

The Procedure for Submitting Electronic Data in Criminal Proceedings: Foreign Experience and Issues of Its Implementation into National Legislation

Ulmasjon Sayfullayev

Lecturer at the Department of Criminal Procedure Law of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Received: 15 July 2026; **Accepted:** 04 August 2026; **Published:** 28 August 2026

Abstract: The article undertakes a comparative analysis of the legal regulation of the institution of the submission of electronic data in criminal proceedings against the background of the experience of foreign states. Assessing the amendments introduced into the Criminal Procedure Code of the Republic of Uzbekistan in 2024, the author identifies three systemic inconsistencies that persist within this institution. On the basis of an analysis of the legislation of the Russian Federation, the Republic of Kazakhstan, the Federal Republic of Germany, the French Republic and the United States of America, as well as of the Budapest Convention and the ISO/IEC 27037 standard, ways of eliminating these inconsistencies are set out. Five criteria for the implementation of foreign solutions into national legislation are elaborated, and concrete legislative proposals are formulated on their basis. Particular attention is devoted to the conditions for introducing these proposals into judicial and investigative practice.

Keywords: Electronic data; digital evidence; submission of evidence; comparative jurisprudence; implementation; checksum (hash value); participation of a specialist; admissibility of evidence; electronic document; inviolability of private life.

Introduction: The digitalisation of social life has brought about a situation in which the greater part of the information of significance for proof in criminal proceedings exists in electronic form. Correspondence, financial transactions, video surveillance recordings and geolocation data are today among the most frequently encountered sources of information in criminal cases. This state of affairs confronts procedural legislation with the task of creating a reliable legal mechanism for introducing electronic data into criminal proceedings.

An important step in this direction has been taken in the Republic of Uzbekistan. Law No. ZRU-1003 of 21 November 2024 introduced into the Criminal Procedure Code the concepts of electronic data (Article 204¹) and digital evidence (Article 204²), laid down the procedure for submitting electronic data on one's own initiative (Article 201¹), and enshrined in Article 95¹ the rule on the inadmissibility of electronic data obtained without the participation of a specialist [1].

At the same time, the reform did not encompass the institution of submission in its entirety. Since the new provisions concerning electronic data have not been integrated into the existing system of Articles 198–202, a number of inconsistencies have arisen within the institution. In these circumstances, the study of the experience of foreign states in resolving this matter acquires particular significance, for the problem of handling digital evidence is common to all legal systems, and in some of them the possible solutions have already been tested in practice.

The purpose of the present article is to analyse foreign experience in the field of the submission of electronic data, to define the criteria for its implementation into national legislation, and, on that basis, to formulate concrete legislative proposals.

METHODOLOGY

The study employs the comparative-legal, systemic-structural, legal-dogmatic and formal-logical methods. The comparative-legal method covered the legislation

of states belonging to three legal families: the states of the Commonwealth of Independent States (the Russian Federation, the Republic of Kazakhstan), states of the continental legal system (the Federal Republic of Germany, the French Republic), and states of the common law system (the United States of America). International instruments and standards, as well as the case-law of the European Court of Human Rights, were likewise examined. The systemic-structural method served to identify the internal links between the provisions governing the institution of submission; the legal-dogmatic method was applied in interpreting the provisions currently in force; and the formal-logical method was used to verify the internal consistency of the provisions proposed.

The state of scholarship on the subject

The general theoretical foundations of the institution of the submission of evidence were elaborated in the studies of S.A. Sheifer [2], P.A. Lupinskaya [3], A.R. Belkin [4] and Yu.K. Orlov [5]. S.A. Sheifer substantiates the proposition that the body of rules governing the methods of collecting evidence must be systemic and internally free of contradiction, and that the defining features of each method must be clearly delineated. Yu.K. Orlov, for his part, emphasises that acceptance of a submitted object by the competent authority is a necessary but not a sufficient condition for that object to become evidence: procedural formalisation is additionally required [5].

The question of the procedural nature of electronic data has been examined in the works of V.A. Meshcheryakov [6], E.R. Rossinskaya [7], A.I. Zazulin [8] and S.V. Zuev [9]. A.I. Zazulin substantiates the view that the evidentiary significance of digital information depends directly upon whether the process of its acquisition has been documented. In foreign scholarship, E. Casey has demonstrated the necessity of preserving access to the original source when handling digital evidence [10], while O.S. Kerr has shown that risks accumulate at the stage of transferring information from one medium to another [11]. S. Mason emphasises that the separation of electronic evidence from its original form destroys entirely the possibility of verifying it [12].

In national doctrine, the problems of the submission of evidence have been studied by Sh.Kh. Inomjonov [13] and F.M. Mukhitdinov [14]. Inomjonov's study analyses the procedural essence of the institution of submission and questions of its formalisation; since the dissertation was defended in 2005, however, the issue of electronic data is not addressed in it. The procedure for submitting electronic data and its improvement on the basis of foreign experience thus remains a subject

that has not been the object of holistic study in national jurisprudence.

Foreign experience in the field of the submission of electronic data

The Russian Federation. Part 4.1 of Article 164 and Article 164.1 of the Criminal Procedure Code of the Russian Federation lay down safeguards of proportionality in the seizure of electronic media, as well as safeguards against the unwarranted disruption of entrepreneurial activity. Part 2 of Article 164.1, for its part, provides for the participation of a specialist during seizure and for the possibility, upon the application of the lawful owner, of copying the information onto another electronic medium [15]. The provision embodies two ideas. The first is the mandatory character of the specialist's participation: the seizure of electronic storage media may be effected only in the presence of a specialist. The second is a mechanism for protecting the interests of the owner of the information: upon the application of the owner of the medium, or of the owner of the information contained on it, the specialist copies the information from the media being seized onto other media.

The second of these ideas is of particular interest for our national legislation. The Criminal Procedure Code currently in force makes no provision for the owner's right to obtain a copy where electronic data, or the medium carrying them, are taken. Yet for a person engaged in entrepreneurial activity this constitutes a vital necessity: the seizure of a server or a computer may bring the whole of that person's activity to a halt.

The Criminal Procedure Code of the Russian Federation likewise enshrines the rule that an object must first be offered for voluntary surrender, and may be taken compulsorily only where it has not been surrendered. This principle of the gradual escalation to coercion ensures that the institution of submission is clearly delimited from coercive investigative actions.

The Republic of Kazakhstan. The distinctive character of the Kazakh experience is manifested in two respects. First, the Criminal Procedure Code requires that the examination of submitted materials, and the taking of a decision upon them, be effected within the procedural time-limits prescribed [16]. Second, the "e-Criminal Case" information system has been introduced, within the framework of which procedural documents are drawn up and stored in electronic form, while submitted materials are uploaded directly into the system [17].

The principal scholarly conclusion to be drawn from the Kazakh experience is that an information system for receiving electronic procedural documents, recording their movement, storing them and exercising control

over them is capable of enhancing the effectiveness of a legal institution. The existence of a technological platform does not, however, in itself guarantee the admissibility of evidence; distinct procedural and technical safeguards are required for that purpose.

The Federal Republic of Germany. The German Code of Criminal Procedure (StPO) regulates the question of submission not according to the type of object but according to the procedural nature of the act. Sections 94 and 95 StPO establish the securing of objects of evidentiary significance and the obligation to surrender them. Under §94(2), where an object in a person's possession is not surrendered voluntarily, the question arises of its compulsory seizure (Beschlagnahme). Section 95, for its part, lays down the duty to produce and surrender the object concerned. Section 98 provides for important mechanisms of judicial control over compulsory seizure: as a rule, seizure is ordered by a court; in cases admitting of no delay it may be effected by the public prosecution office or by its officers vested with investigative powers; and in certain cases judicial confirmation is sought subsequently [18]. Within such a structure, electronic data are not set apart as a distinct category of object but are covered by the general rules.

For this reason, the principal significance of the German experience for Uzbekistan lies not in the creation of a separate category of object for electronic data, but rather in the idea of drawing a procedural distinction between voluntary surrender and compulsory seizure, and of strengthening judicial control over coercive interference.

The French Republic. French law, while belonging like German law to the continental tradition, resolves the same problem by different means. Article 60-1 of the Code of Criminal Procedure (Code de procédure pénale) empowers the public prosecutor and officers of the judicial police to require from any person, private or public body, or public administration in possession of information of interest to the investigation — including information derived from a computer system or from the processing of personal data — the surrender of that information, in particular in digital form and, where appropriate, in accordance with standards laid down by regulation; the obligation of professional secrecy may not be invoked against such a requisition without legitimate reason [19]. Failure to respond promptly and, where applicable, in accordance with the standards required is punishable under the second paragraph of Article 60-1 by a fine of 3,750 euros; the persons enumerated in Articles 56-1 to 56-5 (advocates, journalists, physicians, notaries and others) are exempted from that penalty, and information may be surrendered by them only with their consent. That

same paragraph further provides, on pain of nullity, that material obtained through a requisition made in breach of Article 2 of the Law of 29 July 1881 on the freedom of the press may not be placed in the case file.

Of particular significance is Article 60-1-2, introduced by Law No. 2022-299 of 2 March 2022, which — on pain of nullity — permits requisitions relating to the technical data identifying the source of a connection, to terminal equipment, and to traffic and location data only where the needs of the procedure so require and only in the cases exhaustively enumerated therein: where the proceedings concern a serious crime or an offence punishable by at least three years' imprisonment; where an offence punishable by at least one year's imprisonment has been committed through the use of an electronic communications network and the sole object of the requisition is to identify its perpetrator; where the requisition concerns the victim's terminal equipment and is made at the latter's request; and in proceedings for the search for missing persons [20]. This provision was adopted in response to the case-law of the Court of Justice of the European Union; by its judgments of 12 July 2022 the Criminal Division of the Court of Cassation additionally required that such requisitions be subject to prior review by a court or an independent administrative authority.

The French experience is instructive precisely by contrast with the German. German law strikes the balance through the procedural nature of the act, distinguishing voluntary surrender from compulsory seizure and subjecting the latter to judicial control; France, by contrast, retains requisition as a distinct institution but differentiates within it according to the degree of intrusiveness of the data and the gravity of the offence, reinforcing that differentiation by the sanction of nullity. For Uzbekistan this comparison is of twofold significance. First, it demonstrates that retaining the existing institution of requisition is not in itself an obstacle to securing constitutional guarantees, provided that the institution is internally differentiated (the third and fourth criteria). Second, the French model confirms the soundness of an approach under which the requirement itself is enshrined in the statute while the technical standards for the surrender of data are determined by subordinate regulation (the second criterion), and it demonstrates that a procedural safeguard operates in practice only where it is attended by a specific sanction — a fine for failure to comply, and nullity both for requisitions encroaching upon the protection of journalistic sources and for breach of the conditions governing the requisition of connection data (the fifth criterion).

The United States of America. Rules 902(13) and 902(14) of the Federal Rules of Evidence permit the

authenticity of certain types of electronic evidence to be established through the certificate of a qualified person, without requiring separate testimony at trial. In particular, Rule 902(14) provides for the authentication of data copied from an electronic device, storage medium or file by means of a process of digital identification — in practice, most often through hash values [21]. This mechanism does not, however, resolve automatically all the requirements of admissibility; it serves in the first place to confirm authenticity.

This solution appreciably lightens the burden of proving the authenticity of digital evidence and expedites the trial. Its conceptual foundation lies in the proposition that a technical means of identification (a checksum) is more objective and more readily verifiable than human testimony.

International instruments and standards. Articles 16 to 18 of the Budapest Convention establish interrelated yet substantively distinct procedural mechanisms for handling electronic data. Article 16 governs the expedited preservation of stored computer data; Article 17, the expedited preservation and partial disclosure of traffic data; and Article 18, the production order in respect of specified computer data [22]. Accordingly, in improving the legislation of Uzbekistan, it is necessary to consider as a distinct institutional matter not only preservation but also the production order mechanism.

The international standard ISO/IEC 27037 lays down the requirement of an unbroken chain of custody in the identification, collection, acquisition and preservation of digital evidence [23]. In accordance with the standard, every action performed in respect of digital evidence — by whom, when, by what means and for what purpose it was carried out — must be documented.

The positions of the European Court of Human Rights. In the Court's case-law, the lawfulness of a measure for the collection of evidence is assessed by reference to its proportionality to the aim pursued. In its judgment in *Natunen v. Finland* the Court emphasised that a refusal to examine evidence adduced by the defence must be reasoned, and that the possibility of challenging such a refusal must be secured [24]. This position confirms the necessity of attending the institution of submission with procedural safeguards.

Criteria for the implementation of foreign experience

Mechanical copying constitutes an inadmissible error in transposing foreign legal solutions into national legislation: every provision rests upon the internal logic, the procedural traditions and the institutional capacities of its own legal system. We therefore

consider it expedient to apply the following five criteria.

The first criterion — the commonality of the problem.

A foreign solution must resolve a problem that likewise exists in our own conditions. Where the problem does not arise in the national context, the transposition of its solution creates a superfluous normative burden.

The second criterion — compatibility with legal traditions.

The legal form of the solution must correspond to the national procedural model. Thus, the right of the holders of professional secrets to refuse to produce material, as provided for in the German model, runs counter to our own system: what our system provides is not a right of refusal, but rather measures precluding the disclosure of the information obtained. The idea is therefore adopted, while its form is modified.

The third criterion — institutional feasibility.

The solution must be capable of application within the existing human, technical and organisational capacities. Solutions such as an electronic case-management system require phased introduction.

The fourth criterion — conformity with constitutional guarantees.

The solution must not increase the degree of restriction of individual rights and freedoms. In particular, simplified procedures for obtaining electronic data must be balanced against the guarantees of the inviolability of private life.

The fifth criterion — the presence of an enforcement mechanism.

A transposed provision must be adopted together with its own sanction or means of verification; otherwise it acquires, in practice, a merely recommendatory character. As P.A. Lupinskaya has observed, the true value of a procedural safeguard is measured by the consequences that its breach entails [3].

Inconsistencies in national legislation and ways of eliminating them

The Criminal Procedure Code currently in force divides the objects capable of being submitted into three groups: items, documents and electronic data. This classification leaves a borderline case unregulated: to which of these groups does a document drawn up in electronic form belong?

The question is of direct practical significance. A contract certified by an electronic digital signature, or an extract obtained from an information system, is by its very nature electronic data, yet at the same time performs the function of a document. In practice, such an object is frequently printed out on paper and accepted as an ordinary written document. As a result, all the technical guarantees securing its authenticity —

the checksum, the metadata and the electronic signature certificate — are lost.

The German experience indicates a systemic means of forestalling this problem: since regulation under the StPO rests upon the procedural nature of the act rather than upon the type of object, no separate category is set apart for electronic objects and no borderline cases arise [18]. V.A. Meshcheryakov likewise demonstrated that attempts to accommodate objects connected with computer information within traditional classifications inevitably leave borderline cases unregulated [6].

In national conditions it would not be expedient to abandon the existing classification altogether (the third criterion), inasmuch as it is linked to other institutions of the Criminal Procedure Code. We therefore propose that the problem be resolved on the basis of the principle of the primacy of substance: the procedural regime of an object is determined by its nature and not by its outward form. Article 201 of the Criminal Procedure Code should be supplemented by a new part four in the following terms:

“Documents drawn up in electronic form shall be submitted in accordance with the rules laid down by this Code in respect of electronic data. The printing out of such documents on paper shall not alter their nature as electronic data.”

A document emanating from an organisation has a clearly defined subject matter, and its requisition does not entail the disclosure of the personal data of the person submitting it. The electronic data of a natural person are of a different nature: alongside correspondence of significance for the case, that person’s smartphone or personal computer stores the whole detail of his or her private life. E.R. Rossinskaya emphasises that the modern storage medium has become an object reflecting the entirety of an individual’s life activity, and that this circumstance calls for particular caution in the application of traditional procedural measures to it [7].

The fourth criterion (conformity with constitutional guarantees) and the requirement of proportionality developed by the European Court of Human Rights [24] indicate that obtaining a citizen’s electronic data by way of requisition — that is to say, without judicial or prosecutorial control — constitutes a disproportionate interference. Requisition should therefore be applied in respect of enterprises, institutions and organisations, and should extend to documents in electronic form; the electronic data of natural persons, by contrast, should not constitute the subject matter of requisition and, where the need arises, should be obtained through measures subject to judicial control.

In this connection, the rule of the Criminal Procedure

Code of the Russian Federation on the gradual escalation to coercion [15] may be implemented directly into the national system: the object is first offered for voluntary surrender, and only where it has not been surrendered are coercive measures resorted to.

Under part four of Article 95¹ of the Criminal Procedure Code, electronic data obtained without the participation of a specialist in the course of investigative actions involving seizure or examination are to be held inadmissible evidence [1]. Submission, however, has not been included in that list. As a result, one and the same technical safeguard is mandatory in respect of one method while remaining wholly without consequence in respect of another.

In eliminating this inconsistency, both the fifth criterion (the enforcement mechanism) and the third criterion (institutional feasibility) must be taken into account. To extend the sanction to all instances of submission would in practice give rise to wholesale inadmissibility. At the same time, the principal purpose of involving a specialist consists in preserving the integrity of the electronic data and their exact correspondence in the course of technically complex copying, for during the forensic copying of electronic data those data may be altered, partially lost, or their metadata erased [10; 11]. We therefore propose that part four of Article 95¹ be set out in the following wording:

“Electronic data obtained without the participation of a specialist in the course of investigative actions involving seizure or examination, as well as in the course of the technically complex copying of submitted electronic data, shall be held inadmissible evidence. This shall not extend to cases in which the integrity of the electronic data has been secured by other technical means provided for by this Code and that fact has been recorded in the protocol.”

The formulation of this exception in terms of an objectively verifiable condition is of fundamental importance. Were the exception to be defined by reference to cases in which the participation of a specialist has been “found unnecessary”, the decision to invoke it would be left to the assessment of the very person who dispensed with the safeguard, and the provision would in practice be deprived of its sanction. In accordance with the fifth criterion, the exception must be tied to a circumstance capable of external verification — namely, the employment of a technical means securing integrity and the recording of that fact in the protocol.

In order to secure an enforcement mechanism for this safeguard, the mandatory content of the record of submission must be supplemented by technical

particulars relating to electronic data: the type and identifying features of the storage medium; the volume and format of the data; the checksum and the method of its calculation; and, where copying has been carried out, the method employed, the technical means used and information concerning the participation of a specialist. A checksum constitutes a mathematically unique “digital fingerprint” of electronic data which, if recorded at the moment of receipt, makes it possible to prove objectively — by subsequent recalculation and comparison — that the data have not been altered. This requirement corresponds to the chain-of-custody rule laid down in the ISO/IEC 27037 standard [23].

It should be noted at this point that the technical standard itself ought not to be incorporated into the text of the statute (the second criterion): the provision requires only that a checksum be calculated and recorded, while the methods of its calculation may be determined at the level of departmental instruments. Otherwise the provision will rapidly become obsolete as technology develops.

Issues of introducing the proposals into judicial and investigative practice

The adoption of a legislative provision does not automatically secure its application in practice. In our view, work must be pursued in the following four directions if the proposed solutions are to be introduced into judicial and investigative practice.

The first direction — specification at the level of departmental instruments. It would be expedient for the methods of calculating checksums, the list of software tools that may be employed, and the technical procedure for receiving electronic data to be laid down in guidelines approved by joint decisions of the competent authorities. At the level of the statute only the requirement itself is enshrined, which obviates the need to amend the provision as technology develops.

The second direction — the development of a model form of the record. For the practitioner, completing a ready-made form is considerably more convenient than committing a list of mandatory particulars to memory. The model form should make provision for a separate section devoted to electronic data.

The third direction — the availability of specialists. The practical operation of a provision requiring the participation of a specialist depends upon the availability of a sufficient number of appropriately qualified specialists. Before the provision is introduced, therefore, the level of availability of digital forensics specialists in the territorial units should be assessed and, where necessary, targeted training programmes should be implemented.

The fourth direction — training and methodological support. Methodological recommendations on the new provisions should be prepared for those who apply the law, and questions relating to the handling of electronic data should be incorporated into the relevant curricula of higher education institutions. As S.V. Zuev has observed, the principal obstacle to the introduction of digital technologies into criminal proceedings is not of a normative but of a qualificational character [9].

CONCLUSIONS

The comparative-legal analysis undertaken permits the following conclusions to be drawn.

First, the reform effected by Law No. ZRU-1003 of 21 November 2024 created the legal foundations for introducing electronic data into criminal proceedings; the new provisions were not, however, fully integrated into the existing system of the institution of submission. As a result, electronic data have remained incompletely regulated within that institution by comparison with other categories of object.

Second, it is expedient to apply five criteria in implementing foreign experience: the commonality of the problem; compatibility with legal traditions; institutional feasibility; conformity with constitutional guarantees; and the presence of an enforcement mechanism. These criteria guard against the mere transposition of a solution and secure its correct and effective application in practice.

Third, the procedural regime of a document drawn up in electronic form must be determined on the basis of the principle of the primacy of substance, since the procedure for submitting electronic data is settled by their nature and not by their outward form. The German model demonstrates a systemic solution to this problem; in national conditions, however, it is expedient to retain the existing classification and to resolve the problem by means of a special rule.

Fourth, the procedure for submitting electronic data upon requisition should be differentiated according to the subject concerned: requisition is applied in respect of organisations and extends to documents in electronic form, whereas the electronic data of natural persons, proceeding from the criterion of the inviolability of private life, do not constitute the subject matter of requisition.

Fifth, with a view to eliminating the lacunae in part four of Article 95¹, it is proposed that the rule on the inadmissibility of electronic data obtained without the participation of a specialist be extended to the method of submission as well. The scope of the rule is thereby confined to instances involving the technically complex

copying of submitted electronic data, while an exception is retained in respect of cases in which alternative technical safeguards securing integrity have been applied and that fact has been recorded in the protocol.

Sixth, drawing upon the experience of the United States and upon the ISO/IEC 27037 standard, the guarantees of the authenticity of electronic data should be enshrined at the level of the mandatory particulars of the record, while the technical details should be determined in departmental instruments.

Seventh, proceeding from the experience of the Russian Federation and of the Budapest Convention, it is expedient to introduce, as free-standing provisions, the right of the owner of information to obtain a copy and the institution of the expedited preservation of electronic data.

Eighth, the introduction of these proposals into practice is not confined to legislative amendment: it requires specification in departmental instruments, the development of a model form of the record, an assessment of the availability of specialists, and the establishment of training and methodological support.

The implementation of these proposals will serve to enhance the reliability of the introduction of electronic data into criminal proceedings, to reduce disputes concerning the admissibility of evidence, and to strengthen the protection of the constitutional rights of the individual.

REFERENCES

1. Criminal Procedure Code of the Republic of Uzbekistan. – lex.uz. URL: <https://lex.uz/docs/-111460#-7234994>
2. Sheifer S.A. Sledstvennye deistviya. Sistema i protsessual'naya forma [Investigative Actions: System and Procedural Form]. Moscow, Yurлитinform Publ., 2001. 208 p. (In Russ.)
3. Lupinskaya P.A. Dokazatel'stva i dokazyvanie v sovremennom ugovnom protsesse [Evidence and Proof in Contemporary Criminal Procedure]. Moscow, Norma Publ., 2010. 320 p. (In Russ.)
4. Belkin A.R. Teoriya dokazyvaniya v ugovnom sudoproizvodstve [The Theory of Proof in Criminal Justice]. Moscow, Norma Publ., 2005. 528 p. (In Russ.)
5. Orlov Yu.K. Problemy teorii dokazatel'stv v ugovnom protsesse [Problems of the Theory of Evidence in Criminal Procedure]. Moscow, Yurist Publ., 2009. 175 p. (In Russ.)
6. Meshcheryakov V.A. Osnovy teoreticheskoi modeli prestuplenii v sfere komp'yuterno informatsii [Foundations of a Theoretical Model of Offences in the Sphere of Computer Information]. Voronezh, Voronezh State University Publ., 2002. 92 p. (In Russ.)
7. Rossinskaya E.R. Tsifrovaya kriminalistika: teoreticheskie i prakticheskie problemy [Digital Forensics: Theoretical and Practical Problems]. Moscow, Prospekt Publ., 2019. 328 p. (In Russ.)
8. Zazulin A.I. Pravovye i metodologicheskie osnovy ispol'zovaniya tsifrovoi informatsii v dokazyvanii po ugovnym delam [Legal and Methodological Foundations of the Use of Digital Information in Proof in Criminal Cases]. Yekaterinburg, 2018. 250 p. (In Russ.)
9. Zuev S.V. Informatsionnye tekhnologii v ugovnom sudoproizvodstve [Information Technologies in Criminal Justice]. Moscow, Yurлитinform Publ., 2019. 240 p. (In Russ.)
10. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Waltham, Academic Press, 2011. 840 p.
11. Kerr O.S. Searches and Seizures in a Digital World. Harvard Law Review, 2005, vol. 119, no. 2, pp. 531–585.
12. Mason S., Seng D. (eds.) Electronic Evidence. 4th ed. London, University of London, 2017. 448 p.
13. Inomjonov Sh.Kh. Jinoyat protsessida dalillarni taqdim qilish va ulardan foydalanish muammolari [Problems of the Submission and Use of Evidence in Criminal Proceedings]. Cand. Sci. (Law) Diss. Tashkent, Tashkent State Institute of Law, 2005. 207 p. (In Uzb.)
14. Mukhitdinov F.M. Jinoyat protsessi: mohiyat, mazmun, shakl [Criminal Procedure: Essence, Content, Form]. Tashkent, Adolat Publ., 2002, p. 49. (In Uzb.)
15. Criminal Procedure Code of the Russian Federation (as amended), Articles 164¹, 183. – pravo.gov.ru. (In Russ.)
16. Criminal Procedure Code of the Republic of Kazakhstan (as amended). adilet.zan.kz. (In Russ.)
17. Akhpanov A.N., Akhmetov A.T. Obshchaya kharakteristika e-ugolvnogo dela [General Characteristics of the e-Criminal Case]. Aktual'nye problemy dal'neishego razvitiya zakonodatel'stva v svete realizatsii konstitutsionnykh printsipov deyatel'nosti ugovnoi yustitsii: materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii. Astana, Eurasian National University Publ., 2018, p. 38. (In Russ.)
18. Strafprozessordnung der Bundesrepublik

Deutschland, §53, 94, 95, 97, 98. – gesetz-im-internet.de. (In Germ.)

19. Code de procédure pénale de la République française, art. 60-1, 60-2, 77-1-1. – legifrance.gouv.fr. (In Fr.)
20. Code de procédure pénale de la République française, art. 60-1-2 (introduced by Loi n° 2022-299 du 2 mars 2022). – legifrance.gouv.fr. (In Fr.)
21. Federal Rules of Evidence (USA), Rules 902(13), 902(14). – uscourts.gov.
22. Convention on Cybercrime (Budapest, 23.XI.2001, ETS No. 185), Articles 16–18.
23. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva, ISO, 2012. 46 p.
24. European Court of Human Rights. *Natunen v. Finland*, application no. 21022/04, judgment of 31 March 2009.