LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S4(2025)

INVESTIGATING CYBERCRIMES COMMITTED IN THE FINANCIAL SECTOR: PROCEDURAL STANDARDS, DIGITAL FORENSICS AND INTERNATIONAL COOPERATION

Iryna Dubivka[1], Petro Rekotov[2], Viacheslav Kuliush[3],Dina Rusanivska[4], Larysa Basiuk[5]

[1]Candidate of legal sciences, Associate of professor, Associate professor of the Department of Criminal procedure at National Academy of Internal Affairs (Ukraine); ORCID: 0000-0002-7189-3630
[2]Candidateoflaw, AssociateProfessor, Associate Professor of the Department of Information Economics, Entrepreneurship and Finance (Ukraine); ORCID: 0000-0002-0378-378X
[3]Doctor of Philosophy in Law, Head of the Cybercrime Countermeasures Department in the city of Kyiv Cyber Police Department of the National Police of Ukraine(Ukraine); ORCID: 0009-0007-2131-1413
[4]Doctor of philosophy, lecturer of the Department of criminalistics end forensic medicine at National Academy of Internal Affairs, (Ukraine) ORCID: 0009-0001-7244-1417
[5]Doctor of philosophy, lecturer of the Department of criminalistics end forensic medicine at National Academy of Internal Affairs , (Ukraine); ORCID: 0009-0007-3129-0564

irinadubivka@ukr.net[1]
pvrekotov@gmail.com[2]
Kyliuws@gmail.com[3]
rysanivskad@ukr.net[4]
lara_basiuk@ukr.net[5]

Abstract
The article proposes an integrated model for investigating cybercrimes in the financial sector, which provides procedural standards for the admissibility of electronic evidence, a digital forensics methodology, and tools for international interaction with banks, payment providers, and VASPs. Against the backdrop of the rapid digitalization of financial services and the emergence of cryptoassets, key challenges are identified: cross-border, anonymization, jurisdictional fragmentation, encryption, and volatility of payment and operational logs. The developed matrix «stage - procedural tool - financial action - risk of inadmissibility» formalizes the SOP procedures for collecting, storing, verifying, and transferring e-evidence, including hash identifiers, audit logs, and blockchain trace artifacts. It is shown how the principles of proportionality and minimization of intervention balance the needs of criminal prosecution with human rights guarantees and banking secrecy in transnational inquiries. Special attention is paid to public-private interaction and accelerated channels of data storage/access, which increase the chances of prompt asset freezing and evidentiary stability in court. The proposed practical protocols reduce response time, reduce the risks of challenging the methods and contribute to the approximation of national practice to international standards of cooperation in financial investigations. The results are useful for investigators, expert institutions and courts working with evidence of the movement of funds and crypto-assets in many jurisdictional proceedings.

Keywords: cybercrime, financial sphere, economy, procedural standards, investigation, evidence, digital forensics, electronic evidence, international cooperation.

Introduction

The world is constantly evolving, new scientific discoveries are taking place, digitalization processes are accelerating, modern digital technologies are being created, which are being integrated into the economy, public administration and private life on a large scale (Sysolyatin, 2024, p. 24). Against this background, cybercrimes are becoming increasingly widespread and complex, and in the financial sector they manifest themselves as unauthorized transfers, phishing and Business Email Compromise schemes, compromise of payment instruments, fraud with customer accounts, hacking of information systems of financial institutions, distribution of malicious software to steal credentials and other actions in cyberspace (Larchenko, 2024, p. 71).

The rapid digitalization of social relations and financial services has led to a qualitative transformation of criminal practices: cybercrime has acquired a cross-border nature, relies on distributed infrastructures, cloud storage and payment providers, which complicates jurisdictional

determination, attribution and proof of the origin of assets. The development of electronic financial services, remote identification, next-generation payment instruments and crypto-assets has exacerbated the institutional asymmetry between the pace of innovation and the capacity of state institutions to ensure proper control, as a result of which criminal initiative often outpaces law enforcement response mechanisms. Under such conditions, digital reporting systems and financial data buses become subject to manipulation, forgery and technical interference, and trace information on the movement of funds is distributed across jurisdictions and services.

The effectiveness of financial investigations depends on the ability to integrate procedural standards of admissibility and compliance of digital evidence with digital forensics methodology, which guarantees the authenticity, integrity and reliability of results, as well as with effective international cooperation mechanisms for timely access to relevant banking, payment and blockchain data. The triangle "procedural guarantees – technical verification – cross-border procedures" forms a research framework and practical guidelines for pre-trial investigation bodies and the court, including operational freezing of assets and synchronization of actions with financial intelligence.

The relevance of the topic is enhanced by the heterogeneity of legal regimes for processing financial and personal data and the asymmetry of procedural powers between jurisdictions, which creates risks of inadmissibility of e-evidence due to violations of the principles of proportionality and minimization of interference, gaps in the chain of custody or defects in the documentation of technical operations. Additional technical challenges – encryption, anti-forensics, volatility of operational and payment logs – require coordination of tactical decisions with the requirements of the criminal process and transparent reflection in the conclusions of experts and specialists, in particular regarding the reproducibility of blockchain tracing and verification of access logs to payment systems. Therefore, the complementarity of legal and technical standards becomes a necessary condition for evidentiary capacity in cases of crimes against financial security.

The scientific novelty of the study lies in the proposed integrated model of investigation of cybercrimes in the financial sector, which combines the stage methodology of digital forensics (identification of sources, collection, storage, analysis, interpretation) with procedural standards of admissibility and unified channels of international interaction with banks, payment providers and VASP (Virtual Asset Service Provider). The model formalizes the correspondence matrix «stage – procedural instrument – financial action – risk of inadmissibility» and offers SOP (Standard Operating Procedures) solutions for interaction with providers and MLAT (Mutual Legal Assistance Treaty)/e Evidence requests, checklists for storage and transfer of e-evidence, validation of hash identifiers, audit logs and transaction analysis artifacts. This ensures the replicability of the results and competitive verifiability in court in cases involving the movement of funds and crypto assets.

The practical significance of the research is reflected in standardized procedures for pre-trial investigation bodies and forensic institutions: from the choice between static and live receipt of payment and telemetry data to determining the cross-border access channel, taking into account the urgency, type of data, confidentiality requirements and risk of leakage. The proposed protocols increase the likelihood of achieving admissible e-evidence, reduce response time, reduce the risks of challenging the methods and contribute to the harmonization of national practice with international standards of cooperation in financial investigations.

The aim of the article is to develop and substantiate an integrated model for investigating cybercrimes committed in the financial sector, which: systematizes procedural standards for the admissibility of electronic evidence (authenticity, integrity, reliability, proportionality and minimization of interference); determines the links with the methodology of digital forensics (stages, tools, standard operating procedure and chain of custody); outlines risk-based algorithms for international interaction with financial institutions and providers for fast and legally correct transnational access to e-evidence; provides for the development of practical recommendations for documenting, verifying, submitting and checking digital evidence in cases of financial offenses.

1. General characteristics of cybercrimes in the financial sector and the problems of their investigation

It should be noted that the Criminal Code of Ukraine contains a number of articles aimed at combating cybercrimes, in particular: Articles 361, 361[1], 362 etc. (Criminal Code of Ukraine, 2002), which in financial proceedings are often combined with the norms on money laundering and tax offenses, which complicates the qualification and proof of intent. The combination of these and related components forms the basis of criminal law regulation of cybercrime, however, their practical application faces evidentiary and jurisdictional barriers in the context of cross-border financial transactions.

In addition, in the system of criminal proceedings regarding the legalization of proceeds from crime (Article 209 «Legalization (laundering) of property obtained by crime» of the Criminal Code of Ukraine), or «Evasion of taxes, fees (mandatory payments)» (Article 212 of the Criminal Code of Ukraine), the emergence of crypto-assets has significantly transformed both the nature of criminal behavior and the mechanisms of its procedural detection and proof.

The investigation of cybercrime in the financial sector is characterized by specific obstacles: identification of the perpetrator is complicated by VPN, anonymizers and encryption; collection and storage of electronic evidence requires reliable tools and procedures, otherwise the data may be changed or lost; the cross-border nature of the breed provides jurisdictional uncertainty; Interaction with private companies often occurs through formal waivers or MLAT requirements; complex operational and investigative activities covert investigative (detective) actions require scarce professional competencies (Zhovtan, 2025). These are only some of the priority issues that ensure effective protection against financial cybercrime.

Despite the technical nature of the attacks, specialized examinations remain mandatory, primarily computer-technical ones, but the staff shortage and the long terms of their substantive content slow down the pre-trial investigation. Difficulties in proving the subjective side and installing the perpetrator lead to unfinished proceedings or acquittals, which violates the rights of victims and stimulates the repetition of offenses (Zhovtan, 2025). Among the key characteristics of cybercrimes, it is worth noting the anonymity of subjects, cross-border nature, technological complexity and high dynamics, which enhances the circumvention of crypto-assets and traffic concealment services (Chawki, 2010; Jahankhani et al., 2014; Larchenko, 2024, p. 71; Kolosovsky, 2023, p. 45). The proliferation of Tor, specialized anonymizers, and cryptocurrencies makes it difficult to trace funds and communications (Europol & Eurojust, 2024, p. 8; Velasco, 2025).

The global nature of cyberspace makes transborder attacks possible and requires mechanisms for international legal assistance, the expansion of legal barriers, and the development of common intelligence-sharing platforms (Europol & Eurojust, 2024, p. 15; UNODC, 2024; Jahankhani et al., 2014). The experience of successful operations confirms the importance of unified standards and coordination (Velasco, 2025; Chawki, 2010).

Criminals use tools that are ahead of the capabilities of investigators and experts, using digital forensics, specialized techniques and big data processing (Europol & Eurojust, 2024, p. 10; Legan, 2019, p. 124; Common Challenges in Cybercrime, 2024; World Economic Forum, 2024). The high speed of the spread of attacks requires urgent response, monitoring and innovative solutions, as well as the integration of international experience and multidisciplinary practices (Europol & Eurojust, 2024, p. 7).

A key problem is the collection and procedural use of digital evidence in financial cases, where its receipt, fixation, processing and attachment are accompanied by legal and technical difficulties that directly affect the effectiveness of the pre-trial investigation. The lack of a clearly regulated procedure for working with e-evidence in the Criminal procedure codeof Ukraine creates uncertainty about the admissibility criteria; The technical nature of data (logs, metadata, IP addresses, transaction history) places increased demands on authentication, preservation, and

integrity verification, which requires harmonization of procedural and cross-sectoral norms.
The issue of authenticity and immutability of digital data is particularly acute in decentralized or volatile environments; blockchain simultaneously guarantees the immutability of records and requires specialized knowledge for the correct interpretation, validation, and linking of transactions to specific individuals. For proper judicial use, each piece of evidence must have a reliable source, transparent verification, and technical expertise that ensures reproducibility.
The intersection of the technical and legal planes reveals gaps in the classic institutions of search, seizure, and temporary access when working with online wallets, smart contracts, and intangible assets, which requires the formation of procedural tools for «digital investigative intervention» with clear grounds, guarantees, and liability. This should standardize the algorithms for accessing, fixing, verifying the integrity and presenting e-evidence in compliance with human rights and the principle of proportionality.
Staff shortages and the need for interdisciplinary expertise (digital forensics, cryptoeconomics) increase the risks of errors and data loss; the lack of unified storage and transmission standards (hash identifiers, copying procedures, technical report structure) leads to the loss of evidentiary value due to logging defects. It is possible to update procedural regulations to prevent hot-headed interference in the private sphere during digital investigative actions and increase the predictability of the judicial assessment of e-evidence.
In general, the collection and inclusion of digital evidence in financial cyber cases is a multi-level problem associated with legal gaps, technological complexity, limitations in international data availability and staffing incapacity; coordinated legislative, institutional and methodological responses are needed. Relevant benchmarks include a comprehensive regulatory framework for digital forensics, specialized investigative teams, the integration of IT experts and blockchain analysts into the legal process, and stable channels of legal exchange with international platforms and providers.
The literature review highlights innovative approaches: the use of artificial intelligence and ML to automate big data analysis and anomaly detection (Larchenko, 2024, p. 72); the application of digital forensics to collect, store, analyze, and present e-evidence, exclusively with mobile devices (Kolosovsky, 2023, pp. 46–47; Gutnyk, 2022, pp. 47–48); the development of human resource agility and continuous learning; the unification of international standards and the harmonization of legislation for national cooperation and evidence exchange (Voytsikhovsky, 2011, p. 25; Legan, 2019, p. 124). Such integration of technologies, human capital, and international mechanisms increases the speed and quality of financial cybercrime investigations.
In our opinion, to increase the effectiveness of countering cybercrime, comprehensive measures are advisable: systematic training of investigators in the technical aspects of financial encroachments; creation of forensic centers of digital expertise for the operational accumulation and analysis of data; expansion of international cooperation with the involvement of tools and capabilities of Europol, Interpol and other organizations for the exchange of information, search and extradition of persons involved. This is consistent with the risk-oriented approach of the article and ensures the practical implementation of the proposed model in the financial segment.
If additional stylistic or terminological adjustments are required to meet the requirements of a specific publication (for example, replacing «digital evidence» with «electronic evidence» throughout the text), edits can be made without changing the sizes and their references.

2. Procedural standards for investigating cybercrimes in the financial sector

The emergence of a digital evidence base in criminal proceedings places increased demands on procedural standards that ensure the legitimacy of collection, relevance, admissibility, and persuasiveness of electronic evidence in criminal proceedings. The key parameters are authenticity (identity of source and author), integrity (consistency of content from the moment of recording), reliability (reproducibility and technical correctness of the procedure), as well as compliance with

the principles of proportionality and minimization of interference with privacy when accessing data and its further processing (Gutnyk, 2022, pp. 47–49).

In terms of regulatory principles, electronic evidence occupies a special niche in the system of sources of evidence: it covers data that are created, stored and transmitted in electronic form, including files, event logs, network metadata, copies of information arrays, content from messaging services and web resources. Legislative approaches recognize that the electronic form is not an independent basis for approving admissibility, while the assessment focuses on the procedural legality of ensuring and observing technical guarantees of immutability (Marchuk, 2025, pp. 2–3). At the same time, the doctrine insists on a clear distinction between electronic evidence as information and material carrier(s), with an emphasis on autonomous verification of metadata, hash identifiers and access protocols (Koval, 2023, pp. 118–120; LNU, 2023, pp. 15–18).

The principle of proportionality in the context of digital interference requires that the scope of access to information does not exceed the investigative purpose, and sensitive categories of data (personal, communication, localization) are processed using the least invasive model (targeted extraction, search filters, segmentation by time frame). The principle of minimization includes data scope limitation, «sanitization» of copies, pseudonymization, as well as technical means to prevent reduced copying (selective imaging) while maintaining evidentiary potential (Marchuk, 2025, pp. 3–4).

The procedural block of the practice of working at the scene in a digital environment covers a hybrid «survey» of the physical space (servers, workstations, mobile devices, etc.) and a logical «survey» of the environment (virtual machines, cloud storage, accounts), where the primary actions are aimed at stabilizing the situation and preventing the loss of data volumes. Given the risk of variability of digital artifacts, checking the negative documentation of the system state, time, network configuration, active processes and open sessions, with fixing the tools, versions and parameters of their application.

The tools for temporary access/extraction of electronic media and data should ensure legal access based on appropriate procedural decisions and correct technical implementation: use of a write blocker, full or selective creation of forensic images, fixing hash identifiers, isolation of media from the network and power. In the case of data extraction from cloud services, procedural recording of the legal mechanism of creation is important (Universum, 2021, pp. 69–71).

Recording of technical operations in procedural documents should include a description of the sequence of actions, tools and settings, scope and selection criteria, checksums, media identifiers, access characteristics, names of responsible persons and specialists, as well as illustrative materials (screenshots, logs, visualizations of timelines). Such detailing reduces the risk of doubts about the origin, integrity and replicability of the obtained electronic evidence in subsequent judicial review (Gutnyk, 2022, pp. 95–98).

Typical grounds for declaring digital evidence inadmissible include: receipt without proper legal basis or in violation of the permission limit; logging defects; inability to confirm authenticity and integrity (missing hashes, different checksums, undocumented changes); the use of tools that have not been validated or do not ensure reproducibility; and the non-compliance of the collection method with the principles of proportionality and minimization of interference. It is worth emphasizing that, according to case law, the electronic form is not a basis for refusal in itself, but procedural and technical defects themselves lead to the exclusion of relevant factual data from the evidence system in criminal proceedings.

In summary, we note that procedural standards in the digital sphere must integrate legal requirements with the technical discipline of digital forensics. Only a combination of legality of access, strict adherence to the chain of custody, transparent methodology and proportionality of interference forms the evidentiary base, ensures adversarial and fair trial, including in relation to cybercrimes in the financial sphere.

3. Digital forensics tools for investigating cybercrimes in the financial sector

Digital forensics – an interdisciplinary field at the intersection of criminal process, forensics and information security – provides scientifically sound approaches to the detection, collection, preservation, analysis and presentation of electronic evidence with a focus on the authenticity, integrity and reproducibility of procedures that are critically damaged for payment journals, bank data and blockchain artifacts. (Kolosovsky, 2023, pp. 45–47). The core methodology is a guarantee of replicability of conclusions through standardized protocols, detailed documentation of technical actions and the possibility of independent verification by the other party to the proceedings.

The stages of a digital investigation form an orderly action plan that ensures the procedural security of the results in court; at the stage of identification of sources in financial matters, automated banking systems, payment gateways, processing logs, PSP, VASP and exchange data, as well as crypto wallets and smart contracts are mainly used. Primary fixation of the description of the state of systems and services without including in their work: active processes, network connections, banking/exchange access sessions, screenshots of transaction screens and time zone parameters for a correct timeline.

Data storage is created either as a complete «bit-by-bit» snapshot, or as a live capture – the latter is especially justified for temporary access keys, session tokens, volatile logs of payment services and RAM, where key encryption may be contained. Integrity is ensured at all stages of control: hash calculation, time recording, access and action accounting, documentation of each copy or data transformation in the chain of custody matrix.

Maintaining the chain of custody should include identifiers of carriers and sources (account IDs, wallet addresses, bank case numbers), checksums, marks of relevant persons and the method of transmission (including secure channels and ptosignatures). Any discrepancy in logs or checksums can cast doubt on the suitability of evidence, especially when it comes to the origin of funds and the tracing of transactions in the blockchain.

The analytical phase includes building timelines and correlating events from various sources: system and network logs, bank logs, payment processor data, AML flags, blockchain explorers and analytical platforms for address clustering. Particular attention is paid to the correspondence of timestamps, time zones and logical constitution of events, as well as the separation of content and metadata for autonomous verification of each layer.

The tools and applications used are described in the report with the names, versions and settings: tools for visualization and parsing of logs, hashing, mobile and cloud data analysis, as well as specialized utilities for blockchain tracing and artifact extraction from payment SDKs. Reliability is achieved through repeated testing, cross-validation using a free and fixed methodology, which allows independent verification of conclusions in court.

Typical technical challenges in financial cyber cases: full-disk encryption and secure application vaults; anti-forensics (deletion/forgery of logs, changing timestamps, steganography of payment artifacts in media files); distributed and cloud-based sources. Effective tactics include live dumps of RAM to intercept keys, correlation of independent logs, detection of inconsistencies in time series, and restoration of artifacts from backup channels (push notifications, SMS OTP logs, web caches).

For cloud services and financial data providers, it is critical to prove the origin: attribute the account/client ID, record the parameters of the formation of the relevant providers, the type and completeness of the exported fields, time stamps and time zone, the signature mechanism/time stamps, the chain of transmission to the investigation. These are requirements for procedural documentation, including a description of the legal request, the method of provider authentication and verification of digital signatures.

The expert's conclusion must reportably reproduce the process: conditions, software and settings, checks and tests, checksums, alternative hypotheses and their simplifications, as well as limitations of the method with an explanation of the impact on the results. Typical errors – live fixations, gaps in logs, loss of control over hashes, use of invalidated tools – can be avoided by standards, training

and internal quality audit, which minimizes the risks of rejection of e-evidence in court.
If necessary, the terms («forensic image/snapshot», «electronic/digital evidence», «payment provider/PSP», «virtual asset service provider/VASP») can be unified without changing the size and reference grid.

4. International cooperation and transnational access to e-evidence in the investigation of cybercrimes in the financial sector

Investigating financial cybercrimes requires close cooperation between government agencies and the private sector, including banks, payment providers, processing centers, exchanges, and virtual asset custodian services. Public-private partnerships combine resources, indicators of compromise, and transaction analytics to quickly detect money laundering, phishing, and BEC chains, as well as to quickly freeze assets (Zhovtan, 2025).
The international dimension of financial cybercrime requires constant interstate coordination, although the place of commission, the victim, the infrastructure, and critical financial data are often located in different jurisdictions. This includes the exchange of electronic evidence, synchronization of procedural actions, and requires access to fast channels and storage of payment and blockchain artifacts.
The basic European instrument being reduced remains the Convention on Cybercrime with procedural mechanisms for the interaction of e-evidence and channels, and additional protocols aimed at accelerating access to data from providers and conflicts of jurisdiction (Wojcihowski, 2011, pp. 22–25). For financial cases, this means reducing to obtaining account metadata, login logs and basic transaction identifiers while maintaining confidentiality guarantees.
Institutionally coordinates a network of law enforcement and judicial cooperation: Interpol, Europol (EC3, J CAT), Eurojust, as well as expert forums and analytical platforms for shared use. They accelerate attribution, joint planning of seizures and confiscations of assets, and parallel follow-up actions on accounts and crypto wallets (Lehan, 2019, pp. 118–120).
Practice shows that consolidated multi-jurisdictional «takedown» operations are effective due to simultaneous searches, seizures and confiscations in many countries, which minimizes the risk of data loss and withdrawal of funds; such packages are built on pre-agreed evidence and mutual legal assistance (Gutsayuk, 2021, pp. 31–33). For financial proceedings, a component of rapid «freezing» and notification to providers about the preservation of logs and funds is added.
Transnational access channels for e-evidence in financial cases include: classic MLA/MLAT; direct requests to providers, where permitted; simplified procedures for urgent data preservation. The choice of tool depends on the strings, data categories (content/metadata/transaction logs), standards of necessity and proportionality, and bank secrecy requirements (Saenko, 2021, pp. 372–375).
Jurisdictional challenges arise from the distributed nature of cloud data centers and multi-homing of payment platforms; criteria for «effective control» over data, determination of the “location” of e-evidence, and rules for extraterritorial access with appropriate human rights safeguards are required.
Personal and financial data protection standards require proportionality, minimization of collection, clear justification of the volume, timeframe, and categories of data, as well as transparent auditing of cross-border transfers (Hrebenyuk, 2021, pp. 17–19).
Operational interaction with information and financial service providers relies on unified electronic request formats, clear account/resource identifiers (IBAN, PAN, client ID, wallet addresses, TXID), and proper substantiation of procedural grounds. Continuous verification of the chain of custody is critical: from the provider’s response to integration into the proceedings – with checksums, access logs, and timestamping of data (Saenko, 2021, pp. 375–378).
Bottlenecks of international cooperation include unequal criminalization, diversity standards, differences in SLA responses, and limited channels for urgent «freezing». To minimize them, interstate agreements, bilateral guidelines for requests, and 24/7 contact points are used (Vojtsikhovsky, 2011, pp. 26–28).

To increase the efficiency of access to financial data, it is advisable to use risk-based tool selection matrices: for emergency storage – accelerated procedures; for content – formalized MLA with extended justification; for metadata and transaction logs – simplified forms through authorized persons and a minimum confirmation package. In addition, it is worth providing mechanisms for rapid notification of banks/PSPs/VASPs about blocking assets and preserving logs until court decisions are received. Public-private partnership platforms centralize indicators of compromise, accelerate attribution and identification of infrastructure, and introduce protocols for marking and confirming the integrity of source evidence (Lehan, 2019, pp. 123–125). For financial keys, these are also risk address directories, lists of blocked tokens, and provider directories for prompt verification of the data source.

The generalizing, optimal structure of international cooperation in financial cyber cases includes a multi-level contractual network, institutional mechanisms for rapid coordination, a differentiated choice of procedural instruments depending on the risk and guarantees of privacy and banking secrecy. Such a system provides safe, legitimate and evidentially stable transnational access to electronic evidence that requires constant judicial verification.

Conclusions

As a result of the conducted research, it should be stated that the investigation of cybercrimes in the financial sector creates a complex problem with the interweaving of procedural, legal, technical and international legal dimensions, where the speed of access to payment logs, bank records and blockchain artifacts is crucial. Financial cybercrime is characterized by anonymity of subjects, cross-border activity, high dynamics of technologies and stability of evidence fixation, which determines the need for an integrated approach to their separation, taking into account banking secrecy and data protection standards. The relevance and admissibility of digital evidence directly depend on the support of procedural guarantees and digital forensics methodology, which ensure the authenticity and integrity of information, in particular when working with transactional data and crypto assets.

An effective scheme for countering cyberlegalization requires the use of digital forensics tools, unification of regulation of virtual asset circulation and increasing the role of public-private interaction with banks, PSPs and VASPs, as well as intensification of cooperation with Europol, Interpol and Egmont Group. It is possible to create specialized analytical units at the intersection of IT, financial monitoring and criminal law, favorable fast attributes of transaction chains and initiation of asset freezing in several jurisdictions. Only the integration of legal, technological and criminological tools can provide a comprehensive counteraction to money laundering in the digital environment in accordance with the challenges of transnational cybercrime.

An integrated investigation model is proposed using procedural standards, stages of digital forensics and tools of international cooperation, formalizing procedures for collecting, storing and presenting electronic evidence for financial cases. It provides control mechanisms – hash identifiers, audit logs, SOP decisions, access channel selection matrices (MLA/direct requests/urgent storage) – and minimizes the risks of inadmissibility of evidence in court using transparent methods. The emphasis is on the principles of proportionality and minimization of state interference to balance the interests of criminal prosecution with human rights and banking secrecy through cross-border scenarios.

An important conclusion is the need to create appropriate institutional conditions for digital forensics: specialized centers of expertise, expanding human resources and improving the skills of investigators and experts in blockchain analytics and financial digital intelligence. Additionally, international mechanisms of Europol, Interpol, UNODC and other structures are crucial for overcoming jurisdictional barriers and official access to relevant financial data, including provider metadata and access logs.

Thus, effective investigation of financial cybercrimes should rely on the trinity of legal standards, technical verification and cross-border procedures, supported by public-private interaction and

standardized operating procedures. It is this model that provides a comprehensive, legitimate, and effective approach to countering in the digital environment and improves the formation of consistent international practice in cases of attacks on financial security.

REFERENCES:

Larchenko, M. O. (2024). Certain features of investigating cybercrimes. Scientific Bulletin of Lviv State University of Internal Affairs. Law Series, (2), 123–137. https://doi.org/10.33498/law-ua.2024.2.123

Criminal Code of Ukraine: Law of Ukraine No. 2341-III of April 5, 2001 (consolidated as of July 17, 2025). Verkhovna Rada of Ukraine Official Portal. https://zakon.rada.gov.ua/go/2341-14

Zhovtan, Y. (2025). Cybercrimes and criminal liability in Ukraine. Pravo.ua. https://pravo.ua/kiberzlochyny-ta-kryminalna-vidpovidalnist-v-ukraini/

Chawki, M. (2010). Anonymity in cyberspace: Finding the balance between privacy and security. International Journal of Technology Transfer and Commercialisation, 9(3), 183–199.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime: Criminal threats and international responses. CRC Press.

Europol, & Eurojust. (2024). Common challenges in cybercrime. Publications Office of the European Union.

United Nations Office on Drugs and Crime. (2024). United Nations Convention against Cybercrime. https://www.unodc.org/unodc/cybercrime/convention/home.html

Velasco, C. (2025). Common challenges in cybercrime: 2024 review by Eurojust and Europol. LinkedIn. https://www.linkedin.com/

World Economic Forum. (2024). Cybercrime Atlas: Impact report. https://www.weforum.org/

Kolosovskyi, Ye. Yu. (2023). Digital forensics: Methodology, tools, chain of custody. Scientific Bulletin, (2), 45–47.

Hutnyk, T. V. (2022). Digital evidence in criminal proceedings: Procedural standards of admissibility. Criminal Process, (6), 47–48.

Lehan, O. A. (2019). Public–private partnership platforms in cybersecurity: Legal and organizational aspects. Legal Journal, (4), 124.

Marchuk, N. M. (2025). Electronic evidence as a source of proof in criminal procedure. In Cybercrime and digital evidence: A textbook (pp. 2–4). Lviv: Ivan Franko National University of Lviv.

Koval, I. M. (2023). Psychological expertise in investigating crimes against peace and security of humankind (pp. 118–120). Kharkiv: Pravo.

Ivan Franko National University of Lviv. (2023). Cybercrime and digital evidence: A textbook (pp. 15–18). Lviv: LNU.

Universum. (2021). Procedural recording of electronic evidence in cloud services. Universum: Bulletin of Scientific Research, (3), 69–71.

Kolosovskyi, Ye. Yu. (2023). Digital forensics: Methodology, tools, chain of custody. Scientific Bulletin, (2), 45–47.

Voitsikhovskyi, V. I. (2011). International cooperation in the field of cybercrime: Model agreements and standards. Legal Journal, (5), 22–28.

Hutsaiuk, M. D. (2021). Attribution technologies for cybercrime infrastructure: Key approaches. Scientific Bulletin, (7), 34–36.

Lehan, O. A. (2019). Public–private partnership platforms in cybersecurity: Legal and organizational aspects. Legal Journal, (4), 118–120, 123–125.

Saienko, M. I. (2021). Procedural aspects of cross-border access to e-evidence in cyberspace. Bulletin of Legal Sciences, (2), 372–378.

Hrebeniuk, V. O. (2021). Effective application of proportionality and privacy in cross-border access to electronic evidence. Legal Digest, (1), 17–19.