Xanımana Qafarova, Minurə Cabbarova. Kibercinayətlərin hüquqi-nəzəri xüsusiyyəti və Azərbaycanın beynəlxalq kibertəhlükəsizlik səviyyələrinə inteqrasiyası // Azərbaycan Hüquq Jurnalı. 2025 (№3), s. 104-119. DOI: 10.61638/JVDQ7012

THE LEGAL-THEORETICAL CHARACTER OF CYBERCRIME AND THE INTEGRATION OF AZERBAIJAN TO INTERNATIONAL CYBERSECURITY LEVELS

KHANIMANA GAFAROVA*, MINURA JABBAROVA**

Abstract

The article comprehensively examines the legal and theoretical essence of cybercrimes, their place in the modern criminal law system, and the impact of the rapid development of digital technologies on legal regulation. The dynamic nature of the digital environment has led to the emergence of new forms of cybercrime, more sophisticated methods of committing them, and limitations on the application of traditional legal mechanisms. In this regard, the study analyzes, from a theoretical and practical point of view, the distinctive features of cybercrime compared to classic crimes, their cross-border nature, and their impact on the process of proving guilt. The analysis shows that the existing regulatory and legal mechanisms are not fully effective in the collection, storage, and evaluation of digital evidence in real time, as well as in the investigation of cross-border cybercrimes and the application of international legal assistance mechanisms. Particular difficulties arise in connection with the uncertainty of the legal status of electronic data, the lack of clear regulatory control of the chain of custody, and the discrepancy between technical capabilities and legal requirements, which significantly complicates investigative and judicial practice. The article analyzes contemporary approaches to the legal regulation of cybercrime based on international law, in particular the provisions of the 2001 Council of Europe Convention on Cybercrime (Budapest Convention), its additional protocols, and international judicial practice. It assesses the current state of the national legislation of the Republic of Azerbaijan in this area, determines the level of its compliance with international standards, and scientifically substantiates existing regulatory gaps. The scientific novelty of the study lies in the development of an adaptive legal model aimed at improving the effectiveness of proving and investigating cybercrimes. The proposed model provides for the introduction of flexible procedural rules, the formation of specialized investigative structures with both technical and legal knowledge, the creation of special procedural mechanisms for collecting evidence in real time, and the improvement of international cooperation protocols.

* PhD in Law / Lecturer / Department of Private International law and European law / Faculty of law, Baku State University / email: xanim84.84@mail.ru

** Master of Laws / Department of Private International law and European law / Faculty of law, Baku State University / email: minara2006@mail.ru

Keywords: *cybercrime, digital evidence, legal regulation, international cooperation, cybersecurity, chain of custody, Budapest Convention, harmonization, electronic data protection.*

I. Introduction

The fast development of digital technologies has transformed the relations of information. This process has given place to the appearance of new forms of threats in the cyberspace. Therefore, determining the juridical and theoretical nature of cybercrime is of special importance. The importance of this subject is evident so much in the strategies of global security as in the national politics.

Acts like cyberattacks, data theft and digital fraud are in expansion. These threats demand the continuous update of the defence mechanisms of the States. The improvement of the juridical frame has already become one of the main orientations of modern public administration.

The Republic of Azerbaijan finds itself in an era of increasing digitalisation. This situation demands the integration of the country in the international norms of cybersecurity. The Agreement of Budapest of 2001 creates a global juridical frame in this field. The Agreement demands the member States to harmonise its national legislation. Azerbaijan also looks for strengthening the management of cyber risks adhering to these mechanisms.

This article examines the juridical foundations and theoretical aspects of cybercrime. Simultaneously, it evaluates the mechanisms created by international right. Finally, the characteristics of the process of integration of Azerbaijan in these norms have been object of scientific analysis [1, p. 28].

II. Analysis

The juridical nature of cybercrimes constitutes a new field within modern criminal law. This field differs significantly from the traditional penal structures. As the technological surroundings evolves, the juridical relations acquire a new content. The States are obliged to create a juridical frame adapted for these changes. The methods employed in cybercrimes complicate the juridical evaluation, since the acts are used to carry out secretly and by means of diverse technological means. This situation affects directly the mechanisms of evidence [4].

The cross-border nature of cybercrimes complicates the questions of jurisdiction. The commission of a crime through servers situated in different countries complicates the determination of juridical responsibility. In this case, sometimes it results in controversy in which juridical norms of the State will be applied. The cross-border surroundings also complicates the procedures of extradition and investigation. Thus, the States look for to strengthen international cooperation, since the juridical mechanisms by himself solos are not sufficient to prevent cyberattacks [11, p. 44].

There is no single definition of the concept of cybercrime in international right. Therefore, each State defines this concept using a different juridical criteria. The differences in the definitions slow down the process of juridical harmonisation. This situation has a particularly negative impact on the mechanisms of mutual juridical assistance, since the lack of a uniform recognition of the penal crimes among the States hampers cooperation. This inconsistency, on occasions, reduces the efficiency of the investigation.

The Convention of Budapest partially amends this gap. The Agreement legally classifies the main types of cybercrimes, including unauthorised access, the modification of data and the interference with computer systems. The Agreement also establishes uniform norms for the compilation of electronic evidence. These norms augment the transparency of the investigation and strengthen legal fulfillment among the States. With the adoption of these legal mechanisms, Azerbaijan is approaching its frame regulatorio to the international standards.

In the Azerbaijani legislation, cybercrimes are regulated mainly in the pertinent articles of the Penal Code. These articles foresee acts like interference with information systems, the modification of data and harms to digital property. Although the legislation considers technological development, some lagoons persist, so much technical like juridical. Therefore, it looks necessary to update the frame regulator, since the dynamics of cyberattacks requires a flexible application of the existent norms.

Table 1: Comparative Overview of Cybercrime Trends and Legal Alignment (2018–2023) [6].

Year	*Registered Cyber Incidents in Azerbaijan (CERT-AZ)**	*Main Legislative Developments*	*Alignment with the Budapest Convention*	*Notable Legal Gaps*
2018	Moderate increase in network attacks; phishing cases rising	Initial updates to digital governance policies	Partially aligned	Limited rules on electronic evidence preservation
2019	Growth in malware-related incidents; several large-scale data breaches	Amendments to Criminal Code regarding unauthorized access	Improving alignment	Gaps in cross-border cooperation procedures
2020	Sharp increase due to pandemic-related digital shift; ransomware cases appear	Expansion of national cybersecurity strategy	Moderate–High	No unified framework for digital forensics

2021	Stabilization of incident numbers; targeted attacks on critical sectors	Development of institutional structures in cybersecurity	High	Lack of procedural standards for chain-of-custody of e-evidence
2022	Significant rise in DDoS attacks; social engineering remains dominant	Strengthening of inter-agency coordination	High	Partial harmonization of terminology with international norms
2023	Advanced persistent threats (APT) increase; higher sophistication of attacks	Enhanced international cooperation initiatives	High–Very High	Need for clearer rules on real-time data collection

The table presented systematically reflects the main tendencies observed in the field of cybercrime between 2018 and 2023. The data of the table show the general dynamic statistics and the legal changes in parallel. This parallelism allows to link the development of the surroundings of cybersecurity with the legal regulation. The data are based mainly on open reports of CERT-AZ and international legal documents. Therefore, the table creates a frame of reliable information for scientific investigation.

The table shows the dynamics of cybercrime separately for every year. This approach facilitates the interannual comparison. For example, in some years one observes a strong increase of incidents, whereas in others one observes a stabilisation. These changes show how the response of Azerbaijan has strengthened to the surroundings of digital threats. The annual differences also reflect changes in the technological surroundings. In particular, the expansion of the digital surroundings during the pandemic has caused an increase of incidents.

The table also presents a chronology of the legal reforms. It details separately the regulatory measures adopted every year. This note shows the sequence of legal reforms. The dynamics of legal changes confirms the increasing importance that the State concedes to the politics of cybersecurity. The legislative updates can be compared with the rate of growth of digital threats. This comparison allows to evaluate the suitability of the legal response. Therefore, the table allows the scientific follow-up of the process of legal adaptation [2].

The level of fulfillment of the Agreement of Budapest is shown in a separate column. This column explains clearly the process of integration of Azerbaijan into international right. The evolution of the degree of fulfillment along the years indicates the level of normative harmonisation. This harmonisation applies not only to the normative requirements, but also to the institutional mechanisms [13]. The table shows that legal fulfillment is increasing gradually in this sense. This increase shows that Azerbaijan takes part more actively in global cooperation in the field of cybersecurity.

The legal gaps also are shown separately in the table. This column is important to identify clearly the problems. A clear indication of the legal gaps determines the direction of the future reforms. This approach reinforces the line "problem-analysis-result", necessary in juridical investigation. The evolution of the breaches along the years shows the evolution of the level of state regulation. This creates a solid analytical base for the conclusions and the proposal of the article [12].

As result, the table combines statistical data, legal and institutional. This combination guarantees that the scientific analysis is multidimensional. The table serves as main structure for the legal analysis and the normative evaluation that will be made in the rest of the article. Therefore, the table possesses a tall scientific value in terms of analytical, methodological and comparative investigation.

The data of the table show that the rhythm of development of cybercrime is faster than the one of legal regulation. This difference demands legal mechanisms more flexible. Since the digital surroundings changes quickly, the regulatory frame cannot remain static. Therefore, the legal system needs regulatory models innovative. The flexible legal mechanisms adapt better to the changing nature of the cyberthreats. This approach also allows deleting the regulatory gaps with main rapidity.

The table shows that the cyberthreats are acquiring a more complex form with the step of the years. This complexity is not entirely regulated by the traditional legal methods. This situation makes notable the "legal approach based in the risk". This model involves prioritising the legal measures according to the intensity of the cyberthreats. This approach allows a more efficient assignment of resources. Thus, the State can answer with greater promptness to the most critical threats. This model is useful so much at national level like cross-border.

The annual changes that are observed in the table also indicate the evolutionary process of the legal institutions. The strengthening of the institutional mechanisms is important to augment legal fulfillment. Therefore, institutional coordination has to go in in a new phase. This phase requires the establishment of a unified system of exchange of information. This system speeds up the process of investigation and facilitates the obtaining of evidence. This mechanism also strengthens cross-border cooperation [5].

The table shows that the difficulties with electronic evidence persist. These difficulties require the creation of a new procedural frame. The legal status of electronic evidence has to be determined by means of more precise norms. These

norms augment the reliability of the evidence and reduce judicial litigations. There have to be developed uniform norms for the obtaining and preservation of evidence. These norms can be used so much in national investigations as in international cooperation.

The analysis of the table shows that, in spite of the increase of international fulfillment, the national legislation has not been harmonised fully. This inconsistency generates regulatory gaps. A new model of juridical integration can be applied to delete these gaps. This model can consist of three stages: the first is terminological harmonisation; the second, the clarification of the norms of substantive penal right; and the third, the adaptation of procedural mechanisms to the international norms. This model makes that the process of harmonisation be more systematic.

In conclusion, the tendencies that are shown in the table demand the application of new juridical approaches in the fight against cybercrime. These new approaches augment the adaptability of the juridical system. At the same time, they strengthen cooperation among the State and the international partners. This allows the protection on a long-term basis of cybersecurity.

The tendencies that are shown in the table confirm that cybercrime is acquiring more complex forms. This complexity demands that the legal system adapt not only to the existent technical methods, but also to new emergent technologies. In this point, blockchain technology assumes particular importance, since it affects the structure of cyberincidents and creates new legal problems. This technology is based in the immutability of the data. This characteristic offers an advantage for the protection of legal evidence. However, it also complicates the determination of criminal elements. This difficulty generates the need of new regulatory mechanisms.

Blockchain systems have a decentralised structure. This structure aggravates even more the problems of legal jurisdiction, since the information does not remain stored in a single country. This situation hampers to determine which state's legislation determines penal responsibility. For this reason, there have to be developed jurisdictional norms special for cybercrimes related with blockchain. These norms can make more effective the cross-border legal cooperation.

Blockchain also favours the generalised use of smart contracts. Smart contracts create automated legal transactions. However, these transactions do not indicate clearly who is legally responsible. This uncertainty generates the need of a new legal regulation. There has to be established a special legal status for smart contracts. This status specifies how responsibility will apply in case of contractual breach. This step facilitates the activities so much of the technical parts as of the juridical.

Blockchain technology also facilitates the generalised use of cryptoassets. Cryptoassets are used with main frequency in criminal acts because of their anonymity. For this reason, the legal status of cryptoassets has to be clearly

defined. This status has to indicate specifically in civil right, penal and tax law. This regulation helps to prevent the financing of cyberattacks.

Blockchain technology creates new opportunities of investigation regarding the unalterability of evidence. However, it is necessary to create procedural norms for the use of these opportunities. The confirmation of electronic evidence by means of blockchain requires a new standard for the courts. This standard specifies the conditions for the admissibility of evidence. This regulation facilitates investigation and augments the transparency of the judicial procedures.

Therefore, blockchain technology adds a new stage to the juridical analysis of cybercrimes. This stage spans so much substantive right, procedural right as international right. Therefore, the legal regulation of blockchain has to be implemented systematically. This approach can delete some of the problems indicated in the table. Besides, it determines the direction of future legal reforms in the field of cybersecurity.

New approaches can be applied and less debated to accost the legal and technological emergent problems related with blockchain. These approaches differ from the classical regulatory steps and involve the parallel development of the legal surroundings and technical. In the first place, there can be created a dynamic legal mechanism for the assignment of responsibilities in decentralised systems. This mechanism can work with a model of technical measurement that determines the real degree of influence of all the parts involved in complex blockchain transactions. If responsibility links to technical participation, the legal evaluation will be more objective. This approach clarifies the role of the parts in global blockchain transactions and reduces legal gaps [3, p. 6].

Another innovative solution is the model of "selective transparency" for the legal supervision of blockchain transactions. This model creates a balance between complete anonymity and total transparency. Not all data have to be public. Only the segments of transactions with legal importance can be provided to the competent authorities with special cryptographic keys. This system does not create total control nor allows complete anonymity. In this way, it protects personal liberties and reduces the risks of delinquency.

Compulsory technical audits for the legal regulation of smart contracts can also be an effective solution. Each smart contract can be subjected to a test of legal and technical security before its execution. This test will avert the malfunctioning of the automated legal actions. At the same time, it will facilitate the legal evaluation of the harms that could arise during the execution of the contract. This norm will generate juridical security for both employers and users.

To resolve the problems associated with blockchain-based evidence, a multilayered verification system can be applied to store digital evidence adequately. In this system, evidence can be stored not only in one blockchain, but also in parallel chains. The parallel chains create an additional protection against manipulation of the evidence. This system also provides major technical security to judicial

authorities that evaluate the reliability of the evidence. This method has not yet been widely used, but it can be considered an innovative solution for the future.

A technological identification mechanism can be proposed to prevent the use of cryptoassets in criminal acts. This mechanism does not limit anonymity entirely, but requires only additional verification for high-risk transactions. This verification can act automatically according to the level of risk by means of a technical algorithm. Thus, it does not violate the privacy of regular users. However, high-risk transactions remain under legal control. This approach is balanced and more acceptable from a legal perspective.

Experimental legal zones created specifically for blockchain can also be a solution. In these zones, new technological legal models can be tested in some real-world environments. The legal risk is low, since the application is confined to a territory and a limited subject. This model generates experience for legislation and accelerates the development of innovative solutions.

The increase of cybercrime shows that the juridical system cannot conform only with the existent mechanisms. The new approaches in this field must be more practical and adapt to the changing digital surroundings. To ensure that Azerbaijan integrates into international processes of cybersecurity, the application of these approaches is of major importance. Since international norms are constantly updated, national legislation must adapt to these changes.

Solutions to combat cybercrime must be based on both juridical foundations and technological principles. In this sense, flexible juridical mechanisms can be created that facilitate real-time information exchange. These mechanisms contribute to the early detection of cyberattacks and speed up the investigative process. At the same time, norms must be developed that clearly define the division of responsibilities. These norms clarify the obligations of all entities operating in cyberspace.

Since the majority of cybercrimes are of cross-border nature, juridical cooperation can be strengthened with more specific mechanisms. For this, special information exchange protocols can be developed. These protocols facilitate the activities of investigation bodies and allow a more secure compilation of evidence. The establishment of improved procedures in Azerbaijan in this sense can enhance the efficiency of cooperation with international organisations [10].

It is also important to clarify the legal definitions of new forms of delinquency that arise in cyberspace, as terminological uncertainty complicates both the investigation and judicial processes. The clarity of norms strengthens legal application and facilitates the enforcement of penal responsibility. This approach is also coherent with the process of international standardisation.

Updating norms for working with digital evidence is also an important subject. Independent procedural norms can be established for the acquisition, storage and presentation of electronic evidence. These norms increase the reliability of the evidence and facilitate its evaluation by the court. The application

of international experience in this field in Azerbaijan can strengthen juridical protection mechanisms.

The legal mechanisms should be more flexible and situational to prevent cybercrime. For this, a special system of legal qualification could be created to evaluate the risk level of each cyber incident. This system would allow law enforcement to determine quickly the severity of the incident. At the same time, the priority areas of investigation could be based on this qualification.

A "compulsory security plan" could be introduced for platforms operating in cyberspace. This plan would demand that each platform comply with minimum security standards. These standards could include obligations not only technical but also legal. This mechanism would increase the responsibility of platforms and reinforce user security.

Also, a real-time alert system could be created to improve legal regulation. This system would automatically register suspicious activities and send a legal signal to law enforcement. This signal would allow the initiation of investigations without delay. Thus, it could prevent possible criminal activity before it becomes a crime. It would also be useful to create a special platform for cooperation among the State, private sector and academic institutions for investigating cybercrime. This platform could bring together legal experts and technicians. It can also support the development of standard procedures. This approach would reduce information gaps and speed up the investigation process.

It is also possible to strengthen the legality of identification methods used in cyberspace. For example, two or three levels of identification could be established as mandatory. This requirement would hinder the anonymity of criminals. At the same time, it would increase security without prejudicing the rights of users. Norms for cyberprofiles could also be introduced to develop the legal framework. These norms would identify only activities with a high risk of crime. The system would focus only on risk behaviours, not all users. This would maintain legal balance and improve efficiency.

It is also possible to create specialised cybersecurity certification programs for judges and prosecutors in Azerbaijan. These programs would inform them about new technologies. As a result, the evaluation of electronic evidence would become more professional. This would improve the quality of judicial procedures [7, p. 112].

The legal regulation of cybercrimes can be compared to a map. This map identifies the main routes, but still remains areas without exploration. These empty areas hamper the correct execution of investigations and weaken the operation of legal mechanisms. Since the penal process in the digital surroundings evolves with great rapidity, these gaps in the map become more visible. Therefore, the following stage focuses on one of these gaps, since it affects directly both the practical investigation and the judicial processes.

In Azerbaijan, the compilation of digital evidence in real time is one of the most critical stages in cybercrime investigations. However, there do not exist clear

procedural norms in this regard, which generates a significant legal gap. The valid legislation describes the compilation of evidence in general terms. However, cybercrimes occur so rapidly that these general norms are not sufficient for practical application.

The compilation of evidence in real time requires a special technical process. Data can be modified, deleted, or transferred to another server in a matter of seconds. In this case, the moment of obtaining the evidence is very sensitive. However, the legislation does not define a detailed mechanism to document this moment. This hampers the reliable acceptance of the evidence in courts.

Another problem is that the legal status of the information collected remains uncertain. It is not clear in which category the evidence collected in real time falls, such as "original", "copy", "record", or "operative information". This uncertainty raises questions for both the investigating authorities and the defense. During the judicial process, different approaches arise regarding the value and reliability of the evidence. This gap also hampers cross-border cooperation. Foreign states wish to know through which procedure the evidence was obtained. When the norms are not clear, it hinders the recognition of the evidence. This slows down the penal process and may allow criminals to evade their responsibility [8, p. 239-243].

The technical aspects of the compilation of evidence in real time are also left behind in relation to the legal framework. For example, questions like the confirmation of the hash value at the moment of data capture, the recording of transmitted data packets, or the protection of the chain of evidence from the very first second are not clearly explained. This creates a discrepancy between the technical results of the investigation and the legal requirements. This gap also complicates the work of the investigators, who have to use different technical methods in each case. However, the legal framework does not recognize all these methods with the same intensity. This inconsistency weakens the quality of the investigation and increases the risk of inadmissibility of the evidence in court.

For the compilation of digital evidence in real time, special procedural norms must be developed in advance. These norms must clearly indicate the moment of obtaining the evidence, the technical means used, and how the information will be recorded. This mechanism guarantees juridical coherence from the first moment of the investigation and augments the reliability of the evidence. The next step is to develop a single protocol for the chain of evidence that confirms all the stages, from the generation of the evidence to its presentation in court. This protocol reduces the risk of manipulation of the information and eliminates any doubts the court may have regarding the evidence. Without this protocol, evidence in real time, although sometimes accepted as a technical fact, can appear deficient from a legal perspective.

Another important step is the creation of special investigative squads. These squads can be composed of specialists who combine technical and legal knowledge. These squads can collect data in real time and immediately guarantee that the process

complies with legal requirements. The activities of these squads enhance the quality of the investigation. Furthermore, the list of technical tools that can be used during the investigation must be specified separately in the legislation. The legal validity of each technical means must be confirmed in advance. This approach would reduce the use of non-standardized tools in the investigation and generate uniformity in legal results. Also, a mechanism of rapid court authorization to obtain evidence in real time could be applied. This mechanism would guarantee a fast decision-making process in urgent cases. At the same time, it would increase the efficiency of the investigation without compromising personal data protection [9, p. 182].

A "flexible protocol of independent juridical cooperation" for the exchange of evidence with foreign states must be developed. This protocol could establish uniform standards for the recognition and acceptance of data in real time. This measure would speed up the investigation of cross-border cyberattacks and would allow a more reliable acceptance of the evidence at the international level. A specific technical formula must be developed at the national level on how to store digital evidence. This formula would guarantee the physical and digital security of the evidence. In the absence of these norms, the reliability of the evidence in later stages is reduced.

III. Conclusion

The analysis shows that the juridical and theoretical nature of cybercrimes is directly related to the rapid evolution of the digital environment. These changes demand the renewal of legal mechanisms. For Azerbaijan to integrate into international levels of cybersecurity, it is of main importance to adapt national legislation to international standards. The cross-border nature of cybercrimes requires a flexible and adaptive approach to legal regulation. The legal justification for the compilation of evidence in real time, the exchange of information, and the technical stages of the investigation are still not fully developed. This situation directly affects the investigation process, judicial evaluation, and international cooperation. The analysis also shows that the current gap in obtaining digital evidence is due to the lack of a systematic regulatory mechanism. This gap leads to a weakening of juridical security and hampers the proving of cybercrimes. Therefore, it is important to renew the legal system in accordance with technical capacities and international obligations. This renewal will reduce the general risks in the field of cybersecurity and strengthen the position of the country in the international juridical world.

To prevent cybercrimes and collect evidence reliably, an independent procedural framework must be developed that spans the acquisition of digital data in real time. This framework must clearly indicate the moment of creation of the evidence, the method of recording, and the procedure for its storage. At the same time, a unified mechanism of chain of custody must be applied to confirm the technical reliability of the evidence. This mechanism minimizes the possibility of alteration of the evidence and facilitates its acceptance by the court.

Second, specialized independent investigation squads must be created to research cyber incidents. These squads can be formed by experts with knowledge of both legal and technical aspects. This approach strengthens coordination among different areas and helps reduce the loss of information in the initial phase of the investigation. The legal status of all the technical tools used must also be determined in advance.

The third proposal refers to the creation of a fast mechanism for judicial permission. Time plays a fundamental role in cybercrimes. Therefore, in urgent cases, a mechanism could be applied that guarantees the reception of an operative decision from the court in electronic format. This mechanism increases the efficiency of the investigation without violating principles of personal data protection.

The following proposal consists of systematizing the cross-border exchange of information. To achieve this, a special cooperation protocol should be developed with international partners for the recognition and exchange of evidence in real time. This protocol would increase the compatibility among the legal requirements of different countries and accelerate the investigation process. Additionally, technical norms confirming the reliability of the information should be included in this protocol.

A multilayered protection mechanism should be applied for the secure storage of digital evidence. This mechanism would increase the reliability of both the technical and legal evidence. Storing the data in pairs in alternative servers or in environments based on blockchain could offer an additional advantage to this field. This approach would reduce the risk of destruction or alteration of the evidence and would provide a stronger defense barrier for the investigation process.

REFERENCES (ƏDƏBİYYAT):

1. Balacanov, E. (2020). The role and importance of legal regulation and criminal-law norms in combating cybercrime. Azerbaijan Law Journal, 2020(1), 26–37.
   URL:https://www.academia.edu/43666469/Kibercinay%C9%99tkarl%C4%B1qla_m%C3%BCbariz%C9%99d%C9%99_h%C3%BCquqi_t%C9%99nzimetm%C9%99nin_v%C9%99_cinay%C9%99t_h%C3%BCquqi_normalar%C4%B1n_rolu_v%C9%99_%C9%99h%C9%99miyy%C9%99ti_The_Role_and_Importance_of_Legal_Regulation_and_Criminal_Law_in_the_Fight_against_Cybercrime_ (last access: 15.05.2025).
2. Balajanov, E. (2024). Cybersecurity in Azerbaijan: Legislative measures to protect critical information infrastructure. Scientific and Practical Cyber Security Journal.
   URL: https://journal.scsa.ge/papers/cybersecurity-in-azerbaijan-legislative-measures-to-protect-critical-information-infrastructure (last access: 14.05.2025)

3. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1), Article tyac014. URL:https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060?login=false (last access: 15.05.2025)
4. Council of Europe. (2024). Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe. URL: https://www.coe.int/en/web/cybercrime/convention-on-cybercrime (last access: 16.05.2025)
5. Eurojust. (2022). Second Additional Protocol to the Budapest Convention on Cybercrime and cross-border access to electronic evidence. The Hague: Eurojust. URL: https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access (last access: 15.05.2025)
6. Rzayeva G.A. İnternational legal mechanisms for combating cybercrime: the economic impact on Azerbaijan and global practices. URL: https://doaj.org/article/88915ce8db574b9bbe49e9e91215ffe (last access: 15.05.2025)
7. Kharitoshkin, V. V. (2019). Measures to counter cybercrime in international and Russian criminal law. Bulletin of Tver State University. Series: Law, (3), 111–117. URL: https://eprints.tversu.ru/id/eprint/9262 (last access: 13.05.2025)
8. Navrotskaya, I. N. (2024). Issues of international cooperation in combating cybercrime. Education. Science. Scientific Personnel, 2024(1), 239–243. URL: https://cyberleninka.ru/article/n/voprosy-mezhdunarodnogo-sotrudnichestva-v-borbe-s-kiberprestupnostyu (last access: 15.05.2025)
9. Ng, J. (2016). International cybercrime, transnational evidence gathering and the challenges in Australia: Finding the delicate balance. International Journal of Information and Communication Technology, 9(2), 177–198. URL: https://www.inderscience.com/info/inarticle.php?artid=78879 (last access: 14.05.2025)
10. Oruj, Z. (2023). The first public opinion survey on cybersecurity in Azerbaijan: Selected findings. Analytical report of the Center for Social Research. URL:https://socialresearchjournal.az/index.php/2023/10/04/azerbaycanda-kibertehlukesizlikle-bagli-ilk-ictimai-rey-sorgusu-bezi-neticeler (last access: 15.05.2025)

11. Police Academy. (2020). Criminalistic support for the investigation of cybercrimes. Baku: Police Academy of the Ministry of Internal Affairs of the Republic of Azerbaijan. URL:https://www.pa.edu.az/library/5/36/584_monoqrafiya_kiber_cin_2020.pdf (last access: 15.05.2025)
12. Sarıyerlioğlu, B., & İzzetgil, E. (2024). A comparative analysis of the cybersecurity acquis of Turkey and Azerbaijan within the framework of international conventions. Academia.edu manuscript. URL: https://www.academia.edu/144345904/T%C3%BCrkiye_ve_Azerbaycan_%C4%B1n_Siber_G%C3%BCvenlik_M%C3%BCktesebatlar%C4%B1n%C4%B1n_Uluslararas%C4%B1_S%C3%B6zle%C5%9Fmeler_%C3%87er%C3%A7evesinde_Kar%C5%9F%C4%B1la%C5%9Ft%C4%B1rmal%C4%B1_%C4%B0ncelenmesi (last access: 145.05.2025)
13. Spînu, N. (2021). Azerbaijan cybersecurity governance assessment. Geneva: DCAF – Geneva Centre for Security Sector Governance. URL: https://www.dcaf.ch/azerbaijan-cybersecurity-governance-assessment (last access: 15.05.2025)

Kibercinayətlərin hüquqi-nəzəri xüsusiyyəti və Azərbaycanın beynəlxalq kibertəhlükəsizlik səviyyələrinə inteqrasiyası

XANIMANA QAFAROVA*, MİNURƏ CABBAROVA**

Annotasiya

Məqalədə kibercinayətlərin hüquqi-nəzəri mahiyyəti, onların müasir cinayət hüququ sistemində tutduğu yer və rəqəmsal texnologiyaların sürətli inkişafının hüquqi tənzimləməyə təsiri kompleks şəkildə araşdırılır. Rəqəmsal mühitin dinamik xarakteri kibercinayətlərin yeni formalarının yaranmasına, cinayətlərin törədilmə üsullarının mürəkkəbləşməsinə və ənənəvi hüquqi mexanizmlərin tətbiq imkanlarının məhdudlaşmasına səbəb olmuşdur. Bu baxımdan tədqiqatda kibercinayətlərin klassik cinayət tərkiblərindən fərqləndirici xüsusiyyətləri, onların transsərhəd xarakteri və sübutetmə prosesinə təsiri nəzəri və praktiki aspektlərdən təhlil edilir. Araşdırma göstərir ki, mövcud normativ-hüquqi mexanizmlər real vaxt rejimində rəqəmsal sübutların toplanması, saxlanılması və qiymətləndirilməsi, eləcə də transsərhəd kibercinayətlərin istintaqı və beynəlxalq hüquqi yardım mexanizmlərinin tətbiqi baxımından tam yetərli deyil. Xüsusilə elektron məlumatların hüquqi

* Hüquq üzrə fəlsəfə doktoru / müəllim / Beynəlxalq xüsusi hüquq və Avropa hüququ kafedrası / Bakı Dövlət Universitetinin Hüquq fakültəsi / email: xanim84.84@mail.ru
** Magistrant / Beynəlxalq xüsusi hüquq və Avropa hüququ kafedrası / Bakı Dövlət Universitetinin Hüquq fakültəsi / email: minara2006@mail.ru

statusunun qeyri-müəyyənliyi, sübut zəncirinin (chain of custody) normativ səviyyədə dəqiq tənzimlənməməsi və texniki imkanlarla hüquqi tələblər arasında uyğunsuzluq istintaq və məhkəmə proseslərində ciddi çətinliklər yaradır. Məqalədə beynəlxalq hüquq normaları, xüsusilə 2001-ci il Budapeşt Konvensiyasının müddəaları, onun əlavə protokolları və beynəlxalq məhkəmə təcrübəsi əsasında kibercinayətlərin hüquqi tənzimlənməsinə dair müasir yanaşmalar təhlil edilir. Azərbaycan Respublikasının milli qanunvericiliyinin bu sahədə mövcud vəziyyəti qiymətləndirilir, beynəlxalq standartlarla uyğunluq səviyyəsi müəyyən edilir və normativ boşluqlar elmi əsaslarla göstərilir. Tədqiqatın elmi yeniliyi kibercinayətlərin sübutlandırılması və istintaqının effektivliyini artırmaq məqsədilə adaptiv hüquqi modelin təklif edilməsindən ibarətdir. Təklif olunan model çevik prosessual qaydaların tətbiqini, texniki və hüquqi biliklərə malik ixtisaslaşmış istintaq strukturlarının formalaşdırılmasını, real vaxt rejimində sübutların toplanması üçün xüsusi prosedur mexanizmlərinin yaradılmasını və beynəlxalq əməkdaşlıq protokollarının təkmilləşdirilməsini nəzərdə tutur.

Açar sözlər: *kibercinayətkarlıq, rəqəmsal sübutlar, hüquqi tənzimləmə, beynəlxalq əməkdaşlıq, kibertəhlükəsizlik, sübut zənciri, Budapeşt Konvensiyası, harmonizasiya, elektron məlumatların qorunması.*

Требование всесторонности, объективности и полноты предварительного расследования в контексте принципов уголовного процесса

Ханымана Гафарова[*], Минура Джаббарова[**]

Резюме

В статье комплексно исследуется правовая и теоретическая сущность киберпреступлений, их место в системе современного уголовного права, а также влияние стремительного развития цифровых технологий на правовое регулирование. Динамичный характер цифровой среды обусловил появление новых форм киберпреступлений, усложнение способов их совершения и ограничение возможностей применения традиционных правовых механизмов. В этой связи в исследовании с теоретической и практической точек зрения анализируются отличительные особенности киберпреступлений по сравнению с классическими составами преступлений, их трансграничный характер и влияние на процесс доказывания.

[*] Доктор философии по праву / преподаватель / кафедра международного частного и европейского права / юридический факультет Бакинского государственного университета / email: xanim84.84@mail.ru

[**] Магистрант / кафедра международного частного и европейского права / юридический факультет Бакинского государственного университета / email: minara2006@mail.ru

Проведённый анализ показывает, что действующие нормативно-правовые механизмы не являются в полной мере эффективными в вопросах сбора, хранения и оценки цифровых доказательств в режиме реального времени, а также в сфере расследования трансграничных киберпреступлений и применения механизмов международной правовой помощи. Особые сложности возникают в связи с неопределённостью правового статуса электронных данных, отсутствием чёткого нормативного регулирования цепочки сохранности доказательств (chain of custody) и несоответствием между техническими возможностями и правовыми требованиями, что существенно осложняет следственную и судебную практику. В статье анализируются современные подходы к правовому регулированию киберпреступлений на основе норм международного права, в частности положений Конвенции Совета Европы о киберпреступности 2001 года (Будапештской конвенции), её дополнительных протоколов, а также международной судебной практики. Оценивается текущее состояние национального законодательства Азербайджанской Республики в данной сфере, определяется уровень его соответствия международным стандартам и научно обосновываются существующие нормативные пробелы. Научная новизна исследования заключается в разработке адаптивной правовой модели, направленной на повышение эффективности доказывания и расследования киберпреступлений. Предлагаемая модель предусматривает внедрение гибких процессуальных норм, формирование специализированных следственных структур, обладающих как техническими, так и правовыми знаниями, создание специальных процедурных механизмов для сбора доказательств в режиме реального времени, а также совершенствование протоколов международного сотрудничества.

Ключевые слова: *киберпреступность, цифровые доказательства, правовое регулирование, международное сотрудничество, кибербезопасность, цепочка сохранности доказательств, Будапештская конвенция, гармонизация, защита электронных данных.*

Redaksiyaya daxil olma tarixi: 25.05.2025
Çapa qəbul: 25.12.2025