Multicore Int. J. Multidiscip, Vol 2, No 1, May 2026
e-ISSN: 3108-933X

OPEN ACCESS

MIMP Marasofi International Media and Publishing

The Role of Cyber Expertise and Other Types of Examinations in Solving Cybercrime Cases

Anorboyev Amiriddin Ulug'bek o'g'li[1*]
[1]Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan, Uzbekistan, a.anorboyev786@mail.ru
[*]Corresponding author, e-mail: a.anorboyev786@mail.ru

Abstract— The rapid development of information and communication technologies has significantly increased both the number and complexity of cybercrime cases. These crimes often involve sophisticated technical processes that exceed the professional competence of investigators, prosecutors, and judges who are primarily trained in legal sciences. As a result, the effectiveness of cybercrime investigations largely depends on the proper use of expert examinations based on specialized technical knowledge. This study aims to analyze the role and significance of cyber expertise in solving cybercrime cases, identify the shortcomings of existing computer-technical (digital forensic) expertise, and justify the need for a more comprehensive and specialized classification of expertise in the field of information and communication technologies. The research employs doctrinal legal analysis, comparative analysis, and a descriptive-analytical method. National legislation of the Republic of Uzbekistan, law enforcement and judicial practice, and foreign experience in the application of cyber and digital forensic expertise were examined, alongside technical aspects of telecommunication networks, information systems, software, cryptography, and communication quality. The findings demonstrate that the prevailing reliance on computer-technical expertise is insufficient to address the multifaceted nature of cybercrimes, which frequently involve telecommunication infrastructure, encryption technologies, software applications, and communication quality issues beyond the traditional scope of digital forensics. The study substantiates the need to introduce specialized types of expertise, including telecommunication network and infrastructure expertise, information systems and computer data expertise, software and application expertise, cryptographic expertise, communication coverage and quality expertise, and cyber forensic auditing. Particular emphasis is placed on cyber forensic auditing as a mechanism for ensuring the admissibility and reliability of digital evidence. The study concludes that the current forensic framework should be expanded and systematized, and recommends developing specialized expert training and updating procedural legislation to enhance the effectiveness of cybercrime investigations.

Keywords: *cybercrime, cyber expertise, digital forensics, telecommunication networks, information systems, cryptographic expertise, communication quality, cyber forensic auditing, digital evidence, forensic examination*

1. Introduction

The rapid advancement of information and communication technologies (ICT) has significantly transformed social, economic, and governmental systems worldwide. Alongside these developments, cyberspace has increasingly become a medium for criminal activities, commonly referred to as cybercrimes. These crimes are distinguished by their technical complexity, cross-border nature, and reliance on digital infrastructure such as telecommunication networks, information systems, software,

Received: 14 November 2025, Revised: 18 January 2026 , Accepted: 18 January 2026
https://doi.org/10.64123/mijm.v2.i1.3

and cryptographic technologies. Consequently, effective investigation and adjudication of cybercrime cases require not only legal expertise but also highly specialized technical knowledge.

In general, cybercrimes present serious challenges to criminal justice systems due to the intangible nature of digital evidence and the high risk of its alteration, deletion, or loss in cyberspace. Recognizing these challenges, the Republic of Uzbekistan has adopted a number of legislative acts aimed at regulating cybersecurity and expert examinations, including procedures for conducting expertise on compliance with cybersecurity requirements [1]. Furthermore, state policy emphasizes the training of professional personnel capable of combating crimes committed through digital technologies, highlighting the growing importance of cyber expertise in law enforcement practice [2].

More specifically, the investigation of cybercrime cases in Uzbekistan predominantly relies on forensic computer-technical (digital forensic) expertise. This approach focuses mainly on examining computer devices, information systems, and digital data. However, cybercrimes often involve crypto-assets, telecommunication services, and distributed digital infrastructures, which require broader technical analysis beyond traditional computer forensics [3]–[5]. As a result, the exclusive reliance on computer-technical expertise may lead to incomplete assessments of the technical circumstances of cybercrimes.

The urgency of this issue is further reinforced by practical challenges in monitoring and evaluating telecommunication systems. Telecommunication services are governed by specific regulatory rules and legal standards, yet the forensic potential of telecommunication data and network parameters remains insufficiently utilized in criminal proceedings [4], [5]. In practice, inadequate communication quality can affect not only service delivery but also cybersecurity, as it may hinder the timely detection and investigation of cyber incidents.

From a technical standpoint, telecommunication networks constitute the foundational infrastructure of cyberspace. Any cybercrime necessarily involves some form of telecommunication, whether through wired or wireless networks. Modern technologies for assessing communication quality, such as drive tests, walk tests, mobile device testing, and minimization of drive tests (MDT), are widely applied in international practice using specialized equipment and methodologies [6]–[10]. These methods provide objective data on signal strength, coverage, and quality, which may be critical for reconstructing the technical conditions under which a cybercrime was committed.

Nevertheless, in the Republic of Uzbekistan, there is no independent type of forensic expertise dedicated to assessing communication coverage and quality. Moreover, the absence of specialized personnel and the limited use of advanced measurement technologies reduce the effectiveness of cybercrime investigations. This situation persists despite international experience demonstrating the importance of secure communication systems and network monitoring for ensuring cybersecurity [11]–[16].

The novelty of this study lies in proposing a comprehensive and technically justified reclassification of forensic expertise applicable to cybercrime cases. Unlike the prevailing approach, which treats cybercrime investigation primarily within the framework of computer-technical expertise, this research introduces a broader system of specialized expertise based on the structural components of ICT. In particular, it substantiates the need to establish telecommunication network expertise, telecommunication infrastructure expertise, information systems and computer data expertise, software and application expertise, cryptographic expertise, communication coverage and quality expertise, and cyber forensic auditing. The latter is especially novel for national practice, as it focuses on evaluating the procedural and technical admissibility of digital evidence, an aspect that has not previously been applied in Uzbekistan's investigative or judicial activities.

The objective of this study is to justify the expansion and systematization of cyber-related forensic expertise by aligning criminal procedure with the technical realities of modern ICT. By analyzing national

legislation, examining foreign experience, and identifying gaps in current forensic practice, this research seeks to contribute to the development of a more effective and reliable forensic framework for combating cybercrime.

2. Method

This study adopts a qualitative legal research design with a doctrinal and analytical orientation. The methodology is structured to examine the role of cyber expertise in cybercrime cases by integrating legal analysis with technical perspectives derived from information and communication technologies (ICT).

First, a normative legal analysis was conducted to examine the regulatory framework governing cybercrime investigation and forensic expertise in the Republic of Uzbekistan. This analysis focused on laws, presidential decrees, ministerial regulations, and procedural rules related to cybersecurity, digital evidence, telecommunication services, and expert examinations [1]–[5]. The purpose of this stage was to identify the legal basis, scope, and limitations of existing computer-technical (digital forensic) expertise within criminal proceedings.

Second, a descriptive and analytical approach was applied to assess current investigative and forensic practices in cybercrime cases. This included an examination of how digital evidence is collected, processed, and evaluated by investigators, prosecutors, and courts, as well as the role assigned to specialists and experts during these processes. Particular attention was paid to procedural risks affecting the admissibility and reliability of digital evidence, including errors related to data collection, preservation, and documentation.

Third, a comparative legal method was employed to analyze foreign experience in the application of cyber-related forensic expertise. The study reviewed practices used in developed jurisdictions such as the United States, the United Kingdom, Germany, and other countries, especially regarding network forensics, mobile device expertise, malware analysis, cryptographic expertise, and cyber forensic auditing. Technical standards and measurement methodologies for assessing communication coverage and quality, including drive tests, walk tests, mobile device testing, and minimization of drive tests (MDT), were also examined based on international technical documentation and empirical studies [6]–[10], [11]–[16].

Fourth, a system-structural method was used to classify and systematize types of expertise applicable to cybercrime cases. This method enabled the identification of core ICT components—telecommunication networks, infrastructure, information systems, software, encryption, and communication quality—and the formulation of a comprehensive classification of cyber expertise aligned with these components. Through this approach, traditional computer-technical expertise was re-evaluated as an integrated element rather than a standalone solution.

Finally, a synthesis method was applied to formulate conclusions and recommendations. Legal findings and technical analyses were combined to substantiate proposals for expanding the scope of forensic expertise, introducing new specialized types of cyber expertise, and improving procedural regulation related to the admissibility of digital evidence. This methodological framework ensures the coherence of legal reasoning with the technical realities of modern cyberspace and supports the practical applicability of the research results.

3. Results and Discussion

The results of this study demonstrate that the effectiveness of cybercrime investigations is strongly influenced by the scope, specialization, and technical adequacy of forensic expertise applied during criminal proceedings. The findings reveal structural limitations in the current forensic framework, particularly the overreliance on computer-technical (digital forensic) expertise, which does not fully correspond to the technological realities of modern cybercrime.

1. Limitations of Existing Computer-Technical Expertise

The analysis shows that forensic computer-technical expertise in the Republic of Uzbekistan primarily focuses on examining computer devices, digital files, and information systems. While this type of expertise is essential for identifying, recovering, and analyzing digital data, its scope is largely confined to end-user devices and internal system processes. Cybercrimes, however, frequently involve external network interactions, telecommunication infrastructures, encryption mechanisms, and software-based automation, which are not comprehensively addressed within traditional computer-technical examinations.

As a result, investigators and courts may receive expert conclusions that describe the state of digital data without fully explaining the technical conditions under which the cybercrime was committed. This gap can affect the reconstruction of criminal events, the attribution of actions to specific actors, and the assessment of causality between technical failures and criminal outcomes.

2. Telecommunication Network and Infrastructure Expertise

The findings confirm that telecommunication networks constitute the foundational layer of cyberspace and play a decisive role in all forms of cybercrime. Telecommunication network expertise enables the analysis of data transmission paths, network traffic, IP addressing, signal routing, and connectivity conditions. Telecommunication infrastructure expertise complements this analysis by examining physical and logical network components, including base stations, cables, servers, and switching equipment.

The absence of these specialized types of expertise in national forensic practice limits the ability to assess whether technical disruptions, network instability, or infrastructure deficiencies contributed to the commission or concealment of cybercrimes. International experience demonstrates that separating network and infrastructure expertise enhances analytical precision and reduces ambiguity in expert conclusions.

3. Information Systems and Computer Data Expertise

Information systems and computer data expertise focuses on databases, servers, user accounts, logs, and digital records within complex systems. The results indicate that this type of expertise is crucial for determining the creation time, modification history, functional purpose, and integrity of digital data. In cybercrime cases involving data manipulation, unauthorized access, or system interference, such expertise provides objective technical explanations that cannot be derived solely from device-level analysis.

This specialization also plays an important role in distinguishing between lawful system operations and criminal interference, thereby supporting accurate legal qualification of cyber offenses.

4. Software and Application Expertise

The study reveals that software and application expertise is essential for analyzing malicious programs, automated scripts, and application-level vulnerabilities exploited in cybercrimes. This type of expertise allows experts to identify program functions, execution mechanisms, potential risks, and the degree of harm caused by software operations.

Without dedicated software expertise, malware analysis is often fragmented or oversimplified, which may prevent investigators from identifying the origin, intent, and operational logic of malicious code. The findings support the classification of software and application expertise as an independent forensic category rather than a subsidiary element of computer-technical examinations.

5. Cryptographic Expertise

Cryptographic expertise addresses the encryption of data, secure communication channels, digital signatures, and crypto-asset transactions. The results indicate that crimes involving cryptocurrencies, encrypted storage, and protected communications require advanced cryptographic analysis that exceeds the competence of general digital forensic examinations.

This type of expertise is particularly relevant in cases involving blockchain technologies, anonymous transactions, and encrypted messaging platforms. The study confirms that cryptographic expertise enhances the ability to trace digital assets, analyze encryption mechanisms, and assess the feasibility of data decryption within legal and technical boundaries.

6. Communication Coverage and Quality Expertise

One of the most significant findings concerns the absence of communication coverage and quality expertise in national forensic practice. The analysis demonstrates that communication quality directly affects cybersecurity by influencing data transmission reliability, system responsiveness, and incident detection capabilities. Measurement methods such as drive tests, walk tests, mobile device testing, and minimization of drive tests (MDT) provide objective indicators of network performance that may be critical in reconstructing cybercrime circumstances.

The lack of specialized expertise and trained personnel in this area limits the use of these technologies for forensic purposes, despite their widespread application in international practice.

7. Cyber Forensic Auditing and Admissibility of Digital Evidence

The study identifies cyber forensic auditing as a novel and critically important form of expertise. Unlike traditional examinations that focus on technical content, cyber forensic auditing evaluates the procedural and technical integrity of digital evidence, including data collection methods, preservation processes, chain of custody, and documentation accuracy.

The findings reveal that procedural or technical errors committed during evidence collection may compromise the admissibility and reliability of digital evidence, as recognized by criminal procedural legislation. Cyber forensic auditing addresses this gap by ensuring that digital evidence meets both technical and legal standards, thereby strengthening its probative value in court.

Discussion

Overall, the results support the argument that cybercrime investigation requires a multidisciplinary and system-based approach to forensic expertise. Treating computer-technical expertise as a universal solution fails to capture the complexity of modern cybercrimes. By contrast, the proposed classification aligns forensic practice with the structural components of ICT and enhances analytical accuracy, evidentiary reliability, and procedural fairness.

The discussion confirms that the proposed model not only reflects international best practices but also responds to the specific needs of national legal systems undergoing rapid digital transformation. Implementing this model would contribute to more effective cybercrime prevention, investigation, and adjudication.

4. Conclusion

This study concludes that cyber expertise constitutes a fundamental element in the effective investigation and adjudication of cybercrime cases. The increasing technical complexity of cybercrimes, combined

with their transnational nature and dependence on information and communication technologies, renders traditional forensic approaches insufficient when applied in isolation. The prevailing reliance on computer-technical (digital forensic) expertise does not adequately reflect the multifaceted structure of modern cyberspace.

The findings demonstrate that cybercrimes involve interconnected technical layers, including telecommunication networks and infrastructure, information systems, software applications, encryption mechanisms, and communication quality parameters. Consequently, forensic expertise must be systematically aligned with these components. The proposed classification of cyber-related expertise—encompassing telecommunication network expertise, telecommunication infrastructure expertise, information systems and computer data expertise, software and application expertise, cryptographic expertise, communication coverage and quality expertise, and cyber forensic auditing—offers a comprehensive and technically grounded framework.

Particular emphasis is placed on cyber forensic auditing as a novel and indispensable form of expertise. By assessing the procedural and technical integrity of digital evidence, cyber forensic auditing strengthens the admissibility, reliability, and probative value of such evidence in criminal proceedings. This approach addresses critical risks associated with data collection, preservation, and documentation, which may otherwise undermine the establishment of criminal responsibility.

Overall, the study affirms that expanding and systematizing forensic expertise in cybercrime cases is not merely a technical necessity but a legal imperative. Aligning criminal procedure with the realities of modern information and communication technologies will enhance the effectiveness of cybercrime investigations, ensure procedural fairness, and contribute to the development of a more resilient and technologically responsive justice system.

References

[1] State Security Service of the Republic of Uzbekistan, *Regulation on the Procedure for Conducting Expertise on Compliance with Cybersecurity Requirements*, Order No. 113, Oct. 15, 2024, registered No. 3573, Nov. 14, 2024. [Online]. Available: lex.uz

[2] President of the Republic of Uzbekistan, *On Measures to Introduce a System for Training Professional Personnel to Combat Crimes Committed Using Digital Technologies*, Resolution No. PQ–17, Jan. 22, 2025. [Online]. Available: lex.uz

[3] Ministry of Internal Affairs of the Republic of Uzbekistan, Prosecutor General's Office, and National Agency for Perspective Projects, *Instruction on the Seizure, Arrest, Storage, and Transfer of Crypto-Assets Identified During Pre-Investigation and Criminal Investigation*, Joint Resolution Nos. 44, 14, and 14, Dec. 18–20, 2024, registered No. 3591, Dec. 25, 2024. [Online]. Available: lex.uz

[4] Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan, *Rules for the Provision of Telecommunication Services*, Order No. 208-mh, Jun. 30, 2020, registered No. 3275. [Online]. Available: lex.uz

[5] Republic of Uzbekistan, *Law on Telecommunications*, Law No. ORQ–1015, Dec. 27, 2024. [Online]. Available: lex.uz

[6] Rohde & Schwarz, *TSME6 Network Scanner: Product Brochure*. [Online]. Available: assets-us-01.kc-usercontent.com

[7] TAdviser, *PCTEL SeeGull IBflex Scanner*. [Online]. Available: www.tadviser.ru

[8] Rohde & Schwarz, *TSMA Autonomous Mobile Network Scanner: Product Brochure*. [Online]. Available: cdn.rohde-schwarz.com

[9] Samsung Electronics, *Galaxy S21+ 5G Specifications*. [Online]. Available: www.samsung.com

[10] ShareTechnote, *LTE MDT (Minimization of Drive Tests) Handbook*. [Online]. Available: www.sharetechnote.com

[11] Rohde & Schwarz, *Secure Web Browser Solutions for Cybersecurity*. [Online]. Available:

www.rohde-schwarz.com
[12] Systemics-PAB, *Public Acceptability Benchmarking of Mobile Network Quality*. [Online]. Available: www.syspab.eu
[13] Rohde & Schwarz, *5G Network Quality Evaluation for U.S. Network Operators*. [Online]. Available: www.rohde-schwarz.com
[14] Rohde & Schwarz, *Mobile Network Testing Certificate: Bell Canada Benchmarking Campaign Q4 2021*. [Online]. Available: scdn.rohde-schwarz.com
[15] Rohde & Schwarz, *Benchmarking Icelandic Mobile Network Quality Using ETSI Methodology*. [Online]. Available: www.rohde-schwarz.com
[16] Rohde & Schwarz and Telia, *Comprehensive Mobile Network Benchmarking Campaign in Estonia*. [Online]. Available: www.rohde-schwarz.com
[17] Inspection for Control in the Field of Informatization and Telecommunications, *Report on Public Appeals Concerning Communication Quality, Q1 2025*. [Online]. Available: api-portal.gov.uz