The role of cyber expertise and other types of examinations in solving cybercrime cases

(es) **El papel de la pericia cibernética y otros tipos de exámenes en la resolución de casos de ciberdelitos**

(port) **O papel da perícia cibernética e de outros tipos de exames na resolução de casos de crimes cibernéticos.**

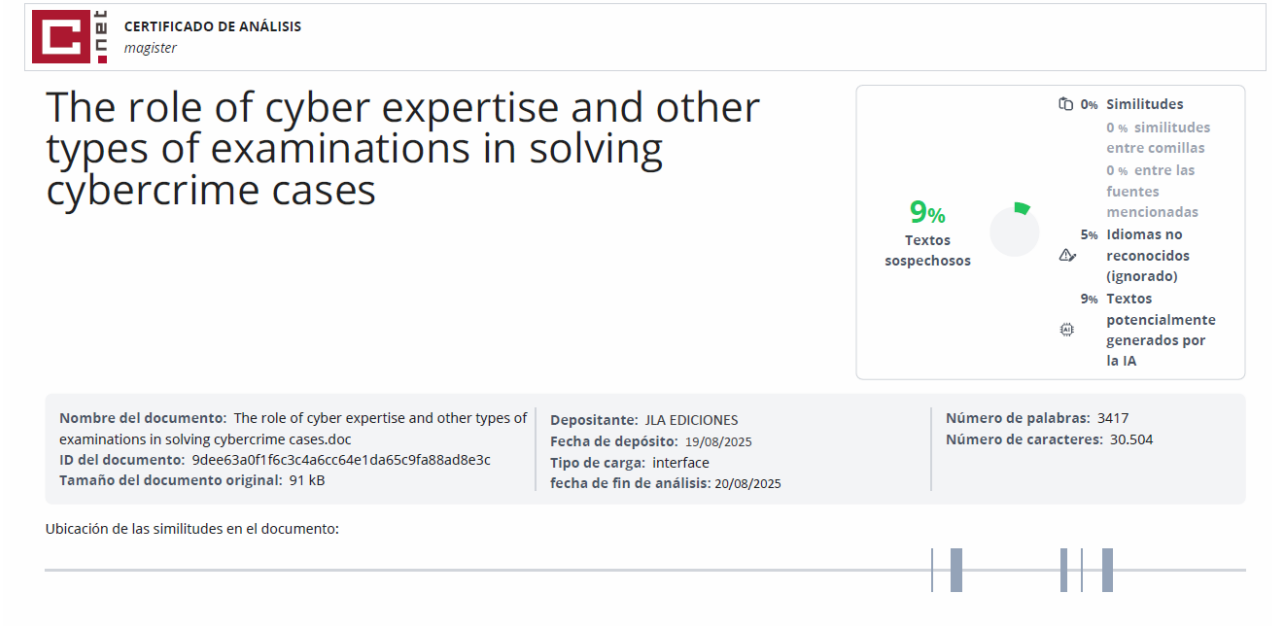
Anorboyev Amiriddin Ulug'bek o'g'li
Institute of Legislation and Legal Information of the Republic of Kazakhstan
a.anorboyev786@mail.ru
https://orcid.org/0009-0003-5355-8753

Anorboyev, A. (2025). The role of cyber expertise and other types of examinations in solving cybercrime cases. *YUYAY: Estrategias, Metodologías & Didácticas Educativas*, *5*(3), 1–15. https://doi.org/10.59343/yuyay.v5i3.126

Recepción: 18-08-2025 / Aceptación: 21-10-2025 / Publicación: 30-11-2025

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Compilatio Master+ IA Similarity Report



CERTIFICADO DE ANÁLISIS
magister

The role of cyber expertise and other types of examinations in solving cybercrime cases

9% Textos sospechosos

0% Similitudes
0 % similitudes entre comillas
0 % entre las fuentes mencionadas
5% Idiomas no reconocidos (ignorado)
9% Textos potencialmente generados por la IA

Nombre del documento: The role of cyber expertise and other types of examinations in solving cybercrime cases.doc
ID del documento: 9dee63a0f1f6c3c4a6cc64e1da65c9fa88ad8e3c
Tamaño del documento original: 91 kB

Depositante: JLA EDICIONES
Fecha de depósito: 19/08/2025
Tipo de carga: interface
fecha de fin de análisis: 20/08/2025

Número de palabras: 3417
Número de caracteres: 30.504

Ubicación de las similitudes en el documento:

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Abstract (en)

The accelerated digitalization of social, economic, and institutional systems has significantly transformed the nature of criminal activity, giving rise to increasingly complex forms of cybercrime. Traditional computer-technical forensic examinations no longer fully respond to the multidimensional structure of contemporary digital offenses. Objective: To analyze the current limitations of conventional digital forensic practices and to propose a restructured and expanded typology of specialized cyber expertise for the effective investigation of cybercrime. Methodology: Normative, descriptive, and comparative legal-technical analysis was conducted using regulatory frameworks, institutional practices, and international experiences in digital forensics and telecommunications expertise. Results: The study identifies substantial gaps in the existing computer-technical examination model and proposes a comprehensive classification of cyber expertise, including telecommunications network and infrastructure expertise, information systems and data analysis, software and application expertise, cryptographic expertise, communication coverage and quality analysis, and cyber forensic auditing. Conclusions: Cybercrime investigation requires a systemic forensic model grounded in the technical realities of digital ecosystems. The reliability of digital evidence, network integrity, and cryptographic validation must be legally and technically reinforced through updated regulatory frameworks and specialized forensic training.

Keywords: *Cybercrime; Digital forensics; Telecommunications; Electronic evidence; Cryptography.*

Resumen (es)

La acelerada digitalización de los sistemas sociales, económicos e institucionales ha transformado de manera profunda la dinámica delictiva, consolidando formas cada vez más complejas de cibercriminalidad. Las pericias informático-técnicas tradicionales resultan insuficientes frente a la naturaleza multidimensional de los delitos digitales contemporáneos. Objetivo: Analizar las limitaciones actuales de las prácticas convencionales de pericia digital y proponer una tipología reestructurada y ampliada de experticias especializadas para la investigación eficaz del cibercrimen. Metodología: Se desarrolló un análisis normativo, descriptivo y comparado de carácter jurídico-técnico, sustentado en marcos regulatorios, prácticas institucionales y experiencias internacionales en materia de pericia digital y telecomunicaciones. Resultados: El estudio identifica vacíos significativos en el modelo vigente de pericia informático-técnica y propone una clasificación integral de experticias, que incluye redes e infraestructura de telecomunicaciones, sistemas de información y datos, así como auditoría forense digital. Conclusiones: La investigación del cibercrimen exige un modelo pericial sistémico, anclado en las realidades técnicas de los ecosistemas digitales. La confiabilidad de la evidencia digital, la integridad de las redes y la validación criptográfica deben fortalecerse mediante marcos normativos actualizados y formación pericial especializada.

Palabras claves: Cibercriminalidad; Pericia digital; Telecomunicaciones; Evidencia electrónica; Criptografía

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Resumo (port)

A aceleração da digitalização dos sistemas sociais, econômicos e institucionais transformou profundamente a natureza da atividade criminosa, consolidando formas cada vez mais complexas de cibercrime. As perícias técnico-computacionais tradicionais já não respondem adequadamente à estrutura multidimensional dos delitos digitais contemporâneos. Objetivo: Analisar as limitações atuais das práticas tradicionais de perícia digital e propor uma tipologia reestruturada e ampliada de expertises especializadas para a investigação eficaz do cibercrime. Metodologia: Foi realizada uma análise normativa, descritiva e comparativa de caráter jurídico-técnico, baseada em marcos regulatórios, práticas institucionais e experiências internacionais em perícia digital e telecomunicações. Resultados: O estudo identifica lacunas relevantes no modelo vigente de perícia técnico-computacional e propõe uma classificação abrangente de expertises, incluindo perícias de redes e infraestrutura de telecomunicações, sistemas de informação e dados, softwares e aplicações, criptografia, cobertura e qualidade das comunicações e auditoria forense cibernética. Conclusões: A investigação do cibercrime exige um modelo pericial sistêmico, fundamentado nas realidades técnicas dos ecossistemas digitais. A confiabilidade da evidência digital, a integridade das redes e a validação criptográfica devem ser fortalecidas juridicamente e tecnicamente por meio de marcos regulatórios atualizados e formação pericial especializada.

Palavras-chave: Competências dos professores; conscientização; família; formação de professores do ensino fundamental.

AI Use Disclosure Statement

The author hereby states that artificial intelligence tools were used solely as technical support for writing assistance and linguistic verification during the preparation of this manuscript. These tools did not replace academic analysis, legal interpretation, or the generation of original ideas, which remain entirely the author's own contribution. The author acknowledges and accepts the 9% similarity report identified by the journal's screening systems, in full compliance with its editorial policies, and confirms that this percentage does not compromise the originality or scientific integrity of the work.

Declaración de Uso de Inteligencia Artificial

El autor declara que en la elaboración del presente manuscrito se emplearon herramientas de inteligencia artificial exclusivamente como apoyo técnico para la redacción y verificación lingüística del contenido. El uso de tales herramientas no sustituyó el análisis académico, la interpretación jurídica ni la generación original de ideas, que corresponden íntegramente al autor. Asimismo, el autor reconoce y acepta el reporte de coincidencia del 9% detectado por los sistemas de revisión de la revista, en conformidad con sus normas editoriales, y declara que dicho porcentaje no afecta la originalidad ni la integridad científica del trabajo.

Declaração de Uso de Inteligência Artificial

O autor declara que, na elaboração deste manuscrito, foram utilizadas ferramentas de inteligência artificial exclusivamente como apoio técnico para a redação e verificação linguística do conteúdo. O uso dessas ferramentas não substituiu a análise acadêmica, a interpretação jurídica nem a geração de ideias originais, que são integralmente de autoria do pesquisador. O autor reconhece e aceita o relatório de similaridade de 9% identificado pelos sistemas de verificação da revista, em conformidade com suas normas editoriais, e afirma que tal percentual não compromete a originalidade nem a integridade científica do trabalho.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Introduction

The development of information and communication technologies and their integration with other technologies have led to the rapid digitalization of all sectors and industries today, including the field of forensic examinations related to cybercrimes. The processes of appointing examinations, conducting them, and preparing expert conclusions are currently being gradually digitalized.

In general, cybercrime and expertise are distinct concepts. Cybercrime refers to a culpable socially dangerous act (action or inaction) committed in the cyber environment, including cyberspace, or by using information and communication technologies—such as telecommunications, informatization, artificial intelligence, digitalization infrastructure, neural, bio, and cyber technologies, as well as other related technical means—that is prohibited by the criminal legislation of each state and entails the threat of punishment.

Expertise, on the other hand, is a procedural activity aimed at establishing the circumstances of a case, involving the conduct of forensic examinations and the provision of conclusions by an expert based on special knowledge in the fields of science, technology, art, or craft.

Accordingly, expertise plays an important role in the detection and investigation of cybercrimes.

It should be emphasized that today large-scale efforts are being carried out in the Republic of Uzbekistan to digitalize the field of expertise. In particular, 152 legislative documents related to expertise have been adopted, with attention being paid to the digitalization of expertise in each area and to the appointment of expertise in relation to cybercrimes.

During the past period, procedures have been established for conducting expertise to assess the compliance of information systems and resources of cybersecurity entities, as well as information systems included in the category of critical information infrastructure objects, and also project specifications for the development of information systems and resources, with cybersecurity requirements1, At the Academy of the Ministry of Internal Affairs, the educational process in the field of “Combating Crimes in the Sphere of Digital Technologies” has been organized within a dual education system, specializing in the prevention of offenses, operational-search activities, and forensic-expert activities. Within the existing staffing structure of the Academy, a Faculty of Cybersecurity and Digital Forensics has been established, which includes departments of Cyber Law, Exact Sciences, Digital Technologies and Information Security, as well as Forensic Examinations2, Along

[1] Ўзбекистон Республикаси Давлат хавфсизлик хизмати раисининг 2024 йил 15 октябрдаги 113-сон буйруғи (14.11.2024 й., рўй.: 3573-сон) билан тасдиқланган “Киберхавфсизлик талабларига мувофиқлик юзасидан экспертизадан ўтказиш тартиби тўғрисида”ги Низом // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

[2] Ўзбекистон Республикаси Президентининг “Рақамли технологиялар воситасида содир этиладиган жиноятларга қарши курашиш соҳаси учун профессионал кадрлар тайёрлаш тизимини жорий этиш чора-тадбирлари тўғрисида”

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

with identifying information on offenses related to crypto-assets by pre-investigation inquiry, inquiry, and preliminary investigation bodies, the implementation of the following measures has been established:

- examining the memory of information storage devices;
- analyzing the distributed ledger of data based on the crypto-wallet address;
- appointing a forensic computer-technical examination;
- sending relevant inquiries to service providers in accordance with the procedure established by law;
- submitting inquiries to obtain information related to banking secrecy3.

Why is expertise necessary for cybercrimes?

- Firstly, individuals serving as investigators, interrogators, prosecutors, and judges in the Republic of Uzbekistan may have studied at different higher educational institutions; however, their main specialization is in law, and almost none of them sufficiently understand or possess knowledge in the field of information and communication technologies;
- Secondly, in the cyber environment created by information and communication technologies, including cyberspace or by using it, there exists a risk of digital evidence related to cybercrimes being deleted, altered, or traces of the cybercrime being lost. To eliminate this risk, mandatory involvement of a specialist or an expert is required;
- Thirdly, to provide a conclusion regarding where, when, and under what circumstances a cybercrime was committed in the cyber environment, including cyberspace or through its use, the participation of a specialist or an expert is required;
- Fourthly, in accordance with Articles 238–240 of the current Criminal Code, a specialist is not warned, whereas an expert is warned, and this, in turn, may serve as a factor that encourages the expert to provide a correct conclusion, realizing the responsibility for the opinion given;

2025 йил 22 январдаги ПҚ–17-сон қарори // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

[3] Ўзбекистон Республикаси Ички ишлар вазирлигининг 2024 йил 20 декабрдаги 44-сон, Бош прокуратуранинг 2024 йил 19 декабрдаги 14-сон ҳамда Истиқболли лойиҳалар миллий агентлигининг 2024 йил 18 декабрдаги 14-сон қарори (25.12.2024 й., рўй.: 3591-сон) билан тасдиқланган “Терговга қадар текширувни амалга оширишда ва жиноятларни тергов қилиш давомида аниқланган крипто-активларни олиб қўйиш, хатлаш, сақлаш ҳамда топшириш тартиби тўғрисида”ги Йўриқнома // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

- Fifthly, cybercrimes are international transnational crimes, and their commission in conjunction with other types of crimes requires extensive knowledge and analytical thinking, for which the field of expertise is specifically specialized.

At present, cybercrime cases are usually examined through forensic computer-technical expertise; however, from a technical perspective, the limited scope of computer technology indicates the necessity of revising this type of expertise.

In particular, forensic computer-technical expertise is considered an examination that reviews computer information, that is, the conditions related to computer technology within information and computing systems[4], networks, and their components. However, it should not be forgotten that computer information may also be connected to infrastructures related to other information and communication technologies.

For example, telecommunications network and computer technology are considered different means. In a telecommunications network, computer information is transmitted through telecommunications, that is, by means of a signal. However, if the speed and quality of this signal do not affect the integrity and wholeness of the computer information, then in such a case it would be incorrect to associate the conducted examination with forensic computer-technical expertise.

The reason is that the main function of telecommunications is the transmission, reception, and processing of information — whether in the form of text, image, sound, video, or other types of signals — by using radio, optical, or other electromagnetic systems[5]. In this process, computer information is transmitted not through computer technology, but through telecommunications networks, facilities, structures, and devices.

In practice, the “Electromagnetic Compatibility Center” State Unitary Enterprise, on the basis of the instructions and cooperation of the Inspectorate for Control in the Field of Informatization and Telecommunications and its regional divisions, measures mobile communication coverage. Insufficient mobile coverage constitutes an administrative offense provided for in Article 153 of the Code of Administrative Liability. However, at present, neither of these organizations uses the technology for fully measuring communication quality. The reason is that this measuring equipment is very expensive, and since the fines imposed for

[4] Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирининг 2020 йил 30 июндаги 208-мҳ-сон буйруғи (рўйхат рақами 3275, 2020 йил 30 июнь) билан тасдиқланган Телекоммуникация хизматларини кўрсатиш қоидалари // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси. [Rules for the provision of telecommunications services, approved by the order of the Minister of Information Technologies and Communications of the Republic of Uzbekistan dated June 30, 2020 No. 208-mh (registration number 3275, June 30, 2020) // lex.uz - National database of legislative information of the Republic of Uzbekistan.]

[5] Ўзбекистон Республикасининг “Телекоммуникациялар тўғрисида” 2024 йил 27 декабрдаги ЎРҚ–1015-сон Қонуни // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси. [Law of the Republic of Uzbekistan "On Telecommunications" dated December 27, 2024 No. ZUR-1015 // lex.uz - National database of legislative information of the Republic of Uzbekistan.]

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

administrative offenses under Article 153 of the Code of Administrative Liability are very small and are transferred to the state budget, sufficient reforms in this regard have not yet been implemented by the aforementioned organizations.

At this point, it should be emphasized that it is possible to measure the quality of mobile communication through the following equipment, devices, and tools. In particular:

1) Drive Test. In this method, vehicles equipped with special measuring equipment move along cities and roads to measure the quality of mobile communication. For example:

- Rohde & Schwarz TSME6: This device is used to assess the quality of LTE and 5G networks. It is integrated with GPS and measures parameters such as signal strength, quality, and interference[6].
- PCTEL SeeGull IBflex®: This scanner operates in the range from 400 MHz to 2.7 GHz and is designed for small-cell and in building testing[7];

2) Walk Test. The quality of communication is measured by walking on foot. This method is especially used in large cities and crowded areas. For example, the Rohde & Schwarz TSMA Autonomous Mobile Network Scanner: this device connects to smartphones via Wi-Fi or Bluetooth, collects data, and performs analysis[8];

3) Mobile Device Testing. This method is used to measure communication quality through mobile phones. For example, Samsung Galaxy S21+ 5G[9]: in tests conducted in Poland, these smartphones were used together with Rohde & Schwarz equipment to evaluate communication quality;

4) MDT (Minimization of Drive Tests). In this method, mobile devices automatically measure the quality of the connection and send the data to the operator. This allows for the continuous collection of extensive and comprehensive information[10].

The technologies mentioned above themselves require cybersecurity, and only when the management system, network encryption, web browser, and endpoint security are ensured can these technologies be fully

[6] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://assets-us-01.kc-usercontent.com/ecb176a6-5a2e-0000-8943-84491e5fc8d1/e502ed4d-81e4-4334-ac7a-3ec80d0f2821/RS-TSME6_brochure.pdf.

[7] https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:PCTEL_SeeGull_IBflex_%D0%A1%D0%BA%D0%B0%D0%BD%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B8%D0%B9_%D0%BF%D1%80%D0%B8%D0%B5%D0%BC%D0%BD%D0%B8%D0%BA.

[8] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cdn.rohde-schwarz.com/au/TSMA_bro_en_3607-1513-12_v0900.pdf.

[9] https://www.samsung.com/ru/smartphones/galaxy-s21-5g/buy/?modelCode=SM-G996BZVDSER.

[10] https://www.sharetechnote.com/html/Handbook_LTE_MDT.html.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

utilized11. In 2016 in Poland12, 2020 in the USA13, 2021 in Canada14, 2022 in Switzerland15, 2023 in Iceland16 and 2024 in Estonia17, separate studies were conducted to assess the quality of mobile communication networks. However, today, there are still several challenges in this regard in the Republic of Uzbekistan. It should be noted that the quality of communication also contributes to cybersecurity, as it allows for the rapid detection of issues, including cybercrimes committed in the cyber environment.

However, in the Republic of Uzbekistan, there is not even a specialized type of expertise for measuring mobile communication quality, and no personnel training has been established in this field, so the relevant technology is not fully utilized. Meanwhile, the authority responsible for monitoring mobile communication quality – the Inspection for Control in the Field of Informatization and Telecommunications – received 1,191 appeals in the first quarter of 2025 alone, the majority of which concerned poor communication quality18. This, in turn, necessitates the implementation of reforms in this field.

Additionally, in the USA, the United Kingdom, Germany, and other developed countries, the following types of expertise related to information and communication technologies are utilized:

The main types of expertise used in foreign countries for cybercrime by investigators, prosecutors, or courts are as follows:

1) Computer-Technical (Digital Forensic) Expertise

---

11 https://www.rohde-schwarz.com/fi/products/cybersecurity/secure-web-browser_232366.html.

12 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.syspab.eu/wp-content/uploads/2017/01/Systemics-PAB_bro_en_5214-6774-32_v0102_final.pdf#:~:text=reliable%20operators%2C%20in%202015%2C%20UKE,quality%20of%20net%02works%20and%20customer.

13 https://www.rohde-schwarz.com/us/solutions/critical-infrastructure/mobile-network-testing/stories-insights/article-qoe-5g-network-evaluation-for-us-network-operators_254564.html#:~:text=The%20independent%20wireless%20industry%20research,buzz%20in%20the%20telecommunications%20industry.

14

15 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/Certificate-MNT-Bell-Canada-Q4-2021-Benchmarking-Campaign.pdf.

16 https://www.rohde-schwarz.com/us/about/news-press/all-news/ecoi-commissions-rohde-schwarz-to-benchmark-icelandic-mobile-network-quality-with-etsi-methodology-press-release-detailpage_229356-1451264.html.

17 https://www.rohde-schwarz.com/us/about/news-press/all-news/rohde-schwarz-and-telia-unlock-estonia-s-full-potential-with-comprehensive-mobile-network-benchmarking-campaign-press-release-detailpage_229356-1533252.html.

18 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://api-portal.gov.uz/uploads/147/2025/05/13/df766256-5068-f1ab-3d42-0b3195f31c82_media_.pdf.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Purpose: To identify, recover, and analyze information and other data from computers, laptops, and servers.

Main Applications: It is primarily used to identify the source of a cyber-attack, analyze cases of file deletion, encryption, and modification, and monitor activities through log files;

2) Mobile Device Expertise

Purpose: To examine information and other data stored on smartphones and tablets.

Main Applications: It is primarily used to analyze calls, SMS messages, applications, GPS data, social networks or messengers—including WhatsApp, Telegram, and Messenger chats—as well as Internet activity and browser history;

3) Network (Network Forensic) Expertise

Purpose: To analyze cyber attacks or data flows carried out through networks.

Main Applications: It is primarily used to investigate DDoS attacks, identify IP addresses, and uncover attempts to hide activity using VPNs or proxies;

4) Data Recovery Expertise

Purpose: To restore deleted, formatted, or damaged data.

Main Applications: It is primarily used to preserve reliable and necessary information in cases of cyber sabotage or cyber theft;

5) Malware Analysis Expertise

Purpose: To analyze programs used in cybercrime, including viruses, trojans, and ransomware.

Main Applications: It is primarily used to identify the source of malicious software and study its operational mechanisms;

6) Email and Personal Communication Expertise

Purpose: To analyze information sent via email or personal communication channels.

Main Applications: It is primarily used to detect threats, fraud, or cases of personal data theft related to information transmitted through email or personal communication channels;

7) Cryptography Expertise

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Purpose: To analyze encrypted data, passwords, and cryptocurrency transactions.

Main Applications: It is primarily used to investigate crimes related to crypto currency and to analyze information concerning encrypted files and programs;

8) Cyber Forensic Auditing

Purpose: To present technical evidence in legal proceedings.

Main Applications: It is primarily used to ensure that expert reports are accepted as legal evidence in court.

In the Republic of Uzbekistan, only the first type of expertise mentioned above is used more frequently, while most others are not applied. Even when expertise is utilized, it is in the form or content of a court computer-technical (digital forensic) expertise. However, in the practice and history of investigation, prosecution, and courts in Uzbekistan, cyber forensic auditing has never been applied, and its nature is still unknown to them.

It is known that, according to Article 81 of the Criminal Procedure Code, digital evidence is included among the types of evidence. Article 951 of the CPC provides for the inadmissibility of evidence obtained from unknown sources or from sources that cannot be identified during the investigation of a criminal case.

In practice, almost all physical items, objects, or the electronic (digital) data and digital evidence they contain are collected by an investigator, prosecutor, or court report and then handed over to a specialist or expert. However, no expertise is conducted to determine whether procedural or technical errors occurred during the collection of such evidence. This, in turn, can affect processes related to determining the method, time, and circumstances of a cybercrime, as different information may arise regarding the source and creation history of the data. For example, information in a computer system may have been created at a different time, copied to another device, or recorded at a different time in the report, potentially showing a creation time that does not match the actual time of the cybercrime. This poses a risk of disconnecting the cybercriminal from the timing of the offense. For this reason, assigning cyber forensic auditing (Cyber Forensic Auditing) is of critical importance.

Furthermore, identifying processes related to artificial intelligence requires extensive knowledge and reasoning.

For this reason, it is appropriate to reconsider the specialization of court computer-technical expertise and to establish a unified list of expertise conducted in the field of information and communication technologies, taking into account the specific characteristics of this field. To accomplish this task, based on the unique features of the field and its developing technologies, it is proposed to assign expertise for cybercrimes by dividing it into the following types:

- Telecommunication Network Expertise

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

- Telecommunication Infrastructure Expertise
- Information Systems and Computer Data Expertise
- Software and Application Expertise
- Cryptographic Expertise
- Communication Coverage and Quality Expertise
- Cyber Forensic Auditing.

In this framework:

- Telecommunication Network Expertise is conducted for cybercrimes committed using or within telecommunication or Internet networks, in accordance with the Criminal Code;
- Information Systems and Computer Data Expertise focuses on information systems, including user servers, databases, devices, files, information, and other data, covering aspects such as data recovery, creation time, purpose, functions, and tasks;
- Cryptographic Expertise deals with the encryption of computer data and software;
- Communication Coverage and Quality Expertise determines the coverage area and quality of wired or wireless communications;
- Software and Application Expertise provides information about various software and applications, identifies the functions of malicious viruses, and assesses the risk level of their execution;
- Telecommunication Infrastructure Expertise involves a comprehensive study of all the above aspects.
- Cyber Forensic Expertise determines the admissibility of computer data and other evidence related to cybercrimes;

Computer-technical (digital forensic) expertise, mobile device expertise, network forensic expertise, data recovery expertise, malware analysis, and email and personal communication expertise are considered as integral components of the above-mentioned expertise.

Why is it appropriate to classify the types of expertise applied to cybercrimes as described above? The reason lies in the technical nature of information and communication technologies. Negative events occurring within or between telecommunication infrastructures today manifest as cybercrimes. A cybercrime cannot occur without telecommunication. Every cybercrime requires some form of communication. For example, if a malicious program on a user's device, such as a flash drive, connects to a computer system, it can damage the system or its data. However, this crime occurs specifically because the malicious program enters the computer system via telecommunication. Therefore, since a cybercrime is also a technical crime, and the telecommunication sector constitutes the foundation of the information and communication field, classifying the types of expertise related to cybercrimes based on this sector is technically justified.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

It should be emphasized that, based on the specific characteristics of information and communication technologies, the above-mentioned types of expertise could be further expanded. However, classifying them according to their specific attributes is of crucial importance. Therefore, it is not an exaggeration to say that the time has come to classify the types of expertise related to cybercrimes in this manner and to broaden the name and scope of judicial computer-technical expertise. This is because cybercrimes are directly linked to the development of information and communication technologies.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

References

Government of the Republic of Uzbekistan. (2025, May 13). *[Official regulatory document]*. https://api-portal.gov.uz/uploads/147/2025/05/13/df766256-5068-f1ab-3d42-0b3195f31c82_media_.pdf

Ministerstvo informatsionnykh tekhnologiy i kommunikatsiy Respubliki Uzbekistan. (2020, June 30). *Telekommunikatsiya xizmatlarini ko'rsatish qoidalari* [Telecommunications services provision rules]. Lex.uz – National legal information database of the Republic of Uzbekistan.

O'zbekiston Respublikasi. (2024, December 27). *"Telekommunikatsiyalar to'g'risida" URQ–1015-son Qonuni* [Law on telecommunications]. Lex.uz – National legal information database of the Republic of Uzbekistan.

O'zbekiston Respublikasi Davlat xavfsizlik xizmati. (2024, October 15). *"Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o'tkazish tartibi to'g'risida"gi Nizom* [Regulation on cybersecurity compliance expertise]. Lex.uz – National legal information database of the Republic of Uzbekistan.

Prezident of the Republic of Uzbekistan. (2025, January 22). *PQ–17 decree on measures for the introduction of a professional training system in combating crimes committed using digital technologies*. Lex.uz – National legal information database of the Republic of Uzbekistan.

Rohde & Schwarz. (n.d.). *5G network evaluation for U.S. network operators* [Web article]. https://www.rohde-schwarz.com/us/solutions/critical-infrastructure/mobile-network-testing/stories-insights/article-qoe-5g-network-evaluation-for-us-network-operators_254564.html

Rohde & Schwarz. (n.d.). *Benchmarking campaign – Bell Canada Q4 2021* [Technical certificate]. https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/Certificate-MNT-Bell-Canada-Q4-2021-Benchmarking-Campaign.pdf

Rohde & Schwarz. (n.d.). *ECOI commissions Rohde & Schwarz to benchmark Icelandic mobile network quality with ETSI methodology* [Press release]. https://www.rohde-schwarz.com/us/about/news-press/all-news/ecoi-commissions-rohde-schwarz-to-benchmark-icelandic-mobile-network-quality-with-etsi-methodology-press-release-detailpage_229356-1451264.html

Rohde & Schwarz. (n.d.). *Rohde & Schwarz and Telia unlock Estonia's full potential with comprehensive mobile network benchmarking campaign* [Press release]. https://www.rohde-schwarz.com/us/about/news-press/all-news/rohde-schwarz-and-telia-unlock-estonia-s-full-potential-with-comprehensive-mobile-network-benchmarking-campaign-press-release-detailpage_229356-1533252.html

Rohde & Schwarz. (n.d.). *Secure web browser: Cybersecurity solutions*. https://www.rohde-schwarz.com/fi/products/cybersecurity/secure-web-browser_232366.html

Rohde & Schwarz. (n.d.). *TSMA brochure*. https://cdn.rohde-schwarz.com/au/TSMA_bro_en_3607-1513-12_v0900.pdf

Rohde & Schwarz. (n.d.). *TS-TSME6 brochure*. https://assets-us-01.kc-usercontent.com/ecb176a6-5a2e-0000-8943-84491e5fc8d1/e502ed4d-81e4-4334-ac7a-3ec80d0f2821/RS-TSME6_brochure.pdf

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677

Samsung. (n.d.). *Galaxy S21+ 5G*. https://www.samsung.com/ru/smartphones/galaxy-s21-5g/buy/?modelCode=SM-G996BZVDSER

ShareTechnote. (n.d.). *Handbook of LTE MDT (Minimization of Drive Test)*. https://www.sharetechnote.com/html/Handbook_LTE_MDT.html

Systemics-PAB. (2017). *Systemics-PAB brochure*. https://www.syspab.eu/wp-content/uploads/2017/01/Systemics-PAB_bro_en_5214-6774-32_v0102_final.pdf

TAdviser. (n.d.). *PCTEL SeeGull IBflex scanning receiver*. https://www.tadviser.ru/index.php/Продукт:PCTEL_SeeGull_IBflex_Сканирующий_приёмник

Uzbekistan Ministry of Internal Affairs, Prosecutor General's Office, & National Projects Agency. (2024, December 25). *Guidelines on the procedure for seizure, storage, and transfer of crypto-assets identified during pre-investigation and criminal investigations* (Reg. No. 3591). Lex.uz – National legal information database of the Republic of Uzbekistan.

Revista YUYAY, Estrategias, Metodologías & Didácticas Educativas ISSN: 2953-6685 e-ISSN: 2953-6677