IRSTI 10.79.91; 10.79.00 https://doi.org/10.26577/JAPJ1171202616

S.B. Bakyt[1*], G.T. Alayeva[1], A.K. Zhanibekov[2], E.E. Juchnevicius[3], B.S. Rakhmetulina[4]

[1]Turan University, Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3]University of Gdansk, Gdansk, Poland
[4]Kokshetau University named after Sh. Ualikhanov, Kokshetau, Kazakhstan
*e-mail: sara.bakyt@bk.ru

DIGITALIZATION OF FORENSIC EXAMINATION: IMPACT ON THE QUALITY OF EVIDENCE AND PROCEDURAL RISKS

This article provides a comprehensive analysis of the impact of digitalization on the quality of proof in criminal cases, with a focus on procedural risks that may arise in this process from the perspective of forensic expertology. The article also substantiates a classification of the principles of digitalization of forensic examination as specific (private) theories that may be applied both to the general procedure of expert research and to particular types of forensic examinations. The study examines the legal and criminalistic significance of digital trace analysis within forensic practice, paying special attention to the mechanisms of their formation, their evidentiary value, as well as issues related to the classification of digital traces and information carriers as objects of forensic examination.

Special attention is given to the problems of algorithmization and digitalization of forensic methods, including the use of artificial intelligence and neural networks. It is demonstrated that the introduction of digital technologies leads to significant changes in traditional approaches to the development of expert methodologies and, while influencing the quality of proof, may also become a source of certain procedural risks.

The scientific significance of the study lies in the theoretical rethinking of the evidentiary status of expert conclusions in the context of the digitalization of forensic examination, as well as in its contribution to the development of specific theories of forensic expertology. The practical significance of the research consists in the possibility of applying the obtained results to improve the legal regulation of forensic expert activity, develop expert methodologies, and reduce procedural risks arising in the conduct of digital forensic examinations.

Keywords: forensic examination, digitalization, expert opinion, quality of proof, procedural risks, proofs.

С.Б. Бақыт[1*], Г.Т. Алаева[1], А.К. Жанибеков[2], Э.Э. Юхневич , Б.С. Рахметулина[4]

[1]Тұран Университеті, Алматы, Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[3]Гданьск Университеті, Гданьск, Польша
[4]Ш. Уәлиханов атындағы Көкшетау университеті, Көкшетау, Қазақстан
*e-mail: sara.bakyt@bk.ru

Сот сараптамасын цифрландыру: дәлелдеудің сапасына ықпалы және процессуалдық тәуекелдер

Аталған мақалада сот сараптамасының экспертологиясы тұрғысынан қылмыстық істер бойынша дәлелдеудің сапасына цифрландырудың ықпалы кешенді түрде зерттеліп, осы үдеріс барысында туындауы мүмкін процессуалдық тәуекелдерге баса назар аударылады. Сонымен қатар, сот сараптамасын цифрландыру қағидаттарын жалпы сараптамалық зерттеу рәсіміне де, сот сараптамасының жекелеген түрлеріне де қолдануға болатын дербес теориялар ретінде жіктеудің негіздемесі ұсынылады. Зерттеуде сот-сараптамалық практика шеңберінде цифрлық іздерді зерттеудің құқықтық және криминалистикалық маңызы қарастырылады. Әсіресе олардың қалыптасу тетіктеріне, дәлелдемелік күшіне, сондай-ақ цифрлық іздер мен ақпарат тасымалдағыштарды сот сараптамасының объектілері ретінде жіктеу мәселелеріне ерекше назар аударылады.

Зерттеу барысында сот-сараптамалық әдістерді алгоритмдендіру және цифрландыру проблемаларына, соның ішінде жасанды интеллект пен нейрондық желілерді қолдану

© 2026 Al-Farabi Kazakh National University

дегі дәстүрлі тәсілдерге елеулі өзгерістер әкелетіні, дәлелдеудің сапасына ықпал ете отырып, белгілі бір процессуалдық тәуекелдердің туындауына себеп болуы мүмкін екені көрсетіледі.

Зерттеудің ғылыми маңыздылығы сот сараптамасын цифрландыру жағдайында сарапшы қорытындысының дәлелдемелік мәртебесін теориялық тұрғыдан қайта пайымдаумен және сот-сараптамалық экспертологияның дербес теорияларын дамытуға қосқан үлесімен айқындалады. Ал практикалық маңыздылығы алынған нәтижелерді сот-сараптамалық қызметті құқықтық реттеуді жетілдіруде, сараптамалық әдістемелерді әзірлеуде және цифрлық сот сараптамаларын жүргізу кезінде туындайтын процессуалдық тәуекелдерді төмендетуде қолдану мүмкіндігімен сипатталады.

Түйін сөздер: сот сараптамасы, цифрландыру, сарапшы қорытындысы, дәлелдеудің сапасы, процессуалдық тәуекелдер, дәлелдемелер.

С.Б. Бакыт[1*], Г.Т. Алаева[1], А.К. Жанибеков[2],
Э. Юхневич[3], Б.С. Рахметулина[4]

[1]Университет Туран, Алматы, Казахстан
[2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[3]Гданьский Университет, Гданьск, Польша
[4]Кокшетауский университет имени Ш. Уалиханова, Кокшетау, Казахстан
*e-mail: sara.bakyt@bk.ru

Цифровизация судебной экспертизы: влияние на качество доказательств и процессуальные риски

В данной статье проводится комплексное исследование влияния цифровизации на качество доказывания в уголовных делах, с акцентом на процессуальные риски, которые могут возникнуть в этом процессе, с точки зрения судебной экспертологии. Статья также обосновывает классификацию принципов цифровизации судебной экспертизы как частных теорий, которые могут быть применены как к общей процедуре экспертного исследования, так и к специфическим видам судебных экспертиз. В данной работе рассматривается правовое и криминалистическое значение исследования цифровых следов в рамках судебно-экспертной практики. Особое внимание уделяется механизмам их создания, их доказательственной силе, а также проблемам классификации цифровых следов и информационных носителей в качестве объектов судебной экспертизы.

В исследовании особое внимание уделяется проблемам алгоритмизации и цифровизации судебно-экспертных методов, включая применение искусственного интеллекта и нейронных сетей. Показано, что внедрение цифровых технологий влечет существенные изменения традиционных подходов к разработке экспертных методик и, оказывая влияние на качество доказывания, может стать источником определенных процессуальных рисков.

Научная значимость исследования определяется теоретическим переосмыслением доказательственного статуса заключения эксперта в условиях цифровизации судебной экспертизы и вкладом в развитие частных теорий судебной экспертологии. Практическая значимость заключается в возможности использования полученных результатов при совершенствовании правового регулирования судебно-экспертной деятельности, разработке экспертных методик и снижении процессуальных рисков, возникающих при проведении цифровых судебных экспертиз.

Ключевые слова: судебная экспертиза, цифровизация, заключение эксперта, качество доказывания, процессуальные риски, доказательства.

Introduction

The rapid development of digital technologies is fundamentally transforming criminal justice. Forensic examination, as a cornerstone of evidence and well-reasoned decision-making, is experiencing these changes with particular intensity. At the beginning of the twenty-first century, digitalization has permeated all areas of forensic activity, reshaping both the nature of the objects under examination and the approaches to their analysis. This process generates not only new opportunities, but also significant risks for the evidentiary process.

Digital traces generated by the operation of information systems are becoming a primary source of evidentiary information. Electronic data, event logs, network logs, multimedia records, and information from cloud storage systems are increasingly used to establish the factual circumstances of criminal cases. This undoubtedly expands the capabilities of forensic examination in terms of the completeness and accuracy of event reconstruction, while also stimulating the development of automated forensic methods.

Nevertheless, the digitalization of forensic science is associated with serious procedural challeng-

es. The volatility of digital traces, the complexity of their seizure, preservation, and transmission, as well as dependence on specialized hardware and software, pose risks to data integrity, lead to procedural violations, and complicate the verification of expert conclusions. Additional difficulties arise when dealing with cross-border electronic data, given differences in national legal frameworks and the growing reliance on algorithmic and intelligent analytical methods, including machine learning.

In this context, the need for a scholarly analysis of the impact of digitalization on the quality of evidence and the admissibility of expert conclusions is growing. The absence of unified approaches to the evaluation of digital traces, insufficient legal regulation of the use of algorithmic methods, and the lack of a clear definition of expert powers may lead to a reduction in the evidentiary value of expert opinions and an increase in procedural risks, including the possibility of their being challenged in court.

In the first quarter of the twenty-first century, against the backdrop of the rapid growth of computer and cybercrime, information and communication technologies have become an integral element of the mechanism underlying the commission of most crimes. Under these conditions, traditional analog methods of recording traces of criminal activity are gradually losing their significance, giving way to electronic forms of representation. This transformation has led to the emergence of fundamentally new objects of forensic examination – digital traces.

Initially, this process was characteristic primarily of forensic computer-technical examinations. However, the transition of image and sound recording processes into the digital environment has resulted in the inevitable integration of phonoscopic, video-technical, and photo-technical examinations into the digital domain, the further development of which outside digital technologies has become virtually impossible.

At the present stage, digital objects have assumed a stable position in most other categories and types of forensic examinations, including fingerprint, portrait, linguistic, economic, as well as forensic technical examinations of documents, among others. This development has led to a substantial transformation of the object composition of forensic examination and has given rise to a complex set of theoretical, legal, and organizational issues related to the detection, examination, evaluation, and procedural use of digital traces in criminal proceedings.

In order to achieve a comprehensive and systematic understanding of these issues, the concept of a new special theory – the theory of the digitalization of forensic expert activity – has been formulated. Its primary purpose is to substantiate scientific and methodological approaches to the examination of digital objects, to define the legal boundaries of their use in the process of proof, and to determine the place of the digitalization of forensic examination within the system of special theories of the general theory of forensic expertology (Rossinskaya E.R., 2022, p.345). The development of this theory contributes to the formation of a coherent scientific approach to digital traces and to the elaboration of unified principles for assessing the evidentiary value of expert conclusions obtained through the use of digital technologies.

Accordingly, the present article is aimed at a comprehensive analysis of the digitalization of forensic examination as a factor that, on the one hand, enhances the evidentiary potential of expert research, and, on the other hand, generates new procedural risks. Particular attention is paid to assessing the impact of digital technologies on the quality of evidence, the transformation of expert methodologies, and the identification of key procedural threats arising in the handling of digital traces. Consideration of these issues is of fundamental importance for the further development of forensic expertology, the improvement of expert practice, and the обеспечение of efficiency and fairness in criminal justice under conditions of digital transformation.

Literature review

In recent years, the issues surrounding the digitalization of criminalistics and forensic expert activity have been extensively developed in scholarly research, driven by changes in the nature of crime and the widespread implementation of information and communication technologies. One of the central directions of academic inquiry in this field has been the formation and further development of the concept of digital traces, which are considered an independent object of criminalistic analysis and forensic examination.

A significant place in contemporary academic discourse is occupied by the theory of information and computer support for criminalistic activity, comprehensively presented in a collective monograph edited by E. R. Rossinskaya (Rossinskaya E.R., 2022, p.416). Within the framework of this concept, digital technologies are interpreted not merely as auxiliary technical tools, but as a system-forming component of criminalistic activity that influences

its organizational foundations, methodology, and the overall effectiveness of crime investigation.

The methodological basis for understanding the technical nature of digital objects is formed by the works of both domestic and foreign researchers in the field of computer systems and network technologies, in particular the studies by A. Tanenbaum and T. Austin (Tanenbaum & Austin, 2013, p.808), as well as by J. Kurose and K. Ross (Kurose & Ross, 2016, p.912), which elucidate the fundamental principles underlying the operation of modern information systems.

The current stage in the development of forensic expertology is characterized by the active introduction of artificial intelligence and machine learning technologies, which is reflected in both theoretical developments and applied research. In particular, E. R. Rossinskaya analyzes the prospects and limitations of using neural networks in forensic expert practice, emphasizing issues of interpretability, reproducibility, and procedural verifiability of the results obtained. These positions are further corroborated by foreign scholarly works, including studies by P. Giverts, K. Sorokina, and V. Fedorenko (Giverts and et all., 2022), which demonstrate the potential of applying Siamese neural networks in the comparative examination of firing pin marks, as well as by foundational works on statistical learning that reveal the principles of operation of machine learning algorithms, including random forest methods.

The analysis of scholarly sources indicates that issues related to the digitalization of forensic examination are predominantly addressed in a fragmented manner – through the prism of studies on digital traces, information and computer support, and the implementation of artificial intelligence technologies. At the same time, a comprehensive approach to assessing the impact of digitalization on the evidentiary value of expert conclusions and the associated procedural risks remains insufficiently developed. This gap underscores the need for further research within the framework of the formation and advancement of a special theory of the digitalization of forensic expert activity.

Materials and methods

The methodological foundation of the study is formed by the system-based expertological approach, within which the digitalization of forensic expert activity is considered as a set of interrelated processes influencing the evidentiary value of expert conclusions and the emergence of procedural risks in criminal proceedings. The application of this approach made it possible to determine the place of the digitalization of forensic examination within the structure of forensic expertology and the system of evidentiary law.

The study employed the formal-legal method and logical-legal analysis, through which the provisions of criminal procedural legislation governing the appointment, conduct, and evaluation of forensic examinations involving digital technologies were examined. This made it possible to identify gaps and conflicts in legal regulation that may affect the admissibility, reliability, and evidentiary weight of expert conclusions.

Criminalistic and expert analysis was applied in the examination of digital traces as objects of forensic expertise, including their characteristics, modes of formation, and the specifics of expert examination, as well as in identifying factors affecting the stability and reproducibility of expert findings. To assess the consequences of the algorithmization of expert methodologies and the introduction of artificial intelligence technologies, a method of expert and model risk analysis was employed, enabling the identification of potential procedural threats arising in the process of proof.

The empirical basis of the study consisted of materials from judicial and expert practice, methodological guidelines, and scholarly publications. Their synthesis and systematization ensured the substantiation of the conclusions regarding the impact of the digitalization of forensic examination on the quality of evidence and justified the need to improve legal and methodological regulation in this field.

Discussion and results

The use of computer technology and information systems in the commission of various categories of crimes, in accordance with the general law of reflection, has led to the formation of a specific mechanism of trace formation determined by the processes of generation, processing, storage, and transmission of digital information. Unlike traditional mechanisms of trace formation, this process is indirect in nature and is realized through the functioning of hardware and software components of computing systems.

As noted by A. Tanenbaum, a digital computer is a technical device designed to solve tasks through the sequential execution of formalized commands (Tanenbaum & Austin, 2013, p.634). At the basic level, the architecture of computer systems is based

on a limited set of elementary instructions implemented in the form of machine code, which is executed by the central processing unit and, as a rule, is not directly perceptible to humans. Such an architecture rests on a digital logic level formed by a set of logic elements that perform basic operations on binary signals represented by the values “0” and “1”. At subsequent architectural levels, comprising a large number of such elements, functional units of computing systems are created, enabling the implementation of complex computational and information processes.

The transmission of digital data is carried out through the physical transfer of bit streams in the form of electrical, electromagnetic, or optical signals within local and global computer networks, including the Internet. The transformation and interpretation of such information are possible exclusively through the use of specialized hardware and software tools that convert digital signals into forms accessible to human perception – textual, visual, or auditory.

These features predetermine the material nature of digital traces, as they are objectively fixed on physical media and components of computing systems, including logic circuits, microchips, and data storage devices. By their nature, digital traces belong to technological traces and are comparable to traces resulting from the use of tools and instruments, since their emergence is directly related to the functioning of computer and information technologies.

At the same time, digital traces are characterized by a high degree of volatility and a multi-layered storage system, which objectively precludes their proper detection, documentation, seizure, and examination without the use of specialized information technologies. Any unauthorized or unqualified interference with the digital environment may lead to the modification, loss, or distortion of the data it contains, which is of fundamental importance for ensuring the authenticity, reliability, and procedural admissibility of evidentiary information (Rossinskaya & Ryadovsky, 2019, p.6).

The processes of digital trace formation vary depending on the type of information carrier. Thus, under electronic storage methods, data are fixed on solid-state drives that use flash memory, including USB devices and SSDs, the operation of which is based on the retention of electric charge in semiconductor microcircuits. Within the electromagnetic mechanism of trace formation, information is recorded on magnetic media, such as hard disk drives and magnetic tapes. The optical mechanism of trace formation is realized, inter alia, through the recording of data on optical discs by means of laser radiation. At the same time, regardless of the physical nature of the signals used for the storage, processing, and transmission of information, their functioning is based on digital technologies, which necessitates a unified theoretical approach to understanding digital traces within the system of forensic expertology.

A logical continuation of the above is the conclusion that there is a need to develop specialized methodological and procedural tools for the examination of digital traces, as well as to elaborate criteria for assessing the evidentiary value of expert conclusions formed on the basis of digital object analysis.

The set of tasks addressed by forensic examinations conducted in the study of digital traces largely coincides with those of forensic computer-technical examination. The subject matter of such studies comprises factual data and circumstances reflecting the regularities of the formation, functioning, and use of computer tools and systems that ensure the application of information technologies (Rossinskaya, 2022, p.134). The establishment of these circumstances is carried out within criminal, civil, and administrative proceedings through the involvement of specialized knowledge in the fields of programming and algorithmic processes, electronics and electrical engineering, information systems and technologies, radio communication systems, computer technology, and automated systems.

Within the structure of forensic computer-technical examination, several independent subtypes are traditionally distinguished, each oriented toward the examination of specific categories of digital objects and the corresponding traces. Thus, forensic hardware–computer examination is aimed at studying the features of operation and functioning of hardware components of computer systems that serve as material carriers of digital information. Within this subtype of examination, personal computers, peripheral devices, network equipment, embedded and integrated systems, as well as individual technical components relevant to the establishment of case circumstances, are analyzed.

Forensic software–computer examination focuses on the study of software and encompasses the set of digital traces generated by the functioning of software tools, the results of their operation, and the characteristics of software products. In particular, this type of examination addresses issues related to the identification of malicious functionality, indica-

tors of counterfeit software, and facts of unauthorized modification of program code.

Of particular significance is forensic information and computer examination of data, the subject matter of which includes the search, recovery, and analysis of information created by users or generated by automated processes, including as a result of malicious software activity. The information obtained through such examinations makes it possible to establish facts characterizing the event of the offense, the mechanism of its commission, and the involvement of specific individuals.

Forensic computer network examination is based on the analysis of the functional purpose of computer and telecommunication tools that ensure network-based information interaction. Through this type of examination, digital data circulating and stored within the network environment are identified and examined, including files of unlawful content, electronic correspondence, messages in social networks and messengers, as well as other forms of network interaction that have evidentiary value.

Taken together, the aforementioned types of forensic computer-technical examinations form the methodological foundation for the study of digital traces. At the same time, the continuous expansion of the range of digital objects and the increasing complexity of information processes objectively require the development of a unified theoretical approach to their analysis. This, in turn, underscores the relevance of developing a special theory of the digitalization of forensic expert activity and the need to reconsider the evidentiary value of expert conclusions based on the examination of digital data (Gavrilin Yu., 2021).

In conducting many types of forensic examinations, already at the initial stage of research the expert is confronted with the task of detecting traces whose identification is impossible without the use of specialized technical and instrumental means. This feature is most pronounced when working with digital traces, since their existence and content are, as a rule, not apparent without the use of specialized software and hardware. Under modern conditions, effective examination of such objects requires from the expert not only traditional specialized knowledge but also advanced training in the field of information technologies.

For certain types of forensic examinations, such a transformation of qualification requirements occurred relatively long ago. Thus, in phonoscopic, video-technical, and photo-technical examinations, the objects of study have for more than two decades been predominantly presented in digital form (Semikalenova, 2019, p. 213). This circumstance has led to the development of integrated expert methodologies and the formation of interdisciplinary competencies among specialists, enabling them to work independently with digital objects without involving experts of other profiles.

At the same time, this situation is mainly characteristic of cases where digital objects are stored on autonomous information carriers. If, however, digital traces are located within distributed information systems, server resources, or cloud infrastructures, their detection and seizure require specialized knowledge and skills pertaining to the field of forensic computer-technical examination. In such situations, the independent extraction of digital data by an expert of another specialization becomes either difficult or procedurally impermissible.

Similar problems also arise in so-called "traditional" types of forensic examinations that were not previously oriented toward working with digital objects. A representative example is forensic accounting examination, within which the expert is often required to identify and seize accounting documents stored in computer systems and effectively constituting digital traces. Since working with digital data does not fall within the professional competence of an economist-expert, the initial stage of such examinations requires the involvement of a specialist in forensic computer-technical examination (Rossinskaya & Usov, 2001, p. 287).

The task of such a specialist is to establish the origin of accounting data sets, determine whether they were generated by legitimate software or created by other means, and ensure the correct and unaltered copying of the required data.

Even where an expert in forensic accounting possesses certain skills in working with computer technologies, they are not authorized to independently carry out the seizure of digital traces, since such actions fall outside the scope of their professional competence. This delineation of powers necessitates interdisciplinary cooperation among specialists from different forensic domains and highlights the need for normative regulation of complex forensic examinations, as well as for revising qualification requirements for experts in the context of the digitalization of forensic expert activity.

It should be noted that, when examining objects classified as digital traces, a forensic expert must have an understanding of the technological methods for extracting forensically significant information recorded in digital form. At the same time, the

expert is required to assess not only the substantive characteristics of such objects, but also their procedural admissibility, technical suitability, and sufficiency for conducting a forensic examination and for formulating a scientifically grounded, reproducible, and verifiable conclusion. Of particular importance is the expert's ability to determine whether the requirements for the preservation of digital data have been observed and whether any interference capable of affecting their integrity and reliability has been excluded.

These circumstances indicate that the examination of digital traces cannot be carried out exclusively through the application of traditional expert methodologies (Savitsky, 2021, p.62). On the contrary, work with digital objects requires a substantial renewal of forensic expert methods, their adaptation to the specific features of the digital environment, and the implementation of modern technological solutions. As a result, a new stage in the development of expert technologies is emerging, characterized by the algorithmization of research procedures, the use of specialized software, and the increasing importance of interdisciplinary knowledge.

These processes have a direct impact on the evidentiary value of expert conclusions, since the reliability and procedural admissibility of expert findings largely depend on the correctness of the detection, documentation, and analysis of digital traces. In the context of the digitalization of forensic expert activity, this necessitates a revision of requirements for expert methodologies, an expansion of experts' professional competencies, and the development of unified standards for working with digital objects in order to minimize procedural risks and ensure an appropriate quality of proof.

The regularities of information and computer support for forensic expert activity, as well as the processes of informatization and computerization of forensic examination – including the introduction of modern information technologies, the creation and improvement of specialized information systems, and the use of special-purpose information and telecommunication networks -are justifiably regarded as fundamental provisions of forensic expertology. Their significance lies in the fact that they determine not only the level of technical equipment of expert activity, but also the direction of development of methods, forms, and organizational models for conducting forensic examinations.

The proliferation of digital traces as specific carriers of investigative and evidentiary information has become an additional stimulus for the active development of processes of algorithmization and digitalization of forensic expert methods and methodologies. In contemporary conditions, digital technologies are used not merely as auxiliary tools, but as instruments that directly influence the logic of expert cognition, the sequence of research actions, and the ways in which the results obtained are interpreted.

The further development of these processes is associated with the introduction of automated and intelligent data processing and analysis systems, which entails the formalization of expert procedures, the translation of certain stages of examination into algorithmic form, and the use of artificial intelligence technologies. At the same time, such a transformation of expert methodologies requires comprehensive theoretical analysis of their compliance with the requirements of scientific validity, reproducibility, and procedural verifiability, since it is precisely these factors that determine the evidentiary value of expert conclusions and the admissibility of their use in judicial proceedings.

In this regard, the algorithmization and digitalization of forensic expert activity are viewed not only as a natural stage of technological progress, but also as a factor capable of generating new procedural risks. This, in turn, necessitates the development of scientifically grounded approaches to their identification and minimization within the framework of forensic expertology (Hastie and et all, 2009: 596).

Digitalization significantly expands the so-called "evidentiary space" by incorporating digital traces such as event logs, metadata, network artifacts, application data, and cloud service records. Unlike most traditional traces, digital objects often contain a detailed temporal and event-based structure, including timestamps, sequences of actions, and correlations between devices and user accounts. When properly extracted and documented, these characteristics make it possible to enhance the completeness of event reconstruction and to ensure a higher degree of logical coherence within the evidentiary framework.

In European practice, the digitalization of forensic examination is developing not as a simple modernization of technical tools, but as a profound transformation of the system of proof, within which electronic data have become a stable – and in many cases key – element of investigation and judicial proceedings. This conclusion is supported by institutional statistics and analytical materials produced by European bodies. According to Eurojust data, there has been a steady increase in the workload related to

cross-border crime: in 2024, the Agency handled approximately 13,000 cases, while the overall volume of work over the past five years increased by more than 60 percent. Cybercrime consistently remains among the priority areas of activity – in 2023 alone, Eurojust processed over 500 cybercrime-related cases, more than half of which constituted new referrals. These figures indicate that digital traces and electronic data have effectively become a universal resource for investigation and proof across a wide range of offenses, particularly in cases involving a cross-border element.

The growing significance of electronic evidence is also confirmed by specialized European reviews dedicated to the handling of electronic data. The joint *SIRIUS EU Electronic Evidence Situation Report* (Europol–Eurojust–EJN) explicitly points to the increasing dependence of criminal investigations on electronic evidence, while simultaneously emphasizing the persistent difficulties associated with its acquisition in a cross-border context. These include differences in procedural rules, timeframes for executing requests, specific features of interaction with service providers, and jurisdictional conflicts. In practical terms, this means that as the share of digital data in the evidentiary base continues to grow, the quality of proof is increasingly determined by how correctly the extraction, preservation, verifiability, and documentation of the origin of electronic information are ensured.

From the perspective of evidentiary quality, the digital environment possesses a number of clear advantages. Digital traces are characterized by a high degree of informational richness: metadata, event logs, network activity data, as well as records of user interaction with devices and services, make it possible to reconstruct factual circumstances, time intervals, and sequences of actions in considerable detail. In addition, digital technologies potentially ensure the reproducibility of expert analysis: where forensic imaging and verification procedures are properly observed, it becomes possible to re-examine an identical dataset and to verify the expert's conclusions.

However, it is precisely at this stage that the first group of procedural risks emerges. Digital objects are highly volatile and may be affected by updates, synchronization processes, deletion, recoding, and dependence on specific software and hardware configurations. In this regard, the evidentiary value of digital data directly depends on the ability of the expert or the authorized party to ensure traceability of the data's origin and effective control over its immutability.

The scale of digital threats and the volume of processed data are clearly reflected in pan-European cyber risk assessments. Thus, the *ENISA Threat Landscape 2024* report analyzes thousands of recorded incidents and highlights the predominance of threats to information availability, as well as the sustained prevalence of ransomware attacks and data-related offenses within the Member States of the European Union. The increasing number of incidents and the growing volume of digital information objectively raise the likelihood of errors in the collection and interpretation of digital traces and, consequently, increase the risk of procedural challenges to the results of forensic examinations.

The second group of risks is associated with issues of admissibility and evidentiary weight (admissibility/weight) of electronic data in the context of cross-border proceedings. European legal doctrine and law-enforcement practice proceed from the premise that the use of evidence obtained in the territory of one State in judicial proceedings of another EU Member State is permissible only where transparent and predictable procedures, as well as adequate guarantees of a fair trial, are ensured. In the work by Garamvölgyi, Ligeti, Ondrejová, and von Galen (EUCRIM), it is substantiated that the growing number of cross-border investigations elevates the problem of admissibility of evidence collected outside national jurisdiction to a key issue, both in terms of the effectiveness of criminal prosecution and the protection of the rights of procedural participants.

In the field of digital evidence, this problem becomes particularly acute, since electronic data are often stored by service providers located in other jurisdictions, are subject to different regimes of data retention and disclosure, and are accessed through procedures that are not always harmonized in terms of requirements and time limits. Analytical materials produced by SIRIUS point precisely to this "zone of tension": the dependence of criminal investigations on electronic data is increasing, while cross-border cooperation in obtaining such data continues to be accompanied by significant difficulties.

The third group of risks arises from the algorithmization of expert methodologies and the introduction of artificial intelligence technologies, which significantly increase the requirements for the verifiability of expert conclusions (Chesnokova and et all, 2023, p.65). European law – enforcement and judicial authorities note that the widespread use of encryption and "privacy-by-default" concepts objectively complicates access to data and stimulates

reliance on automated analytical tools. At the same time, this intensifies the risk of the "black box" effect and errors in the interpretation of results.

In parallel, a regulatory framework of the European Union is being formed: scholarly research actively discusses the relationship between the forensic application of AI and the provisions of the AI Act, including the regime of "high-risk" systems depending on the subjects and conditions of their use. For forensic examination, this means that the application of neural networks and other machine-learning models must be accompanied not only by the presentation of final results, but also by disclosure of the limitations of the methods used, the conditions of their applicability, mechanisms for version control, reproducibility, and the sources of model risks. Otherwise, procedural opponents are provided with substantial grounds for challenging the evidentiary value of expert conclusions.

Finally, the European scholarly tradition in the study of digital evidence is closely linked to the legal frameworks for combating cybercrime. The works of Marco Gercke (Germany), directly connected with the practice of the Council of Europe and the Budapest Convention, emphasize the key role of electronic data in the investigation of cybercrime and the necessity of harmonizing procedures for their acquisition. Significant importance is also attached to the Anglo-European doctrine of digital investigations: Ian Walden (United Kingdom) consistently analyzes the legal and technological aspects of computer crime and digital investigations, providing valuable theoretical foundations for defining procedural requirements governing the handling of electronic evidence.

Taken together, the analysis of statistical data and doctrinal sources in Europe demonstrates the dual nature of the impact of the digitalization of forensic examination. On the one hand, the introduction of digital technologies contributes to improving the quality of evidence through greater informational detail, the ability to trace actions within the digital environment, and the potential reproducibility of expert analysis. On the other hand, digitalization gives rise to a stable set of procedural risks, including challenges to the admissibility of electronic evidence due to violations in extraction and documentation procedures, procedural conflicts in cross-border investigations, difficulties in accessing data held by service providers, as well as methodological and "model-related" risks associated with the use of artificial intelligence technologies. In this context, the digital transformation of forensic examination requires not only the implementation of technological solutions, but also the development of forensic methodology, particularly with regard to the validation and standardization of expert methods, the clarification of experts' competencies and procedural roles, and the harmonization of procedures for handling electronic evidence at the level of legal regulation and European cooperative practice.

A representative example can be found in European judicial practice. In one case involving corruption and money laundering, heard by a court of an EU Member State, electronic logs of network transactions reconstructed by experts through the correlation of file metadata stored on distributed server resources played a key evidentiary role (Belkin & Rossinskaya, 1993, p.147). The absence of proper documentation of hash values of data images at the initial stage of the investigation served as grounds for the defense to challenge part of the evidence. The court noted that failure to comply with digital forensic procedures reduced the evidentiary value of the materials presented (EU Criminal Case Review, 2023, § 57) (https://eur-lex.europa.eu/EN). This case clearly demonstrates how procedural violations in handling digital traces can adversely affect the quality of evidence.

Similar issues have been identified in cases involving the dissemination of child sexual abuse material through messaging services in one of the European Union Member States. Expert examination of messages and network logs made it possible to establish not only the content of communications, but also the presumed location of the devices used. At the same time, the defense questioned the methodology used to obtain data from cloud storage, pointing to a possible violation of the principle of "data sovereignty." As a result, the court was required to request additional confirmation that the procedure complied with personal data protection legislation, which led to the suspension of the proceedings and the initiation of additional checks (Transnational Cybercrime Proceedings, 2022). This example underscores that, in the absence of reliable procedural mechanisms, electronic evidence may not only complicate the process of proof, but also lead to significant delays in judicial proceedings.

Particular attention in European academic discourse and law-enforcement practice is devoted to the relationship between digital evidence and guarantees of human rights protection. According to data from the European Union Agency for Fundamental Rights (FRA), in a number of cases issues concerning the lawfulness of law-enforcement access to

data – taking into account the requirements of the GDPR and national personal data protection legislation – have led either to the exclusion of certain evidence or to the inclusion in judicial decisions of specific instructions emphasizing the need to maintain a balance between the effectiveness of criminal investigations and the protection of suspects' rights (FRA, 2022) (https://fra.europa.eu/en). This circumstance increases the burden on forensic experts, as they are required not only to conduct technically sound analyses, but also to substantiate the lawfulness of data acquisition and demonstrate compliance with applicable legal safeguards.

Conclusion

The conducted study allows us to assert that the digitalization of forensic examination represents an objective and irreversible stage of development that exerts a multifaceted impact on the system of proof in criminal proceedings. The active implementation of digital technologies, the widespread proliferation of digital traces, and the use of algorithmized expert methodologies lead to a profound transformation of both the substance of forensic expert activity and the role and evidentiary significance of expert conclusions.

On the one hand, digital transformation possesses substantial potential for improving the quality of the evidentiary base. Digital traces are characterized by a high degree of informational capacity and create conditions for a more accurate reconstruction of the circumstances of a crime, the establishment of temporal, spatial, and causal relationships, and the reproducibility of expert examinations, provided that proper procedures for data extraction, preservation, and analysis are observed. The application of algorithmized methods and specialized software contributes to the standardization of expert procedures, reduces the influence of subjective factors, and enhances the scientific validity of expert conclusions.

At the same time, digitalization generates a stable set of procedural risks that directly affect the admissibility, reliability, and evaluation of evidence. Among the most significant risks are the high volatility of digital traces, the dependence of their content on technical and software environments, difficulties in ensuring data integrity and maintaining an uninterrupted chain of custody, as well as the vulnerability of procedures for the seizure and documentation of digital information. Particular importance is attached to issues of cross-border access to electronic data, differences in legal regimes governing their acquisition and storage, and the need for strict compliance with personal data protection requirements and human rights guarantees.

An additional source of procedural threats is associated with the expanding use of algorithmized and intelligent analytical methods, including artificial intelligence and neural network technologies. Despite their high analytical effectiveness, such tools are characterized by limited interpretability, susceptibility to model-related risks, and dependence on the quality of training datasets. In the absence of transparent mechanisms for validation and procedural oversight, this may lead to a reduction in the evidentiary value of expert conclusions and their successful challenge in judicial proceedings.

European statistics and law-enforcement practice indicate that electronic evidence has already assumed a central role in the investigation and adjudication of criminal cases, particularly in the fields of cybercrime and cross-border criminal activity. At the same time, it is precisely in these categories of cases that problems of admissibility of digital evidence, delineation of expert competencies, and compliance of applied methodologies with procedural law requirements are most clearly manifested.

Under these conditions, the digitalization of forensic examination requires not only technological progress, but also comprehensive scientific and regulatory support. Improving the quality of evidence is possible only if forensic methodologies for the examination of digital traces are further refined, procedures for their extraction and preservation are unified, interdisciplinary competencies of experts are developed, and the use of algorithmized and intelligent technologies is clearly regulated at the procedural level. Only under such an approach can the digital transformation of forensic examination fulfill its core function – contributing to the establishment of truth in a case without creating additional procedural risks or diminishing the level of guarantees of fair and adversarial judicial proceedings.

Authors' Contributions

S.B. Bakyt: Conceptualization; Methodology; Investigation; Writing – Original Draft. G.T.Alayeva: Data Curation; Formal Analysis; Visualization; Writing – Review & Editing. A.K.Zhanibekov: Validation; Legal Analysis; Writing – Review & Editing; Resources. E.E. Juchnevicius: Supervision; Project Administration;; Writing – Review & Editing. B.S.Rakhmetulina: Legal Analysis; Writing – Review & Editing

Литература

Белкин, А. Р., & Россинская, Е. Р. (1993). KBS for criminology and forensic expertise. В *Proceedings of the European Congress on Artificial Intelligence and Knowledge Representation (Kennistechnologie'93)* (с. 147–149). Амстердам.

Европейское агентство по основным правам (FRA). (2022). *Fundamental rights and criminal justice in the digital age*. https://fra.europa.eu/en/publication/2022/fundamental-rights-criminal-justice-digital-age

Гаврилин, Ю. В., & Гаспарян, Г. З. (2021). *Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий* (учеб. пособие). Москва: Проспект.

Гивертс, П., Сорокина, К., & Федоренко, В. (2022). Examination of the possibility to use Siamese networks for the comparison of firing pin marks. *Journal of Forensic Sciences, 67*(6), 2416–2424. https://doi.org/10.1111/1556-4029.15143

Хасти, Т., Тибширани, Р., & Фридман, Д. (2009). Chapter 15: Random forests. В *The elements of statistical learning: Data mining, inference, and prediction* (2-е изд., с. 587–604). Нью-Йорк: Springer-Verlag.

Куроуз, Д., & Росс, К. (2016). *Компьютерные сети. Нисходящий подход* (6-е изд.). Москва: Эксмо.

Regulation (EU) 2023/1543 – Electronic Evidence (e-Evidence). (2023). https://eur-lex.europa.eu/EN/legal-content/summary/electronic-evidence-in-criminal%20proceedings.html

Россинская, Е. Р., & Рядовский, И. А. (2019). Концепция цифровых следов в криминалистике. В *Аубакировские чтения: Материалы международной научно-практической конференции* (Алматы, 19 февраля 2019 г.) (с. 6–9). Алматы.

Россинская, Е. Р., & Усов, А. И. (2001). *Судебная компьютерно-техническая экспертиза*. Москва: Право и закон.

Россинская, Е. Р., & Зинин, А. М. (2022). *Экспертиза в судопроизводстве* (учебник) / под ред. Е. Р. Россинской. Москва: Проспект.

Савицкий, А. А. (2021). Актуальные вопросы становления и развития судебной экономико-цифровой экспертизы в условиях цифровизации социально-экономической сферы государства. *Законы России: опыт, анализ, практика, (3)*, 60–64.

Семикаленова, А. И. (2019). Цифровые следы и их носители как объекты судебно-экспертного исследования. В *Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: Материалы научно-практической конференции с международным участием* (Москва, 5 апреля 2019 г.) (с. 212–215). Москва: РГ-Пресс.

Таненбаум, Э. С., & Остин, Т. (2013). *Structured Computer Organization* (6-е изд.). Лондон: Pearson.

Теория информационно-компьютерного обеспечения криминалистической деятельности (монография) / под ред. Е. Р. Россинской. (2022). Москва: Проспект.

Чеснокова, Е. В., Усов, А. И., Омельянюк, Г. Г., & Никулина, М. В. (2023). Искусственный интеллект в судебной экспертологии. *Теория и практика судебной экспертизы, 18*(3), 60–77. https://doi.org/10.30764/1819-2785-2023-3-60-77

References

Belkin, A. R., & Rossinskaya, E. R. (1993). KBS for criminology and forensic expertise. В *Proceedings of the European Congress on Artificial Intelligence and Knowledge Representation (Kennistechnologie'93)* (pp. 147–149). Amsterdam.

FRA – European Union Agency for Fundamental Rights. (2022). *Fundamental rights and criminal justice in the digital age*. https://fra.europa.eu/en/publication/2022/fundamental-rights-criminal-justice-digital-age

Gavrilin, Yu. V., & Gasparyan, G. Z. (2021). *Rassledovanie khishcheniy denezhnykh sredstv, sovershennykh s ispolzovaniem informatsionnykh bankovskikh tekhnologiy* [Investigation of theft of funds committed using banking information technologies] (ucheb. posobie [Textbook]). Moscow: Prospekt.

Giverts, P., Sorokina, K., & Fedorenko, V. (2022). Examination of the possibility to use Siamese networks for the comparison of firing pin marks. *Journal of Forensic Sciences, 67*(6), 2416–2424. https://doi.org/10.1111/1556-4029.15143

Hastie, T., Tibshirani, R., & Friedman, J. (2009). Chapter 15: Random forests. В *The elements of statistical learning: Data mining, inference, and prediction* (2nd ed., pp. 587–604). New York: Springer-Verlag.

Kurose, J., & Ross, K. (2016). *Komp'yuternye seti. Niskhodyashchiy podkhod* [Computer networking: A top-down approach] (6-e izd.). Moscow: Eksmo.

Regulation (EU) 2023/1543 – Electronic evidence (e-Evidence). (2023). https://eur-lex.europa.eu/EN/legal-content/summary/electronic-evidence-in-criminal%20proceedings.html

Rossinskaya, E. R., & Riadovskiy, I. A. (2019). Kontseptsiya tsifrovykh sledov v kriminalistike [The concept of digital traces in forensic science]. В *Aubakirovskie chteniya: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii* (Almaty, 19 February 2019) (pp. 6–9). Almaty.

Rossinskaya, E. R., & Usov, A. I. (2001). *Sudebnaya komp'yuterno-tekhnicheskaya ekspertiza* [Forensic computer-technical examination]. Moscow: Pravo i zakon.

Rossinskaya, E. R., & Zinin, A. M. (2022). *Ekspertiza v sudoproizvodstve* [Forensic examination in legal proceedings] (uchebnik [Textbook]) / ed. by E. R. Rossinskaya. Moscow: Prospekt.

Savitskiy, A. A. (2021). Aktualnye voprosy stanovleniya i razvitiya sudebnoy ekonomiko-tsifrovoy ekspertizy v usloviyakh tsifrovizatsii sotsialno-ekonomicheskoy sfery gosudarstva [Topical issues of the formation and development of forensic economic-digital expertise in the context of digitalization of the socio-economic sphere of the state]. *Zakony Rossii: opyt, analiz, praktika, (3)*, 60–64.

Semikalenova, A. I. (2019). Tsifrovye sledy i ikh nositeli kak obyekty sudebno-ekspertnogo issledovaniya [Digital traces and their carriers as objects of forensic examination]. В *Sovremennye problemy tsifrovizatsii kriminalisticheskoy i sudebno-ekspertnoy deyatelnosti: Materialy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem* (Moscow, 5 April 2019) (pp. 212–215). Moscow: RG-Press.

Tanenbaum, A. S., & Austin, T. (2013). *Structured computer organization* (6th ed.). London: Pearson.

Teoriya informatsionno-komp'yuternogo obespecheniya kriminalisticheskoy deyatelnosti [Theory of information and computer support of forensic activity] (monografiya [Monograph]) / ed. by E. R. Rossinskaya. (2022). Moscow: Prospekt.

Chesnokova, E. V., Usov, A. I., Omelyanyuk, G. G., & Nikulina, M. V. (2023). Iskusstvennyy intellekt v sudebnoy ekspertologii [Artificial intelligence in forensic expertology]. *Teoriya i praktika sudebnoy ekspertizy [Theory and Practice of Forensic Science], 18*(3), 60–77. https://doi.org/10.30764/1819-2785-2023-3-60-77

Information about authors:

Bakyt Sara Burkitbekkyzy (corresponding author) – master of Law, PhD doctoral student, Higher School of Law, Turan University (Almaty, Kazakhstan, e-mail: sara.bakyt@bk.ru).

Alaeva Gulnaz Tursunovna – candidate of Law, Professor, Higher School of Law, Turan University (Almaty, Kazakhstan, e-mail: alaevagulnaz@mail.ru).

Zhanibekov Akynkozha Kalenovich – PhD, Professor, Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University (Almaty, Kazakhstan, e-mail: zhan.akin@gmail.com).

Edvardas Juchnevicius – doctor of Law, Professor, Faculty of Law and Administration, University of Gdańsk (Gdańsk, Poland, e-mail: edvardas.juchnevicius@ug.edu.pl).

Rakhmetulina Bagdat Saginganovna – candidate of Law, Head of the Department of Law at Kokshetau University named after Sh. Ualikhanov (Kokshetau, Kazakhstan, e-mail: bagdat_82@mail.ru).

Авторлар туралы мәлімет:

Бақыт Сара Буркитбекқызы (корреспондент-автор) – заң ғылымдарының магистрі, Тұран университеті Құқық жоғары мектебінің докторанты (Алматы, Қазақстан, e-mail: sara.bakyt@bk.ru).

Алаева Гульназ Турсуновна – заң ғылымдарының кандидаты, Тұран университеті Құқық жоғары мектебінің профессоры (Алматы, Қазақстан, e-mail: alaevagulnaz@mail.ru).

Жанибеков Акынкожа Каленович – PhD докторы, әл-Фараби атындағы Қазақ ұлттық университеті, қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедрасының профессоры (Алматы, Қазақстан, e-mail: zhan.akin@gmail.com).

Эдвардас Юхневичус – заң ғылымдарының докторы,, Гданьск университеті, құқық және басқару факультетінің профессоры (Гданьск, Польша, e-mail:edvardas.juchnevicius@ug.edu.pl).

Рахметулина Багдат Сагингановна – заң ғылымдарының кандидаты, Ш.Уәлиханов атындағы Көкшетау университетінің Құқық кафедрасының меңгерушісі (Көкшетау, Қазақстан, e-mail:bagdat_82@mail.ru).

Сведения об авторах:

Бакыт Сара Буркитбекқызы (автор-корреспондент) – магистр юридических наук, докторант Высшей школы права Университета Туран (Алматы, Казахстан, e-mail: sara.bakyt@bk.ru).

Алаева Гульназ Турсуновна – кандидат юридических наук, профессор Высшей школы права Университета Туран (Алматы, Казахстан, e-mail: alaevagulnaz@mail.ru).

Жанибеков Акынкожа Каленович – доктор PhD, профессор кафедры уголовного права, уголовного процесса и криминалистики Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: zhan.akin@gmail.com).

Эдвардас Юхневичус – доктор юридических наук, профессор факультета права и управления Гданьского университета (Гданьск, Польша, e-mail: edvardas.juchnevicius@ug.edu.pl).

Рахметулина Багдат Сагингановна – кандидат юридических наук, заведующая кафедрой права Кокшетауского университета имени Ш. Уалиханова (Кокшетау, Казахстан, e-mai: bagdat_82@mail.ru).

Previously sent (in English): January 26, 2026.
Re-registered (in English): February 12, 2026.
Accepted: March 20, 2026.