IRSTI 10.77.51
UDC 343.14
JEL K41

https://doi.org/10.46914/2959-4197-2026-1-2-192-201

RYSKULBEKOVA B.R.,*[1]
PhD student.
*e-mail: balzhan.ryskulbekova.76@mail.ru
ORCID ID: 0000-0002-2572-8781
ALAYEVA G.T.,[1]
c.l.s., professor.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
MUKHANOVA A.T.,[2]
master of law, senior lecturer.
e-mail: adema1986@mail.ru
ORCID ID: 0000-0002-3973-7339
AITMUKHANOVA D.U.,[3]
master of law, senior lecturer.
e-mail: didroz_12345@mail.ru
ORCID ID: 0000-0002-0803-063X
[1]Turan University,
Almaty, Kazakhstan
[2]Kazakh National Agrarian
Research University,
Almaty, Kazakhstan
[3]Atyrau University named
after Kh. Dosmukhamedov,
Atyrau, Kazakhstan

FEATURES OF THE USE OF DIGITAL EVIDENCE IN FRAUD CASES IN THE CRIMINAL PROCEEDINGS OF THE REPUBLIC OF KAZAKHSTAN

Abstract

This article is devoted to the specific features of the use of digital evidence in criminal proceedings in fraud cases. The choice of topic is обусловлено by the fact that the modern development of technology has had a significant impact on the nature of criminal offenses, including fraud, as well as on the process of collecting evidence. In law enforcement practice, investigative and inquiry authorities are increasingly confronted with the growing role of digital evidence, which is manifested in data obtained from electronic correspondence. This, in turn, gives rise to additional issues. The authors of this article set out to identify the specific features of the use of digital evidence in criminal proceedings during the investigation of fraud cases. The methods selected from the arsenal of general scientific and special methods used in writing this article enabled the authors to conduct a critical analysis of both the current legislation of Kazakhstan and academic doctrine. The conclusions formulated by the authors make it possible not only to identify the emerging problems, but also to suggest possible ways of resolving them through the prism of the unique features of digital evidence in fraud cases.

Keywords: features, evidence, digitalization, fraud, criminal proceedings, electronic information, judicial practice.

Introduction

Modern realities dictate to society and the state the need to expand the approaches used, including those applied in judicial proceedings. This is due to the widespread introduction of digitalization into all social relations. Taking into account the existence of the global information space as an integral part of our daily life, we are faced with the need to transform both approaches to the collection and recording of evidence and approaches to its evaluation.

Undoubtedly, the issue of digital evidence has already been raised by various scholars; however, in the context of fraud, this topic acquires a particular dimension and specificity. The current criminal procedure legislation does not reject the use of technical means for the collection and recording of evidence and does not focus exclusively on the "handwritten" format of evidence [1, p. 66], in particular when it comes to records of investigative actions.

In law enforcement practice, investigative and inquiry authorities are increasingly confronted with the growing role of digital evidence, which is manifested in data from electronic correspondence, in particular in various messengers, transactions carried out through online services, information stored on various media (computers and mobile devices), and so forth. This, in turn, leads to additional questions regarding the lawfulness of collecting such evidence, the proper procedural documentation and/or recording thereof, and the examination and evaluation of such evidence in the criminal process of Kazakhstan.

At present, the provisions of the Criminal Procedure Code of the Republic of Kazakhstan (hereinafter, the CPC RK) [2] contain a general concept of evidence and its types. However, although the CPC RK is the conceptual source of criminal proceedings, it does not define either the legal nature of digital evidence or its legal status. Even though the provisions of the CPC RK do allow for digital evidence, considering it within the framework of documentary and/or material evidence, the technical and substantive peculiarities of such evidence are not taken into account. This leads to an increase in the number of cases in judicial practice where there are divergent interpretations regarding the admissibility of such evidence and the assessment of its evidentiary value.

Academic literature has repeatedly described approaches to solving problems related to digital evidence. This has led to the emergence of an independent direction within the doctrine of criminal procedure law, the provisions of which focus specifically on digital evidence. This is confirmed by the fact that a number of scholars already propose considering digital evidence as an independent procedural category [3], rather than attaching it merely to one of the forms of "traditional" evidence.

All of the above only confirms the relevance and timeliness of the topic chosen by the authors.

In the course of writing this article, the authors analyzed academic literature, including foreign scholarship, which made it possible to determine that foreign authors, when defining the legal status of digital evidence, pay close attention to such categories as authenticity, integrity, and reliability. These categories serve as evaluative criteria in the use of digital evidence and in determining its evidentiary value [4].

In this regard, we consider justified the proposals of some researchers who insist on the need to develop and subsequently adopt unified standards to be applied and taken into account when collecting, recording, and evaluating digital evidence [5]. We dare to suggest that this position is well-founded and may serve as a starting point in determining areas for improving, inter alia, the national criminal procedure law of Kazakhstan and the CPC RK in particular.

The proposed directions for the modernization of the CPC RK and the criminal procedure law of the Republic of Kazakhstan are general in nature. However, this does not mean that such changes will not affect the evidentiary process in fraud cases. In this regard, since fraud has moved to a new level of commission through the use of digital and information technologies, the problem of complying with legislative requirements concerning evidence has become particularly acute. Most often, this arises when, due to violations of the CPC RK during the collection and recording of digital evidence in fraud cases, such evidence is subsequently recognized as inadmissible (Article 112 of the CPC RK).

In this regard, we agree with the opinion of M.A. Utanov, who points out that such circumstances negatively affect the implementation of the fundamental principles of criminal proceedings. Therefore, as the author argues, when addressing the issue of the use of digital evidence, it is important to determine not only the technical side of collecting and recording digital evidence. According to M.A. Utanov, the legal aspects underlying criminal proceedings are of fundamental importance [6].

The object of our article is the social relations arising in connection with the use of digital evidence in fraud cases, taking into account the peculiarities of its legal nature and the procedural requirements for its collection, recording, and evaluation.

As for the subject matter of our research, it includes the norms of the current legislation of Kazakhstan and certain foreign states (in particular, Georgia), which establish the foundations for the

use of digital evidence, including in fraud cases, as well as a generalization of scholarly approaches to the problem under consideration.

In preparing this study, the authors formulated a goal and identified corresponding objectives. Thus, the goal is a comprehensive analysis of the key features of digital evidence through the prism of the provisions of the current criminal procedure legislation of Kazakhstan, with an emphasis on the use of digital evidence in fraud cases. The stated goal also includes the need to develop well-founded approaches to determining the trajectory for improving Kazakhstani legislation, which will directly affect criminal proceedings.

To achieve this goal, the authors also identified a number of objectives, including the need to determine the legal essence of digital evidence, as well as the need to analyze the particularities of collecting, recording, and evaluating digital evidence not so much from a technical as from a legal perspective, in order to reduce the risks of such evidence being declared inadmissible.

The methods used in this study were selected from the arsenal of general scientific and special methods, among which the methods of analysis, synthesis, comparative legal analysis, as well as the systemic-structural method were most frequently employed.

The practical significance of the study lies in the fact that the conclusions reached by the authors are aimed at determining the need to develop unified standards establishing criteria for the collection, recording, and evaluation of digital evidence, including those necessary in fraud cases. The formulated conclusions are intended to determine the trajectory for improving the national criminal procedure legislation of Kazakhstan.

Materials and methods

In preparing this article, the authors employed a wide range of methods of scientific cognition. The choice of particular methods was determined by the interdisciplinary nature of the features of digital evidence used in fraud cases. Thus, we employed methods from the set of general scientific and special legal methods of cognition.

Of particular importance in writing this article was the dialectical method, which is rightly considered a basic one and which enabled us to reveal the nature of digital evidence while taking into account its unique characteristics that affect the process of its collection, recording, and evaluation.

The methods of analysis and synthesis were also actively used, allowing the authors to identify the important features inherent in digital evidence.

In order to clarify and subsequently formulate the authors' conclusions, the authors also resorted to special methods of scientific cognition. Among such methods, the authors gave preference to the formal legal and comparative legal methods. It should be noted that the combination of these methods made it possible to identify "growth points" in determining the trajectory for improving the national criminal procedure legislation of Kazakhstan.

The methods indicated above were used to process the relevant material. Such materials include not only doctrinal sources of theoretical significance. They also include materials of a practical nature reflecting the peculiarities of the use of digital evidence in fraud cases.

In addition, the materials used in writing the article include the legislative provisions of the CPC RK [2] aimed at regulating evidence and proof, including in fraud cases. The procedural features encountered by law enforcement agencies conducting investigations into fraud cases were also studied.

The choice of methods was oriented toward a comprehensive study of the criminal procedural aspects and features of the use of digital evidence in fraud cases, as well as toward ensuring the scientific accuracy and reliability of the results obtained. The methods and materials used correspond to the goal set by the authors and the objectives identified by us, which guarantees the reliability of the results obtained and the conclusions formulated.

Results and discussion

The specific features of the use of digital evidence in the investigation and subsequent proof of fraud are inevitably linked to the unique characteristics of the unlawful act under analysis itself. We ventured to assume this on the basis of the existing debate in academic literature regarding the method

of committing fraud through means of digitalization. Thus, a number of authors, among whom we note A.E. Boronina [7, p. 255] and A.V. Sypacheva [8, p. 3], believe that digital technologies used in the commission of a criminal offense leave corresponding traces and therefore may act as an independent method of committing virtually any unlawful act (as we believe, including fraud).

Other authors, such as G.A. Gunderich [9, p. 14], adhere to a somewhat opposite point of view, indicating that the key element is still deception/misleading conduct, which is implemented through the use of one or another technology. Moreover, the said author insists on a certain combination of technology and deception.

Having considered various, even contradictory, scholarly viewpoints, we believe that it is not entirely correct to equate digital and information technologies with the evidence obtained through their use. This is also due to the fact that the essence of the criminal act remains the same; only the method of commission and the mechanism of trace formation change. This position, in turn, will subsequently reduce the risks of judicial practice requiring additional qualification of such acts, including under Article 190 of the Criminal Code of the Republic of Kazakhstan [10].

However, the inclusion in Article 190 of the Criminal Code of the Republic of Kazakhstan of a corresponding qualifying element indicates that the evidence should be of the same nature as the method of committing fraud, that is, evidence generated through ICT.

Moreover, in our opinion, this may indicate the impossibility of combining all methods of committing fraud into some single method of committing an unlawful act with only a set of unified trace characteristics of the offense. Accordingly, the forensic characteristics of fraud and the use of digital evidence in relevant cases acquire priority and are transformed into a system-forming element of criminal procedural proof.

Thus, if trace formation arising from the commission of fraud, which we are able to prove by means of digital evidence, is transformed into a system-forming component, this indicates that it is advisable for us to move away from the traditional perception of criminal procedural principles and to begin thinking about expanding approaches to understanding digital evidence.

In principle, we are already taking cautious steps toward such a transformation of the theory of evidence. This is confirmed both by the provisions of the CPC RK [2] and by academic research. Thus, according to D.K. Tleubaev, S.M. Imanbaev, and R.Sh. Karymsakov, it was after the entry into force of the current CPC RK that the procedure for registering criminal offenses underwent changes [11, p. 33]. This is also connected with the expansion of the understanding of evidence, when law enforcement agencies base their decision to initiate criminal proceedings precisely on digital evidence.

In practice, the main issue encountered here is that the sphere of informatization is not a material category. This is a property of information, and of any information. Only the carrier of such information is material. Consequently, information requires the determination of its legal status. This feature of information as evidence distinguishes it from classical types of evidence, since the evidence is the information itself, yet it still must be recorded through material and/or documentary evidence. Such recording is necessary, inter alia, in order to protect evidentiary information from distortion, destruction, or other types of unlawful modification [12, p. 47].

Therefore, in Kazakhstan there is a real need for the legislative consolidation of fundamental procedural guarantees that would be activated when digital evidence is obtained and approved. It is important to emphasize that the guarantees of which we speak must take into account both the technical specifications relevant to the conduct of a number of investigative actions and the procedural and legal aspects. Bearing in mind that digital evidence constitutes evidence of a complex nature, one should not forget that, like any other type of evidence, it covers all stages of criminal proceedings provided for by the CPC RK. Consequently, we once again emphasize that there is an objective need to modify Kazakhstani legislation, including through the introduction of procedural guarantees.

Our point of view is also supported by an analysis of the process of evaluating evidence, which is based on the inner conviction of the court. We argue that, despite the presence of the judge's inner conviction, evidence should not be evaluated contrary to such fundamental principles as "lawfulness, reliability, and relevance to the case." Since these criteria, according to both legislation and academic doctrine [13, p. 132], are key, failure to comply with them will result in evidence losing its probative force.

Based on the analysis conducted within the framework of our research, we came to the conclusion that the volume and content of digital evidence, particularly in fraud cases, tend to grow. Within the framework of preliminary verification measures and/or pre-trial investigation, law enforcement agencies widely use data extracted from various information systems and networks (we do not list them, since there are many of them and such a listing would not change the substantive content of the study). The information seized that may have evidentiary value is generated in the digital environment. Moreover, as we wrote above, every offense committed with the help of ICT leaves characteristic traces (specialists and/or experts subsequently assist in obtaining and recording such traces), which will later indicate one or another unlawful act.

Given that digital evidence has unique characteristics, it is important, when working with it, to distinguish it from traditional evidence. Therefore, the approach to working with it and to its procedural formalization must be reconsidered. This reconsideration should include the development and adoption of unified standards to be applied and taken into account in the collection, recording, and evaluation of digital evidence. Returning to the concept of our study, we again emphasize that this position appears justified and may serve as a starting point in determining areas for improvement of, inter alia, the national criminal procedure law of Kazakhstan and the CPC RK [2] in particular.

Our opinion is partially confirmed in academic literature as well. The doctrine emphasizes that the very process of collecting/recording digital evidence does not create difficulties in technical terms, whereas issues of legal regulation of the process of collection/recording, which may also include the integration thereof, raise numerous questions [14, p. 88]. This is due to the fact that only the correct legal formalization of such evidence will contribute to fair administration of justice.

The opinion expressed is based on the fact that, when it comes to fraud, various types of violations are encountered quite frequently during the seizure and/or formalization of digital evidence. Such violations may be related to the incorrect recording of digital evidence, errors in the record of the investigative action, including cases where the technical means used in collecting/recording such evidence are incorrectly indicated.

Another feature of digital evidence that generates problems is the issue of its preservation. The study of procedural legislation has shown that in Kazakhstan there is no unified approach to the implementation of this process and to its procedural formalization.

Such an omission may also lead to the loss of the probative force of digital evidence. Moreover, this is not related to the correctness of the use of technical means. Everything stems from procedural and legal violations [15].

Through the analysis of academic literature and information found in open sources, we encountered a feature of the use of digital evidence that is connected not so much with technical characteristics as with legal and procedural aspects.

In our opinion, another important conclusion is that the authors identified the specific features of the offense provided for in Article 190 of the Criminal Code of the Republic of Kazakhstan. These features influenced the digital evidence formed, which in turn had a direct connection with the methods of committing fraud. Such features are also a characteristic of the objective element of fraud.

We formulated two principal conclusions that together form a complex clearly demonstrating the indisputable existence of specific features of digital evidence, particularly those encountered in fraud cases.

The existence of these features, along with the parallel formation of the information society and the expansion of digitalization processes, dictates the need to modernize legislation regarding work with digital evidence [16, p. 119].

In this context, the approach of Georgia appears interesting to us, and we express solidarity with it. From the point of view of the Georgian legislator, information as such (regardless of the manner in which it was obtained) acts as a source of data and may be presented in court. At the same time, however, Georgian legislation establishes an imperative requirement according to which, in order to verify the information submitted, the primary source of such information must be provided. This provision is enshrined in the Criminal Procedure Code of Georgia, namely in Article 78, “Probative Force of a Document” [17], the substantive meaning of which shows that a document serving as a carrier of information, if there are grounds to believe it is authentic, will have probative force.

At the same time, the degree of reliability may also be determined through the questioning of a person connected with the origin (discovery/storage) of such a document/information. It is important to indicate that, according to the analyzed provision of the Criminal Procedure Code of Georgia [17], where necessary (for example, taking into account the use of the document/information), such digital evidence may be returned or transferred for temporary use to its lawful owner. A copy of such digital evidence may also be returned or transferred.

Turning to the legal doctrine of foreign academic schools, we found that such criteria as authenticity, integrity, and reliability of digital evidence are considered fundamental and constitute the core of its evidentiary value [18, p. 242; 19].

Summarizing the analysis of legislative provisions and certain scholarly approaches disclosed by us in the course of this study, we may note that the conclusions we have drawn, on the one hand, substantiate the need for further research concerning digital evidence in fraud cases. On the other hand, these conclusions have identified "growth points" and the trajectory for improving the criminal procedure legislation of Kazakhstan in the area of the use of digital evidence.

Conclusion

The study conducted allowed us to formulate a number of conclusions. Thus, we determined that digital evidence in fraud cases constitutes a complex and system-forming element of criminal justice. Such a transformation indicates that it is advisable for us to move away from the traditional perception of criminal procedural principles and to begin considering an expansion of approaches to understanding digital evidence.

Taking into account the growing role of digital evidence, which is manifested in data from electronic correspondence, in particular in various messengers, transactions carried out through online services, information stored on different carriers (computers and mobile devices), and so forth, there is now an urgent need to resolve additional issues concerning the lawfulness of collecting such evidence, the correctness of its procedural formalization and/or recording, and its examination and evaluation in the criminal process of Kazakhstan. The resolution of these issues is also connected with the fact that digital evidence has its own particular features reflected in its immateriality, variability, and vulnerability.

In addition, the authors attempted to develop a trajectory for improving approaches to this process. Thus, the study enabled the authors to argue that information as such, without emphasis on the method by which it was obtained, should play the role of a source of certain data and, consequently, should be presented to the court. To verify the admissibility of such information, it is necessary to legislatively enshrine, in Article 112 of the CPC RK, a requirement to provide the primary source of such information. At the same time, the degree of reliability may also be determined through the questioning of a person connected with the origin (discovery/storage) of such a document/information.

Issues surrounding the legal regulation of the collection/documentation of digital evidence, including its potential integration, give rise to numerous complexities, as only the proper formalization of such evidence, from both legal and procedural perspectives, can ensure the administration of justice. In cases of fraud, various violations frequently occur during the seizure and/or documentation of digital evidence. These violations may be associated with improper recording of digital evidence, errors in the protocol of investigative actions, including the incorrect identification of technical tools used in the process of collecting and documenting such evidence.

Accordingly, both the approach to handling digital evidence and its procedural formalization require reconsideration. Such reconsideration should include the development and adoption of unified standards applicable to, and taken into account in, the collection, documentation, and evaluation of digital evidence. In particular, it is proposed to introduce into the Criminal Procedure Code of the RK a requirement that the collection/documentation of digital evidence be conducted in accordance with principles ensuring the integrity/security of data against unauthorized access, loss, alteration, or destruction. It is crucial, moreover, to establish that this principle must be implemented at all stages of handling digital evidence.

As a further proposal for improving national legislation in this field, it is advisable to ensure continuous documentation of all processes involved in the acquisition, transfer, storage, use, and

examination of digital evidence. This should include recording the time and place of each action, as well as identifying the individuals responsible for each stage of the process.

When working with digital evidence, it is necessary, particularly from a legal and procedural standpoint, rather than merely a technical one, to provide for legislative regulation of requirements concerning the use of specialized technical tools, the creation of digital copies (forensic images) of data carriers, and the application of cryptographic methods. In our view, such measures would reduce the risks of unlawful modification of information capable of serving as evidence in fraud cases.

A separate direction for improving the institution under consideration involves ensuring the verifiability of results. This would enhance the transparency of the process of examining digital evidence through the use of recognized methodologies and/or control mechanisms. It would also enable, where necessary, the reproducibility of procedures, thereby increasing the likelihood of obtaining consistent and comparable results (which may be required when reapplying a particular methodology and/or tool under similar conditions).

Finally, it should become an imperative rule that all legally significant actions of authorized persons must be duly documented, ensuring their transparency, verifiability, and the possibility of subsequent oversight.

REFERENCES

1 Кужабаева Г.М., Калиев А.К. Формирование правовых основ использования электронно-информационных технологий в уголовном процессе и производстве по делам об административных правонарушениях // Вестник Карагандинского университета. – Серия «Право». – 2022. – № 2(106). – С. 64–71.

2 Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. В редакции Закона РК от 03.01.2026 № 252-VIII // ИПС «Әділет». URL: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения: 10.01.2026)

3 Смирнов А.В., Калиновский К.Б. Уголовный процесс: учебник. 8-е изд., перераб. и доп. – М.: Норма, 2021. – 784 с.

4 Horsman G. Digital evidence strategies for digital forensic science device examinations // Digital Investigation. 2023. Vol. 44. Article 301544. URL: https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/a7d8d978-b391-4983-a110-d30a3612baaf/content (accessed: 01.02.2026)

5 Miha E., Pekmezi I. Electronic evidence in the criminal process // Academic Journal of Business, Administration, Law and Social Sciences. 2024. Vol. 10. No. 2. P. 1–11.

6 Утанов М. А. Использование электронных доказательств в судебном разбирательстве в странах СНГ и дальнего зарубежья // Право и правореализация в современных условиях. URL: file:///C:/Users/Asus/Downloads/editor,+journal-3-2016-10-18.pdf (дата обращения: 07.02.2026)

7 Боронина А.Е. Использование информационных технологий как способ совершения хищения // Вестник науки. – 2023. – № 11. – С. 252–257.

8 Сыпачев А.Ю. Основные способы хищений с использованием сети Интернет // Концепт. – 2019. – № 10. – С. 1–6.

9 Гундерич Г.А. Использование информационных технологий в качестве способов совершения преступления // Противодействие правонарушениям, совершаемым с использованием информационных технологий: сборник статей по материалам научно-практической конференции (III школы-семинара молодых ученых-юристов). – М., 2020. – С. 11–17.

10 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК. В редакции Закона РК от 03.01.2026 № 252-VIII // Ведомости Парламента РК, 2014 г. № 13-II. Ст. 83.

11 Тлеубаев Д.К., Иманбаев С.М., Карымсаков Р.Ш. Цифровизация уголовного процесса в Республике Казахстан: становление и практика применения // Colloquium-journal. – 2021. – № 11(98). – С. 31–37.

12 Utepov D.P. Digital Information as Proof in Criminal Proceedings // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2021. – № 3. – С. 45–56.

13 Шарипова А.Б., Мухамадиева Г., Аманкулов А.Х. О свойствах доказательств в уголовном процессе // Вестник КазНУ им. аль-Фараби. Заң сериясы. – 2020. – № 1(93). – С. 128–138.

14 Jshi N., Kumar R., Patel P. The Role of Electronic Evidence in the Civil Case Evidence Process // Rechtsnormen Journal of Law. 2025. Vol. 3(1). P. 80–90.

15 Досаев Т.Б. Цифровизация доказательственной базы в гражданском процессе: практика судов Республики Казахстан // ИС «Параграф». URL: https://prg.kz/document/?doc_id=32329244&utm_source=chatgpt.com (дата обращения: 20.02.2026)

16 Шарипова А.Б., Арын А.А., Куаналиева Г.А. Ақпараттық қоғамның жаһандануы жағдайында қылмысқа қарсы күрестің құқықтық аспектілері // Қазақстан Республикасы Заңнама және құқықтық ақпарат институтының хабаршысы. – 2023. – № 2. – С. 112–123.

17 Уголовно-процессуальный кодекс Грузии от 9 октября 2009 года № 1772-IIс (с изменениями и дополнениями по состоянию на 16.10.2025 г.) // ИС «Параграф». URL: https://prg.kz/document/?doc_id=37807676 (дата обращения: 05.03.2026)

18 Brenner S.W. Law in an era of smart technology: digital evidence and criminal justice // Oxford Journal of Legal Studies. 2020. Vol. 40(2). P. 233–259.

19 Ибрагимова А.М. Модернизация доказывания в уголовном судопроизводстве в условиях трансформации // Вестник Казанского юридического института МВД России. – № 3. – Т. 16. URL: https://vestnikkui.ru/ru/storage/viewWindow/229677 (дата обращения: 05.03.2026)

REFERENCES

1 Kuzhabaeva G.M., Kaliev A.K. (2022) Formirovanie pravovyh osnov ispol'zovanija jelektronno-informacionnyh tehnologij v ugolovnom processe i proizvodstve po delam ob administrativnyh pravonarushenijah // Vestnik Karagandinskogo universiteta. Serija «Pravo». No. 2(106). P. 64–71. (In Russian)

2 Ugolovno-processual'nyj kodeks Respubliki Kazahstan ot 4 ijulja 2014 goda No. 231-V ZRK. V redakcii Zakona RK ot 03.01.2026 № 252-VIII // IPS «Ədilet». URL: https://adilet.zan.kz/rus/docs/K1400000231 (data obrashhenija: 10.01.2026) (In Russian)

3 Smirnov A.V., Kalinovskij K.B. (2021) Ugolovnyj process: uchebnik. 8-e izd., pererab. i dop. M.: Norma. 784 p. (In Russian)

4 Horsman G. (2023) Digital evidence strategies for digital forensic science device examinations // Digital Investigation. Vol. 44. Article 301544. URL: https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/a7d8d978-b391-4983-a110-d30a3612baaf/content (accessed: 01.02.2026). (In English)

5 Miha E., Pekmezi I. (2024) Electronic evidence in the criminal process // Academic Journal of Business, Administration, Law and Social Sciences. Vol. 10. No. 2. P. 1–11. (In English)

6 Utanov M.A. Ispol'zovanie jelektronnyh dokazatel'stv v sudebnom razbiratel'stve v stranah SNG i dal'nego zarubezh'ja // Pravo i pravorealizacija v sovremennyh uslovijah. URL: file:///C:/Users/Asus/Downloads/editor,+journal-3-2016-10-18.pdf (data obrashhenija: 07.02.2026). (In Russian)

7 Boronina A.E. (2023) Ispol'zovanie informacionnyh tehnologij kak sposob sovershenija hishhenija // Vestnik nauki. No. 11. P. 252–257. (In Russian)

8 Sypachev A.Ju. (2019) Osnovnye sposoby hishhenij s ispol'zovaniem seti Internet // Koncept. No. 10. P. 1–6. (In Russian)

9 Gunderich G.A. (2020) Ispol'zovanie informacionnyh tehnologij v kachestve sposobov sovershenija prestuplenija // Protivodejstvie pravonarushenijam, sovershaemym s ispol'zovaniem informacionnyh tehnologij: sbornik statej po materialam nauchno-prakticheskoj konferencii (III shkoly-seminara molodyh uchenyh-juristov). M. P. 11–17. (In Russian)

10 Ugolovnyj kodeks Respubliki Kazahstan ot 3 ijulja 2014 goda № 226-V ZRK. V redakcii Zakona RK ot 03.01.2026 No. 252-VIII // Vedomosti Parlamenta RK, 2014 g. No. 13-II. St. 83. (In Russian)

11 Tleubaev D.K., Imanbaev S.M., Karymsakov R.Sh. (2021) Cifrovizacija ugolovnogo processa v Respublike Kazahstan: stanovlenie i praktika primenenija // Colloquium-journal. No. 11(98). P. 31–37. (In Russian)

12 Utepov D.P. (2021) Digital Information as Proof in Criminal Proceedings // Vestnik Akademii pravoohranitel'nyh organov pri General'noj prokurature Respubliki Kazahstan. No. 3. P. 45–56. (In Russian)

13 Sharipova A.B., Muhamadieva G., Amankulov A.H. (2020) O svojstvah dokazatel'stv v ugolovnom processe // Vestnik KazNU im. al'-Farabi. Zaң serijasy. No. 1(93). P. 128–138. (In Russian)

14 Jshi N., Kumar R., Patel P. (2025) The Role of Electronic Evidence in the Civil Case Evidence Process // Rechtsnormen Journal of Law. Vol. 3 (1). P. 80–90. (In English)

15 Dosaev T.B. Cifrovizacija dokazatel'stvennoj bazy v grazhdanskom processe: praktika sudov Respubliki Kazahstan // IS «Paragraf». URL: https://prg.kz/document/?doc_id=32329244&utm_source=chatgpt.com (data obrashhenija: 20.02.2026). (In Russian)

16 Şaripova A.B., Aryn A.A., Kuanalieva G.A. (2023) Aqparattyq qoğamnyñ jahandanuy jağdaiynda qylmysqa qarsy kürestıñ qūqyqtyq aspektıleri // Qazaqstan Respublikasy Zañnama jäne qūqyqtyq aqparat institutynyñ habarşysy. No. 2. P. 112–123. (In Kazakh)

17 Ugolovno-processual'nyj kodeks Gruzii ot 9 oktjabrja 2009 goda No. 1772-IIc (s izmenenijami i dopolnenijami po sostojaniju na 16.10.2025 g.) // IS «Paragraf». URL: https://prg.kz/document/?doc_id=37807676 (data obrashhenija: 05.03.2026). (In Russian)

18 Brenner S.W. (2020) Law in an era of smart technology: digital evidence and criminal justice // Oxford Journal of Legal Studies. Vol. 40(2). P. 233–259. (In English)

19 Ibragimova A.M. Modernizacija dokazyvanija v ugolovnom sudoproizvodstve v uslovijah transformacii // Vestnik Kazanskogo juridicheskogo instituta MVD Rossii. V. 16. No. 3. URL: https://vestnikkui.ru/ru/storage/viewWindow/229677 (data obrashhenija: 05.03.2026). (In Russian)

РЫСКУЛБЕКОВА Б.Р.,*[1]
докторант.
*e-mail: balzhan.ryskulbekova.76@mail.ru
ORCID ID: 0000-0002-2572-8781
АЛАЕВА Г.Т.,[1]
з.ғ.к., профессор.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
МҰХАНОВА А.Т.,[2]
з.ғ.м., аға оқытушы.
e-mail: adema1986@mail.ru
ORCID ID: 0000-0002-3973-7339
АЙТМУХАНОВА Д.У.,[3]
з.ғ.м., аға оқытушы.
e-mail: didroz_12345@mail.ru
ORCID ID: 0000-0002-0803-063X
[1]«Тұран» университеті,
Алматы қ., Қазақстан
[2]Қазақ ұлттық аграрлық зерттеу университеті,
Алматы қ., Қазақстан
[3]Х. Досмұхамедов атындағы Атырау университеті,
Атырау қ., Қазақстан

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚЫЛМЫСТЫҚ ПРОЦЕСІНДЕ АЛАЯҚТЫҚ ТУРАЛЫ ІСТЕР БОЙЫНША ЦИФРЛЫҚ ДӘЛЕЛДЕМЕЛЕРДІ ПАЙДАЛАНУ ЕРЕКШЕЛІКТЕРІ

Аңдатпа

Ұсынылған мақала алаяқтық істер бойынша қылмыстық процесте цифрлық дәлелдемелерді қолдану ерекшеліктеріне арналған. Тақырыпты таңдау технологияның қазіргі дамуы қылмыстық құқық бұзушылықтардың, соның ішінде алаяқтықтың сипатына, сондай-ақ дәлелдемелер жинау процесіне айтарлықтай әсер еткендігіне байланысты. Құқық қолдану шеңберінде тергеу және анықтау органдары электрондық хат-хабарлардан алынған мәліметтерде көрінетін цифрлық дәлелдемелердің рөлінің өсуіне тап болады. Бұл өз кезегінде қосымша сұрақтардың пайда болуына әкеледі. Осы мақаланың авторлары алаяқтық істерді тергеу кезінде қылмыстық процесте цифрлық дәлелдемелерді қолдану ерекшеліктерін анықтауды мақсат етті. Мақала жазу кезінде қолданылатын жалпы ғылыми және арнайы әдістердің арсеналынан таңдалған әдістер авторларға Қазақстанның қолданыстағы заңнамасына да, ғылыми доктринаға да сыни талдау жүргізуге мүмкіндік берді. Авторлар тұжырымдаған тұжырымдар туындаған мәселелерді ғана емес, сонымен қатар алаяқтық істердегі цифрлық дәлелдемелердің бірегей ерекшеліктерінің призмалары арқылы осындай мәселелерді шешудің нұсқаларын ұсынуға мүмкіндік береді.

Тірек сөздер: ерекшеліктері, дәлелдемелері, цифрландыру, алаяқтық, қылмыстық процесс, электрондық ақпарат, сот практикасы.

РЫСКУЛБЕКОВА Б.Р.,*[1]
докторант.
*e-mail: balzhan.ryskulbekova.76@mail.ru
ORCID ID: 0000-0002-2572-8781
АЛАЕВА Г.Т.,[1]
к.ю.н., профессор.
e-mail: g.alayeva@turan-edu.kz
ORCID ID: 0000-0003-1672-2238
МҰХАНОВА А.Т.,[2]
м.ю.н., ст. преподаватель.
e-mail: adema1986@mail.ru
ORCID ID: 0000-0002-3973-7339
АЙТМУХАНОВА Д.У.,[3]
м.ю.н., старший преподаватель.
e-mail: didroz_12345@mail.ru
ORCID ID: 0000-0002-0803-063X
[1]Университет «Туран»,
г. Алматы, Казахстан
[2]Казахский национальный аграрный
исследовательский университет,
г. Алматы, Казахстан
[3]Атырауский университет им. Х. Досмухамедова,
г. Атырау, Казахстан

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПО ДЕЛАМ О МОШЕННИЧЕСТВЕ В УГОЛОВНОМ ПРОЦЕССЕ РЕСПУБЛИКИ КАЗАХСТАН

Аннотация

Представленная статья посвящена особенностям использования цифровых доказательств в уголовном процессе по делам о мошенничестве. Выбор темы обусловлен тем, что современное развитие технологий оказало существенное влияние на характер уголовных правонарушений, включая мошенничество, а также на процесс сбора доказательств. В рамках правоприменения органы следствия и дознания сталкиваются с ростом роли цифровых доказательств, которые проявляются в данных из электронной переписки. Это, в свою очередь, ведет к возникновению дополнительных вопросов. Авторы этой статьи своей целью определили выявление особенностей использования цифровых доказательтсв в уголовном процессе при расследовании дел о мошенничестве. Выбранные методы из арсенала общенаучных и специальных методов, используемых при написании статьи, позволили авторам провести критический анализ как действующего законодательства Казахстана, так и научной доктрины. Сформулированные авторами выводы дают возможность не только определиться с возникающими проблемами, но и предположить варианты решения таких проблем через призмы уникальных особенностей цифровых доказательств в делах о мошенничестве.

Ключевые слова: особенности, доказательства, цифровизация, мошенничество, уголовный процесс, электронная информация, судебная практика.

Article submission date: 08.04.2026