requests often takes a period incompatible with the actual period of storage of digital information by providers or operators of electronic services. That is why specialized literature emphasizes that the effectiveness of international cooperation in the field of cybercrime directly depends on the ability of states to create accelerated mechanisms for accessing electronic evidence and preserving it (Brown, 2013, p. 193–194).

A separate systemic challenge is the problem of jurisdictional uncertainty. In the case of cyber fraud, the place of commission of a crime can be determined simultaneously by the location of the victim, server, financial infrastructure, digital platform or the person of the offender. As a result, situations arise where several states conduct parallel investigations or, conversely, there is no clearly defined competent authority. Such competition between jurisdictions creates risks of duplication of procedural actions, loss of evidence and conflict of legal regimes. Along with legal difficulties, technical limitations in the coordination of investigations have a significant impact. Modern fraudulent schemes actively use distributed resource allocation technologies, traffic anonymization, encrypted communication channels and tools for hiding digital traces. The use of multi-level routing networks and privacy protection services significantly complicates the establishment of the actual source of criminal activity and the subsequent procedural linking of the collected information to a specific person.

In addition, the investigation of fraudulent acts is increasingly associated with the processing of large volumes of digital data. The analysis of event logs, information from

payment systems, telecommunications records, social media data and cloud services requires the use of specialized digital analytics tools. At the same time, the different level of technological equipment of law enforcement agencies creates inequality of opportunities between states, which negatively affects the quality of international interaction.

An important procedural barrier is the lack of universal standards for interdepartmental information exchange. Cyberfraud investigations involve not only criminal justice agencies, but also banks, electronic service providers, telecommunications operators, cyber incident response centers and private companies. However, the formats for transmitting information, requirements for its documentation and criteria for confirming authenticity often remain incompatible between individual entities.

The issue of the correlation between the effectiveness of the investigation and the protection of fundamental human rights deserves special attention. The use of electronic data collection tools is directly related to the risks of excessive interference with privacy and violation of the principle of proportionality. The Council of Europe's recommendation documents emphasize that any procedural powers to access computer data should be accompanied by appropriate guarantees of legality, necessity and judicial control (Council of Europe. Guide to the Convention, 2001).

An additional complexity is the need to promptly preserve electronic information until permission is obtained to extract it or transfer it to another state. Unlike physical objects, digital data can be automatically deleted, modified or moved without external intervention. Therefore, a delay of even a few hours sometimes leads to the loss of critical traces of criminal activity.

At the same time, a separate problem remains the interaction of law enforcement agencies with global digital platforms and technology companies. A significant part of the evidentiary information is now under the control of private entities that operate in accordance with internal privacy policies and corporate procedures for considering state requests. This means that actual access to information is increasingly determined not only by law, but also by the regulatory rules of digital ecosystems.

The personnel factor has a significant impact on the effectiveness of coordination. Cyberfraud investigations require specialists who are able to work simultaneously with

criminal procedural norms, digital forensics methods, network traffic analysis, and international cooperation procedures. The use of computer science research findings is also important (Klymchuk *et al.*, 2022, pp. 12–13). Digital forensics studies also emphasize that the quality of the initial stage of collecting digital evidence directly determines its further procedural value and the possibility of using it in interstate proceedings (Casey, 2011, pp. 60–66).

Thus, the legal, technical, and procedural barriers to coordinating national investigations of fraudulent actions in cyberspace are complex and interdependent. They manifest themselves through the fragmentation of legislation, the heterogeneity of digital infrastructure, the complexity of international evidence exchange and the lack of specialized competencies. Overcoming these limitations is possible only if legal harmonization, the development of digital forensics, standardization of interagency interaction procedures and systematic professional training of investigation subjects are combined.

4.3 Analysis of the main methodologies for collecting and preserving digital evidence, issues of reliability and chain of custody

Collecting and preserving digital evidence in proceedings concerning fraudulent actions in cyberspace requires a combination of criminal procedural, forensic and technical approaches, since evidentiary information exists not only in the form of files or messages, but also in the form of metadata, event logs, network records, backup copies, digital identifiers and traces of user interaction with the information system. The peculiarity of such evidence is that it can be quickly changed, deleted, overwritten or moved between different digital environments, therefore the methodology for working with it should be aimed not only at obtaining information, but also at ensuring its integrity, authenticity and further procedural suitability.

Methodologically, the first stage of working with digital evidence is its identification, i.e. establishing potential sources of evidentiary information. In cyberfraud cases, such sources can be mobile devices, computers, servers, email, instant messengers, banking applications, cloud services, payment platforms, websites, social networks and authorization logs. At this stage, it is important not to narrow the evidentiary base only to

obvious media, since significant digital traces are often not contained in the content of the message itself, but in the technical parameters of its creation, sending, editing or access to it. As rightly noted in the literature, traces can be contained both in the device itself and in information about its use" (Klimchuk and Kuntiy, 2020, p. 113). The second stage is the fixation of digital information in a way that minimizes the risk of its distortion. In practical terms, this means creating forensic copies, using hardware or software means of blocking recording, documenting the state of the device at the time of removal, fixing the time, place, conditions of access to data and persons who performed the relevant actions. It is at this level that the initial basis for the reliability of evidence is formed, since any uncontrolled interference with the medium or information system may call into question the further use of the obtained data in criminal proceedings.

Ukrainian scientific literature rightly emphasizes that the electronic form of evidence has its own specifics, as it covers information created, processed, stored or transmitted using analog or digital signals, and also contains parameters inaccessible to traditional forms of evidence, in particular metadata. Because of this, digital evidence cannot be considered only as a type of ordinary document: it requires separate rules for detection, fixation, removal, verification and evaluation (Figursky, 2023, p. 97).

The third stage is related to the preservation of digital evidence in an unchanged state. The most common methodology is to create a bit-by-bit copy of the medium or the corresponding information array with the subsequent calculation of hash values, which allow to verify the immutability of the data in the future. Hashing serves as a technical indicator of integrity: if after copying, transmission or examination the value of the checksum has not changed, this confirms that the evidentiary information has remained identical to the original digital object. At the same time, the preservation of digital evidence is not reduced to technical copying. No less important is the proper procedural documentation of each action: who gained access to the medium, when exactly this happened, under what conditions the copying was carried out, what tools were used, where the original was stored and who had the opportunity to contact it in the future. The insufficiency of such documentation creates the risk that even technically reliable information will be questioned due to a violation of the procedure for its receipt or storage.

This is where the chain of custody becomes central. Its content is to continuously

document the movement of evidence from the moment of discovery to the moment of examination by the court. For digital evidence, this chain should cover not only the physical movement of the medium, but also all operations with the data: creating a copy, exporting files, analyzing metadata, transferring to an expert, uploading to a secure repository, opening access to other participants in the proceedings. Any gap in this chain can be used by the defense to substantiate doubts about the authenticity of the evidence.

The problem of the reliability of digital evidence obtained from open sources or online platforms is particularly complex. Screenshots, web pages, messages on social networks or data from instant messengers can be quickly changed or deleted, and their appearance does not always confirm the real origin of the information. Therefore, such information should be accompanied by technical recording of the URL address, access time, metadata, digital environment, recording tools used, and, if possible, additional confirmation through requests to providers or administrators of relevant services.

An important organizational aspect is the availability of appropriate technical infrastructure by law enforcement agencies. Modern work with digital evidence requires forensic workstations, write-blocker devices, software for creating and analyzing forensic images, hashing tools, secure storage, and access control systems. Recent Ukrainian studies emphasize that material and technical support, human resources, and regulatory framework are three key elements of the organizational readiness of subjects of criminal proceedings to work with evidence in electronic form (Kalancha, 2025, p. 261).

A separate problem is the storage of digital evidence for a long time. Physical media degrade, file formats become obsolete, software changes, and cloud environments depend on the policies of private providers. Therefore, evidence preservation must include not only protecting the media from physical damage, but also ensuring the possibility of future reproduction of information without losing its content, structure, and context. This requires centralized secure storage, backup, access logging, and regular verification of control hash values.

A significant challenge is also the lack of a unified practice of evaluating electronic evidence by courts. If an investigator or prosecutor cannot clearly explain the origin of digital information, the method of its acquisition, storage conditions, and immutability, the judicial perspective of such evidence is significantly weakened. Therefore, electronic evidence requires a specific procedure for collection, verification,

and evaluation, is perceived only with the help of technical means, and is not inextricably linked to the physical medium.

Therefore, the methodology for collecting and preserving digital evidence in cases of fraudulent actions in cyberspace should be based on a combination of a clear procedural form, forensic accuracy and technical reproducibility. Its key elements are timely identification of information sources, secure data capture, creation of forensic copies, hashing, documentation of all operations, secure storage and maintenance of a continuous chain of custody. Only under such conditions can digital information be transformed from a technical trace into proper, admissible and convincing evidence in criminal proceedings.

4.4 Recommendations for improving cooperation between public authorities, the private sector and international platforms: standards, information exchange and training

Effective investigation of fraudulent acts in cyberspace increasingly depends less and less on the procedural powers of public authorities and is increasingly determined by the level of intersectoral cooperation in the field of cybersecurity and cyber protection between law enforcement agencies, private companies and international digital platforms. The modern architecture of cyberspace has effectively formed a new model of distribution of responsibility for the safe functioning of the digital environment: the state carries out criminal prosecution and implements cyber protection policies, the private sector owns critical digital infrastructure and data, and international technological platforms control significant arrays of communication information and mechanisms for accessing it. Under such conditions, the effectiveness of countering cyber fraud increasingly depends on building an integrated system of cybersecurity cooperation capable of ensuring timely detection of threats, coordinating responses and maintaining an appropriate level of cyber resilience. One of the key areas for improving such cooperation is the standardization of cooperation procedures and unification of approaches to managing digital information in the field of cybersecurity. In practice, law enforcement agencies, financial institutions, electronic communications operators and international digital platforms often use incompatible mechanisms for documenting cyber incidents, different event logging

standards and different rules for storing digital data. This complicates the implementation of cyber protection and creates risks of losing the evidentiary value of digital information. Modern studies of cybersecurity governance argue that standardization of information exchange procedures should include not only technical compatibility of systems, but also harmonization of legal criteria for access, processing and use of data within the framework of criminal proceedings.

The next strategic direction for strengthening cyber defense is the development of mechanisms for structured information exchange between the public and private sectors. In cases of cyber fraud, private actors are often the first to record signs of cyber incidents, suspicious activity and compromise of digital services. However, the potential of such information is not sufficiently used due to the lack of unified notification procedures, unclear data transfer guarantees and limited level of trust between participants in cybersecurity interaction. In this context, it is advisable to form permanent cyber information exchange platforms (information sharing mechanisms), which would allow for a prompt response in compliance with the requirements of personal data protection and cybersecurity principles.

Cooperation with international digital platforms is of particular importance as a separate direction of ensuring cyber protection and international cybersecurity coordination. It is such platforms that are increasingly becoming a source of critically important information for establishing the method of committing fraudulent actions, digital identification of users, tracing transactional activity and localization of the digital infrastructure of offenders. At the same time, access to relevant information is often determined by the internal policies of the platforms, which does not always meet the needs of a prompt response in the field of cybersecurity. In this regard, a promising direction is the development of specialized mechanisms for cooperation between states and platforms, including standardized communication channels, electronic request formats and simplified procedures for storing digital data.

An essential tool for the development of the cyber defense system should be the creation of joint information and analytical platforms and cybersecurity coordination centers. Their operation allows integrating information about cyber incidents, automating request processing, accumulating information about typical scenarios of fraudulent activity and ensuring the prediction of new cyber risks. The effectiveness of interagency

cybersecurity interaction directly depends on the principles of efficiency, continuity of information exchange, technological compatibility and consistency of management decisions.

A separate direction for improving the cyber defense system is related to the development of human resources. Modern fraudulent actions in cyberspace combine technical complexity with multi-level procedural mechanisms, which requires specialists to have comprehensive training in the field of cybersecurity, digital forensics, data analysis, international law and cyber risk management. Special attention needs to be paid to the development of interdisciplinary educational programs that will provide training for a new generation of specialists to implement cyber security tasks and investigate digital crimes.

At the same time, professional training should not be limited to the formal education system. A condition for ensuring an adequate level of cybersecurity is the creation of mechanisms for constant knowledge exchange between government agencies, the private sector and international expert communities. Practice shows that the most effective models of cybersecurity are formed precisely through joint learning environments, professional networks, cyber training grounds, training simulations and mechanisms for accumulating applied experience.

Therefore, improving cooperation between government agencies, the private sector and international platforms in the field of countering fraudulent actions in cyberspace should be considered as a component of the overall system for ensuring cybersecurity and developing national and international cybersecurity. The implementation of this approach involves the formation of unified standards of interaction, the development of information exchange mechanisms, the creation of coordination institutions and investment in professional competencies. It is the integration of these elements that creates the prerequisites for the transition from a fragmented response to cyber incidents to a sustainable model of collective cybersecurity and increasing the efficiency of investigating fraudulent actions in the digital environment.

5 CONCLUSIONS

The conducted research allowed us to establish that fraudulent actions in cyberspace constitute an independent complex criminal law and forensic phenomenon, the development of which is directly related to the digitalization of social relations, the transformation of economic activity and the growth of modern cyber threats. Unlike traditional forms of fraud, the corresponding acts are characterized by the use of digital infrastructure, a high level of technological adaptability, cross-border nature and the complexity of forming evidentiary information. It is advisable to apply a multi-level classification of fraudulent actions in cyberspace by the method of implementation of fraudulent influence, the subject of the attack, the technological environment, the degree of automation and the jurisdictional structure. The proposed approach allows to link the criminal-legal characteristics of the relevant acts with the features of their investigation, the organization of evidence and the identification of sources of digital evidence, which creates a methodological basis for the construction of specialized forensic methods.

The effectiveness of investigating fraudulent acts in cyberspace is significantly limited by a complex of interrelated legal, technical and procedural barriers. The main ones include the fragmentation of regulatory regulation, the heterogeneity of approaches to the procedural status of digital evidence, the complexity of international coordination, the technological dynamics of the digital environment and the lack of unified procedures for interagency interaction. The procedural value of methodologies for collecting and preserving digital evidence is determined not only by the content of the information obtained, but also by compliance with the requirements of reliability, integrity and maintaining an uninterrupted chain of custody. Ensuring proper evidence in cyberfraud cases requires the integration of digital forensics tools, standardized procedures for working with electronic information and modern cyber protection mechanisms.

It is necessary to transition from a predominantly fragmented model of responding to fraudulent acts in cyberspace to a comprehensive system for ensuring cybersecurity and organizing investigations. Such a system should be based on the harmonization of legal regulation, the development of institutional interaction between state bodies, the private sector and international digital platforms, the standardization of information exchange mechanisms, the improvement of procedures for working with digital evidence

and the systematic training of specialists in the field of cybersecurity and cyber defense. The implementation of these areas creates the prerequisites for increasing the efficiency of investigations, strengthening the state's ability to counteract current cyber threats and ensuring an adequate level of protection of the rights of participants in digital legal relations.

REFERENCES

Brown, I. (Ed.). (2013). Research handbook on governance of the Internet. Edward Elgar Publishing. https://doi.org/10.4337/9780857938855

Bryzhko, V. M., & Pylypchuk, V. G. (2021). Personal data security: legal standards of the European Union and modern applied problems. Information and Law, 1(36), 17–28. https://doi.org/10.37750/2616-6798.2021.1(36).238174

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press. https://doi.org/10.1016/C2009-0-64056-6

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. arXiv. https://doi.org/10.48550/arXiv.2205.12911

Council of Europe. (2001). The Budapest Convention. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Dunsin, D., Ghanem, M.C., Ouazzane, K., & Vassilev, V. (2023). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. arXiv. https://doi.org/10.48550/arXiv.2309.07064

Figurskyi, V. M. (2023). Evidence in electronic form in criminal proceedings. Galician Studies: Legal Sciences, 4, 97–105. https://doi.org/10.32782/galician_studies/law-2023-4-14

Kalancha, I. G. (2025). Organizational aspects of working with evidence in electronic form in the criminal process of Ukraine. Scientific Bulletin of the Uzhhorod National University. Series: Law, 90(4), 258–263. https://doi.org/10.24144/2307-3322.2025.90.4.36

Klymchuk, M. P., & Kuntiy, A. I. (2020). Detection and removal of traces of criminal offenses committed using cellular communication devices. Socio-Legal Studies, 3(9), 111–118. URL: https://sls-journal.com.ua/web/uploads/pdf/S&LS_2020_Vol.%203,%20No.%203_111-118.pdf

Klymchuk, M. P., Komissarchuk, Y. A., Marko, S. I., & Stetsyk, B. V. (2022). Forensic

Computer Technical Expertise in Criminal Proceedings. Lviv: Lviv State University of Internal Affairs. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4399/1/Судова%20к-т%20експертиза...%20--верстка.pdf

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications. https://doi.org/10.1109/TPS-ISA63395.2024.00010

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, 42, 105575. https://doi.org/10.1016/j.clsr.2021.105575