European Journal of Economics, Finance and Business Development
**ISSN (E):** 2938-3633
Volume 2, Issue 10, October - 2024

# PROCEDURAL ASPECTS OF ENSURING THE PRESERVATION OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Б. У. Умаров
Слушатель магистратуры Правоохранительной академии
Республики Узбекистан
e-mail: baxtiyor-7797@mail.ru

**Abstract**
In the context of the digital transformation of society, electronic evidence, such as digital documents, audio and video recordings, data from mobile devices and Internet logs, are playing a key role in judicial practice. However, their unique characteristics create serious challenges related to the preservation of authenticity, admissibility and integrity of data. major problems, such as the changeability, forgery or loss of electronic evidence at the stages of its seizure, storage and presentation in court. Particular attention is paid to the legislative and technical aspects of the protection of electronic evidence, as well as the analysis of international experience in this area. It outlines procedural measures aimed at ensuring the protection of data from external interference and destruction, including the use of technologies such as digital signature, hashing, and blockchain. In addition, the issue of the need to improve national legislation, create new standards and guidelines for working with digital evidence is raised.
The article emphasizes the importance of implementing legal and technical solutions to ensure the reliability of electronic evidence and offers directions for further research and improvement of the legislative framework.

**Keywords**: Electronic evidence, criminal procedure, preservation, authenticity, admissibility, digital data, legislation.

## Introduction

The relevance of the study related to the procedural aspects of ensuring the preservation of electronic evidence in criminal proceedings is determined by a number of factors that confirm the importance of this topic in the context of modern justice. Modern technologies are changing all aspects of life, including the field of criminal proceedings, and in this context, electronic evidence occupies an increasingly important place in judicial practice. Consideration of this issue requires an in-depth analysis of procedural rules and regulations, which should be aimed at preserving the integrity and reliability of electronic data.
Electronic evidence represents a new reality in the criminal process faced by law enforcement agencies, lawyers, and courts. These are not only new forms of evidence, but also new ways of obtaining, recording and presenting them in court. Electronic evidence includes a wide range of data: emails, files, audio and video recordings, data from mobile devices, surveillance camera recordings, internet traffic data, server logs, and more. This data is of great importance

in the investigation of crimes, especially in cases involving cybercrime, fraud, corruption, and other complex crimes.

Today, it is impossible to imagine the investigation of crimes without the use of electronic evidence. Almost any criminal case can contain elements that are somehow related to digital data, whether it is the use of mobile phones, computers or other gadgets. Electronic evidence can greatly facilitate the establishment of the facts of the case, making it possible to reconstruct the sequence of events, identify connections between suspects and victims, or confirm alibis.

One of the most striking examples of the importance of electronic evidence is the fight against cybercrime. Cybercrimes, such as hacker attacks, identity theft, or malware distribution, leave digital footprints that can be used as evidence in court. In such cases, electronic evidence may be the only way to establish the guilt of the offender.

Despite the obvious advantages of using electronic evidence in criminal proceedings, law enforcement officers face serious problems related to their safety. Electronic evidence, unlike traditional evidence, can be easily altered, destroyed, or tampered with without any noticeable trace of tampering. This is due to the peculiarities of working with digital data: any file or record can be changed in a matter of seconds, while the process of identifying and restoring it can require significant effort.

The problem of the safety of electronic evidence begins from the moment of its seizure. If no measures were taken to ensure the integrity of the data during the seizure phase, such evidence may lose its legal force. An example is a situation when data is seized from the suspect's computer without proper recording of all actions. In the future, this may lead to the inadmissibility of such evidence, since it will be impossible to prove that the data has not been changed from the moment of seizure to the moment of their submission to the court.

The problem of authenticity of electronic evidence is also an important aspect. Unlike physical evidence, such as fingerprints or physical evidence, electronic data does not have a "natural" mechanism to prove its authenticity. This requires additional measures to prove that the electronic evidence is authentic and has not been altered. The specifics of working with digital files require the use of technologies such as digital signature, hashing, blockchain, and other data protection tools.

The storage and management of electronic evidence throughout the investigation and trial is also a central concern. There are situations where electronic evidence can be lost or damaged due to improper storage or lack of proper protection from external influences, such as hacker attacks or hardware failures. This leads to the fact that not only law enforcers, but also judges, lawyers and experts must have special knowledge and skills in the field of working with electronic data in order to ensure their safety and proper processing.

In order to work effectively with electronic evidence, it is necessary to review and modernize the existing procedural norms of criminal proceedings. At present, Russian legislation is not yet fully adapted to the new challenges that the digital era brings. Electronic evidence requires special approaches, ranging from its seizure to its storage and presentation in court.

A key procedural aspect is the need for strict procedures for the seizure of electronic evidence. These procedures should include a detailed recording of each step, from the moment the evidence is discovered to its submission to the court. Without such measures, it becomes difficult to prove that the evidence has not been altered or destroyed.

Another important aspect is the procedural need to protect the rights of participants in criminal proceedings in the context of working with electronic evidence. An important point is to ensure the right to a defence, including the right to an independent examination of electronic evidence, especially in cases where its authenticity or authenticity is in doubt.

In this context, it is important to pay attention to the international experience of working with electronic evidence. Many countries have already adopted special laws regulating the work with digital data, as well as developed standards for their safety. Examples of such initiatives can be found in the legal systems of the European Union and the United States, where the preservation of electronic evidence is governed by special procedural rules.

In this regard, there is a need to develop and implement national standards and guidelines for working with electronic evidence. Such standards should include not only procedural rules but also technical requirements for the seizure, storage and protection of electronic evidence.

Electronic evidence plays an important role in the modern criminal process, providing new opportunities for the investigation and proof of crimes.

Electronic evidence is information stored or transmitted in digital form that can be used in court to confirm or refute facts that are relevant to the case. This can be data stored on computers, mobile devices, servers, as well as information transmitted over the Internet.

Electronic evidence can be classified according to various characteristics.

First, by source of origin: data obtained from computers, mobile devices, network servers, and cloud storage.

Secondly, by data type: text files, emails, messages in instant messengers, audio and video recordings, photos, system logs and network logs.

Thirdly, by the method of receipt: data seized directly from the device, data obtained through remote access, and data recovered after deletion.

Examples of electronic evidence in criminal proceedings. In criminal cases, electronic evidence can include a wide range of information. For example, emails and messages in instant messengers can be used to confirm the fact of communication between suspects. Audio and video recordings can serve as evidence of the commission of a crime or an alibi. System logs and network logs can help establish the time and place of the crime, as well as identify the participants. Photos and screenshots can be used to visually confirm the facts.

Electronic evidence requires special attention to its safety and authenticity, as it can be easily altered or destroyed. Therefore, an important aspect is compliance with procedural rules when they are seized, stored and presented in court.

Electronic evidence is becoming increasingly important in Uzbekistan's criminal process, requiring clear legal regulation to ensure its admissibility and credibility.

Regulatory framework. In Uzbekistan, the use of electronic evidence is regulated by a number of legal acts. The recently adopted draft law amends and supplements legislative acts, defining the concept of digital evidence and establishing the procedure for its identification, collection, submission, verification, evaluation, recording and storage. This draft law is aimed at eliminating gaps in procedural legislation and improving the quality of justice.

International Standards and Recommendations. International organizations such as the Council of Europe and the United Nations have developed guidelines and recommendations on the use of electronic evidence. For example, the Committee of Ministers of the Council of Europe has

adopted the Guidelines on the Use of Electronic Evidence in Civil and Administrative Proceedings. These principles are aimed at ensuring uniformity of approaches to electronic evidence and increasing its reliability and admissibility. The UN has also released a Practical Guide for Requesting Electronic Evidence across borders, which is especially important in the context of globalization and the rise of cybercrime.

Analysis of the legislation of different countries. In different countries, approaches to the regulation of electronic evidence can vary significantly. In the UK, the use of electronic evidence is regulated by the Justice and Security Act, which sets strict requirements for its preservation and authenticity. In Germany, electronic evidence is regulated by the Code of Criminal Procedure (StPO), which provides for special procedures for its seizure and storage. In China, the use of electronic evidence is regulated by the Cybersecurity Law, which sets out requirements for data protection and security.

Thus, the legal framework for the use of electronic evidence in Uzbekistan includes both national legal acts and international standards and recommendations aimed at ensuring their admissibility and reliability in criminal proceedings.

The procedural aspects of ensuring the preservation of electronic evidence in Uzbekistan include several key elements, such as methods and means of recording, seizure and storage procedures, and technical and organizational measures to ensure preservation.

Methods and means of recording electronic evidence. Draft laws aimed at improving the system of working with electronic evidence are being actively discussed in Uzbekistan. An important aspect is the establishment of clear procedures for identifying, collecting, verifying, evaluating, recording and storing electronic evidence. Modern information and communication technologies (ICTs) play a key role in recording electronic evidence, ensuring its reliability and admissibility in court proceedings.

Procedures for seizure and retention. Procedures for the seizure and retention of electronic evidence should be clearly regulated to ensure its safety and integrity. In Uzbekistan, amendments to the legislation are proposed aimed at establishing the rights and obligations of all participants in the process using electronic evidence. This includes procedures for seizing, transporting, and storing electronic data to prevent it from being lost or damaged.

Technical and organizational measures to ensure the preservation. To ensure the safety of electronic evidence, it is necessary to introduce modern technical and organizational measures. This includes the use of secure data transmission channels, encryption, as well as regular software updates to protect against cyber threats. Organizational measures include training of employees responsible for working with electronic evidence and the development of internal regulations and instructions for their processing.

Thus, ensuring the preservation of electronic evidence in Uzbekistan requires a comprehensive approach, including legal, technical and organizational measures. This will increase the efficiency of judicial and investigative processes, as well as protect the rights and freedoms of participants.

Electronic evidence plays an important role in the modern criminal process, but its preservation and authenticity often cause serious problems. One of the main threats is the possibility of data being altered, destroyed, or tampered with. These threats can occur as a result of deliberate actions as well as due to technical glitches or errors.

Deficiencies in legal regulation also contribute to the vulnerability of electronic evidence. Some jurisdictions do not have clear rules regarding the procedures for collecting, storing and presenting electronic evidence in court. This may result in important evidence being declared inadmissible due to procedural violations.

Various technical and organizational measures are used to ensure the preservation of electronic evidence. One of these measures is data encryption, which allows you to protect information from unauthorized access and modification. Encryption ensures the confidentiality and integrity of data, which is especially important when it is transmitted and stored.

The use of electronic signatures also contributes to the safety of electronic evidence. An electronic signature allows you to certify the authenticity of a document and its author, as well as protect the document from forgery. This is especially important when exchanging legally significant documents and evidence.

Backing up your data is another important safeguarding measure. Regular backups allow you to restore your data if it is lost or damaged. This is especially true for organizations that store large amounts of information and must ensure its availability and safety.

The organization of control and supervision over the preservation of evidence also plays a key role. For this purpose, special units can be created or responsible persons can be appointed to monitor compliance with data storage procedures and standards. Regular audits and inspections will help identify and fix possible vulnerabilities and breaches.

In conclusion, the preservation of electronic evidence requires a comprehensive approach that includes both technical and organizational measures. It is also important to improve legal regulation in this area in order to ensure reliable protection and admissibility of electronic evidence in court.

Improvement of procedural regulation in the field of electronic evidence is an urgent task to ensure fair and effective justice. In modern conditions, when digital technologies penetrate into all spheres of life, it is important to ensure reliable protection and admissibility of electronic evidence in criminal proceedings.

One of the key steps is the adoption of additional legislative acts aimed at protecting electronic evidence. It is important to develop clear procedures for collecting, storing and presenting electronic evidence in court. This will minimize the risks of their change, destruction or falsification. For example, it is possible to provide for the mandatory use of certified means of recording and storing data, as well as establish liability for violation of these procedures.

The introduction of new norms should take into account international experience and best practices. It is important to adapt Uzbek criminal procedure legislation to modern challenges and threats associated with the use of digital technologies. For example, you can borrow the experience of the European Union, where standards for the protection of electronic evidence have already been developed and are successfully applied.

International experience shows that the effective protection of electronic evidence requires a comprehensive approach, including both legal and technical measures. It is important to take into account the recommendations of international organizations such as Interpol and Europol, which develop standards and methodologies for the protection of digital data.

The development of national standards for the storage and protection of electronic evidence is an important step to ensure its preservation and authenticity. These standards should include

requirements for data encryption, the use of electronic signatures and backups. For example, data encryption protects information from unauthorized access and alteration, while electronic signatures ensure the authenticity of documents.

Improvement of technical means of data recording and storage. It is also important to improve the technical means of recording and storing data. This may include the development of new software and hardware solutions that will provide strong protection for electronic evidence. For example, the use of blockchain technologies can significantly increase the level of security and transparency in the storage and transmission of data.

In conclusion, the improvement of procedural regulation in the field of electronic evidence requires a comprehensive approach, including both legal and technical measures. It is important to take into account international experience and adapt it to Russian realities in order to ensure reliable protection and admissibility of electronic evidence in criminal proceedings.

**References**

1. Smith, J. (2020). Digital Evidence in Criminal Cases. Legal Journal.
2. Brown, A. (2019). Classification of Digital Evidence. Forensic Science Review.
3. Johnson, M. (2018). Types of Digital Evidence. Cyber Law Review.
4. Davis, L. (2021). Methods of Obtaining Digital Evidence. Journal of Digital Forensics.
5. Williams, R. (2017). Use of Emails as Evidence. Criminal Law Quarterly.
6. Thompson, P. (2016). Audio and Video Evidence in Court. Legal Studies.
7. Garcia, S. (2019). System Logs as Evidence. Network Security Journal.
8. Lee, K. (2020). Visual Evidence in Criminal Cases. Journal of Forensic Photography.
9. The concept of "digital evidence" is introduced into the legislation of Uzbekistan.Darakchi.uz. 2:
10. Council of Europe Guidelines on the Use of Electronic Evidence.
11. UN Practical Guide for Requesting Electronic Evidence Across the Border.
12. Justice and Security Act, United Kingdom. 6: German Code of Criminal Procedure (StPO).
13. Cybersecurity Law, China.
14. https://weekly.uz/articles/11839/
15. https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-grazhdanskom sudoproizvodstve-v-epohu-tsifrovizatsii-pravosudiya-teoreticheskie-i-prakticheskie-aspekty
16. https://inlibrary.uz/index.php/evidence-criminal-proceedings/article/download/29371/30193
17. Smith, J. (2020). Digital Evidence and Computer Crime. Elsevier.
18. Casey, E. (2011). Digital Evidence and Computer Forensics. Academic Press.
19. Smith, J. (2020). Digital Evidence and Computer Crime. Elsevier.
20. Casey, E. (2011). Digital Evidence and Computer Forensics. Academic Press.
21. Sevryugin V. E. (2022). Administrative Procedural Law of Russia: State, Problems and Prospects. Siberian Legal Review.
22. Interpol. (2021). Digital Data Protection Guidelines. Interpol.