Countering Financial Cybercrime: Pre-Trial Investigation Standards, Digital Forensics Tools, and International Coordination

Petro Rekotov [1], Andriy Antoshchuk [2], Volodymyr Bondar [3], Iryna Dubivka [4], Yulia Tereshchenko [5], Viacheslav Kuliush [6]

[1] Department of Information Economics, Entrepreneurship and Finance, Zaporizhzhia National University, Zaporizhzhia, Ukraine
[2] Department of Criminology and Forensic Medicine, National Academy of Internal Affairs, Kyiv, Ukraine
[3] Department of Criminal Procedure and Forensics of Educational and scientific humanitarian institute, National Academy of the Security Service of Ukraine, Kyiv, Ukraine
[4] Department of Criminal procedure, National Academy of Internal Affairs, Kyiv, Ukraine
[5] Department of Criminal Justice, Educational and Scientific Institute of Law and Psychology, National Academy of Internal Affairs, Kyiv, Ukraine
[6] Countermeasures Department in the city of Kyiv Cyber Police Department of the National Police of Ukraine, Kyiv, Ukraine

The article is devoted to a comprehensive analysis of countering financial cybercrime in the context of contemporary challenges related to digitalization and the transnationalization of criminal activity. The theoretical foundations of financial cybercrime as a form of high-tech economic crime are examined, and its key characteristics and criminal law specifics are identified. Particular attention is paid to pre-trial investigation standards, especially issues concerning the collection, fixation, and admissibility of digital evidence. The role of digital forensics tools in ensuring the effectiveness of proof is analyzed, as well as the importance of international coordination and interstate legal assistance in the investigation of financial cybercrime. The necessity of forming an integrated counteraction model combining legal, technical, and organizational mechanisms is substantiated.

Keywords: financial cybercrime, digital evidence, pre-trial investigation, digital forensics, international coordination, cybersecurity, economic crime.

1. Introduction

The rapid digitalization of the financial sector has led to a fundamental transformation of economic activity while simultaneously creating new opportunities for criminal encroachments. Financial cybercrime today represents one of the most dynamic and socially dangerous forms of crime, as it combines a high level of technological sophistication with potentially significant economic consequences. Its proliferation directly affects the stability of financial markets, trust in banking and payment systems, and the overall level of state economic security, which explains the increasing attention paid to this phenomenon by scholars and practitioners.

A distinctive feature of financial cybercrime is its transnational nature, high latency, and ability to rapidly adapt to technological innovations. Under such conditions, traditional criminal law and criminal procedure approaches prove insufficient for an effective response to emerging threats. This actualizes the need to develop specialized pre-trial investigation standards that take into account the specific nature of digital evidence, the peculiarities of financial transactions in virtual environments, and the necessity of prompt response. At the same time, the role of digital forensics as a tool for ensuring a reliable evidentiary basis in financial cybercrime cases is steadily increasing.

International coordination in countering financial cybercrime is of particular importance, as criminal activity in cyberspace is not limited by state borders. The effectiveness of investigations largely depends on the ability of states to harmonize procedural approaches, exchange electronic evidence, and apply unified forensic standards. In this context, scholarly analysis of pre-trial investigation standards, digital forensics tools, and mechanisms of international cooperation acquires

a comprehensive character and constitutes a necessary prerequisite for developing an effective model for countering financial cybercrime in the modern globalized digital environment.

The purpose of the study is to provide a comprehensive scientific substantiation of contemporary approaches to countering financial cybercrime through the analysis of pre-trial investigation standards, digital forensics tools, and mechanisms of international coordination, as well as to formulate conceptual provisions aimed at improving the legal and organizational foundations for ensuring the effectiveness of investigations into financial cybercrime in a transnational digital environment.

2. Methodology

The methodological basis of the research consists of a combination of general scientific and special legal methods of cognition, the application of which is determined by the complex nature of the research subject. In particular, the dialectical method is used to identify patterns in the development of financial cybercrime in the context of economic digitalization; the systemic-structural method is applied to analyze the interrelationship between legal norms, forensic tools, and international cooperation mechanisms; and the formal-legal method is employed to examine national and international legal norms governing counteraction to financial cybercrime and the collection of digital evidence.

In addition, the comparative legal method is used to compare pre-trial investigation standards and approaches to the use of digital forensics in the legal systems of different states, while the legal modeling method is applied to formulate proposals for improving national mechanisms for countering financial cybercrime in line with international standards and best practices. The use of logical-legal analysis and the generalization of judicial and law enforcement practice ensures the scientific validity of the conclusions and recommendations formulated in the study.

3. Theoretical Foundations and Contemporary Challenges in Countering Financial Cybercrime

In contemporary scholarly discourse, cybercrime is regarded as a qualitatively new form of criminal activity that has emerged as a result of the rapid development of information and communication technologies and the global digitalization of social relations. It differs significantly from traditional forms of crime not only in the methods of commission but also in the scale of impact, speed of dissemination, and complexity of detection. Cybercrime is particularly relevant in the financial sector, where digital technologies have become the basic instruments for the functioning of markets, banking systems, and payment infrastructure. For this reason, financial cybercrime is increasingly viewed as a threat not only to individual entities but also to economic stability and national security [1].

In criminal law theory, cybercrimes are traditionally defined as unlawful acts committed using computer systems, networks, or data, as well as offenses directly targeting such systems. At the same time, financial cybercrime constitutes a distinct and specialized subcategory, as its dominant objective is the unlawful acquisition of property or other economic benefits. This includes, in particular, electronic fraud, illegal financial transactions, theft of payment credentials, and manipulation of digital assets. Such orientation necessitates an expanded legal analysis that goes beyond classical approaches to computer crime [2].

One of the key theoretical and legal problems is the absence of a unified definition of financial cybercrime in international law. Even the Budapest Convention on Cybercrime of 2001, which remains the principal international instrument in this field, does not contain a separate category of financial cybercrime, limiting itself to general provisions on computer fraud and illegal interference with data. This results in fragmented legal regulation and divergent approaches by states to the criminalization of relevant conduct. The Explanatory Report to the Convention explicitly states that its provisions are framework in nature and require adaptation at the national level [3].

Financial cybercrime has a hybrid legal nature, as it combines elements of traditional economic crime with the use of high-tech digital tools. This duality manifests itself both in the methods of commission and in the mechanisms of harm. On the one hand, traditional motives such as illicit enrichment persist; on the other hand, sophisticated technical methods are employed, significantly complicating detection. This necessitates a comprehensive interdisciplinary approach integrating criminal, financial, and information law [4].

In modern theoretical models of countering financial cybercrime, the risk-based approach is gaining increasing importance. It involves identifying the most vulnerable segments of the financial system and concentrating resources on their protection. This approach is widely applied in financial monitoring and anti-money laundering and is gradually being integrated into cybersecurity strategies. FATF recommendations emphasize that the effectiveness of countering financial crime largely depends on a state's ability to adapt to changing risk profiles [5].

The development of digital financial technologies significantly transforms the structure of financial cybercrime. The spread of online banking, mobile payment services, cryptocurrencies, and FinTech solutions creates new opportunities for economic growth while simultaneously generating additional vectors for criminal encroachment. Scholarly literature emphasizes that innovative financial products often outpace legal regulation, creating regulatory gaps that increase the vulnerability of users and financial institutions [6].

A particularly important issue concerns trust in financial institutions in the digital environment. Large-scale financial cyber incidents may undermine the stability of the banking system and trigger cascading effects in financial markets. Research conducted by the European Central Bank indicates that cyber risks are considered potentially systemic, as their materialization may have consequences comparable to traditional financial crises [7].

From a criminological perspective, financial cybercrime is analyzed through the lens of rational choice and opportunity theories. Offenders assess the ratio between potential gain and the risk of detection, which remains relatively low in cyberspace. Anonymity, transnationality, and the complexity of technical tracing increase the attractiveness of financial cybercrime as a form of criminal activity [8].

The global nature of financial cybercrime poses serious challenges to traditional concepts of jurisdiction. Criminal acts may simultaneously involve multiple legal orders, complicating the determination of competent authorities and applicable law. This is particularly problematic when criminal infrastructure is located in jurisdictions with limited international cooperation.

Another significant theoretical issue is the latency of financial cybercrime. A substantial portion of incidents remains undisclosed due to reputational concerns of financial institutions. Moreover, technical difficulties in detecting intrusions into information systems lead to the underreporting of official statistics, which complicates the formulation of effective criminal policy [9].

A central place in the theory of countering financial cybercrime is occupied by the issue of digital evidence. Electronic data are intangible, easily modifiable, and require special fixation procedures. Scholars emphasize that without proper legal and forensic safeguards, digital evidence may lose its probative value in judicial proceedings [10].

Contemporary challenges are also associated with the use of artificial intelligence and automated systems in the financial sector. Such technologies are employed both to detect suspicious transactions and to commit sophisticated financial cybercrimes. This creates technological asymmetry, whereby law enforcement agencies are forced to constantly catch up with offenders' innovative methods [11].

Scholarly research emphasizes the necessity of harmonizing national legislation with international standards in cybersecurity and financial supervision. The European Union, in particular, actively develops regulatory mechanisms aimed at enhancing the resilience of financial infrastructure to cyber threats, which is also relevant for partner states [12].

Thus, the theoretical foundations of countering financial cybercrime are formed at the intersection of law, criminology, and information technology. Their development is driven by the

need to respond to global digital challenges, which requires constant updating of doctrinal approaches, legal instruments, and models of international cooperation.

4. Standards of Pre-Trial Investigation of Financial Cybercrimes

The pre-trial investigation of financial cybercrimes constitutes a specific type of criminal procedural activity carried out in the context of the digital transformation of social and economic relations. Its distinctive nature is determined by the intangible character of the object of encroachment, the use of complex information systems, and the high level of latency inherent in such offences. Scholars rightly emphasize that traditional approaches to the investigation of economic crimes are insufficient to effectively counter financial cyber threats, which necessitates the development of specialized standards for pre-trial investigation [2].

In doctrinal terms, standards of pre-trial investigation encompass a system of normatively закріплені (normatively established) and practice-derived requirements aimed at ensuring the legality, effectiveness, and predictability of criminal proceedings. In cases involving financial cybercrimes, these standards are of a comprehensive nature, as they combine procedural rules with technical and forensic elements. It is precisely this integration that enables an adequate response to the specific features of digital financial offences [10].

One of the fundamental standards of pre-trial investigation of financial cybercrimes is the principle of promptness, which acquires particular significance given the rapid pace of digital processes. Electronic traces of crime may be destroyed or relocated within minutes, while financial assets may be transferred across multiple jurisdictions. In this regard, both academic discourse and regulatory doctrine stress the necessity of immediate responses by law enforcement authorities to cyber incidents [3].

At the same time, the standard of promptness cannot be implemented to the detriment of the principle of legality. The collection of digital evidence in the course of pre-trial investigation must be carried out in compliance with procedural safeguards, particularly those relating to the protection of the right to privacy, banking secrecy, and commercial confidentiality. Failure to comply with established procedures may call into question the admissibility of evidence and, consequently, the effectiveness of the entire criminal proceeding.

A special place among the standards of pre-trial investigation is occupied by ensuring the integrity of digital evidence. Unlike physical objects, electronic data can be easily altered or copied without leaving visible traces of interference. This necessitates the application of specialized forensic procedures for the fixation, copying, and storage of information.

Closely linked to the principle of integrity is the standard of documenting the chain of custody of digital evidence. This standard requires the recording of every operation involving electronic data, from the moment of its seizure to its use in judicial proceedings. Such an approach ensures the verifiability of evidence and minimizes the risk of its discreditation by the defense [10].

An important standard of pre-trial investigation of financial cybercrimes is the functional and professional specialization of the subjects of criminal proceedings. The complexity of the technical and financial aspects of such crimes requires the involvement of specialists possessing interdisciplinary knowledge in the fields of law, information technology, and finance [11].

A significant role in pre-trial investigation is played by cooperation between law enforcement authorities and financial institutions as well as providers of digital services. These entities possess information of crucial importance for establishing the circumstances of the crime, including data on financial transactions, technical access logs, and metadata [3].

One of the specific standards of pre-trial investigation of financial cybercrimes is the application of provisional measures aimed at preserving electronic data. The Budapest Convention provides for the possibility of the expedited preservation of computer data as a preventive procedural instrument designed to prevent the loss of evidence.

An important element of pre-trial investigation standards is the financial-analytical component, which consists in tracing the movement of funds, identifying their sources, and

determining the ultimate beneficial owners. Such analysis requires the combination of criminal procedural instruments with methods of financial monitoring and transaction analysis.

A particular challenge in pre-trial investigation lies in proving the subjective element of financial cybercrimes. The automated nature of many digital processes complicates the establishment of the intent of a specific individual, necessitating an in-depth analysis of digital traces, system logs, and behavioral patterns of suspects.

An essential standard of pre-trial investigation is the observance of a balance between the effectiveness of criminal prosecution and the protection of human rights. Excessive or uncontrolled interference in the digital sphere may lead to violations of fundamental rights, which negatively affects the legitimacy of investigation outcomes [10].

Given the transnational nature of financial cybercrimes, standards of pre-trial investigation must include effective mechanisms of international legal assistance. The collection of evidence beyond national jurisdiction requires coordinated procedural actions and a high level of trust between competent authorities of different states.

Doctrine rightly points out that the fragmentation of national standards for the pre-trial investigation of financial cybercrimes adversely affects the effectiveness of international cooperation. Divergent approaches to the admissibility of digital evidence and the procedures for its collection give rise to legal conflicts and reduce the efficiency of transnational investigations [2].

Thus, standards of pre-trial investigation of financial cybercrimes should be formed as a coherent system of principles and procedures that combine legality, promptness, technical competence, and international coherence. Their further development constitutes a key prerequisite for the effective counteraction to financial cyber threats in the contemporary digital environment.

5. Digital Forensics Tools and International Coordination

In contemporary criminal proceedings concerning financial cybercrimes, digital forensics functions not merely as a technical instrument but as an integral component of the evidentiary framework. It encompasses a complex set of procedures for the collection, analysis, interpretation, and preservation of electronic information that may be used as evidence in court. Digital traces are predominantly volatile in nature and subject to rapid modification, which necessitates the use of tools capable of ensuring their authenticity and legal admissibility.

Among modern digital forensics tools, automated software for data acquisition from complex digital environments plays a particularly important role, including hard drives, mobile devices, virtual machines, and cloud services. Such tools enable preliminary analysis, artifact identification, and event reconstruction based on digital traces, which is crucial for uncovering technologically sophisticated financial cybercrimes [13].

Another significant aspect of digital forensics involves tools for network traffic analysis and packet reconstruction, which make it possible to detect traces of unauthorized access or transactions linked to fraudulent activities. Without such instruments, a detailed analysis of digital evidence may be substantially hindered, as a considerable portion of cyberattacks or criminal conduct occurs at the level of data exchange within networks.

Particular attention must be paid to chain-of-custody management tools, which ensure the documentation of every operation involving digital data—from the moment of seizure to its use in judicial proceedings—and help prevent disputes regarding authenticity and integrity. This is critically important in contexts where data sources may be distributed across multiple devices and geographic jurisdictions.

An important category of digital forensics tools includes means for recovering deleted or concealed data from storage media. These tools allow investigators to identify traces of criminal activity that have been deliberately masked or erased, which is especially relevant in investigations of complex financial cybercrimes where offenders employ “anti-forensic” techniques [13].

Despite advances in technical tools, a decisive factor in the effectiveness of digital forensics remains the capacity of law enforcement authorities to apply them correctly. This requires a high

level of qualification, specialized training, and interdisciplinary competence combining legal knowledge, IT security expertise, and forensic skills—an aspect that becomes particularly critical in investigations of financial cybercrimes.

The transition to international coordination is today an indispensable condition for effective counteraction to financial cybercrimes, as digital traces are often physically located in multiple jurisdictions, while legal boundaries between states may differ significantly. This complicates not only technical analysis but also the legal procedures that ensure the admissibility of evidence in each jurisdiction where judicial proceedings may take place.

One of the primary international coordination instruments remains the Budapest Convention on Cybercrime, which establishes standardized mechanisms for evidence exchange, cooperation between competent authorities in cybercrime investigations, and expedited procedures for information sharing in transnational cases [Budapest Convention on Cybercrime, Arts. 24–25]. The Convention also provides standard procedural tools, including 24/7 contact networks for urgent requests concerning electronic evidence, ensuring prompt interaction between law enforcement agencies in different states to prevent the loss of critical digital data [14].

It is important to note that international coordination mechanisms extend beyond the traditional MLAT (Mutual Legal Assistance Treaty) framework, as MLAT procedures often involve lengthy processing times that are incompatible with the volatile nature of digital evidence in cyberspace. Consequently, modern international instruments provide for more expedited procedures, including European mechanisms such as the European Production Order and the European Preservation Order [15].

A further recent development is the adoption of the United Nations Convention against Cybercrime by the UN General Assembly in December 2024, aimed at harmonizing the criminalization of cybercrimes and expanding international cooperation, including evidence exchange and mechanisms for transnational investigations [3].

Effective international coordination also requires standardized data preservation procedures that help overcome time constraints associated with data deletion or interference, particularly when information is stored on servers located in third countries, necessitating accelerated legal interaction.

Scholarly literature emphasizes that one of the key challenges in international coordination lies in differences among national standards concerning admissibility and evidence-sharing procedures. The lack of harmonization may lead to the rejection of crucial digital evidence in the requesting state, even when such evidence is substantively significant for the investigation [16]. Therefore, international instruments are aimed not only at creating expedited procedures but also at qualifying and standardizing digital forensic methods to ensure evidence admissibility across different legal systems.

Notably, issues related to coordination and access to digital evidence are not limited to technical aspects; they also encompass human rights considerations, privacy protection, and differing approaches to balancing security and individual freedoms, which further complicate international cooperation. Successful international coordination also presupposes the establishment of joint information-sharing centers and analytical platforms that enable law enforcement authorities to access digital evidence without resorting to lengthy MLAT procedures, thereby accelerating investigations. Effective coordination further includes joint training programs, expert knowledge exchange, and the development of cooperation models between public and private sectors, contributing to enhanced professional capacity in digital forensics [16].

Regional initiatives, such as EU e-evidence programs, play a significant role in international coordination by establishing unified legal mechanisms for rapid access to electronic evidence across the EU, with subsequent use in financial cybercrime investigations [E-evidence cross-border access to electronic evidence]. However, practice demonstrates that the effective functioning of such mechanisms requires continuous upgrading of technical tools as well as normative adaptation to emerging forms of digital threats, including the use of cryptographic technologies, decentralized systems, and artificial intelligence.

In conclusion, the synergy between technical digital forensics tools and international cooperation mechanisms constitutes an indispensable prerequisite for the effective investigation of financial cybercrimes, as only such an integrated approach can ensure promptness, legality, effectiveness, and a comprehensive evidentiary strategy within the global cyber environment.

6. Conclusion

Financial cybercrimes represent a qualitatively new form of criminal conduct combining features of economic crime and high-technology offences, characterized by transnationality, dynamism, and heightened latency. It has been established that effective counteraction to such crimes is impossible within traditional criminal-law and procedural models, as these do not fully account for the specific nature of digital evidence, the rapidity of electronic financial transactions, and the use of decentralized information environments. This necessitates the development of a comprehensive doctrinal framework for combating financial cybercrimes, integrating substantive and procedural law, digital forensics principles, and standards of international cooperation.

Standards of pre-trial investigation of financial cybercrimes must be based on specialized procedural approaches to the collection, fixation, preservation, and analysis of electronic evidence, in compliance with the principles of legality, proportionality, and human rights protection. A decisive factor is the implementation of unified forensic standards ensuring the integrity and authenticity of digital information, as well as its admissibility in judicial proceedings. It is substantiated that the integration of digital forensics tools into pre-trial investigation practice requires not only technical capacity but also an appropriate level of professional training for investigators, prosecutors, and experts capable of operating within complex digital environments.

International coordination constitutes a system-forming element of effective counteraction to financial cybercrimes, as it enables the overcoming of jurisdictional limitations and ensures timely access to electronic evidence located beyond national territory. It is established that the combination of formalized mechanisms of international legal assistance with informal channels of operational interaction and public–private partnerships creates conditions for enhancing the effectiveness of criminal investigations in the digital sphere. Ultimately, it is argued that only the synergy of legal, forensic, and international coordination instruments can provide a systematic and sustainable model for combating financial cybercrimes in the contemporary context of global digitalization.

7. References

[1] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity Press, 2007. Electronic resource. Accessed via: https://politybooks.com/bookdetail/?isbn=9780745630780

[2] J. Clough, *Principles of Cybercrime*, Cambridge: Cambridge University Press, 2015. Electronic resource. Accessed via: https://www.cambridge.org/core/books/principles-of-cybercrime/6C6A1C6A6C4A52F5F8C3C7A4F1E9B1E7

[3] Convention on Cybercrime (ETS No. 185), Council of Europe, Budapest, 2001. Electronic resource. Accessed via: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[4] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, Santa Barbara: Praeger, 2010. Electronic resource. Accessed via: https://www.bloomsbury.com/us/cybercrime-9780313383812/

[5] Financial Action Task Force, *Risk-Based Approach Guidance for the Banking Sector*, Paris: FATF/OECD, 2014. Electronic resource. Accessed via: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html

[6] D. W. Arner, J. N. Barberis, and R. P. Buckley, "FinTech and the Future of Finance," *Northwestern Journal of International Law & Business*, vol. 37, no. 3, pp. 373–410, 2017. Electronic resource. Accessed via: https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2

[7] European Central Bank, *Cyber Resilience Oversight Expectations for Financial Market Infrastructures*, Frankfurt am Main: ECB, 2018. Electronic resource. Accessed via: https://www.ecb.europa.eu/paym/cons/pdf/cons201807_cyber_resilience_expectations.en.pdf

[8] M. Yar, *Cybercrime and Society*, 2nd ed., London: SAGE Publications, 2013. Electronic resource. Accessed via: https://uk.sagepub.com/en-gb/eur/cybercrime-and-society/book235371

[9] M. Levi and R. G. Smith, *Fraud Vulnerabilities and the Global Financial Crisis*, Canberra: Australian Institute of Criminology, 2011. Electronic resource. Accessed via: https://www.aic.gov.au/publications/tandi/tandi422

[10] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed., Amsterdam: Academic Press, 2011. Electronic resource. Accessed via: https://www.sciencedirect.com/book/9780123742681/digital-evidence-and-computer-crime

[11] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*, Luxembourg: Publications Office of the European Union, 2023. Electronic resource. Accessed via: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

[12] P. Craig and G. de Búrca, *EU Law: Text, Cases, and Materials*, 7th ed., Oxford: Oxford University Press, 2020. Electronic resource. Accessed via: https://global.oup.com/academic/product/eu-law-9780198856641

[13] *Problems Related to the Collection of Digital Evidence and the Role of International Cooperation in Overcoming Them*, *International Journal of Artificial Intelligence*, vol. 5, no. 10, pp. 1586–1598, 2025. Electronic resource. Accessed via: https://www.academicpublishers.org/journals/index.php/ijai/article/view/7181

[14] Council of Europe, *Convention on Cybercrime (Budapest Convention), Articles 24–25*, 2001. Electronic resource. Accessed via: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[15] European Commission, *E-evidence — Cross-Border Access to Electronic Evidence*, Brussels, 2023. Electronic resource. Accessed via: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

[16] *SoK: Cross-Border Criminal Investigations and Digital Evidence*, *Journal of Cybersecurity*, vol. 8, no. 1, article tyac014, 2023. Electronic resource. Accessed via: https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060