UDC: 343.98.067

# LEGAL BASIS FOR COLLECTION AND ATTACHMENT OF DIGITAL INFORMATION AS PROOF IN CRIMINAL CASES IN THE REPUBLIC OF KAZAKHSTAN

**Utepov Dauren Pakhatovich,**
Doctoral student at the Academy
of Law Enforcement Agencies
under the General Prosecutor's Office
of the Republic of Kazakhstan,
Junior Justice Adviser
e-mail: Dauka_1986@mail.ru
ORCID: 0000-0002-2423-5053

**Zhempiisov Nazarbek Sharunovich,**
Head of the Department of Special Legal Disciplines
of the Academy of Law Enforcement Agencies
under the General Prosecutor's Office
of the Republic of Kazakhstan,
Senior Justice Adviser, Candidate of Legal Sciences
e-mail: Oxbridge23@gmail.com
ORCID: 0000-0001-6835-5834

***Abstract.*** *The constantly increasing volume of natural science, technical and other knowledge at the present stage determines the technical saturation of the criminal process in the investigation of crimes. The increasing complexity of forensic tools used in the collection and consolidation of digital traces of crime and evidence, the extensive instrumentalization of expert research methods, determines the need for a set of issues related to the use of special knowledge by participants in the criminal process. The purpose of this study is to identify, generalize and analyze the theoretical and practical aspects of the legal grounds for collecting and consolidating digital information in proving criminal cases, taking into account world experience and the opinions of scientists. The issues of legal grounds for collecting, consolidating digital information in proving in criminal cases in the realities of the current legislation of the Republic of Kazakhstan is highlighted in this article. The historical aspects of the development of collecting evidence are also reviewed. In addition, the problems associated with the search, consolidation and application of digital information in evidence in criminal cases are addressed. Covert investigative actions aimed at collecting digital information are discussed. The author concludes that it is necessary to consolidate the concept of "Investigative actions" in the criminal procedural legislation, as well as investigative actions such as "Inspection" are not applicable to the collection of evidence in the form of digital information. Thus, authorization of investigative actions in the form of a search and seizure is required when receiving digital information.*

***Keywords:*** *a collection of evidence, digital information, computer-technical expertise, hash function, covert investigative actions, inspection, seizure, search.*

# QOZOG‘ISTON RESPUBLIKASIDA JINOIY ISHLARNI ISBOTLASHDA RAQAMLI AXBOROTNI YIG‘ISH, MUSTAHKAMLASH UCHUN HUQUQIY ASOSLAR

**Utepov Dauren Pakhatovich,**
Qozog‘iston Respublikasi
Bosh prokuraturasi huzuridagi
Huquqni muhofaza qilish organlari akademiyasi doktoranti,
Adliya kichik maslahatchisi

**Zhempiisov Nazarbek Sharunovich,**
Qozog‘iston Respublikasi Bosh prokuraturasi huzuridagi
Huquqni muhofaza qilish organlari akademiyasi
“Maxsus yuridik fanlar” kafedrasi mudiri,
Adliya katta maslahatchisi

***Annotatsiya.*** *Hozirgi bosqichda tabiiy fanlar, texnik va boshqa bilimlarning tobora ortib borayotgan miqdori jinoyatlarni tergov qilishda jinoiy jarayonning texnik to‘yinganligini aniqlaydi. Jinoyat va dalillarning raqamli izlarini to‘plash va mustahkamlash uchun ishlatiladigan sud-meditsina vositalarining murakkabligi, ekspert tadqiqotlari usullarini keng qo‘llash jinoyat protsessi ishtirokchilari tomonidan maxsus bilimlardan foydalanish bilan bog‘liq bo‘lgan bir qator masalalar zarurligini belgilaydi. Ushbu tadqiqotning maqsadi olimlarning jahon tajribasi va fikrlarini hisobga olgan holda, jinoiy ishlarda isbotlashda raqamli axborotni yig‘ish va mustahkamlashning huquqiy asoslarining nazariy va amaliy jihatlarini aniqlash, umumlashtirish va tahlil qilishdan iborat. Ushbu maqolada muallif Qozog‘iston Respublikasining amaldagi qonunchiligida jinoyat ishlarini isbotlashda raqamli axborotni yig‘ish, mustahkamlash uchun huquqiy asoslarni qamrab oladi. Dalillarni to‘plashning tarixiy jihatlari qamrab olingan. Bundan tashqari, jinoyat ishlarini isbotlashda raqamli axborotni qidirish, aniqlash va ulardan foydalanish bilan bog‘liq muammolar ko‘rib chiqiladi. Raqamli axborotni to‘plashga qaratilgan norasmiy tergov harakatlari qayd etildi. Muallif o‘z ishida jinoyat-protsessual qonunchiligida “tergov harakati” tushunchasi, shuningdek, “tekshirish” kabi tergov harakatlarini raqamli axborot shaklida dalillarni to‘plash uchun qo‘llamaydi va raqamli axborotni olishda tergov harakatlarini qidirish va olib tashlash shaklida sanksiyalashni talab qiladi.*

***Kalit so‘zlar:*** *dalillarni to‘plash, raqamli axborot, kompyuter va texnik ekspertiza, Xash funksiyasi, yashirin tergov, tekshirish, chizish, qidirish.*

# ПРАВОВЫЕ ОСНОВЫ ДЛЯ СБОРА И ПРИЛОЖЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ ПО УГОЛОВНЫМ ДЕЛАМ В РЕСПУБЛИКЕ КАЗАХСТАН

**Утепов Даурен Пахатович,**
младший советник юстиции,
докторант Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан

**Жемпиисов Назарбек Шаруанович,**
кандидат юридических наук,
старший советник юстиции,
заведующий кафедрой специальных юридических дисциплин
Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан

***Аннотация.*** *Постоянно возрастающий объем естественнонаучных, технических и иных знаний на современном этапе обуславливает техническое насыщение уголовного процесса при расследовании преступлений. Усложнение криминалистических средств, используемых при сборе и закреплении цифровых следов преступления и доказательств, широкая инструментализация экспертных методов определяют необходимость исследований комплекса вопросов, связанных с использованием специальных знаний участниками уголовного процесса. Целью данного исследования является выявление, обобщение и анализ теоретических и практических аспектов правовых оснований сбора и закрепления цифровой информации в доказывании по уголовным делам с учетом мирового опыта и мнений ученых. В статье автор освещает правовые основы сбора, закрепления цифровой информации в доказывании по уголовным делам в реалиях действующего законодательства Республики Казахстан. Охвачены исторические аспекты развития процесса сбора доказательств. Кроме того, рассматриваются проблемы, связанные с поиском, приложения и применения цифровой информации в доказывании по уголовным делам. Отмечены негласные следственные действия, направленные на сбор цифровой информации. В своей работе автор приходит к выводу о том, в уголовно-процессуальном законодательстве необходимо закрепить понятие «следственные действия», а такое следственное действие, как «осмотр», не применим к сбору доказательств в виде цифровой информации, для этого требуется санкционирование следственных действий – обыска и выемки полученной цифровой информации.*

***Ключевые слова:*** *сбор доказательств, цифровая информация, компьютерно-техническая экспертиза, хэш-функция, негласные следственные действия, осмотр, выемка, обыск.*

## Introduction

The order of collection and the method of securing digital information are elements of the concept of evidence. Without these elements, the evidence is not formed to the end, and, therefore, remains outside the scope of criminal procedural proof. According to the norms of the law, evidence obtained in violation of the procedural order for detecting and securing them cannot be used in criminal proceedings.

In fact, it is with the collection of evidence information that the cognitive activity of the subject of proof begins, as well as the introduction of this information into the criminal process. However, evidence in the form of digital information requires a different approach to its collection and consolidation than other types of physical evidence.

The objectives and goals of this article are to obtain a scientific result on the possibility of collecting and consolidating evidence in the form of digital information in the realities of the current legislation.

## Research methods

In preparing the article, general scientific and private scientific methods of cognition in terms of analysis, synthesis and the method of an expert survey.

## The results of the study

The collection of evidence is the first stage in the activity of obtaining evidence, which is the stage of accumulating evidence that consists of identifying the sources of evidence. The term “collecting evidence” was used in Articles 266 and 281 of the Charter of Criminal Procedure of the Russian Empire in 1864 [1] and has since been used by the legislator in the texts of all criminal procedural laws. The use of this term is due to the fact that at the beginning of the XIX century in Russia, an active process of codification of law began, including civil law, culminating in the adoption in 1822 of the Code of Laws of the Russian Empire, which also extended to the territory of Kazakhstan.

The term was also used in Articles 114 and 306 of the Code of Criminal Procedure of the RSFSR from 1922, and Article 48 of the

Code of Criminal Procedure of the Kazakh SSR from 1959. Article 122 of the current Code of Criminal Procedure of the Republic of Kazakhstan (hereinafter referred to as the CCP of the RK) is devoted to the collection of evidence, according to which this action is understood as the production of procedural actions by the subject of proof.

The gathering of evidence is a rather complex process, consisting of several stages:

- search;
- collection;
- procedural registration of evidence.

B.C. Balakshin, taking into account the fact that evidence does not exist in a "ready form", but becomes such after collecting, consolidating and checking, instead of the term "collecting evidence" suggests using the term "collecting factual data and their sources" [2, p. 316]. By this term, he understands the criminal procedural activity of authorized bodies and officials to identify, search, find and obtain factual data and their sources in order to establish circumstances that are important for the correct resolution of a criminal case

S. A. Sheifer proposes a more accurate and correct use of the term "Formation of evidence" instead of the term "Collection of evidence". In his opinion, "The formation of evidence is the initial element of proof, the active purposeful function of the pre-trial investigation body, the court, which consists of extracting traces left by the event, factual data pertaining to the case, transforming the consolidation of these data, i.e. forming them into the proper procedural condition" [3, p. 191].

Taking into account the above opinions of scientists, we also believe that at the stage of collection, the procedural formation of evidence is not yet completed. Gathering in criminal procedural evidence has as its purpose the search and discovery of information about the circumstances that are important for the criminal case. Only after the appropriate consolidation of the information and the attachment of its carrier to the materials of the criminal case is the evidence ready. Thus, we should not talk about collecting evidence, but about collecting information, which can later become evidence in criminal cases.

Such information, according to Art. 122 of the CCP of the RK, can be collected through procedural actions.

Currently, there is also a point of view according to which the status of criminal procedural evidence can be recognized from the results of operational-search activities.

Nevertheless, this point of view does not seem entirely justified. According to Paragraph 1 of Art. 14 of the Law of the Republic of Kazakhstan "On Operational - Search Activities", materials obtained in the process of operational - search activities (OSA) can be used in the process of proving in criminal cases are subject to verification in accordance with the provisions of the criminal procedure legislation of the Republic of Kazakhstan governing the collection, research and assessment of evidence [4].

Thus, the criminal procedural legislation does not equate the results of the OSA to evidence in criminal cases, considering only the possibility of using these results in the process of proving. Operational-search knowledge differs from criminal procedure knowledge, which explains the difference in the nature of the results of the OSA. The latter "initially cannot meet the requirements for procedural evidence, since they are obtained by an inappropriate subject (an operational officer, not an investigator/ interrogator) and in an inappropriate manner (during OSA, and not investigative actions)."

Collecting digital information is carried out through investigative actions, however, in the criminal procedure legislation there is no definition of the concept of "investigative actions", even though they are "one of the

main ways of collecting information for the further formation of evidence."

Analyzing this problem, we can say that an even greater number of problems are caused by the impossibility of determining the essence of investigative actions from the very meaning of the legislation. "Comparison of various provisions of the Code of Criminal Procedure excludes the possibility of a uniform understanding of investigative actions in the system of criminal procedural regulation."

Taking into account the opinions of scientists, we propose to introduce into Article 7 of the Code of Criminal Procedure of the Republic of Kazakhstan the definition of the concept of "investigative actions" with the following content:

"Investigative actions are procedural actions carried out by a person conducting criminal prosecution in accordance with the criminal procedure law, the purpose of which is the search, collection, verification and procedural execution of evidence".

According to the criminal procedural legislation of Kazakhstan, the grounds and procedure for collecting, securing and assessing are carried out according to the following investigative actions:

1. Inspection, examination, investigative experiment. These investigative actions are based on the observation method, that is, purposeful and direct perception of the object under investigation.

2. Search, seizure, seizure of property and other covert investigative actions. The investigative actions of this group are characterized by the collection of information through the seizure or receipt of their carrier.

3. Interrogation, confrontation, identification, verification of testimony on the spot. These investigative actions are related to each other by the method of questioning, that is, obtaining verbal information, although it is not applicable in collecting digital information, except for obtaining passwords and other accounts from the direct participant.

4. Forensic examination. The production of forensic examination includes a whole range of different cognitive techniques and methods.

The essence of the investigative action as a cognitive act is to obtain information about the circumstances that are important for the criminal case. That is, the essence of any investigative action is to obtain new information on the case by searching and discovering its primary source (person or object).

Features of this type of information as digital information determine the specificity of its collection through investigative actions. Its distinctive features determine the possibility and peculiarities of carrying out some investigative actions and the impossibility of carrying out others. It should be noted that these signs have an impact not only on the tactical and forensic features of the production of investigative actions but also on their legal nature.

First, due to the fact that digital information is not directly perceived by a person, he or she cannot act as the primary carrier of digital information. Accordingly, it is impossible for the subject of proof to obtain digital information by means of observation or questioning, i.e. through interrogation, face-to-face confrontation, and examination.

Meanwhile, in the procedural literature, several opinions have been expressed about the possibility of collecting digital information through conducting such an investigative action as an inspection. Thus, some authors (S.P. Kushnirenko, N.N. Fedotova and E.I. Panfilova) believe that information stored on a computer device or removable media can be given evidentiary value by examining it using analog computer components (monitor, printer, etc.).

Thus, according to N.N. Fedotov, in order to carry out a computer-technical

examination, it is still necessary to remove the storage medium or copy its contents. And these actions, in their complexity and in the application of special knowledge, do not differ much from the examination of computer information on the spot. A specialist is required in any case. Qualified witnesses are still desirable. The expert's actions still lead to viewing and printing the required data. So isn't it easier to carry out the same actions in the order of inspection (Art. 219-220 of the Code of Criminal Procedure) [5, p. 209].

In addition, S.P. Kushnirenko and E.I. Panfilova believe that information stored on a computer device or removable media can be given evidentiary value by examining it using analog computer components (monitor) [6, p. 103].

The results of the survey of law enforcement officers showed (more than 100 respondents participated) that 76% of respondents believe that digital information contained on a computer cannot be obtained as evidence during investigative actions such as an examination of a computer or other technical device.

In addition, we believe that interaction with the subject of inspection may lead to the loss of important information and to the destruction of their traces. Thus, if the access is not disabled by disconnecting from the Internet, the necessary information stored in the computer can be destroyed or changed remotely.

It should also be noted that when viewing digital information with programs, files, etc. the chance of falsification of information by the investigator is significantly increased. Evidence obtained in this way will raise reasonable doubts about its reliability both on the part of the defense and the court.

Even if scientific and technical means (videorecording) were used when viewing digital information, there is a possibility of changing its hash sum.

As mentioned in our previous article, the hash-sum has the tendency to change when mishandled [7, pp. 116-122].

If you look at any digital information carrier, be it a RAM device or a motherboard, only the external parameters of the information carrier are available to perception (volume, weight, shape, the presence of traces of physical impact on the surface). The digital information itself, when visually inspecting its carrier, remains outside the perception of the subject of proof.

Only a special technical device can perceive (read) digital information directly: a CD or hard disk reader, USB port, etc. But even this is not enough: in order for digital information to become available to a person, it must be recoded into an analog or a simple discrete signal. Such transformation of digital information into ordinary one is carried out by means of software products (for transcoding information) and appropriate technical devices.

In conclusion, we came to conclusion that investigative actions such as Inspection are not applicable to the collection of evidence in the form of digital information.

Secondly, the primary carrier of digital information is always a special technical device - a carrier of digital information. Digital storage media range from devices as simple as punched cards and punched tapes to complex digital integrated circuits based on flash card technologies. Accordingly, the most effective way to collect digital information is to remove its carrier.

The main investigative actions based on the method of confiscating the information carrier are search and seizure.

In Art. 252 of the Code of Criminal Procedure of the Republic of Kazakhstan, the objectives of the search are determined: the discovery and seizure of objects or documents that are significant for the case, that is, such objects that can be recognized as material evidence. Their detection is

first carried out by inspection, and then - withdrawal if the object itself and (or) the traces left on it are found to be important for the investigation of a criminal case.

With regard to such specific traces as digital information, which are not accessible to the direct perception of a person, the following question, which has already been raised in the analysis of such an investigative action (i.e., inspection), acquires particular importance: is it possible to turn on these devices, launch programs on them and view files with the purpose of finding evidence of a committed crime?

U.S. legal scholars are inclined to believe that the search for files on a digital device during a search is a kind of "search within a search." O. Kerr writes that "the evidence is a separate file, not the hard drive itself". [8, pp. 3-60]. The hard drive is not evidence, but a repository of evidence. "Accordingly, finding a file on a hard disk is a search for evidence inside a discovered object, among other "non-evidence" objects. This position is due to the fact that in the U.S., evidence refers to the information itself, without reference to the material medium.

In most cases, American courts perceive the search for files on a computer necessary for the investigation as a search of a digital device. In some cases, the search is legalized, while in others it is found unjustifiably broad and violating the Fourth Amendment to the U.S. Constitution.

In Germany and South Korea, the prevailing point of view is that digital information cannot be considered separately from its carrier; therefore, it is incorrect to talk about a search and seizure of digital information: a search is made for items containing the information, and not for the necessary information on a certain subject. Accordingly, using a computer to search for files in it is not considered a "search within a search", but a legitimate process of filtering information to assess its evidentiary value.

Despite the differences in the understanding of the legal nature of searching and viewing files on a digital storage medium, we note that in all these countries, scientists admit the necessity of performing these actions during a search. In the criminal procedure of Kazakhstan, the law enforcement bodies also tend to be on the side of this point of view, as will be discussed below.

In contrast to the inspection, the purpose of launching a digital device and conducting operations to find files during a search is to detect traces of a crime in order to justify the subsequent seizure of the material carrier of this information. That is, the examination of the files during the search makes it possible to identify those items that can be subsequently recognized as material evidence and become the object of a special computer examination. On examination, viewing the files is the ultimate goal of the investigative action: the information displayed on the monitor is entered into the protocol, becoming the information aspect of the evolving evidence. The same reasoning is true for a seizure.

The basis for conducting a search is the availability of sufficient data to believe that the specified items or documents may be in a certain room or other place or in a particular person, which may be significant for a criminal case. Such objects, in particular, can be digital information carriers. For the performance of a body search, a reasoned decision is required in some cases, it must be authorized by the investigating judge.

In exceptional cases, search and seizure can be conducted without a warrant from the investigating judge if there are sufficient grounds to believe that the person who is on the premises or in another place where the search is carried out is hiding documents or objects that may be relevant to the case, as well as in cases of the person's arrest or detention.

The factual basis for conducting a seizure is the fact that the investigator has accurate information that certain objects and documents that are significant for the criminal case and subject to seizure are in a specific place with a specific person. The order of the investigator alone can serve as a legal basis for the seizure. However, in a number of cases, the investigator also needs to obtain a court warrant for the seizure. For example, in accordance with Art. 254 of the Code of Criminal Procedure of the Republic of Kazakhstan, a court decision is required for the seizure of documents, items, the information contained in them, containing state secrets or other secrets protected by law.

Taking into account the peculiarities of the seizure, namely the need to obtain a legal warrant in some cases determined by law, in addition to the order of the investigator, the following should be noted. The modern development and spread of digital technologies have led to the fact that information constituting a secret protected by law can exist in digital form and be stored on various media of digital information. At the same time, the appearance or type of the latter may not always clearly indicate what kind of information they contain. Thus, on a digital information carrier subjected to seizure, in addition to information that is important for a criminal case and does not require obtaining a sanction, information that constitutes any secret protected by law (family, medical, etc.) may also be stored.

Therefore, we believe that it is always necessary to obtain the authorization of an investigating judge when to carry out search and seizure to detect digital evidence of crimes.

Among the investigative actions, the nature of which is expressed in the collection of primary information carriers, along with the search and seizure, the legislation has also provided grounds for covert investigative actions, within the framework of which digital information may also exist.

The factual basis for the production of this investigative action is that the investigator has sufficient grounds to believe that the suspect, the accused and other persons have information relevant to the criminal case. The legal grounds for conducting secret investigative actions are the following: a) the proceedings are being conducted in a criminal case of a crime of average, moderate or high severity (i.e., grave crime); b) the presence of a court decision.

The investigative actions listed earlier, based on the method of seizing the primary carrier of digital information, make it possible to detect and attach the latter to a criminal case. However, their implementation alone is not enough to obtain reliable and unambiguous conclusions in a criminal case on the basis of digital information. Often in the process of investigating crimes related to the use of digital information, the following negative factors arise:

1. Comparative ease of distortion or falsification of digital information, the impossibility of detecting traces of these operations without special equipment and knowledge.

2. The complexity of studying the digital information by the subject of proof who may also not have special knowledge, which leads to the difficulty of finding and recognizing the part of the information important for a criminal case.

It is possible to eliminate these difficulties only by conducting a forensic examination. A special need for an examination arises in the investigation of so-called computer crimes, which is covered in Chapter 7 of the Criminal Code of the Republic of Kazakhstan.

The very same cognitive activity of an expert in the study of digital information lies outside of the scope of investigative action and proof. When making an examination, an expert does not carry out criminal procedural

knowledge, but another type of knowledge - scientific. Both of these types of cognition belong to the general category of cognition associated with criminal proceedings.

Appointment and conduction of an examination as an investigative action is a way of collecting new information - which did not exist before, but was formed as a result of expert research. The conduct of this investigative action is not aimed at collecting information that has already been seized together with its carrier during a search, seizure or other procedural actions, but at obtaining completely new information based on the collected information - an expert's opinion.

The essence of the appointment of an expert examination as an investigative action lies in the establishment by the investigator of the information that he needs to obtain in the form of posing the relevant questions to the expert. This is a kind of procedural request for information that the investigator must obtain, but cannot collect through procedural knowledge. The expert's conclusion is the provision of the necessary information to the investigator, obtained in the course of non-procedural scientific knowledge. A forensic examination is thus a complex mechanism consisting of:

- leaving the sphere of criminal procedural knowledge into the sphere of scientific knowledge related to criminal proceedings;
- obtaining the relevant information from the field of scientific knowledge;
- legal introduction of this information back into the sphere of criminal procedural knowledge.

The main problem in appointing an examination is the correct presentation of the question to an expert.

In Kazakhstan, the Forensic Science Center of the Ministry of Justice conducts 30 types of forensic examinations in 57 forensic specialties. The list of conducted expert studies was approved by the Order No. 306 of the Minister of Justice of the Republic of Kazakhstan dated March 27, 2017. [9]

The legislation of the Republic of Kazakhstan on forensic activity is based on the Constitution of the Republic of Kazakhstan, consisting of the Criminal Procedure and Civil Procedure Codes of the Republic of Kazakhstan, the Code of the Republic of Kazakhstan on Administrative Offenses, the Law No. 240-IV of the Republic of Kazakhstan "On Forensic Expert Activity in the Republic of Kazakhstan" dated January 20, 2010, and other regulatory legal acts of the Republic of Kazakhstan, regulating forensic expertise.

Forensic examination of computer technology is carried out to determine the reasonability of the facts and circumstances given in digital information recorded in the materials of a civil, criminal case or administrative offense case.

A forensic examination is carried out on computer technology tools, hardware (various types of computers and their components), software (various applied software products), information objects (files in different formats developed using software products), as well as other objects containing information (documents, materials related to computer, computing technology) [10].

In addition, in 2016, for convenience, the Center for Forensic Expertise of the Ministry of Justice of the Republic of Kazakhstan created a "Handbook for law enforcement, special bodies and courts on the appointment of forensic examinations" [11, pp. 166-219].

Thus, when conducting an investigative action, the investigator (interrogator), based on the provisions of the Criminal Procedure Code of the Republic of Kazakhstan, and based on the established goals, searches, consolidates the information received and uses it to disclose crimes.

**Conclusions**

The theoretical research carried out and the generalizations made show the

expediency of legislating the concept of "investigative actions".

Considering the opinions of scientists, we propose to introduce into Article 7 of the Criminal Procedure Code of the Republic of Kazakhstan the definition of the concept of "investigative actions" of the following content:

"Investigative actions are procedural actions carried out by a person conducting criminal prosecution in accordance with the criminal procedure law, the purpose of which is the search, collection, verification and procedural execution of evidence".

In conclusion, investigative actions like "Inspection" are not applicable to the collection of evidence in the form of digital information. In addition, in accordance with the right to personal secrecy, it is required to obtain a court order in all cases of seizure and search performed to identify evidence in the form of digital information.

## REFERENCES

1. "Charter of criminal proceedings" dated November 20, 1864. Available at: https://constitution.garant.ru/history/act1600-1918/3137/ (accessed: 09.11.2021).

2. Balakshin B.C. Admissibility of evidence: concept, legal nature, meaning, assessment algorithm. Yekaterinburg, Publishing house of UMC UPI, 2013, 316 p.

3. Sheifer S.A. Investigative actions. Grounds, procedural order and evidentiary value. Samara, SSU, 2004, 191 p.

4. "About operational and investigative activities". The Law of the Republic of Kazakhstan dated September 15, 1994 No. 154-XIII. Available at: https://adilet.zan.kz/rus/docs/Z940004000/ (accessed 10.01.2022).

5. Fedotov N.N. Forensics – computer criminalistics. Moscow, Legal World Publ., 2007, 209 p.

6. Kushnirenko S.P., Panfilova E.I. Criminal procedural methods of seizing computer information in cases of economic crimes. St. Petersburg, Publishing house of St. Petersburg Institute of Law, 2003, 103 p.

7. Utepov D.P. Problematic issues of collecting and recording digital information. Materials of the international scientific and practical conference, 2020, pp. 116-122.

8. Kerr O.S. Digital Evidence and New Criminal Procedure. *Columbia Law Review*, 2008, pp. 3-60.

9. Order of the Minister of Justice of the Republic of Kazakhstan "On approval of the List of types of forensic experts conducted by the relevant forensic examination, expert specialties, qualifications according to the assigned system of justice of the Republic of Kazakhstan" dated March 27, 2017 No. 306. Available at: https://adilet.zan.kz/rus/docs/V1700014992/ (accessed 10.01.2022).

10. The official website of the Ministry of Justice of the Republic of Kazakhstan and the Forensic Science Center. Available at: https://www.gov.kz/memleket/entities/adilet/activities/222?lang=en/ (accessed 10.01.2022).

11. "Handbook for law enforcement agencies and courts on the appointment of forensic experts at the Forensic Science Center of the Ministry of Justice of the Republic of Kazakhstan", Ministry of Justice of the Republic of Kazakhstan, Astana, 2016, pp. 166-219.

# YURISPRUDENSIYA

## HUQUQIY ILMIY-AMALIY JURNALI

1 / 2022



**Tahririyat manzili:**
100047. Toshkent shahar, Sayilgoh ko‘chasi, 35.
**Tel.:** (0371) 233-66-36, 233-41-09.
**Faks:** (0371) 233-37-48.

**Web-sayt:** www.tsul.uz
**E-mail:** lawjournal@tsul.uz
**E-mail:** tn.tdyu@mail.ru

Jurnal 15.03.2022-yilda tipografiyaga topshirildi.
Qog‘oz bichimi: A4. Shartli 22,08 b.t. Adadi: 100.
Buyurtma: № 6.
TDYU tipografiyasida chop etildi.