CIRCUMSTANCES TO BE PROVEN IN CRIMES COMMITTED THROUGH THE USE OF INFORMATION TECHNOLOGIES

Aghayev Sayyad Aghamir oglu[1], **PhD**
Police Academy of the Ministry of Internal Affairs, Azerbaijan

ABSTRACT

Purpose: This article aims to explore the key legal and technical issues in proving crimes committed using information technologies, analyze the system of facts to be proven in such crimes, and propose effective approaches to address current challenges.

Design/Methods/Approach: Using the comparative legal method, the article analyzes the legislation of the Republic of Azerbaijan alongside international norms and best practices. The legal status of digital evidence and its role in the investigation process are examined. Practical court decisions are also reviewed to assess the current situation.

Findings: Research shows that normative-legal mechanisms for collecting and analyzing digital evidence are still under development. The findings suggest a need for new approaches to ensure the reliability and legality of information technology-related evidence submitted to courts in such crimes.

Originality/Value: The novelty of the research lies in the author's presentation of a unified conceptual approach to the system of facts to be proven in crimes committed using information technologies. The author also offers practical proposals for improving national legislation in this field, creating real application opportunities for law enforcement agencies and courts.

Keywords: digital evidence, information technologies, cybercrime, proving, investigation.

About the author

Aghayev Sayyad Aghamir oglu, Colonel of Police, PhD in Law, is the Head of the Department of Criminal Procedure, Police Academy of the Ministry of Internal Affairs, Azerbaijan.

INTRODUCTION

In the modern era of accelerated globalization, one of the most characteristic trends is the process of digitalization, which almost entirely encompasses our lives through the active application of modern information and telecommunication technologies, as well as digital devices and tools. This includes the development and expansion of artificial intelligence engineering, biometric identification, "cloud" services, cognitive technologies, online banking, and other services, among others. The Okinawa Charter on the Global Information Society, adopted on June 22, 2000, explicitly emphasizes that information and communication technologies are among the most significant factors shaping society in the 21st century. These technologies have a revolutionary impact on people's lifestyles, their education

1 seyyad.agamir@gmail.com

and work, as well as on the interactive cooperation between governments and civil society [20, pp. 51–56; 21, p. 3].

Modern civilization has entered the era of global digitalization, a period characterized by the fundamental transformation of all spheres of human activity. People use the internet on a daily basis, communicate through social networks, establish connections, and pay for many services and goods using digital means. At the same time, alongside all the positive and progressive aspects of digital technologies, it should be noted that they also serve as a source of certain threats and risks [115, p. 26].

According to international research, in 2024 cybercrime reached an extremely dangerous scale, with the global damage caused by this type of crime amounting to 9.5 trillion USD. Experts predict that the financial losses resulting from cybercrime will continue to grow exponentially, following a geometric progression. Research by the International Monetary Fund (IMF) forecasts that by 2027 the damage inflicted by cybercrime worldwide will reach 23 trillion USD. These figures surpass the damages caused by natural disasters and indicate that cybercrime is becoming a more profitable form of criminal activity than global drug trafficking [9;10;11].

It is rightly noted that the use of high technologies for criminal purposes has led to serious challenges for law worldwide, including substantive, procedural, and international law. As in other countries, in Azerbaijan as well, certain criminal-law aspects of the use of artificial intelligence and the most modern digital technologies are not adequately regulated in legislation, while gaps remain in the criminal-procedural framework [30, p. 65].

Judicial-investigative practice and official statistical data show that, starting from the second decade of the 21st century, there has been a significant increase in crimes committed through the use of information and telecommunication technologies. Such growth is particularly observed in crimes against property and in the illicit circulation of narcotic drugs and psychotropic substances committed by means of these technologies. The use of information technologies in the commission of crimes often eliminates direct contact between the offender and the victim, which in turn complicates the process of identifying the perpetrator [27, p. 126].

In recent years, among the more widespread types of cybercrimes, particular mention should be made of cyber fraud, extortion through the use of cyber means, cyber espionage, cyber theft, online drug trafficking, cyberterrorism and cyber extremism, cyberbullying, and others [29, p. 8]. R. Sh. Mahmudov rightly points out that "criminal elements actively make use of the internet's opportunities; terrorist organizations conduct the advertising and sale of narcotics and weapons, pornographic materials are disseminated, and racist, nationalist, and extremist-oriented websites are widely spread across the global network. The high social danger of crimes in this virtual space is of a transnational nature. In other words, the consequences of such activities affect large groups of people and various countries" [6, pp. 59–60].

The analysis of the practice of law enforcement agencies of the Republic of Azerbaijan, particularly the preliminary investigative bodies, shows that in recent years information technologies have been increasingly used for the commission of crimes related to the illicit trafficking of narcotic drugs and psychotropic substances (advertising, promotion, and sale of narcotics). It can be stated that cyberspace has become one of the most difficult and complex links in the chain of detecting crimes connected with the illegal circulation of narcotic drugs and psychotropic substances. This is because it is extremely challenging to identify and bring to justice the individuals who commit such criminal acts through contactless methods.

According to official statistics, in the Republic of Azerbaijan, 2,558 crimes were registered in 2023 and 2,057 crimes in 2024 by the Ministry of Internal Affairs and the Prosecutor's Office through the use

of information technologies. Of these, 1,027 crimes were solved in 2023, and 1,129 crimes remained unsolved in 2024. Thus, the detection rate amounted to 49.8% in 2023 and 51.8% in 2024.

In January–June 2025, a total of 1,046 crimes committed using information technologies were registered across the republic, of which 549 were solved and 321 remained unsolved. The detection rate amounted to 65.0%.

Each type of crime has its own specific characteristics and therefore requires a particular approach to a complex of criminalistic and procedural matters, including the detection and investigation of the crime, determination of the circumstances to be proven, identification and recording of digital traces, collection and analysis of digital evidence, and the organization and conduct of individual investigative actions – particularly urgent investigative measures – and digital forensic examinations.

The primary characteristic that defines a particular legal violation as a cybercrime is that it is committed through the use of computers, network technologies, digital technical devices and tools, or malicious software [12, p. 7; 13, p. 81].

The relevance of this research lies in examining the distinctive features of evidence in crimes committed through information technologies, which differ significantly from traditional forms of legal violations. The digital nature of traces of criminal activity, their volatility, the risk of loss or destruction, and the high probability of alteration present fundamentally new challenges to investigative and judicial bodies worldwide, particularly to courts. For this reason, studying the problems that arise in the process of proving crimes committed through the use of information technologies during detection and investigation is of great significance.

RESEARCH

Crimes committed through the use of information technologies represent a qualitatively new type of unlawful activity, characterized by a number of specific features that significantly affect the process of proving them. In accordance with international conventions, these crimes are socially dangerous acts committed through the use of information technologies, information systems, and information and telecommunication networks.

As is known, on December 24, 2024, the United Nations adopted a new, more comprehensive, and unified Convention against Cybercrime.

The Convention covers a broad scope, including combating crimes committed through information and communication technology systems and strengthening international cooperation for the exchange of electronic evidence in serious crimes.

The positive aspects of the new Convention can be highlighted as follows:

International cooperation – the Convention facilitates joint work of law enforcement agencies by strengthening relations between countries in the fight against cybercrime; legislative harmonization – the Convention is aimed at unifying the national legislations of the participating states, which allows the development of common approaches to countering cybercrimes; effective information exchange – the Convention establishes a framework for the exchange of electronic evidence in relation to serious cybercrimes, thereby simplifying and accelerating the investigation of these categories of crimes; unified standards – the Convention helps in the development of uniform criminal-law policies and standards for combating cybercrime.

At the same time, the ratification and entry into force of the Convention may create challenges arising from the existing diversity in national legal systems and technical infrastructures of the states. Furthermore, the expansion of powers in the exchange of electronic information and obtaining electronic data may give rise to issues related to confidentiality and the protection of privacy. Another factor that could complicate the ratification and implementation of the universal treaty is that countries may have differing perspectives and approaches regarding cybersecurity, sovereignty, and information freedom.

The UN Convention against Cybercrime (Article 2) provides definitions for a number of terms, including "information and communication system," "electronic data," "traffic data," "content data," "personal data," and others, clarifying their essence and meaning. For example, according to paragraph (b) of Article 2 of the Convention, "electronic data" means the representation of facts, information, or concepts in a form suitable for processing by an information and communication system. Electronic data also include a program that enables the information and communication system to perform a particular function as a result of operations or commands.

Chapter 2 of the Convention is titled "Criminalization", and it emphasizes the obligation of the participating states to classify the following acts as criminal offenses under their national legislation: Illegal access to an information and communication system or any part thereof with the intent to obtain electronic data (Article 7); Illegal interception of electronic data (Article 8);

Intentional and unlawful damage, deletion, deterioration, alteration, or blocking of electronic data (Article 9); intentional and unlawful interference with the functioning of an information and communication system by inputting, transmitting, damaging, deleting, deteriorating, altering, or blocking electronic data, causing serious disruption (Article 10); intentional and unlawful use of devices, including software specifically designed or adapted for committing any offense, for obtaining, producing, selling, procuring for use, disseminating, or otherwise making available passwords, access codes, electronic signatures, or analogous data that allow unauthorized access to any information and communication system or part thereof (Article 11); intentional and unlawful input, alteration, deletion, or blocking of electronic data, leading to the creation of non-authentic data and intended to be considered authentic for legal purposes (Article 12); computer-related fraud or theft using an information and communication system (Article 13); distribution of material online involving sexual abuse or exploitation of children (Article 14); deceptive or trust-inducing conduct aimed at committing sexual offenses against children (Article 15); distribution of intimate images of a person without their consent (Article 16); money laundering, i.e., the legalization of proceeds obtained from criminal activity (Article 17).

As can be seen, compared to the Budapest Convention of 2001, the Convention against Cybercrime adopted in 2024 has significantly expanded the range of acts that must be criminalized.

The characteristics of traces of criminal activity in the digital environment fundamentally distinguish cybercrimes from traditional forms of criminal behavior. Digital traces are characterized by high variability, the potential for rapid destruction or modification, and the ability to be automatically replicated and disseminated. Unlike physical traces, digital traces can simultaneously exist across various technical devices and geographic locations [18, p. 114].

Currently, behind the organization and commission of crimes carried out through the use of computer technologies, electronic information carriers, and information and telecommunication networks, including the internet, are primarily transnational organized groups and criminal organizations specializing in the illegal circulation of narcotics, extremist and terrorist activities, and the commission of crimes against property through the use of these technologies and networks [16, p. 3].

The Internet also provides new opportunities that facilitate the commission of various crimes against property, public safety, morality, and other interests. Among these, the following can be highlighted:

1. Anonymity – the Internet allows criminals to commit unlawful acts while maintaining their anonymity. Offenders use networks such as Tor and VPNs, fake accounts, and stolen identifiers to conceal their identity and ensure anonymity, which complicates their detection and the prosecution of those responsible.

2. Global reach – the Internet has no geographic boundaries, enabling criminals to carry out illegal activities from anywhere in the world.

3. Technical complexity – many cybercrimes require specialized technical knowledge for their detection and investigation.

4. Scale – the extremely large number of users and transactions online significantly complicates monitoring of illicit activities and detecting criminal conduct.

5. Accessibility of the object of criminal intent – the location of the intended target is practically irrelevant for committing the act; the availability of favorable conditions for preparation and execution of the crime means that planning and committing offenses can be done from virtually any computer with internet access.

6. Systematic latency (hyper-latency) – another feature of cybercrime is its hidden nature. It is practically impossible to determine the real scale of cybercrime or measure it quantitatively.

7. Transnational nature of cybercrimes – the cross-border character of these offenses creates additional challenges in the process of proving them. For example, the perpetrator may be in one country, the servers used in another, and the victims in a third country.

This, in turn, dictates the necessity of international cooperation but creates jurisdictional challenges when collecting and securing digital evidence.

8. Incomplete development of laws and other normative-legal acts – in many countries, existing legislation does not allow for effective counteraction against new types and forms of cybercrimes, primarily because cybercrimes are in a constant state of evolution and change. As a result, many perpetrators of these acts can evade criminal liability and remain unpunished.

9. Underestimation of risks – many Internet users fail to properly assess cybersecurity risks and do not take the necessary measures for cyber protection. This ultimately makes them easy targets for criminals [14, p. 11–12; 29, p. 11].

Taken together, these attributive features and characteristics provide a clear understanding that combating crimes committed through the use of information and communication technologies must be carried out comprehensively with the support of criminal law, criminological, criminalistic, and procedural tools. They also highlight the necessity of fundamentally revising scientific and practical approaches to identifying the problem and determining ways to address it [21, p. 10–11].

As noted earlier, the development of information technologies and their penetration into all spheres of public life significantly affect the nature of modern criminality. Economic and financial crimes, as well as offenses against property, public safety, morality, and other interests, are increasingly being committed through the use of various high-tech means. This substantially complicates their detection and the process of proving them. Under these circumstances, the identification, seizure, examination, and evaluation of digital evidence and other electronic information – such as electronic documents, digitally significant criminal data, and transaction-related information – becomes particularly important during the investigation of crimes committed through the use of information technologies [17, p. 38].

It should be noted that the Criminal Code of the Republic of Azerbaijan (CC RA) includes provisions on liability for cybercrimes in Chapter 30, titled "Cybercrimes." This chapter establishes criminal liability for acts such as unauthorized access to a computer system (Article 271), illegal acquisition of computer data (Article 272), unauthorized interference with a computer system or computer data (Article 273), circulation of tools prepared for committing cybercrimes (Article 273-1), and falsification of computer data (Article 273-2) [3, p. 40].

The use of Internet information resources, information and telecommunication networks, electronic data carriers, or information technologies in the commission of a crime is recognized as an aggravating factor. Among such criminal acts are theft (Article 177.2.3-1), acquisition, possession, shipment, or sale of narcotic drugs, psychotropic substances, or their precursors (Article 234.4.4), and organization or conduct of gambling activities (Article 244-1.2.2), among others. In addition, under the national criminal legislation, liability is also established for acts such as defamation or insult using fake usernames, profiles, or accounts on Internet information resources (Article 148-1), and illegal organization of international telecommunication services through connection to a telecommunication network (Article 233-4) [7, p. 55–57; 8, p. 18–19].

A portion of the numerous challenges encountered in the practical investigation of this category of crimes is determined by the large number of investigative actions that must be carried out, the complexity of conducting judicial examinations, and the specific characteristics of the evidentiary process. During the investigation of crimes committed through the use of information and communication technologies, particularly artificial intelligence, it becomes necessary to identify the circumstances to be proven as stipulated by Article 139 of the Criminal Procedure Code of the Republic of Azerbaijan (CCP RA).

According to Article 139 of the Criminal Procedure Code of the Republic of Azerbaijan (CCP RA), the circumstances to be proven include the fact and circumstances of the commission of the criminal incident; the connection of the suspect or accused person to the criminal act; the elements of the crime as defined by the criminal law; the culpability of the person in committing the act; mitigating and aggravating circumstances; and the circumstances relied upon by a participant in the criminal process or another person involved in the proceedings to substantiate their claim. The circumstances established in this article represent the general scope of matters included in the subject of proof [1, p. 301–302].

At the same time, it is clear that when determining the scope of circumstances to be proven in each criminal case, one cannot rely solely on the provisions of Article 139 of the CCP RA [2, p. 415]. Doctor of Law, Professor M.Ə. Cəfərquliyev correctly notes that "as can be seen from the content of Article 139 of the CCP, the law defines the subject of proof in general terms." The author emphasizes that this is natural, stating that "it is impossible to provide a fully comprehensive list of circumstances to be determined in advance for a case. During the investigation of a criminal case, the determination of which facts are of significant importance or which circumstances should be directly proven depends on the specific characteristics of the case under investigation" [4, p. 242–243].

The authors of the national commentary indicate the necessity of including the following circumstances in the list of matters to be proven: the consequences of the crime, namely the volume and nature of the damage caused; circumstances eliminating the criminal nature of the act; grounds for exemption from criminal liability; whether the accused person should be punished for the committed act; circumstances characterizing the personality of the accused; and the reasons and conditions that contributed to the commission of the crime [2, p. 415].

It should also be noted that, although traditional elements are included in the subject of proof for cases involving crimes committed through the use of information technologies, their content increasingly reflects the digital nature of criminal activity and the specific characteristics arising from the commission of offenses in cyberspace and virtual environments.

In cases involving crimes committed through the use of information technologies, in addition to the general circumstances to be proven, it is essential to identify and establish the following:

Technical and electronic information demonstrating that the crime was committed using information technologies, social networks, the Internet, mobile devices, or other digital tools;

Determination of whether computer data served as the object or instrument of the crime;

Identification of which computers, servers, or networks were used, by whom, and during what periods; establishing what actions and operations were performed on these devices; determining whether the devices belong to the perpetrator, the victim, or a third party; how and for what purpose the perpetrator used information technologies and digital tools, including how they accessed the victim's data or misappropriated funds; assessment of the suspect's or accused person's ability to use information technologies and their habits in using modern digital devices, which may involve investigative actions such as investigative experiments; identification of the software used in committing cybercrimes, how it was obtained and applied, and the actions and operations performed with computer data; functional purpose of malicious software used in the commission of the crime, and at which stage of the criminal activity viruses, trojans, password-cracking tools, or other malware were employed; determination of which actions and operations (addition, deletion, modification, blocking) were carried out on computer data, or how the integrity of network resources was compromised; establishing the ownership of the devices, electronic data, and information stored on computers or other digital media; identification of the nature of personal information disseminated via the Internet, such as defamation, pornography, or material promoting national, racial, or other forms of hatred and hostility; in crimes against property or in the economic sector, determination of how funds were misappropriated or how illegal interference with bank accounts was carried out, specifying which computers, digital devices, and software tools were used, and other related circumstances.

In cases concerning the sale of narcotics through the use of information and telecommunication technologies, the circumstances to be proven may also include the following:

Establishing the use of the Internet, mobile communication devices, messengers, social networks, or other digital platforms during the process of selling narcotic substances; determining how exactly information technologies were used in committing narcotics-related crimes, including searching for buyers, coordinating the actions of accomplices, posting advertisements for sale, performing calculations, or organizing delivery; clarifying how narcotics were delivered to buyers; based on analysis of messenger correspondence, calls, and notifications, establishing agreements on sales and information about the locations where narcotics were placed; identifying the use of IP addresses, mobile devices, digital information, and payment systems to track the narcotics transfer chain; determining the use of information and telecommunication technologies, such as the Internet, social networks, or messengers, for online sales, promotion, advertisement, or encouragement of narcotics consumption; obtaining information about transactions conducted via online services, as well as correspondence in messengers.

In these and other cases, investigative and inquiry bodies, with the assistance of experts, must collect, record, preserve, and analyze digital data (such as logs, transaction records, Internet traffic, etc.).

It is necessary to determine the use of specific information technologies and digital tools as instruments and means of committing the crime, the characteristics and functional purpose of these tech-

nical-digital devices and tools, the content of the information obtained, and the technical aspects of how the act was carried out.

Since digital evidence forms the core of the evidentiary base in this category of crimes, digital evidence refers to information in electronic form that is significant for establishing the circumstances to be proven. Digital evidence can be classified as follows: data stored on physical media; information transmitted via telecommunication networks; metadata characterizing the conditions of file creation, modification, and transmission; system event logs, IP addresses, user activity logs, and similar records [18, p. 115].

At the same time, in the criminal procedure legislation of many countries, digital (electronic) evidence has not been formally included among the types of evidence, and the essence and content of digital evidence and digital (electronic) documents have not been defined at the procedural law level. For example, the Criminal Procedure Code of the Russian Federation (Articles 74 and 84) does not explicitly provide for the possibility of using electronic documents as evidence in criminal cases during the preliminary investigation stage [27, p. 127–128].

Article 124.1 of the Criminal Procedure Code of the Republic of Azerbaijan (AR CPC) states that "reliable evidence (information, documents, objects) obtained by the court or the parties to the criminal process shall be considered evidence in criminal prosecution."

According to Article 124.2 of the CPC, the statements of the suspect, the accused, and the victim, as well as witnesses, expert opinions, physical evidence, protocols of investigative and court actions, and other documents are recognized as evidence in criminal proceedings. Article 135.1 of the AR CPC defines the concept of a document, specifying that any paper, electronic, or other medium that contains information relevant to criminal prosecution, represented in the form of letters, numbers, graphics, or other symbols, shall be considered a document.

Only in Article 1 of the Law of the Republic of Azerbaijan "On Electronic Signature and Electronic Document", dated March 9, 2004, is an electronic document defined as "a document presented in electronic form for use in an information system and confirmed by an electronic signature."

It should be noted that, unlike many post-Soviet countries, Uzbekistan has established the main provisions regarding the use of electronic (digital) evidence in its Criminal Procedure Code and the Law "On Electronic Document Circulation." According to the legislation of this country, electronic documents, records, information, and other digital data, provided that the requirements for their registration, seizure, and examination are observed, can be accepted as evidence in criminal cases. Digital (electronic) evidence is defined as information in electronic-digital form that is significant for establishing the circumstances of a criminal case. This type of evidence may include electronic documents (text files, spreadsheets, graphics, etc.); audio and video recordings; information on electronic payments and financial transactions; data extracted from electronic devices (smartphones, computers, servers, etc.); and information from transmission networks and social media [17, p. 38–39].

Determining the method of committing a crime also holds particular significance [19, p. 51–56]. "The method of committing a crime is the specific technique or approach used by a person while carrying out a socially dangerous act. Regardless of whether the method is included in the elements of the crime, it must be clarified in each criminal prosecution" [2, p. 416–417].

In the digital environment, methods of committing crimes may include: the use of specialized software; exploiting existing vulnerabilities and flaws in information systems; application of social engineering techniques; use of artificial intelligence, particularly network technologies; and other similar methods.

Analysis of statistical data indicates that a significant portion of crimes such as theft, fraud, drug trafficking, and others are increasingly committed using "social engineering" methods and techniques. A.N. Ibrahimova notes in this regard: "Social engineering involves interacting with people to collect information from them. One of its main elements is deceiving the user by employing fake profiles (under a different name or representing a fictitious company, organization, etc.), virtual friendships, or acquaintances. Its primary goal is to collect information by exploiting trust gained through acquaintance, virtual friendship, or any other reliable source. Therefore, users must pay special attention to the addresses of incoming messages. Even a single altered character can create a fake website" [5, p. 8–9].

The technique of "social engineering" aimed at obtaining confidential information is commonly referred to in the literature and among specialists as phishing.

Phishing is a type of internet fraud in which personal user information—such as logins, passwords, mobile phone numbers, bank card numbers, and so on—is obtained by sending mass electronic messages, such as emails or text notifications, through email or other digital telecommunication channels. Unauthorized emails often contain links to websites specifically created for phishing, where users are prompted to enter their identifiers and passwords [24, p. 131]. Typically, criminals first send a fake notification to the victim via email or SMS, disguised as an official message from a bank, requesting that certain information be "verified" or that certain actions be performed. Subsequently, the criminal obtains the victim's personal information, account details, or card number and password, resulting in the theft of funds from the victim's bank account. Another method involves a criminal calling the cardholder, pretending to be a bank employee, and claiming that, due to a problem with the bank system or the victim's account, the password must be provided; otherwise, the card will be blocked. Yet another approach is when the criminal, posing as a bank employee, gives false information about the victim's eligibility for a loan and later extracts a certain amount of money under the pretext of insurance payments or other excuses. An additional online or internet fraud method involves posting fake offers about services or goods on public websites, initially requiring the transfer of a certain amount of money. These funds are, of course, transferred to the offender's bank account [15, p. 27–28].

The algorithm (method) of committing drug-related crimes using information technologies can be described as follows: criminals create a website and post an advertisement for the sale of drugs on that site; they contact potential buyers via the specified electronic address or messaging apps to confirm the buyer's intention to purchase; the order and payment agreement is reached remotely; and after the payment is made, information about the location of the drugs is sent via SMS, email, messaging apps, WhatsApp, or other social networks. For example, the scheme of drug distribution is characterized by high adaptability, which is determined by the following factors: the creation of websites on platforms that are difficult to block, the use of networks of bots as administrators, and the fact that participants in committing the crime do not know each other [25, p. 148].

In the specialized literature, it is noted that the use of artificial intelligence (AI) for criminal purposes can be considered a method of committing a crime. However, it should also be noted that this has not yet been codified at the legislative level. Among procedural scholars and law enforcement officers, there is no unified position on this issue. Some believe that in the near future AI will be regarded as an independent criminal subject, while others consider that, at present, AI should be assessed as a method for committing a crime [30, p. 66].

The investigation of crimes committed using information technologies is characterized by significant criminalistic and procedural features, which are determined by the specifics of the digital environment, i.e., cyberspace, and by the necessity of applying special technical and hardware-software tools for the collection of evidence.

According to Article 143 of the CPC of the Republic of Azerbaijan, the collection of evidence is carried out during preliminary investigation and court proceedings through procedural actions such as interrogation, confrontation, seizure, search, inspection, expert examination, presentation for identification, and other procedural measures.

One of the most effective tools for obtaining and collecting digital evidence is the OSINT method (sometimes also referred to as Internet intelligence). The use of open information sources, including the Internet, social media, open databases, and other resources, provides investigators and experts with additional opportunities to collect evidentiary information in cases under investigation. The application of OSINT methods allows filling gaps in traditional sources of evidence and helps to reveal digital traces of criminal activity that carry criminalistic significance.

Considering that OSINT methods consist of a set of analytical techniques aimed at the collection, processing, and analysis of information from publicly accessible sources, it can be noted that their application in the context of cybercrime investigation significantly expands the capabilities of investigators and experts when conducting actions aimed at establishing the circumstances of the case. In this process, the use of Internet resources (websites, social networks, forums, blogs), open databases and registries, and mass media, as well as specialized information-analytical resources, enables the collection of various digital evidence, including electronic documents and correspondence, financial transactions and payments, data stored on mobile devices and computers, and information from social networks and other online sources.

It should also be noted that digital evidence obtained through OSINT methods requires strict compliance with procedural rules during its recording and collection. This means that during the search, collection, and extraction of copies of information, the integrity and immutability of digital evidence must be ensured, and the seizure and packaging of information carriers must be carried out in accordance with procedural regulations and properly documented.

All of these measures are essential to ensure the admissibility and reliability of digital evidence [17, p. 38–39].

The search and seizure of computer-technical devices, including digital devices, and the electronic information they contain that has forensic significance, require strict adherence to procedural rules to ensure the preservation and integrity of digital evidence. The main requirements include: immediately disconnecting the devices from the power supply to prevent remote deletion or destruction of data; creating exact copies of the information carriers; documenting all technical actions and operations in accordance with procedural legislation; ensuring the immutability of the original information carriers. A decisive factor is also the timing of these investigative actions, since digital traces can be destroyed within seconds. This necessitates rapid response from law enforcement agencies [18, p. 116].

In response to the dangers, threats, and challenges posed by cybercrime, there is a significant need for a specialized field that enables the detection and investigation of such crimes, as well as the identification, preservation, analysis, and presentation of digital traces of criminal activity. Currently, in the doctrines, judicial-investigative, and expert practices of post-Soviet countries, this field is recognized as computer-technical expertise (digital expertise) within forensics or digital criminalistics [22, p. 196].

The term "forensics" originates from the Latin word *foren* – meaning "speech before the forum," i.e., a presentation in court. This term has entered our language from the English word *forensic* or the abbreviated form forensic science and refers to the science of evidence examination, meaning "judicial science." In short, forensic computer criminalistics is the science of studying digital evidence and the mechanisms of the formation of digital traces, as well as the methods, techniques, and digital technical-software tools and technologies for their detection, analysis, and evaluation [26, p. 11].

Forensics encompasses a wide range of methods and technologies aimed at the collection, analysis, and presentation of digital evidence in court. This field of knowledge integrates elements of criminalistics, information security, and both substantive and procedural law [22, p. 196; 31, p. 235].

The purpose of digital criminalistics is to collect, record, preserve, analyze, and present evidence related to the issues that need to be resolved. From a technical perspective, digital criminalistics helps determine what has occurred within an information-computer system and networks, as well as uncover the causes of system intrusions, identify legal violations that occurred in the system, and trace their sources.

The purpose of digital expertise (digital forensics) is to detect, identify, collect, record, preserve, restore, analyze digital data (digital traces) stored on digital media such as computers, mobile devices, and so on, and to present the results of these specialized investigations in the form of a report. In this context, digital traces refer to any information of criminalistic significance, that is, data presented in the form of electrical signals regardless of the means of storage, processing, or transmission [28, p. 73].

The main types of digital expertise can be classified as follows: software digital forensics, data digital forensics, digital network forensics, and mobile device digital forensics.

The purpose of software digital forensics is to study a set of issues related to the software installed on the computer system or other computerized digital devices submitted for investigation. This includes analyzing the software's functional purpose, properties, characteristics, algorithms, structural features, current state, and the causal relationship between the user's actions and the outcomes, among other aspects.

Data digital forensics is primarily focused on the examination of structured digital information within systems and databases in cases of cybercrimes, including crimes committed in the property and economic sectors using computer and information technologies, as well as in the judicial resolution of certain civil disputes. The purpose of digital data forensics is to obtain evidentiary digital information by searching for, detecting, analyzing, recovering, and evaluating information generated as a result of information process management programs within a computer system or created by a user. This is achieved through solving diagnostic and identification-related tasks [23, p. 526].

The main task of network forensics is the monitoring, recording, and analysis of network activity. Network data are highly dynamic and even volatile, often at risk of being lost after transmission. This means that network forensics is a proactive, specialized investigative process conducted within the framework of digital forensics.

The tasks of mobile device digital forensics include bypassing screen locks, extracting data from drones, locked devices, mobile phones, smartphones, and iPhones, reading memory cards, retrieving information from SIM cards, collecting data from messengers such as WhatsApp, Viber, Skype, and Twitter and from cloud services like Mi Cloud, Samsung Cloud, etc., as well as determining geolocation, frequently visited locations, routes, and other relevant information.

Although most national criminal procedure legislations do not formally define a specific concept of "digital evidence," courts generally admit such evidence in various categories of cases.

At the same time, procedural legislation establishes certain criteria regarding admissibility. Thus, according to Article 125.1 of the Criminal Procedure Code of the Republic of Azerbaijan (admissibility of evidence), information, documents, and other items may be accepted as evidence if there are no doubts regarding their authenticity, sources of origin, and the circumstances of their acquisition.

The main criteria for the admissibility of digital evidence include: compliance with evidence collection procedures; ensuring the integrity of data during seizure and examination; documenting the chain of

actions and operations performed with digital media; and the authorization of personnel handling the digital evidence.

Among the specific challenges that arise during the detection and investigation of cybercrimes, the following can be highlighted: the possibility of creating forged digital documents, accounts, profiles, and domain names using modern technologies; the complexity of determining the creation and modification times of files; problems with authentication of electronic notifications and digital signatures; the potential for altering file metadata, adding to or deleting data, and other operations; the use of anonymizing networks such as "Tor" or "VPN" by criminals to conceal their identity; the use of cryptocurrencies and other digital currencies in financial transactions that complicate tracking of money flows; and the application of modern encryption algorithms that practically prevent decrypting information without the key, among others.

CONCLUSION

The conducted research has made it possible to reveal a number of systemic features of cybercrimes that distinguish them from traditional forms of legal violations. Among them, the following can be highlighted:

1. The digital nature of traces of criminal activity requires the development and application of fundamentally new approaches to their collection, recording, examination, and evaluation. There is a need to adapt traditional procedural mechanisms to the realities of the digital era.

2. The characteristic features of cybercrimes, which differentiate these criminal acts from other crimes, include: anonymity; global reach; technical complexity; large scale; accessibility of the object of the criminal intent; existence of favorable conditions accompanying the preparation and commission of the crime; systematic latency, i.e., hyper-latency; transnationality; gaps in substantive and procedural legislation regulating the detection and investigation of cybercrimes, and the incomplete formation of the normative-legal framework in this field, etc.

3. The absence of norms and provisions in the majority of national procedural legislations that specifically regulate digital evidence creates legal uncertainty and significantly hinders the evidentiary process.

From this perspective, it can be considered that the adoption of the UN Convention on Cybercrime on December 24, 2024, represents a significant step toward the harmonization of international approaches and the implementation of international standards into national legislation.

The evidentiary process in cases of crimes committed using information technologies is characterized by significant features determined by the digital nature of criminal activity. It is possible to predict that the rapid growth of cybercrime will continue exponentially in the coming years. These dangerous trends make it essential to improve the evidentiary system in cases of the aforementioned categories of crimes, both at the national and international levels.

In the evidentiary process for crimes committed using information technologies, the main problem lies in the presence of certain gaps in substantive and procedural law, considering the current level of technological development. From this perspective, it is necessary to identify directions for improving the existing legislative system and to develop concrete proposals and recommendations for each of them.

Moreover, it is unequivocally important to enhance the scientific-methodological, organizational-technical, technological, and procedural foundations for investigating and examining the criminalistic aspects of crimes committed using information technologies. This particularly concerns in-

dividual investigative actions in such cases, especially urgent procedures such as on-site inspections, searches, seizures, and the conduct of digital forensic examinations.

Considering the dangerous trends observed regarding the state, structure, and dynamics of cybercrimes, as well as the emergence of crimes committed using artificial intelligence in developed countries in recent years, characterized by a steady growth rate, it is necessary that in Azerbaijan criminal liability be established at the legislative level for acts committed using information technologies, including artificial intelligence, for criminal purposes. Provisions of the Criminal Code, particularly those establishing liability for crimes against property, public safety, and morality, should include this feature as an aggravating circumstance. Similarly, provisions should be added to Article 7 of the Criminal Procedure Code clarifying the essence of terms and concepts such as "electronic (digital) evidence," "information and telecommunication technologies," "information resources," "artificial intelligence," and others. In addition, Article 124 of the Criminal Procedure Code should include "digital (electronic) evidence" as a new type of evidence.

In addition, the criminal and criminal-procedural legislation should be harmonized with the provisions of the 2024 Convention on Cybercrime, and the implementation of these provisions at the national level must be ensured.

In cases involving crimes committed using information technologies, the circumstances to be proven, as well as the collection, preservation, recording, analysis, evaluation, and presentation of digital evidence in such cases, should be developed based on tactical-criminalistic and procedural principles. The search, detection, seizure, and examination of digital traces must utilize the most advanced tactical-criminalistic methods, techniques, and tools, including hardware-software resources, the latest digital technologies, and the capabilities of artificial intelligence.

The fight against cybercrime is an international-scale issue. This is because the prevention, detection, investigation, and prosecution of crimes committed using modern information technologies cannot yield effective results at the national level alone, given the transnational and cross-border nature of the Internet.

REFERENCES

Abbasova, F.M. Criminal Procedure. Textbook. General Part. 2nd revised edition. Baku: Zardabi LTD, 2015.

Commentary on the Criminal Procedure Code of the Republic of Azerbaijan. Edited by C.H. Movsumov, B.C. Karimov, and A.H. Huseynov. Baku: Digesta Publishing, 2016.

Javadov, F., Abdullaev, Y. "Public Danger of Cybercrime in the Context of Globalization and Current Problems of Combating It." Collection of Scientific Papers on Forensic Expertise, Criminalistics, and Criminology. 2013, № 58.

Jafarquliyev, M.A. Criminal Procedure of the Republic of Azerbaijan. Textbook. Baku: Qanun, 2008.

Ibrahimova, A.N. "Cyber Threats and Their Classification." Baku University News, Social and Political Sciences Series. 2020, № 1.

Mahmudov, R.Sh. "Current Issues in Internet Regulation." Information Society Problems. 2010, №2.

Rzayeva, C., Saigli, B. "Commission of Crime by Cyber Methods as an Aggravating Circumstance." Scientific News of Police Academy. 2022, № 4(36).

Zahidov, B.S. "Legal Protection of Information Security." 2nd Republican Scientific-Practical Conference on Multidisciplinary Problems of Information Security. Baku, 2015.

Cybersecurity Ventures. “Cybercrime To Cost The World $9.5 Trillion Annually in 2024.” Cybersecurity Ventures, 2023. October 25. URL: http://cybersecurityventures.com/cybercrime-to-cost-the-9-trillion-in-2024

S. “Digital Forensics Research: The Next 10 Years.” 2010. DOI: 10.1016/j.diin.2010.05.009

SentinelOne. “Key Cyber Security Statistics for 2025.” URL: http://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

Viano, E. Cybercrime, Organized Crime, and Societal Responses: International Approaches. Springer International Publishing, 2017, p. 7.

Wall, D. “Cybercrime as a Conduit for Criminal Activity.” In Information, Technology, and the Criminal Justice System. Beverly Hills, CA: Sage Publications, 2005, p. 81.

Antropov, A.N. “Methods of Internet Traffic Anonymization and Countermeasures.” In Problems of Countering Cybercrime: Proceedings of the 2nd International Scientific-Practical Conference (Moscow, April 26, 2024), ed. O.Yu. Antonov, E.B. Khatov. Moscow: Moscow Academy of the Investigative Committee, 2024.

Baranov, A.A., Solomatina, E.A. “On Methods of Committing Crimes Using ICT.” Criminological Journal, 2023, № 3.

Grib, D.V. Criminal Liability for Theft Committed Using Information Technology under the Legislation of Belarus and Russia. PhD Dissertation, Moscow, 2021.

Konovalov, I.B. “Admissibility of OSINT Methods in Investigating Economic Crimes.” In Problems of Countering Cybercrime: Proceedings of the 2nd International Scientific-Practical Conference (Moscow, April 26, 2024), ed. O.Yu. Antonov, E.B. Khatov. Moscow: Moscow Academy of the Investigative Committee, 2024, pp. 146.

Kurmychkina, A.R. “Features of Evidence in Cases of Crimes in the ICT Sphere.” Science and Technology in the Modern World. 2025, Vol.4, № 19.

Leletova, M. V. (2022). Use of information and telecommunication technologies as a means of committing violent crimes against individuals. Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia, (2[48]), 51–56.

Okinawa Charter on Global Information Society. Diplomatic Bulletin, 2000, № 8, pp. 51–56.

Russkevich, E.A. Criminal Law and Digital Crime: Problems and Solutions. Monograph. Moscow, 2022.

Sedykh, D.Yu., Lunev, D.Yu., Wilson, N.G. “Forensics as the Science of Investigating Cybercrime.” 20th Anniversary International Youth Scientific-Practical Conference “Modern Problems of Radioelectronics and Telecommunications, RT-2024”, Sevastopol, 2024.

Sysenko, A.R., Smirnova, I.S., Timoshenko, S.E. “Problems of Conducting Judicial Computer-Technical Expertise.” Siberian Law Review, 2020, Vol.17, № 4.

Teppeev, A.A. “Methods and Problems of Qualifying Crimes Committed via the Internet.” Law and Governance, 2023, № 3.

Tretyakova, E.I. “Information Technologies in Crimes Related to Illegal Trafficking of Narcotics.” Criminalistics: Yesterday, Today, Tomorrow, 2022, Vol.23, № 3.

Fedotov, N.N. Forensics: Computer Criminalistics. Moscow: Legal World, 2007, p. 432.

Khramtsov, E.S. “Electronic Documents in Evidence for Crimes Against Property Using ICT.” Bulletin of Kazan Law Institute of the Ministry of Internal Affairs of Russia, 2024, № 1(55), pp. 125–132.

Digital Criminalistics: Textbook for Universities. Ed. Prof. K.Zh. Kapsalyamov. Astana, 2024.

Shatalov, A.S. "Development of Methodological Bases for Investigating Crimes Using Computer and Network Technologies: Problems, Prospects, and Trends." Bulletin of Siberian Law Institute of the Ministry of Internal Affairs of Russia, 2018, № 3(32), pp. 8–11.

Shmyatkova, N.V. "Features of Evidence in Crimes Against Public Safety Committed Using AI Systems." Universum: Economics and Jurisprudence, 2024, № 8(118), pp. 65–66.

Shuvaeva, M.S., Nikolaeva, A.V. "Role of Forensics in Investigating Cybercrime: Criminalistic Aspect." International Journal of Humanities and Natural Sciences, Vol. 6-2(57), 2021.