DOI: 10.2507/29th.daaam.proceedings.070

ELECTRONIC DOCUMENT AS A TOOL OF DIGITAL ECONOMY

Anna Zharova[a,b], Vladimir Elin[b] & Peter Panfilov[b]

[a] *The Institute of State and Law of The Russian Academy of Sciences, Znamenka St. 10, Moscow 119019, Russian Federation*
[b]*National Research University – Higher School of Economics, Myasnitskaya St. 20, Moscow 101000, Russian Federation*

This Publication has to be referred as: Zharova, A[nna]; Elin, V[ladimir] & Panfilov, P[eter] (2018). Electronic Document as a Tool of Digital Economy, Proceedings of the 29th DAAAM International Symposium, pp.0479-0485, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/29th.daaam.proceedings.070

Abstract

The article reviews the problems of using an electronic document (i.e. legally significant computer information) as a necessary tool for building a digital economy. This problem becomes of special importance in terms of implementation of distributed computing in the interests of modern technologies, including Big Data, Artificial Intelligence, Blockchain, Industry 4.0, Industrial Internet of Things, Virtual and Augmented Reality technologies, etc. The authors show that in case of development and adoption of the Law "On Electronic Document", we can link the concepts of "Electronic Document" and "Data Message", and can identify several categories of Computer Information (Electronic data interchange) having a significance: specified Computer data, traffic data, stored Computer data, traffic data, content data.

Keywords: electronic document; digital technologies; electronic signature; digital economy

1. Introduction

At present time as necessary condition for the creation of innovative development of the Russian market of products and services we must address the problem of transition to advanced Digital technologies and the creation of systems for processing large volumes of data, machine learning and artificial intelligence 0.

The purpose of the State Policy of the Russian Federation is to create an ecosystem of the Digital economy, in which data in Digital form is a key factor of production in all spheres of socio-economic activity 0. As the main tool for solving these problems are considered end-to-end digital technologies, including Big Data, Neural Networks and Artificial Intelligence, Blockchain, Quantum Computing, new production technologies, Industrial Internet of Things (IIoT), Robotics, Sensor and Wireless Communication Technologies, Virtual and Augmented reality technologies. According to some experts: “The growing role of the Internet of Things (IoT) concept is proved by its application in the number of areas such as the development of smart cities, the management of energy resources and networks, mobility, transport, logistics, etc.” [3, 4]. The peculiarity of Digital Technology is the possibility of unlimited increase in productivity through scaling. At the same time, the work is dynamically and automatically distributed to different machines of the system for parallel processing of Information by a complex of network machines.

At the same time, the user has no idea on what machine and to what extent the Information processing activities are carried out [5, 6, 7]. The use of Digital Technology is based on the property of Information to be freely transferred among the participants of Information relations, which creates the need to give information some degree of organization, allowing to take into account, identify, and perform other orderly actions with respect to Information. Information loses its integrity when processed in a distributed system and the question arises of the legal regulation of Information relations within the framework of taking into account the problems of decision-making under uncertainty [8].

The modern practical approach to Electronic Document emphasizes its component as a Documented Information suitable for human perception with the use of electronic Computers, leaving without attention its presentation in a form suitable for transmission over Information and telecommunication networks and for processing in Information systems.

2. Statement of the problem

In accordance with Law "On Information, Information Technology and Information Protection" (hereinafter: "The Law "On Information") [23], an Electronic Document is a Documented Information provided in electronic form, i.e. in a form suitable for the:

- Human perception, when using computers
- Transmission over information and telecommunication networks
- Processing in information systems.

As an Electronic Document, first of all, files containing text, graphic, audio-visual (multimedia) information are considered. This point of view is not entirely correct, since a significant amount of Computer Information is contained precisely outside the contents of the files.

It should be taken into account that the Electronic Document as Computer Information can be presented at several levels: physical (on a physical medium and in the process of interaction with the carrier); logical; syntactic; semantic; pragmatic [52].

The Electronic Document as a form of Information submission should be correlated with the norms of civil Law, which define oral and written forms of transactions. At the same time, par. 2 of article 160 of the Civil Code establishes that the use of an Electronic Signature or other analogue of a handwritten signature in transactions is allowed in cases and in the manner provided by Law, other legal acts or agreement of the parties. Par. 2 art. 434 the Civil Code of the Russian Federation establishes that a contract in writing can be concluded by exchanging Documents by mail, Telegraph, teletype, telephone, electronic or other communication, which allows to establish reliably that the Document comes from the party to the contract [9].

The Resolution of the Plenum of the Supreme Court of the USSR of April 3, 1987 № 3 (now no longer valid) determined that: "On strict compliance with the procedural legislation in the administration of justice in civil cases" determined that, if necessary, the court may be accepted as written evidence Documents obtained using electronic Computer Technology, which materials are evaluated in conjunction with other evidence" [10].

The Supreme Arbitration Court of the Russian Federation assessed the evidence produced and signed with the help of electronic Computer Technology, which uses a system of Digital (electronic) signature [11].

There are two points of view that determine the place and role of an Electronic Document related to the possibility of applying the legislation by analogy:

The possibility of applying the analogy of the Law in determining the place and role of an Electronic Document was expressed: Chechot D., who claimed that "the specific features of the Information carrier suggest specific ways of its reproduction, i.e. if the Document on a conventional medium can be perceived in the usual way (directly read), then" the technical medium in many cases requires decoding» [12], Tikhinya V. considered magnetic records as material evidence [13], Tkachev A. believed that " ... Computer Documents are already widely and effectively used in a variety of legal relations as Documents, ... the legislative definition of the Document-proof allows to regulate the technical and technological features of these Documents», ets. [14, 15].

The opposite point of view was expressed: Treushnikov M., who pointed out that "the reproduction of Information stored on magnetic media requires methods different from written and material evidence" [16]; Bonner A.: "machine Documents can hardly be automatically attributed to the traditional written and other modern means of recording Information and physical evidence, as they and other modern procedural media: videos, photos, movies, etc., possess significant characteristics, which should be reflected in both the material and procedural legislation." [17]; Karas I.: "new ways of fixing Information in the Computer memory" allow to raise the question of the separation of records in the Computer memory in a new class of Information and computational evidence." [18]. Baturin Yu. included Electronic Documents in a separate kind of "Documentary and Computer evidence" [19], Prokhorov A. offered to provide magnetic recording independent means of proof [22]. This problem is of particular importance in cross-border data transmission [20, 21].

In terms of building a Digital economy, the problem of determining the status of an Electronic Document that allows to:

- Identify material carriers containing Documented Information as a expressed subject form of Documented Information
- Develop a set of measures aimed at the perception, use of Information, transfer and provision of Information in the course of interaction of various subsystems in the storage, processing and production of Information; in relation to an Electronic Document as a Documented Information
- Formulate requirements for the composition of the details of Documents and forms of Documents
- Develop rules for the organization of Document flow, creation, provision, storage and accounting of media

3. Computer Information as an Object of Legal Regulation

According to the provisions of the Law "On Information", the Information is defined as knowledge (messages, data), regardless of the form of their presentation [23]. The legal definition reflects the need for the relationship of Information as a phenomenon of the material world with the problems of its knowledge, i.e. the definition, transmission, preservation of properties, parameters and characteristics of Objects, phenomena and processes, when the concept of Information, its characteristics and properties comes to the fore. Actually, this point of view is interfaced with the scientific perception of Information as a result of reflection, when carried out "the process and the result of the impact of one material system on another, which is a reproduction in a different form features (features, sides, structure) of one system in features (features, structure) of another system" [24]. The reflection is related to the philosophical categories of matter, movement, space, time, energy and field.

The formation of an approach to Information as a result of reflection should be associated with the need to obtain results from the practical use of knowledge about Information.

For the first time about the theory of Information referred to in the late 40-ies of the XX century in the work of C. Shannon [25], however, by the mid 50-ies scientists began to distinguish between the quantity and quality of Information [26], then, began to highlight the mathematical, semantic [27] and pragmatic [28, 29] approaches, which allowed to distinguish approaches to Information as a phenomenal characteristic of the properties of matter.

In the middle of the last century, the question of the material essence of Information was devoted to a significant number of works of scientists of various branches of knowledge, including scientists-philosophers [30-36]. At the same time, it was assumed that the concept of "energy" was added to the two main forms of reality (Matter and field) as natural science developed. Next, Wiener N. proposed to consider the basis of all existing as the unity of Matter and field, on the one hand, Information — on the other, and energy — on the third.

Referring to the statement of N. Wiener that "…Information is Information, not Matter and not energy…", should be borne in mind that he further pointed out: "that materialism, which does not recognize this, can not be viable at the present time" [37]. Thus, the basis of Information relations is the material essence of Information.

In modern science, the content of Matter is understood as the unity of matter, field and plasma generated by vacuum fluctuations. In addition, the concept of Matter includes the Information aspect of the existence of all material systems, which expresses the order of things and phenomena in the material world [38].

Linking Information with reflection highlights the direct and indirect types of reflections. Direct reflection is all forms of contact reflection - changes in position, structure, shape, contour, magnitude and other parameters of the reflecting Object under its influence with the reflected Object. Indirect reflection occurs when there is no direct contact between the reflected and reflective Objects, reflection is mediated through the transmission medium of reflection.

Thus, the activity of providing Information about the Object, Matter or Phenomenon is a physical activity to find, record and analyse changes in the world that have occurred as a result of the interaction of material Objects, based on the following principles:

- Any Phenomenon of the material world can be individually defined and must have a stable structure
- The set of represented reflections of the properties of the Phenomenon of the material world also includes the relationship between the reflected Object and the environment
- Information about the Object, Matter or Phenomenon is a practical activity to display the stable properties of Objects
- Information about the Object, Matter or Phenomenon arises as a result of interaction with the environment and characterizes the set of changes made to the environment.

When the relationship between the Information and its material carrier properties of each of them vary greatly recording of the results can be done by Documenting the Information, and the most developed methods of Documentation with proper details only on paper. At the same time, both the details and the content of the Document record not only the actual Information about the changes in the surrounding world that are of interest to us, but also the process of obtaining and recording it, which leads us to the concept of Documented Information. In this regard, it is reasonable to include in the legislation the concept of "Document", which means a material carrier with fixed on it in any form of Information in the form of text, sound, images and (or) their combination, which has details that allow its identification, and is intended for transmission in time and space for public use and storage [48].

Thus the Documented Information is understood as the Information recorded on the material carrier by Documenting with the details allowing to define such Information or in the cases established by the legislation of the Russian Federation its material carrier [23];

The result of Documenting the Information is a number of clearly expressed legal consequences, which include:

- The expressed subject form of the Documented Information allowing to realize the property right and other real rights to the material carriers containing the Documented Information
- The possibility of making an ordered action against the Documented Information,- the perception, use of Information, communication and provision of Information during the interaction of the various subsystems in storage, processing and extraction of Information
- The presence of certain rules of Document management, creation, provision, storage and accounting of media
- The greatest effectiveness of legal, organizational and technical protection measures aimed at ensuring the protection of Information
- The ability to formulate requirements for the composition of the details of Documents and forms of Documents
- Availability of requirements for the characteristics of Document management systems, including reliability, integrity, complexity and consistency.

By the physical nature of the medium it is possible to classify the Documented Information as Information on the classical material medium, the attribute of which is the possibility of perception of the specified Information without special technical means; and the Documented Information in the form of an Electronic Document.

Currently, the concepts of "Electronic Document Exchange" and "Electronic Document" are widely spread in the regulations. Some experts are of the opinion that the legal regulation of an Electronic Document Exchange is carried out in full by a significant number of regulations. Indeed, the sample in the legal system "Consultant plus" gives more than a thousand regulations, one way or another related to Electronic Document Exchange.

The foreign experience of legal regulation in this sphere is of interest. Thus, in the US, the legal status of an electronic document is revealed through the prism of admissible evidence.

Initially, the U.S. judicial system imposed extremely high requirements on an electronic document submitted as evidence. There are facts that the us courts initially imposed increased requirements on electronic documents (in addition to General evidentiary requirements), including the indication of the original source of the computer program with which they were obtained, the procedures under which the information was entered, as well as the results of tests confirming the accuracy and reliability of electronic devices [39].

Currently, the legal status of an electronic document is regulated by a number of regulations, including the USA Patriot act, Federal rules of criminal procedure and Federal rules of evidence, court precedents.

In regard to the Federal Rules of Criminal Procedure, it should be borne in mind that the electronic documents as evidence are divided into direct (non-hearsay), indirect (hearsay), and combine the properties of both.

The direct evidence includes those that are generated by a computer without human subdivided into two categories, namely: Computer-generated records and Computer-stored records.

There is also quite a reasonable view on the allocation of the third category, which includes a combination of two of these [40].

Besides, classification of electronic documents is determined by the form of presentation of the fact that there are two formats of electronic information: hard copy (hard or hard copy) and machine readable format (machine-readable copy).

The shape of the proof electronic documents are divided [41-43]:

- Raw data (source data) including data entered by the person and related documents in general
- Databases
- Codes necessary to interpret computer information (codes needed to decrypt the e-information)
- Commercial software
- Computer systems, which are defined as computers, servers, local area networks, magnetic media of various kinds.

The U.S. experience in the form of an electronic document as evidence of procedural shows that Federal Rules of evidence require the provision of information in a usable form. In many cases such recognized hardcopy-print file contents on the paper. However, the rule does not contain any provision prohibiting or restricting the use of the second format. Sets a number of precedents that, under certain circumstances, hard copy can not be recognized as "fitness for use" and requires parties to provide data in machine-readable format; in the form of punched cards, magnetic tapes, floppy disks, CD; ROMs, zipp; drive or directly to your hard drive [44]. Similar measures to determine the legal status of electronic documents are being taken in the UK [45], India [46], China and a number of other countries.

A similar approach is taken by the European Convention on cybercrime [47], under which the procedural law should include measures to improve:

- Expedited preservation of stored computer data (Article 16)
- Expedited preservation and partial disclosure of traffic data (Article 17)
- Production order (Article 18)
- Real-time collection of traffic data and search and seizure of stored computer data (Articles 19, 20).

4. Relationship between the concepts of "Electronic Document" and " Electronic Signature"

When determining the legal status of an Electronic Document, the main attention is paid to the Federal Law No. 63-FZ "On Electronic Signature", which defined Information in electronic form attached to other Information in electronic form (signed Information) or otherwise connected with such Information and which is used to determine the person signing the Information [49].

Thus, an Electronic Document in the sense of this Law means Information in a form suitable for processing, storage and transmission using electronic means of communication.

The Law establishes only one type of Electronic Signature developed on the basis of asymmetric cryptographic transformation and does not provide for the possibility of using other analogues of a handwritten signature. The Law also establishes a fairly complex procedure for the use of Electronic Digital Signatures, regulates in detail the procedure for confirming the authenticity of Electronic Signatures in public and corporate Information systems. Thus, if the Electronic Signature and the text of the Document are accepted as such, the public key of the Electronic Signature is subject to confirmation: either the parties accept it as an original on the basis of an additional agreement, or use a third independent party (certification center), which under its responsibility confirms the ownership of the public key to a particular person by issuing a certificate.

In its present form, the concept of an Electronic Signature is identical to that of the UNCITRAL Model Law "On Electronic Signature" [50]. These provisions are developed in the Model Law "On Electronic Digital Signature" adopted in St. Petersburg on 09.12.2000 by Resolution 16-10 at the 16th plenary session of the inter-parliamentary Assembly of the CIS member States [51].

A feature of the Russian Law № 63-FZ "On Electronic Signature" is the fact that the Law distinguishes between a simple and enhanced Electronic Signature. Reinforced is divided into unskilled and qualified. The main emphasis is not on the recognition of the equivalence of an Electronic Document and a paper Document, but on the definition of the conditions of equivalence of an Electronic Document (only signed by an Electronic Signature) to a paper Document [49].

Thus, the final refusal to introduce into the legal space of a transaction in electronic form as a third form of transactions, along with oral and written forms, is fixed. The Law stipulates that only if certain criteria for Electronic Signature are present, an Electronic Document with such signature is recognized as equivalent to a paper Document with a handwritten signature.

Information, signed by the strengthened qualified Digital signature, admits equivalent to the Document on paper, except when Federal Law or adopted in accordance with them normative legal acts established the requirement for a Document solely on paper.

Information signed with a strengthened unqualified Electronic Signature is recognized as equivalent in the cases established by Federal Laws, adopted in accordance with their regulatory legal acts or an agreement between the participants of electronic interaction, providing for the procedure for verification of Electronic Signature.

5. Conclusion

The existing approach in the Russian Federation, in which an Electronic Document can be equated to a paper Document under the condition of using an Electronic Signature, has a number of disadvantages:

- Normative Legal Acts or an agreement between the participants of electronic interaction shall provide rules for the definition of the person signing an Electronic Document by its simple Electronic Signature and the obligation of the person creating and (or) using the key of a simple Electronic Signature to observe its confidentiality
- It is the responsibility of the Information system operator to establish rules for the use of a simple Electronic Signature key
- There is no possibility of formal reference to an Electronic Document, but only to the equivalence of a paper Document under certain conditions
- This circumstance is a significant concession to a number of participants of business turnover, who believe that Electronic Documents are only text documents "made with the help of Computers".

Herewith the concept of "Electronic Document" does not relate to the items "Certified Records Generated by an Electronic Process or System" or "Certified Data Copied from an Electronic Device, Storage Medium, or File" which are used in the U.S. Federal Rules of Evidence. Thus, an Electronic Document in the sense of this Law means Information in a form suitable for processing, storage and transmission using electronic means of communication.

As a prospective solution to the problem could be the development and adoption of the Law "On Electronic Document", postulating the provision of the Model Law "On Electronic Commerce" by the UN Commission on International Trade Law stating that "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message. Data message means Information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (the electronic transfer from Computer to Computer of Information using an agreed standard to structure the Information), electronic mail, telegram, telex or telecopy".

Linking the concepts of "Electronic Document" and "Data Message", one can identify several categories of Computer Information (Electronic data interchange) having significant legal significance: specified Computer data, traffic data, stored Computer data, traffic data, content data.

6. Acknowledgments

We thank the Russian Foundation for Basic Research (RFBR) for their assistance in the project "Comparative legal research methods of Information security in the Russian Federation and EU Members (№ 16-03-00679)".

7. References

[1] The decree of the President of the Russian Federation from 01.12.2016 N 642 (2016), "On the strategy of scientific and technological development of the Russian Federation". Collected legislation of the Russian Federation, 05.12.2016, N 49, p. 6887 (Consultant plus)

[2] The decree of the RF Government from 28.07.2017 N 1632-p (2017), "On approval of the program "Digital economy of the Russian Federation". Collected legislation of the Russian Federation, 07.08.2017, N 32, p. 5138 (Consultant plus)

[3] Ivan, C.; Vujic, M. & Husnjak, S. (2016). Classification of Security Risks in the IoT Environment, Proceedings of the 26th DAAAM International Symposium, pp.0731-0740, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-07-5, ISSN 1726-9679, Vienna, Austria DOI:10.2507/26th.daaam.proceedings.102

[4] Draskovic, N.; Markovic, M. & Hruskar, D. (2017). Challenges of the Challengers: An Insight into the Internationalization Pathway of Croatian Digital Agencies, Proceedings of the 28th DAAAM International Symposium, pp.0895-0901, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/28th.daaam.proceedings.124

[5] Baranov A. P. (2012). Whether it is Possible to protect Confidential Information in the "cloud". High Availability Systems, № 2, vol. 8, 2012, P. 12

[6] Zharova, A.; Elin, V. (2017). The use of Big Data: A Russian perspective of personal data security. Computer Law & security review, 2017, Vol: 33., No. 4., pp. 482–501.

[7] Tanenbaum, Andrew S., van Steen, Maarten. "Distributed systems. Principles and paradigms". - St. Petersburg: Peter, 2003. - 877 pages.

[8] Hansson, S.O. (1994) «Decision Theory: A Brief Introduction», Available from: from: https://web.archive.org/web/20060705052730/http://www.infra.kth.se/~soh/decisiontheory.pdf

[9] The Civil Code of the Russian Federation (part one)" of 30.11.1994 N 51-FZ (1994), Collected legislation of the Russian Federation, 05.12.1994, N 32, St. 3301

[10] Resolution of the Plenum of the Supreme Court of the USSR of April 3, 1987 № 3 (1987), "On strict observance of procedural legislation in the administration of justice in civil cases" // Bulletin of the Supreme Court of the USSR. 1987, No. 3.

[11] Letter of the Supreme Arbitration Court of the Russian Federation dated August 19, 1994 № C1-7/OP-587 (1994), "On individual recommendations adopted at meetings on judicial arbitration practice".

[12] The Soviet Civil Process (1984). Chechina N., Chechot D. (eds.). Leningrad, 1984. P. 156.

[13] Tikhinya, V. (1976). The Use of Criminal tactics in the Civil process. Minsk, 1976. pp. 10 - 11.

[14] Tkachev, A. (2000). Legal status of Computer Documents: main characteristics. Moscow: Gorodets-Izdat, 2000. 54 pages.

[15] Vershinin, A. (2000). Electronic Document: legal form and evidence in court. Moscow: 2000. P. 109.

[16] Treushnikov, M. K. (1999). Judicial evidence. Moscow, 1999. P. 97.

[17] Bonner, A.T. (1990). The rule of admissibility of evidence in civil proceedings: necessity or anachronism? Soviet state and Law. 1990. No. 10. P. 30.

[18] Karas, I. Z. (1988). Legal facts and evidence in the Information relations. Soviet state and Law. 1988. No. 11. P. 92.

[19] Baturin, Yu. M. (1991). Problems of Computer Law. Moscow: Yurid. lit., 1991. P. 184.

[20] Zharova, A.; Elin, V. & Panfilov, P. (2017). Personal Data in Cloud. Russia Experience, Proceedings of the 28th DAAAM International Symposium, pp.1136-1142, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria.DOI: 10.2507/28th.daaam.proceedings.158
[21] Suleykin, A & Panfilov, P. (2017). The Simulation-Based Smart Management Approach for Cellular Network Operation and Planning, Proceedings of the 28th DAAAM International Symposium, pp.0423-0432, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/28th.daaam.proceedings.059
[22] Prokhorov, A. G. (1979). The principle of admissibility of evidence in the Soviet civil procedural Law. Abstract of the thesis for the degree of candidate of legal Sciences. Sverdlovsk, 1979.
[23] Federal Law of 27.07.2006 N 149-FZ (2006), "On Information, Information Technologies and Information Protection". Collected legislation of the Russian Federation, 31.07.2006, N 31 (1 h.), article 3448
[24] Paskov, J. A. (2010). Bases of Information security of investigative and legal actions / ed. by V. A. Shurunov. Moscow, 2010. P.6.
[25] Shannon, C.E. (1948). Mathematical Theory of Communication. Bell System Technical Journal. 1948/ Vol. 27, pp. 379 -423
[26] MacKay, D. (1969). Information, mechanism and meaning. Cambridge and London. 1969
[27] Schrader, Yu. (1989). A. social aspects of Informatics. NTI. 1989. pp. 3-14.
[28] Presman, A. S. (1997). Organization of the biosphere and its space connections. Moscow, 1997.P. 93.
[29] Cities, O. A. (2000). Information Law. Textbook. Moscow, P. 32
[30] Pavlov, T. (1967). Information, reflection, creativity. Moscow, 1967.
[31] Ukrainians, B. S. (1969). Reflection in inanimate nature. Moscow, 1969.
[32] Tyukhtin, V. S. (1972). Reflection, systems, Cybernetics. Moscow, 1972.
[33] Biryukov, B. V. (1974). Cybernetics and scientific methodology. Moscow, 1974.
[34] Ursul, A. D. (1973). Reflection and Information. Moscow, 1973.
[35] Tsonev, V. (1977). Information and reflection. Sofia, 1977.
[36] Yankov, M. (1976). Matter and Information. Sofia, 1976.
[37] Wiener, N. (1958). Cybernetics or control and communication in animal and machine. M., 1958.
[38] Basics of modern philosophy. SPb.: 1999. P. 57
[39] Goode S. (2010). The Admissibility of Electronic Evidences. Review of Litigation. 2010. N 29. P. 5.
[40] Orin Kerr, S. (2001) Computer Records and the Federal Rules of Evidence.March, accessed 19 April 2016. Available from: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/KerrComputerRecords.pdf
[41] Federal Criminal Code and Rules (1997). Federal Rules of Criminal Procedure. West Group. St. Paul, Minn. 1997. P. 257, 342, 379.
[42] Federal Rules of Evidence for United States Courts and Magistrates (2004). Federal Rules of Evidence, 2004 - 2005 Edition. Also including California Evidence Code (with selected comments)
[43] Uniform Rules of Evidence (2004), Westlaw Electronic research guide, Report on caselaw divergence from FRE. West Group; 3d Bk & Map edition, 2004.
[44] Jarrett, H. M., Bailie, M.W. (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. U.S. Department of Justice. Published by Office of Legal Education Executive Office for United States Attorneys. Available from: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf
[45] Montasari, R. (2016). Digital evidence: Disclosure and admissibility in the United Kingdom jurisdiction Communications in Computer and Information Science. 2016 .630, pp. 42-52
[46] Sethia, Aradhya. (2016). Rethinking admissibility of electronic evidence. International Journal of Law & Information Technology Volume: 24 Issue 3 (2016) ISSN: 0967-0769 Online ISSN: 1464-3693
[47] The Convention on Cybercrime (ETS N 185) concluded in Budapest 23.11.2001 (2001). Decree of the President of the Russian Federation of 15.11.2005 No 557-p Russian Federation decided to sign the Convention, a statement about the condition of a possible revision of the provisions of paragraph "b" of Article 32 of the Convention. In 2008, the Order of the President of the Russian Federation of 22.03.2008 No 144-p, the Order of the President of the Russian Federation of 15.11.2005 No 557-p invalidated.
[48] Federal Law "On mandatory copy of Documents" (1995). Collected legislation of the Russian Federation, 02.01.1995, No. 1, article 1
[49] Federal Law of 06.04.2011 N 63-FZ (2011), "On Electronic Signature". Collected legislation of the Russian Federation, 11.04.2011, N 15, art. 2036.
[50] UNCITRAL model Law “On Electronic Signature” (2001). Adopted in Vienna on 05.07.2001 at the 34th session of the UNCITRAL/ United Nations Commission on international trade Law. Yearbook. 1996. Vol. XXVII. New York: United Nations, 1998. pp. 319 - 323.
[51] Model Law "On Electronic Digital Signature" (2001). Inter-parliamentary Assembly of the Commonwealth of Independent States / / newsletter. 2001. N 26. Pp. 310 - 326.
[52] Dulenko, V. A. (2006). On the evidential value of Computer Information / / Legal issues of communication, 2006, № 2