International Journal of Economics and Business Administration
Volume VIII, Issue 4, 2020

pp. 598-612

Information Technologies in Criminal Proceedings of Russia: Controversial Issues of Proof

Submitted 06/06/20, 1st revision 22/07/20, 2nd revision 13/08/20, accepted 15/09/20

A.V. Gavritsky[1], Yu.V. Demidchenko[2], O.N. Palieva[3], V.B. Paliev[4], L.I. Poltavtseva[5], B.A. Tsoi[6]

Abstract:

Purpose: *The objective of this article is to use information technologies within the framework of national criminal proceedings for the investigation of crimes.*
Design/Methodology/Approach: *Studies were performed of international provisions governing the procedure of investigation of criminal cases in different countries and the order of preservation of evidence received from electronic sources. The authors analyzed the provisions of Code of Criminal Procedure of the Russian Federation and legal enforcement practice of taking and preservation of evidence received via information and telecommunication technologies in the course of investigating a criminal case.*
Findings: *Based on the results, it was concluded on the need in fundamental modernization of criminal proceedings of the Russian Federation towards improvement of both procedural order of taking and preservation of evidence received via electronic technology processes and deployment of electronic form of investigating crimes into criminal proceedings. There is a need in calculation of risks related to leakage of information of confidential nature. The risk is heavily influenced by the number of objects of judicial protection against which a cybercrime might be committed.*
Practical Implications: *In the article, proposals are set for improving the provisions of national legislation, which would lead to enhanced forms of investigation of criminal cases related to extensive use of modern information technologies, which would legislatively perpetuate the procedural order for the seizure and preservation of criminal evidence.*
Originality/Value: *Transition to electronic form of investigation will lead to extensive use of electronic means of preservation in performance of investigative activities, which will greatly facilitate their performance, ensuring thereby entirety and reliability of evidence, while also reducing the risks of possible evidence tampering.*

Keywords: *Information and telecommunication technologies, electronic document flow, electronic document, electronic evidence, electronic data storage device, electronic signature, evidence, economic criminal cases, risk.*
JEL codes: *O33, K40, K42.*
Paper type : *Research article.*

[1]*Candidate of law, associate professor, Russian State University of Justice, Rostov-on-Don, Russian Federation, priemnaja_rfrrap@mail.ru;*
[2]*As in 1, ydemid_76@mail.ru;*
[3]*As in 1, palievaoksana@mail.ru;*
[4]*As in 1, radanpal58@mail.ru;*
[5]*As in 1, lar_poltav@mail.ru;*
[6]*As in 1, bronislav.tzoi@yandex.ru;*

1. Introduction

Within a market economy, information technologies implemented in all spheresof functioning of the society, while being of systematic and continual nature, have significant value. In the Russian Federation, large-scale cybernation has started as early as in 1991, but Russia's joining to the Council of Europe in 1996 caused a need in formation of a system which would allow exchange of legal information between state offices, legal bodies and citizens.

The development direction of information technologies in the country is governed by the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030, the purpose of which is "development of information society by the state, creation of conditions to organize knowledge platform and provide access to it, improve the mechanism for dissemination of knowledge, and its application in practice in the interests of individual, society and state". According to the Doctrine of Information Security of the Russian Federation: "Expansion of areas for application of information technologies, being a factor of development of the economy and improvement of functioning of public and state institutions, is simultaneously generating new information threats." Resolution of the Government of the Russian Federation of April 15, 2014 No. 313 "On approval of the state program of the Russian Federation 'Information Society 2011-2020" aims at improving the quality of the citizens' life through the use of information and telecommunication technologies. Currently, there are 15 main Federal laws governing the general process of the country informatization.

Rapid development of the information society has inevitably led to introduction of information technologies into criminal proceedings. The Internet has become a vast "field" for the criminal world, which has recourse to various and sophisticated methods of committing crimes. The most widespread criminal offenses include crimes in the domain of computer technologies, economic activities, and, in particular, in the financial, credit and tax spheres, as well as a number of other crimes related to ordinary crimes (Artemenko *et al.,* 2020)

Unfortunately, global information networks are used to commit crimes, the responsibility for which is provided for by the criminal legislation of many countries, including that of the Russian Federation. Legal enforcement bodies of all countries are involved in counteracting the criminal challenges to society and state and, subsequently, in the process of extensive use of information technologies therewith.

The values of crimes committed in the area of computer information in the territory of the Russian Federation are growing every year. The statistical data on crimes committed with the use of information and telecommunication technologies or in the area of computer information in the territory of the Russian Federation are given in the following Table 1.

Table 1. *Crimes committed with the use of information and telecommunication technologies*

Values	2019 (January-December)		2020 (January-June)	
	quantity	in % to the same period of the previous year	quantity	in % to the same period of the previous year
Total number of crimes	294,409	68.5	225,463	91.7
including: with the use of payment (plastic) cards	34,383	109.3	82,339	489.2
computer equipment	18,261	21.5	13,799	389
software	6,283	43.6	4,935	66.4
fictive electronic payments	984	101.2	606	27.8
Internet	157,036	45.4	128,525	81.9
mobile communications	116,154	89.5	96,365	104.6

Source: *Own study.*

Total value of the number of crimes committed in 2018 was 174,674, while the rest of the values in the statistical reporting of the Ministry of Internal Affairs of the Russian Federation were previously not taken into account at all. From the values given above one can see growth in all directions. The values for the first half of 2020 are rather large. It was the period of the pandemic of coronavirus infection COVID-2019 that had a certain impact on the commission of crimes in the information environment, since during period of self-isolation, a necessity emerged in the society in intensified communication via the Internet, and this has motivated the criminal world to commit Internet crimes. It should be recognized that modern national legislation does not completely meet the development level of science, technology and legal regulation, which would make it possible to resist this type of crimes to the full extent, and therefore requires certain legislative adjustments.

2. International Legislation Governing Information Technologies in the Course of Investigation and Proof in Criminal Cases

While developing criminal procedure measures in the criminal proceedings of the Russian Federation, Russian legislators pay attention to the positive experience of foreign countries in implementing information technologies into the framework of criminal investigation and procedure of proof. Some foreign countries have long been successful in promoting the possibility of investigating criminal cases electronically and, subsequently, in preserving evidence in the required format. For example, in the USA, Great Britain, Canada, Germany, Belgium, Switzerland, Saudi Arabia, South Korea, Kazakhstan, Georgia and other countries, the system of electronic legal proceedings has been implemented for a long time. Let us try to make a brief analysis of some of them.

The UK business model of digital criminal justice claims its phased implementation

as a digital end-to-end system using the so-called Common Platform, wherein the information initially obtained by a police officer in charge of investigating a crime is then passed on to other bodies of the criminal justice system without duplication or modifications. These phases imply entering information on the case materials and evidence, exchanging files of criminal cases between respective bodies and the defense, preparing the case for the court, presenting the case in the court, as well as the final decision of the criminal case.

Police officers are provided with the tools necessary for them to be able to take digital evidence at a crime scene, receive statements and upload digital case information using mobile devices without need to return to the police station. The police record the testimony of witnesses and victims of crimes electronically on their mobile device or by video message from the crime scene (if possible) while the events of the crime are still fresh in the victim′s or witnesses′ memory. Information on the incident is not duplicated in paper form. Thus, evidence is subject to immediate preservation on electronic devices, without any additional preservation.

In recent years, the USA has faced an increase in the number of cybercrimes. According to the data for 2017-2018, the damage from cybercrimes is estimated at $115 bln per year, while the cost of eliminating the consequences of such crimes exceeds $270 bln. In the territory of the USA, any criminal act committed with the use of a computer, mobile device, or the Internet is qualified as a cybercrime. Computer crimes are often of an inter-state nature, when the legal offense falls under the jurisdiction of several national or US states. In the United States, investigation of this type of crimes is under the jurisdiction of the Federal Bureau of Investigation, while as applicable to computer crimes, priority is given to the jurisdiction of the state.

The emergence of electronic data storage devices, means of communication and other electronic resources has caused additional problems of proof in criminal cases for the United States. This is largely due to digitalization of evidence, when the main bulk of evidence over the case is in electronic form. First of all, certain problems emerge with searching for such evidence, their preservation and safe storage. Once a law enforcement officer is unskilled with computer, they will not be able to recognize and then investigate a crime related to the use of computer technologies. To eliminate this problem, the US Department of Justice, in association with the National Institute of Justice, has developed the Digital Evidence Forensics Guide, which explains in detail the possibilities and ways of using digital evidence in a case. At that, the Guide is of open nature and is oriented not only towards investigators, but also towards the attorney service employees, judges and defense lawyers, which contributes to a unified approach to the use of digital evidence in a criminal case.

There is an independent chapter of the Guide devoted to creation of an expert evaluation, its form and content. Besides, the Guide provides examples of handling digital evidence, samples of expert evaluations, as well as sample request forms for the most adequate description of one or the other evidence in order to obtain and/or

attach it to the case. One of the greatest problems of digital evidence (considering the ease with which it could be modified) is still its authentication to recognize evidence as admissible in a criminal case. The Guide introduces a unified standard for permissive authentication: electronic evidence is first validated in a way whereby "a responsible juror would be leaned more towards authenticity or identification". This approach has created a situation where all doubts concerning authenticity of digital evidence lead to a diminution in the degree of relevance of the given evidence, but not of its admissibility. At that, it is noted that the Guide is advisory and is rather a consensus of the points of view of lawyers and technical experts.

It is interesting to observe the Swiss experience in this regard. It is the developed banking system in the country, the presence of a huge number of international organizations (both governmental and non-governmental) that have a significant influence on the activities of the legal enforcement system of Switzerland. This circumstance determines the use of cutting-edge information technologies in the course of the activities of these institutions.

According to the criminal procedural law science of this country, the term "informatization" (informatisierung) is currently interpreted at least by two major meanings. It is, on the one hand, a certain procedure for endowing the participants of the proceedings and the public with procedurally significant information, and, on the other hand, introduction of modern information technologies used by criminal justice bodies in the course of investigating criminal acts and hearings in courts of various instances (forensics technology, video-conferencing, etc.).

One of the basic legal acts in the area of criminal proceedings is the Law on the Principle of Openness in Governance, which should forward transparency in respect of tasks of organization and activities of federal and cantonal institutions (Art. 1). This act determines the procedure for covering the work of criminal justice bodies on their official websites and in the media, as well as provides for cases when such data is not subject to publication (Art. 7).

Another important document is the Regulations on processing of biometric data for official purposes. The preamble to the Regulations states that it was adopted in order to implement Art. 354 of the Swiss Criminal Code, under which "the competent body registers and stores for official purposes the data collected by the authorities of the cantons, the Federation and foreign institutions in the course of criminal prosecutions or during performance of other tasks prescribed by law, and transferred to it."

The Code of Criminal Procedure of Switzerland has also fixed the development of electronic document flow in criminal proceedings. According to Part. 2 of Art. 39 of the Code of Criminal Procedure of Switzerland, the parties may indicate an e-mail address with its official cryptographic password and declare their consent for electronic delivery. According to Part. 4 of Art. 42 of the Code of Criminal Procedure of Switzerland, upon electronic delivery, a file containing a legal document and

annexes should be sealed by a party or its representative with a recognized electronic signature. The Federal court determines the format, in which electronic delivery can take place in regulations. At the same time, basic procedural documents (order of detention, indictment, court decision to take proceedings, sentence) are delivered to the interested persons in paper form, which, however, does not exclude their subsequent posting on the website of the respective criminal justice body. In addition, the Code of Criminal Procedure of Switzerland represents up-to-date technical advances and provides for that the prosecutor's office and the courts have the right to conduct an interrogation using video-conferencing in criminal proceedings, once the interrogated person cannot appear or their arrival will come at a high cost. According to Part. 6 of Art. 78 of the Code of Criminal Procedure, in the course of interrogation using video-conferencing, an oral statement of the interrogated person replaces recognition of the protocol, its signing and validation.

Unlike Russian legislation, the Swiss Criminal Procedure Code thoroughly regulates such investigative action as banking supervision. For investigation of crimes or criminal offenses, the coercive court may, upon the request of the prosecutor's office, order the surveillance over the relationship between the accused person and the bank or a similar financial institution. This investigative action is automated, i.e. is carried out by the criminal justice bodies not manually, but via program that processes information on bank account activity. If the coercive court grants the request, it issues written guidelines to the bank or similar financial institution on the information and documents to be provided and on the measures to be taken to protect secret information. The bank or other financial institution is not obliged to provide information or documents, once through their issuance they could convict themselves of the possibility to be subject to criminal or civil liability themselves. The persons whose relationships with banks have been surveilled have the right to submit a complaint to the court. The period for appeal starts from the moment the notification is received.

Development of effective measures to counteract cybercrimes is indicated in the Address of the President of the Republic of Kazakhstan of January 31, 2017 "The third modernization of Kazakhstan: global competitiveness" as a priority task in transforming the country's legal system. To solve this problem, on the basis of the Concept of cybersecurity ("Cyber Shield of Kazakhstan"), the pool of technical means for preservation and forensic examination of "digital" evidence has been expanded.

In the State Program "Digital Kazakhstan", which has been launched on December 12, 2017, in order to improve the efficiency of law enforcement, transition to paperless document flow, implementation of "electronic criminal cases" and information and analytical systems were specified. In the courts of the Republic of Kazakhstan, implementation of the pilot project "Electronic Criminal Case" has started since August 15, 2017. Upon adoption of the Law of the Republic of Kazakhstan No. 118-VI LRK of December 21, 2017 "On amendments and modifications to some legislative acts of the Republic of Kazakhstan concerning modernization of the

procedural basics of legal enforcement", the technological initiative on the implementation of criminal proceedings in electronic format has been legalized since January 1, 2017.

The possibility of conducting criminal proceedings in electronic format is provided for in Art. 42-1 of the Criminal Procedure Code of the Republic of Kazakhstan. According to the Rules for conducting the Unified Register of Pre-Trial Investigations (hereinafter URPTI) and the Guideline on conduct of criminal proceedings in electronic format, a person conducting the criminal proceedings, at their own discretion, makes a decision on the electronic format of the proceedings upon acceptance of pre-trial investigation into its proceedings. A motivated order should be issued on choice of the electronic format, a duly executed electronic form should be filled in the URPTI, and an automatic notification to the supervising prosecutor should be generated within 24 hours. Simultaneously, the parties in the criminal process should be informed of the decision taken. Conducting of electronic legal proceedings lies in carrying out of a pre-trial investigation in electronic format through entering an electronic document or attaching a PDF document in the URPTI information system on the basis of procedural decisions and actions taken by an official, as well as filling in the necessary details of electronic forms signed with an electronic digital signature in compliance with the URPTI Maintenance Rules. The criminal proceedings in electronic format should be carried out by the criminal prosecution body for one or several criminal acts through using the "Electronic Criminal Case" module in the remote functionality of the URPTI, designated to organize preparation, conduct, dispatch, receipt and storage of a separate proceeding in the form of electronic criminal case.

Information technologies are used in criminal proceedings in other countries as well. Undoubtedly, their implementation includes many positive aspects. Nevertheless, in addition to the positive experience of transferring criminal proceedings to electronic format in the course of implementation of provisions of the respective Laws, there are apparent shortcomings, minimization of which should contribute to large-scale fitting-out with software and development of unified law enforcement practice for conducting electronic criminal proceedings and gathering and preserving evidence in a criminal case. Such law enforcement practice is being gradually formed, made public and adjusted to gain its objectives.

3. National Provisions of Criminal Procedure Legislation Governing Information Technologies for Collection, Validation and Evaluation of Evidence

The current information revolution could not but affect the procedure for investigating criminal cases, and, in particular, criminal procedural proof. Use of telecommunication technologies in committing crimes requires relevant procedural methods to preserve evidence within the framework of the criminal case under investigation from the officials of preliminary investigation bodies. However, the

existent criminal procedure doctrine is not yet ready to adapt the results of the information revolution. The existent technology of criminal procedural proof has been developed under a completely different social and historical formation based on another cultural and informational (written, logocentric) pattern. Therefore, the existing investigative (written) form, by which the criminal procedural evidence is formed, and whereon the legal standard of admissibility of evidence is based, creates a conceptual obstacle to realization of the potential of information technologies in criminal proceedings. This circumstance produces an institutional problem of improving the legal regulation of the activities of law enforcement agencies to counteract crimes in the information sphere. At the present stage, the issue of introducing an electronic form of criminal investigation into criminal proceedings is being actively discussed by the scientists, in order to effectively accomplish the tasks of criminal proceedings (Pechnikov and Shinkaruk, 2019).

Hence, the issue arises of the necessity to develop and adopt a number of specific provisions of criminal procedure legislation governing the procedural order for taking and preserving evidence on crimes and practical recommendations for their use in the course of proof within the framework of criminal investigation.

The issues of trace formation are of paramount importance for the proof. Since gathering of traces of crimes, their research, evaluation and further use are the essence of the process of proof, this process procedure is mandatory and is intended to identify all significant circumstances in a criminal case. Official monopoly in proof is one of the basic ideas of the investigative process. In the investigative process, only the data obtained by authorized officials in observing the provisions of relevant procedures should be considered as evidence. Subsequently, computer data would become evidence when the investigator recognizes it as relevant and admissible, which is possible upon its reproduction, examination and inclusion as material evidence. Taking of evidence is associated with the procedure for seizure of "electronic media" and copying of electronic information through conducting of investigative actions (Bikmiev and Burganov, 2015).

As the legal enforcement practice displays, it is impossible to collect complete and comprehensive information on criminal activity, for example, in the area of business and other economic activities only by performing investigative actions. These crimes are often categorized using criminal-intelligence means, and the material of verification, collected in the course of the criminal-intelligence measures, contains evidential information, which is subsequently vested in a criminal-procedural form. Such evidential data gives grounds, first of all, to suspicion and then to initiation of a criminal case and accusation on behalf of the state.

Considering the fact that electronic data storage devices are the most widespread and at the same time difficult to seize objects, it is necessary elaborate this matter in detail. Taking and preservation of evidence is carried out from electronic sources, mainly computer equipment and cell phones. Data from social networks, e-mail

correspondence, messengers (ICQ, Skype, Viber, WhatsApp, etc.) are used.

On June 23, 2016, the Code of Criminal Procedure of the Russian Federation was supplemented by Chapter 58 "Procedure for the Use of Electronic Documents and Forms of Procedural Documents", in which the legislator operates with such concepts as "electronic document", "electronic data storage device", "electronic signature", "enhanced qualified electronic signature". However, these concepts are not fixed in the provisions of the Criminal Procedure Code of the Russian Federation, but are systematically used in legal enforcement practice. This kind of modifications in legislation testify to the need of further improvement of the the proof process in criminal proceedings.

The "electronic data storage device", according to "GOST 2.051-2013. Inter-State standard. Unified system for design documentation. Digital documents. General Principles", refers to cell phones, smartphones, computers, portable GPS devices, digital cameras, video recorders, payment systems, floppy disks, hard drives, memory cards of various formats (flash memory, SSD drives, etc.), optical disks of various types (CD-ROM, DVD-ROM, Blu-ray Disc), USB flash drives, computer random access memory and others (ROSSTANDART, 2013).

The absence of the concept of "electronic data storage device" in the Criminal Procedure Code of the Russian Federation leads to contradictory practice. For example, in one situation an investigator might seize a laptop as an electronic data storage device, while in another situation they seize only a hard drive or refuse to copy information, since they believe that they have carried out a seizure of the item, that being a laptop, and not a seizure of electronic data storage device. Yu.N. Sokolov (2017) states that the lack of interpretation in the criminal procedural law for the relevamt material carrier necessary for the isolation of electronic information does not contribute to an unambiguous understanding of its meaning. O.V. Dobrovlyanina (2019) points out that "interpretation of this term is important for successful implementation of the rules". As for us, we do agree with the opinion of scholars and suppose that to gain a uniform understanding and its use in criminal proceedings, the term "electronic data storage device" must be fixed in Art. 5 of the Criminal Procedure Code of the Russian Federation.

Evidence obtained in the form of electronic documents, namely: e-mails, electronic messages, "screenshots" and other data recorded on special media, has been long attached to the materials of criminal cases. In legal enforcement practice, investigators and courts regard electronic evidence as other documents, in accordance with p. 6 of Part. 2 of Art. 74 of the Criminal Procedure Code of the Russian Federation.

The concept of "electronic document" is explained in the Federal Law No. 149-FZ of July 27, 2006, "On information, information technologies and information protection". According to Art. 2 of this Law, "an electronic document is documented information presented in electronic form, i.e. in a form suitable for human perception

using electronic computers, as well as for transmission through information and telecommunication networks or processing in information systems". Apparently, such a definition represents to a greater extent its technical nature.

According to Resolution of the Plenum of the Supreme Court of the Russian Federation No. 57 of December 26, 2017 "On some issues of application of legislation governing the use of documents in electronic form in the activities of courts of general jurisdiction and arbitration courts" an electronic document is referred to as "a document created in electronic form without preliminary documenting on paper, signed with an electronic signature in the manner prescribed by the legislation of the Russian Federation."

The legislator unambiguously points out that "electronic document" should also be validated with an electronic signature or an enhanced qualified signature. Thus, information in electronic form, validated by the above mentioned method is similar to a document executed on paper and signed with a handwritten signature. Such document should be recognized as an electronic document in all cases determined by federal laws.

Considering the specifics of electronic document, the informational "nature" of electronic document, i.e. its material carrier, is of substantial significance (Palieva and Paliev, 2019). I.N. Smolenskiy (2018), the judge of the Arbitration Court of the Volga District, believes that material carrier is an object of the material world, which contains electronic information. I.N. Podvolotskiy (2003) supposes that electronic document is any data stored, processed and transmitted using automated information and telecommunication systems, on the basis of which a court, a prosecutor, an investigator, an interrogator, in the manner prescribed by the criminal procedure legislation, identifies presence or absence of circumstances subject to proof in the course of criminal proceedings, as well as other circumstances relevant to the criminal case, obtained in compliance with the procedural order of their collection and attached to the criminal case by a special resolution (order).

We come into line with the suggestion of Ye.A. Moshkov (2016) that over all the diversity of opinions concerning the nature of electronic document, the proceduralists have agreed that the principal distinguishing feature between written and electronic documents is "direct human participation in creation of a document", where in the first case it has a clear nature, while in the second case it manifests itself least of all, and in some cases is nearly absent".

Thus, the subject (suspect, accused) that have created certain electronic document on a material medium and placed it in other information systems (posted it on the Internet, sent it to another addressee, etc.) assumes great importance in investigation of a criminal case, as well as, certainly, the electronic document itself, which is evidence in a criminal case. The analysis of the above mentioned concepts allows us to conclude that the distinctive features of "electronic document" are determined by the source, i.e.

the carrier of preserved information. The source of evidential data should be electronic. However, development of the Internet and increased scope of information, development of means for identification and possibilities of identifying the persons who have created the document, blur the boundaries between written and electronic document as evidence.

Criminal procedural legislation allows the use of electronic documents as means of evidence, defining that "documents may contain information preserved both in writing and in other form". These may include materials from photography and filming, audio and video records and other data carriers received, requested or submitted in the manner prescribed by Art. 86 of the Criminal Procedure Code of the Russian Federation. Thus, the legislator makes the main demand for electronic evidence ─ it should be obtained through production of investigative and other legal actions. This allows us to make a conclusion that the legislator equates electronic and written evidence.

The legal enforcement practice of seizing digital data is ambiguous. Some investigators seize a whole item, i.e. cell phone or video recorder, others remove the memory card and immediately inspect its data. Procedural scholars have long been discussing the issue of recognition of copying the electronic carriers as an independent investigative action. For ex., S.V. Zuev (2017) affirms that "seizure of electronic carriers and copying electronic information are two complementary, and in some cases competing with each other, recognition methods of handling electronic means of criminal procedural proof. The advantages of one or another action depend on the tasks being solved, conditions and complexity of the process. It seems that recognition of electronic information copying as an independent investigative action within the framework of a criminal investigation is an actual necessity, which has long matured and requires legislative affirmation.

To conclude, it should be said that, as a whole, it is impossible to exhaust all the issues related to implementation of "electronic technologies" within the framework of proof in a criminal case without a global revision of the provisions of criminal procedure legislation. Implementation of "electronic innovations" into pre-trial criminal proceedings is carried out inconsequently and inefficiently. There is a need for transition to new technical technologies related to investigation of a criminal case in electronic form.

4. Assessment of the Risks Related to Implementation of Information Technologies within the Framework of Criminal Proceedings

There is a certain obstacle to implementation of new digital technologies, and it is the fact that people are afraid of the risks related with the use of such technologies (technophobia). It is not always convenient for an investigator to operate with new practices, for example, to investigate a criminal case in the form of electronic document, to take evidence applying new procedural possibilities. The investigator is

used to traditional (paper-based) work methods. Implementation into legal practice of such tools as predictive coding, "electronic criminal case", creation of automated procedural documents suggests facilitating the working conditions of the persons conducting criminal investigations and increasing efficiency in the conditions of digitalization of legal practice. Digitized information becomes more verifiable, reliable and searchable, while the administrative burden on employees decreases.

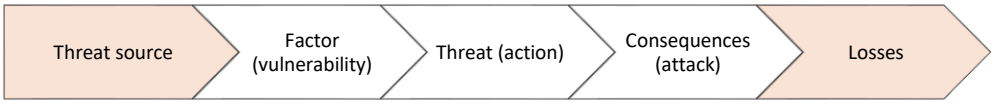
At the same time, global informatization has led to emergence of computer crimes, massive "hacker" attacks, which can entail loss of information. With regard to electronic criminal cases, there is a risk of leakage of information related to the data of preliminary investigation. The Criminal Code of the Russian Federation provides for criminal liability for disclosure of such information on the case (Art. 310).

In the period of active implementation of digital technologies and storages of large databases, an effective system of information system protection becomes the most important strategic factor in functioning of legal enforcement bodies. In fact, information is one of the key elements of activity of a government institution. Electronic information environment of the subject of functioning, regardless of the scope and composition of the stored information, should be provided with a cyber protection system. Information of human rights and law enforcement organizations can be represented not only by static complex of accumulated data (databases, current equipment settings, etc.), but also dynamic data processing information processes.

At the local level of threats to computer security, information leakage channels are distinguished, which are interpreted as a set of information sources, material carriers or the propagation media of signals carrying this information and means of extracting information from signals or carriers. Information threat factors should be considered as a potential opportunity to use information leakage channels. Objective existence of these leakage channels supposes their possible use by malefactors for unauthorized access to information, its copying, destruction, modification, blocking and other illegal manipulations.

The concept of "threat" in the information systems of the bodies of preliminary investigation. One of the key points in creating a loss model are the reasons that suggest such losses. The causes of losses are external threats and vulnerabilities of the system itself. The threat implementation model follows the path shown in Figure 1.

Figure 1. *Threat implementation model*



Security threat in information systems (IS) is a potentially possible event, process or

phenomenon that can lead to destruction, loss of integrity, confidentiality or availability of information, that is, damage the resources of the system. The entire multitude of potential security threats can be divided into intentional and unintentional ones.

Approach to assessment of losses from confidentiality threats. Confidentiality of information is the need to prevent leakage (disclosure) of any information. When the information is disclosed, its owner will have losses that may be associated with the "secret" of investigation, reputational loss of the preliminary investigation bodies, disclosure of data of the participants of criminal proceedings, etc. Therefore, confidential information implies the right to use it only by a limited number of persons (investigator, head of investigative body, prosecutor), while for the rest it shall remain classified (IPIS, 2018).

The most convenient method for calculation of losses is the expert evaluation method. The essence of the method lies in the fact that a group of experts in certain area analyzes losses out of the significance of the information itself. The cost of information obtained on the basis of expert evaluations will be not absolute, but subjective, thus, it will be fair under certain conditions. Sources of information leakage can be both domestic (insider), alien (outsider) and other stakeholders (Voronina et al., 2018)

According to the risk formula (1), its average annual percentage could be specified:

$$AR = FTI \times MV \times AD \quad (1)$$

where AR is an average annual risk of leakage of legal protection objects;
FTI is frequency of threat implementation (expert evaluation, depending on importance of the information);
MV is magnitude of vulnerability (methods of cyber protection of the information);
AD is amount of damage (depends on the extent of stakeholder interest in the information).

Due to violation of several categories of information, evaluation of losses can be different depending on the properties under the threat. In legal enforcement activity, this assessment is very subjective and can be expressed by the formula (2):

$$AL = C + \max (I \times A) \quad (2)$$

where AL is absence of losses;
A is loss of availability of information;
C is loss of confidentiality of information;
I is loss of information integrity.

The risks of leakage of confidential and undisclosed information should be evaluated

taking into account these factors. The number of objects of legal protection, against which cybercrime can be committed, has a serious impact on the risk as well.

5. Conclusion

Digitalization has a significant impact on lawmaking activity, while modern system of information and communication technologies reveals new opportunities for lawmaking in general and modernizing the criminal procedural norms in particular.

It might be concluded that, as a whole, the problem of taking evidence in criminal proceedings cannot be completely resolved by rearranging the rules on seizure of electronic carriers. Implementation of "electronic innovations" in pre-trial criminal proceedings is performed in a selective way, inconsequently and inefficiently. Therefore, there is a need for global revision of the provisions of criminal procedure legislation aimed at implementation of electronic form of criminal investigation, which would lead to normative fixation of procedural rules for taking and preserving electronic evidence in a criminal case.

It is not only the relevance of transition to electronic document management that should be spoken of, but also the need to develop specific proposals into criminal procedure legislation. At that, there is a need to create relevant technical conditions allowing not only to lay a basis for creating electronic criminal cases and their investigation, but also to ensure security of confidential information constituting an "investigative secret".

References:

Artemenko, D., Gurba, V., Evnevich, M. 2020. Countering the Legalization of Criminal Income as a Factor to Deal with the Risk of Terrorist Threats and Increasing Competitiveness in Foreign Economic Markets. Scientific and Technical Revolution: Yesterday, Today and Tomorrow, 1076-1088, DOI: 10.1007 / 978-3-030-47945-9_117 .

Bikmiev, R.G., Burganov, R.S. 2015. Collection of electronic evidence in criminal proceedings. Information law, No. 3, p. 12.

Dobrovlyanina, O.V. 2019. Several aspects of procedural seizure (copying) of electronic carriers of information. Perm legal almanac, 1.

FL. 2006. Federal Law "On Information, Information Technologies, and Information Protection" of July 27, No. 149-FZ.

IPIS. 2018. Information protection and information security. Available at: http://www.zashita-informacii.ru/

MIA. 2019. The state of criminality in the Russian Federation in January-June 2018. Available at: https://xn--b1aew.xn--p1ai/reports/item/16053092

MIA. 2020. The state of criminality in the Russian Federation in January-December 2019. . Available at: URL: https://xn--b1aew.xn--p1ai/folder/101762

MIA. 2020. The state of criminality in the Russian Federation in January-June 2020. Available at: https://xn--b1aew.xn--p1ai/reports/item/20597695/

Moshkov, Ye.A. 2016. The concept of electronic document and its use as evidence in civil and arbitration proceedings in the Russian Federation. Arbitration and civil process, 20.

Palieva, O.N, Paliev, V.B. 2019. The concept of electronic document and its use as evidence in the course of investigation of a criminal case. Science and education: household and economy; business; law and governance, 7(110), 103.

Pechnikov, G., Shinkaruk, V. 2019. Computing Systems (Computers) and Criminal Trial. Computing and the Internet of Things: Prerequisites for the Development of ICT. Studies in Computational Intelligence, 826, 265-274. DOI: https://doi.org/10.1007/978-3- 030-13397-9_30.

Podvolotskiy, I.N. 2003. Legal and criminalistic aspects of the term "document" . Black holes in the Russian legislation, 2, 125.

ROSSTANDART. 2013. Rosstandart order No. 1628 of November 22.

Smolenskiy, I.N. 2018. Identification of person (subject of arbitration process) in electronic justice. Bulletin of civil process, 1, 26.

Sokolov, Yu.N. 2017. Electronic data carrier in criminal proceedings. Information law, 3, 22.

Voronina, A.V., Osipyan, N.B., Dmitrieva, M.A. Elchaninova, O.V., Vatolina, M.V. 2018. Legal and economic methods as an environmental risk management mechanism. Research Journal of Pharmaceutical, Biological and Chemical Sciences, 6 (9), 1671-1677.

Zuev, S.V. 2017. Electronic information and its carriers in criminal procedural evidence: development of legal regulation. Bulletin of SUSU, Series: Law, 1(17), 32.