International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 06, 2020
ISSN: 1475-7192

EVALUATION OF THE RESULTS OF JUDICIAL COMPUTER AND TECHNICAL EXPERTISES BY THE INVESTIGATORS AND THE COURT

[1]Kadirova Mokhigul Khamitovna, [2]Abdullaev Rustam Kahramanovich,[3]Khujanazarov Azizjon Anvarovich, [4]Rahimkulova Lola Ulugmurodovna

ABSTRACT-- *Scientific and technological progress does not stand still, and today scientists and lawmakers are predicting the prospects of speedy normative consolidation of the procedure for using the latest technical developments, such as video conferencing (video communication), a strain gauge platform for assessing a person's stressful psychophysical state, a system for conducting "electronic" criminal cases, video protocols, electronic referees and judicial expertise. Based on this, this article discusses and analyzes various aspects of the legal regulation of the use of technical and electronic means in the process of proof. In this case, the author draws attention to the types and significance of the conflict of laws governing forensic-computer expertise, including the collection, verification, and evaluation of evidence.*

Keywords--*criminal procedure, electronic evidence, electronic criminal case, information, expertise, expert opinion.*

I. INTRODUCTION

telephone communications these days. The rapid growth of information technology in various fields of human activity, on the one hand, has allowed achieving high achievements and results, and on the other hand, has become a source of harmful consequences for human society. The increase in the number of people using the Internet and computer technology has opened up new opportunities for criminal activity. The Strategy for the Further Development of the Republic of Uzbekistan as a priority in the field of security, religious tolerance, and interethnic consent indicates the improvement of the information security and information protection, timely and adequate response to threats in the information sphere.

II. LITERATURE REVIEW

[1] *Associate professor, Department of Criminal Procedure Law and Criminalistics of the Tashkent State University of Law, Tashkent city, Uzbekistan. aax1990@mail.ru*

[2] *Abdullaev Rustam Kahramanovich, Teacher, Department of Criminal Procedure Law and Criminalistics of the Tashkent State University of Law, Tashkent city, Uzbekistan. r.abdullaev@tsul.uz*

[3] *Teacher, Department of Theory and history of state and law, Tashkent city, Uzbekistan.,: a.xujanazarov@tsul.uz*

[4] *Teacher, Department of Labour law of the Tashkent State University of Law, Tashkent city, Uzbekistan., l.rahimkulova@tsul.uz*

Received: 22 Sep 2019 | Revised: 13 Oct 2019 | Accepted: 15 Jan 2020

Currently, among specialists in criminal procedure law, as the most common classification, evidence theory is considered as one of the branches of criminal procedure law. Technical tools are used in the production, storage, and transmission of digital information, which may contain personal data, as well as state or commercial secrets.

The information can be used both for the achievement of criminal goals and for proving in criminal proceedings.

With regard to evidence in criminal proceedings, first of all, we are talking about the collection, verification, and evaluation of evidence obtained using technical tools.

One of the problems remains the use of electronic tools as evidence. N.A. Selivanov was one of the first to analyze the legal and methodological foundations for the use of technical devices and outlined a new category of "scientific and technical tools". A comprehensive analysis of the enforcement of technical means in criminal proceedings was carried out by V.A. Panyushkin. V.A. Sementsov examined the problems of using audio and video recordings as part of a system of investigative actions and operational-search measures.

The use of information obtained by technical and electronic means in the process of proving is directly related to questions of the theory of proving the criminal process, the development was studied by scientists such as R.S. Belkin, A.A. Davletov, Z.Z. Zinatullin, L.D. Kokorev, V.A. Lazareva, P.A. Lupinskaya, A.R. Ratinov, S.B. Rossinsky, M.S. Strogovich, F.N. Fatkullin, S.A. Sheifer, A.A. Eisman, Yu.K. Yakimovich and others.

The issues of applying modern technical means are closely related to the possibility of using electronic (digital) information in proving since it can only be obtained with the help of appropriate technical means. K.B. Kalinovsky, V.B. Vekhov, N.A. Zigura, V.V. Krylov, S.V. Krygin, S.I. Kustavkov, A.V. Kudryavtseva, T.Yu. Markelov, D.V. Ovsyannikov, P.S. Pastukhov, R.I. Okonenko, Yu.N. Sokolov, V.Yu. Stelmakh and others devoted their work to the collection, verification, and evaluation of electronic evidence.

Many legal scholars devoted their works directly to the study of the issues of criminal procedural regulation of the use of technical means in criminal proceedings, the theoretical and practical aspects of the concept of technical means, the principles of admissibility of the use of technical means. Contribution to the disclosure of various aspects of the use of technical means was made by G.F. Gorsky, G.I. Gramovich, E.A. Zaitseva, E.P. Ischenko, I.V. Kaznachey, L.D. Kokorev, A.A. Levy, Yu.N. Milenin, D.V. Mulenkov, V.A. Panyushkin, A.I. Sadovsky, N.A. Selivanov, V.A. Sementsov, A.E. Fedyunin and other scientists.

At the dissertation level, the problem was conducted of the legal regulation of the use of technical means and the evidentiary value of the information obtained with their help A.E. Fedyunin and S.D. Tsomaya, I.V. Kaznachey considered the importance of technical means in criminal proceedings from the point of view of the communicative function. V.A. Rodivilina drew attention to the modern forms of application of technical means, such as video conferencing and electronic translator.

However, despite the significance of the contribution of these authors to the study of certain issues of the use of technical means and the use of information obtained through their use, in the field of criminal proceedings, there is practically no comprehensive analysis of the probative value of information obtained using traditional technical tools, and modern electronic devices that record information in the form of electronic (digital) information during the investigation, as a result of operational-search measures or by third parties. Therefore, it seems important to study the theoretical and practical problems of the procedural use of technical and electronic

means in the process of proving, to identify the shortcomings of legal regulation and to develop relevant proposals aimed at improving the criminal procedure legislation.

III. DISCUSSION AND ANALYSIS

The term “Computer crimes” began to be used for the first time in American and then other foreign literature in the early 60s, when crimes committed using computers began to be detected[1]. It should be emphasized in this connection that it was during this period, in the Criminal Code of the Republic of Uzbekistan in 1994, article 174 "Violation of the rules of information" appeared, which provides criminal penalties for a number of crimes in this area, in turn, was established responsible for the kinds of theft with the use of computer technology. Also in 2007, it was adopted a special chapter XX, establishing responsibility for crimes in the sphere of information technologies[2].

Every year, crime on the Internet masters appears new forms, using contactless settlements in most cases, and therefore the bodies of inquiry and preliminary investigation have the difficult task of exposing criminal acts in the Internet space and recording evidence. In recent years, for law enforcement officials, concepts such as IP and MAC addresses, hosting provider, domain, account, network protocol have become more familiar and familiar, in connection with which the electronic-digital "traces" left by users of Internet resources, have become more accessible in the understanding of persons conducting criminal prosecution. However, the discovery, preservation, and recording of information related to the Internet space, in practice, is not an easy task for most employees of the bodies of inquiry and preliminary investigation.

The insufficient training of such employees on this issue, the continuous improvement of computer technology, the specificity and complexity of the technical processes for establishing the source of evidence, the lack of a unified practice of fixing the necessary computer information and the technical means for its processing, the absence of recommendations on the issue under consideration, undoubtedly contribute to the emergence of new problems with investigation of crimes involving the use of Internet resources and fixation and evidentiary information stored on electronic media and the Internet resources.

The Criminal Procedure Law determines that each evidence is subject to assessment in terms of relevance, admissibility, reliability, and all the evidence collected in aggregate - is sufficient to resolve the criminal case. The expert's opinion refers to the evidence in a criminal case; for consideration of this issue, the general forensic assessment scheme developed in the forensic literature can be applied: admissibility of the conclusion: on compliance with the order of appointment and expertise; compliance with the procedure for raising questions to the expert at the trial; whether the expert is subject to challenge; the correctness of the conclusion; admissibility of objects of expertise: whether the procedural procedure for their receipt has been followed; whether the rules of transportation and storage are observed; determination of the reliability of the conclusion: the reliability of the applied methodology; the legality of applying the methodology in a particular case; sufficiency of the research material presented to the expert; the correctness of the presented source data; determination of the validity of the obtained results: determination of the completeness of the research conducted by an expert; o the degree of confirmation of the conclusion of the study; determination of the evidentiary value of the conclusion [3].

In criminal proceedings, there is no predetermined stronger evidence and superiority of one over the other. Although the conclusion of the expertise does not have any advantages over other evidence. It possesses, in comparison with them, significant specificity, since it is a conclusion, an inference made on the basis of research conducted using special knowledge. Evaluation of such evidence often presents for individuals who do not have such knowledge, considerable difficulty.

For the initial period of criminal law practice related to the disclosure and investigation of crimes in the field of computer information, a characteristic feature is an excessive trust in the conclusion of a forensic-computer expertise, assessment of its evidentiary value. Meanwhile, the expert's opinion, like any other evidence, may turn out to be doubtful or even worthless for various reasons and become inadmissible evidence. This necessitates an assessment of the conclusion, not only from the point of view of the possible fallacy of the conclusion but also from the standpoint of the evidence of the expert opinion.

So, an expert may be presented with incorrect initial data or non-authentic objects - computer tools. Therefore, in this case, the expert opinion, like any evidence, should be checked by thorough, comprehensive verification and critical assessment. First of all, it must be checked whether the procedural procedure for the appointment and production of a forensic-computer expertise is observed. After the expertise, the expert's opinion is presented to the suspect, accused, his/her defense counsel, which explains the right to apply for the appointment of an additional or repeated forensic expertise. In practice, these requirements of the law are not always respected, especially when the expertise is carried out before the person is brought in as an accused.

As already noted above, in addition to observing the procedural order and the procedural form of expertise, it should also be checked whether the expert is not subject to challenge. This also applies to private experts (expertise can be carried out in a state or private expert institution), the data on the specialty and competence of which the investigator must find out[4]. Among the basic requirements for a subject having special knowledge conducting a forensic-computer expertise, one can name: competency - for conducting a forensic-computer expertise, an expert must have special knowledge that can be confirmed by a diploma of higher education, valid at the time of the expertise certificates of improvement qualifications, on passing training and certification in relevant specialties; impartiality - the expert cannot be in any way dependent on the body or person who appointed the expertise, the parties and other persons interested in the outcome of the case. Also, it is not allowed to influence the expert from the courts, judges, prosecutors, bodies of inquiry, investigation, as well as other government bodies, organizations, associations, and individuals in order to obtain an opinion in favor of any of the participants in the process or in the interests of other persons; Responsibility - experts conducting a forensic-computer expertise bear criminal responsibility for giving a deliberately false conclusion and for divulging the data of the preliminary investigation.

When conducting an expertise in a state expert institution, the expert is appointed by the head of this institution, fully aware of the specialization of his employees. Therefore, the practical basis for the rejection of such experts can only be revealed by their personal, direct or indirect, interested in the outcome of this criminal case, interest in the outcome of the case involving the use of computer tools.

Assessing the admissibility of the conclusion, it is necessary to verify the correctness of its design, the availability of all necessary details specified in the law.

So, there are cases when there is no introductory or research part, there is no expert signature or the conclusion is signed by the wrong person indicated in the introductory part. If the expertise was complex, the conclusion should indicate which expert, which studies were carried out, and each part of the study is signed only by the experts who carried out it.

Particular attention should be paid to the admissibility of the studied objects. If the studied computer tools are recognized as unacceptable, then automatically loses this property and the very conclusion of the expertise. Therefore, the procedural soundness of the objects of expert research should always be checked. To do this, you must first establish whether the method of obtaining them was legal. An analysis of the practice of collecting evidence shows that computer tools can be seized during some investigative action (inspection, search, seizure) or presented by one of the participants in the process or by unauthorized persons. Documents with computers (or other, for example, operational) information can be, moreover, requested by institutions, enterprises, and officials. It should be borne in mind that in any case, the procedural procedure for obtaining these objects by the investigator (court) must be followed. This is especially true for obtaining during the investigative actions, the objects examined above - possible material evidence. If significant violations were made (for example, computer information on the data medium was changed) that cast doubt on the reliability of the results of the investigative action (for example, an inspection of the contents of the computer's hard drive), then material evidence may be recognized as inadmissible. And this, in turn, entails the inadmissibility and conclusions of an expert in the study of objects.

Of the materials studied in criminal cases, in most cases, the defense questioned the conclusions of the expertise precisely in connection with the investigation of objects of poor quality in the procedural sense. The explanation of this situation is as follows: investigators still do not have the skills to work with computer equipment and information, so the seizure occurs with gross tactical violations. Seized objects are not examined in detail on the spot and their individual characteristics are not reflected in the protocols in any way. So, for example, in one of the cases of fraud using "virtual trade" in the apartment of the offender during the search, three Winchesters were seized. From the protocol of the search, it is not clear in what condition and where they were found. The admissibility of the object of expertise is influenced not only by the observance of the rules for its receipt but also by its proper storage after the seizure (especially for computer storage media). It should exclude the possibility of intentional or accidental changes (substitution) of the object since doubt about the authenticity of the object of expert research of a computer tool can also lead to the inadmissibility of an expert's conclusion.

It seems that the expert should pay attention to the impeccability of the seizure of objects, which can be carried out as part of the inspection, search or seizure, and the correct packaging, transportation, storage. The latter causes the greatest concern since it is during storage that most often investigators "compromise" future research objects. Many of them try to examine and investigate information independently without observing procedural requirements. Some use seized computer tools for business or personal purposes, which leads to a change or even destruction of information, and also calls into question the immutability of the seized object. An analysis of practice shows that it is such a version of protection (making changes to computer information after it has been removed from the user) that prevails in cases where the expertise was conducted.

Sometimes forensic studies of computer tools are carried out with insufficient materials. Experts rarely exercise the right to participate in investigative actions, to demand additional materials from a criminal case, which the investigator must provide, if necessary, for research. They must verify the correctness of the source data specified in the investigator's decision or the court ruling on the appointment of the expertise.

Evidence can be divided into the following groups: verbal (voice) information; research results using special knowledge; direct perception (by observation method); other information not related to the above groups.
Based on this classification, the following system of types of evidence facts; expert opinion; Protocols of procedural actions; other documents are proposed.

Moreover, in the framework of criminal proceedings, homogeneous information must be contained in one type of evidence. In order to optimize the use of evidence generated on the basis of verbal information, it is necessary to abandon the division of testimonies into types depending on the procedural status of the interrogated person and combine the testimonies of the witness, victim, accused, suspect, specialist into one type of evidence - testimony. It seems unjustified that there are various methods and procedural forms of recording verbal information in the framework of criminal procedure activities.

And also, forensic-computer expertise belongs to the section of engineering and technical expertise. The purpose of this expertise is to determine the status of the computer, its serviceability as an information medium. The expertise is carried out including a computer and inspecting the contents in the presence of a specialist, witnesses, investigator, interrogator or court. If the investigative action (inspection) is framed without violations of the CPC, the computer can be used as evidence in a criminal case.

During the expertise, several important points are taken into account, therefore, the procedure is carried out in several stages. At the first stage, only a visual inspection is applied: the system unit, monitor and other components. In the second stage of computer expertise, technical tools are used to detect hidden defects. In this case, electrical, mechanical systems, blocks, devices, and devices are studied. The timing of the expertise of a computer usually depends on the type of expertise. If the range of questions for the study is not outlined, the expert conducts a comprehensive expertise. When conducting a study, an expert must identify such a fact as the life of the computer and its intensity. Depending on this, all questions of interest can be identified. Only a person with qualifications corresponding to the status of an expert can conduct a forensic computer expertise. The progress and results are recorded in a special document called expert opinion. The Criminal Procedure Code allowed the designation and production of investigations prior to the initiation of a criminal case, which makes it possible to more quickly study the media and seize evidence.

The forensic-computer expertise is divided into the following types: computer-software expertise; computer network expertise; computer information expertise; computer-technical expertise; computer-digital expertise.

A forensic computer expertise may relate to its software part. That is, computer-software expertise considers the software development that was used in it. Software testing reveals the following information: components of software devices; access protection; the formation of functional problems; unified software algorithm; signs of counterfeit products; use of devices for design studies; the presence of initial files in information carriers; name and type of program.

Computer network expertise includes testing network technologies. For this study, the expert will need data such as the telecommunication and network technologies used. Separately, Internet technology should be

mentioned. In exploring this aspect, a computer connected to the Internet, as well as a network of computers, can be examined.

What network services were used when using the Internet is also an important issue. This expertise is more extensive and requires the attention of several issues, such as: international network security; Messages sent and received features and significance of networks; Bookmarks prohibitions; continuity; configuration changes; use of hardware; applications; all users.

Computer-information expertise considers information development, which was used in it and reveals the following information: type of information recording; features of use; access to information; types and features of information; user information; information security features; preliminary information; changes and place of information; attempted information; chronological file movement; compliance with operating rules; saved files; information integrity; changes made to the storage media.

Unlike forensic investigations, computer-technical expertise is a subtype of forensic expertise that answers questions that are relevant to the matter within the strict framework of the law: establishing a computer system; chronological order of use; the presence of damage; technical properties; model; regulations; value in a computer system.

The objects of computer-technical expertise can be: hardware: computers, laptops, mobile phones, cash registers, servers, workstations, etc., as well as their peripheral devices and components; software, including its source codes; information objects (data): text, graphic, audio and video files, electronic documents, databases, log files, etc.

Computer-digital expertise is a subtype of forensic expertise that answers questions based on digital accounting. The objects of computer-digital expertise can be computers, laptops, smartphones, printers, scanners, cameras, mobile phones, GPS navigators, storage media, cash registers with fiscal memory [5].

Questions for a forensic computer expertise are posed by the person or body appointing the forensic expertise, but a specialist may be involved in the preparation of the questions. The involvement of a specialist provides a guarantee that questions that are not within the competence of an expert will not be posed for resolution. This is extremely important since going beyond the limits of competence when answering a question can lead to the recognition of such an answer or the whole conclusion invalid. In some cases, the appointment of the expertise indicates the expert institution. In the expert center, experts share their specialization work and then summarize the information received. Thus, the expertise includes a rather comprehensive concept, which includes a lot of requirements and factors.

The expert must ensure the safety of the submitted research objects and case materials. However, today there are storage media that cannot be accessed without making changes to their contents. For example, mobile devices, etc. In this case, the permission of the investigator, interrogator or court to make changes that do not entail damage or destruction of the research object or part thereof is required. The corresponding permission may be indicated in the decision on the appointment of a forensic computer expertise or obtained by satisfying a special request by a court or investigator, interrogator of a special application.

A repeated expertise on the same issues is appointed in cases of doubt about the validity of the expert's opinion or the presence of contradictions in the conclusions of the expert (or commission of experts). Such an expertise is assigned to another expert or commission of experts.

An additional expertise is appointed in case of insufficient clarity or completeness of the expert's opinion, as well as in case of new questions regarding previously investigated circumstances of the case. An expertise is assigned to the same or another expert. The previous participation of the expert in the proceedings as an expert or specialist is not a ground for his challenge. The issue of attracting a person as an expert, if he had previously conducted research under an agreement with one of the parties, should be decided to take into account the law. Very often, a specialist is interrogated as a witness, which excludes his further participation in the case as an expert on formal grounds. Commission expertise is carried out by two or more experts of the same specialty. A comprehensive expertise is appointed if it requires experts from different specialties.

Disclosure and investigation of crimes involving the use of computer tools, at present, cannot be carried out without the use of special knowledge in the field of modern information technologies. Computer facilities - modern means of providing automated information systems and information technologies - software, technical, information, etc., used or created in the design of information systems and ensuring their operation. Scientific and technical means, in principle, can successfully organize an investigation, but cannot do without the help of a specialist in collecting and examining evidence. The peculiarities of identifying and investigating forensically significant computer information are related, first of all, to the fact that this area of special knowledge includes a number of rather diverse science-intensive areas (electronics, electrical engineering, information systems and processes, radio engineering and communications, computer technology (programming) and automation) Crimes of the considered categories are often latent in nature, do not leave visible traces and are difficult from the point of view of disclosing and collecting evidence in connection with the widespread use of remote access, data protection, etc. The main procedural form of using special knowledge in these cases is a forensic-computer expertise. It is expert research that provides the results that have the greatest evidence in the study of hardware, software and computer information.

R.S.Belkin divides the traces into the material (in material evidence) and ideal (in the memory of the victim or witness) [6].

V. A. Mesheryakova and A. N. Kolycheva define virtual tracks, "electronic-digital track" as forensic information expressed through electromagnetic interactions or signals in a form suitable for processing using computer technology, as a result of creating a specific set of binary machine code or its conversion, expressed in the modification, copying, deletion or blocking, fixed on a tangible medium, without which it cannot exist [7]. The basis of the mechanism for the formation of traces of this category is their electronic digital display, which occurs in artificially created environments: the memory of electronic information carriers, information and telecommunication networks, communication channels for transmitting information, information systems. The main objects of fixation in terms of evidence are IP addresses, MAC addresses, log files, cached application data, user history or logs contained in the computer system, on the organization and provider server, files, their physical addresses, names, drill down connections. The recording of evidence stored on the Internet resources should be presented in the form of a consistent and complete chain of information reflected in the procedural documents (such investigative actions as search, seizure, and inspection of the scene).

Given the position of D.A. Ilyushina and A.L. Osipenko, the provisions included in the doctrine of the recording of evidence, as well as the features of the functioning of the Internet identified the main objects of evidence-based information posted on the Internet[8], which are recorded in a certain way, including:

- the procedural component, the content of which is the protocol form established by the criminal procedure legislation, as a reflection of the situation, actions, phenomena, and verbal signals;

- a forensic component containing a graphic (plans, diagrams, drawings, graphs, drawings), subject (seizing objects in full or their parts, making casts, mock-ups, impressions) and visual-figurative (photographing and video shooting, screenshots) forms fixation [9].

An analysis of the theoretical aspects of fixing evidence-based information stored on Internet resources has led to the conclusion that it is possible to develop further recommendations for fixing relevant information, which in the future may have evidentiary value. One of the properties of electronic digital tracks is the ability to easily duplicate them without changing the original data source, as well as the ability to create an unlimited number of easily and quickly changeable duplicates of information, and it can be destroyed a fairly large amount of information in a rather short time period. It is believed that the division of electronic-digital tracks into tracks that occur on electronic computers and tracks located on the global Internet is wrong, since the Internet is, in fact, a communication network system and a set of technical tools that combine various computer systems, in connection with then it can be considered as a means of transmitting information. With phonoscopic and genomic traces, using technical means, such information is converted on a material medium in which a person can perceive it visually, audibly or otherwise.

Therefore, despite the fact that computer information does not have physical parameters inherent in material objects, it has certain fixed characteristics that significantly differ from ideal traces, such as volume (size), format (type of information), location information (location details) on the carrier), time (creation, modification, use, destruction), etc., as well as a number of other properties, such as objectivity, reliability, completeness, accuracy, relevance, usefulness, etc. traces can serve as not only transformed objects, but also recorded information about the course of their transformations, and often they will play an equally important role in the evidence process.

Without analyzing information about the means of its modernization, time, subjects of access to this file, it is impossible to get a complete picture of the event and the forensic information. In turn, the mechanism of traceability in information networks depends on a number of the following factors:

factors that do not depend on the identity of the victim or criminal;
factors that are directly dependent on the identity of the victim or criminal.

Thus, in contrast to the criminal doctrine of tracing, where the main factor is the mechanical contact interaction of tracing and tracing objects with physical properties in the formation of digital traces, due to the lack of physical shape of the object, only changes in the level of electromagnetic interactions of the digital signal can be recorded that can only be identified with the help of technical means that convert the electronic-digital model of the object into a view accessible for human perception. Moreover, in each case, to identify traces, it is necessary to determine such an information environment, due to certain rules and algorithms, in which information was processed, where this information will be forensic information, and not a set of encoded characters that do not represent practical value.

At the global level, work is underway to create mechanisms for the traceability of evidence in information networks through the features of storage on Internet resources, to record evidence, to disclose methods for recording evidence in criminal files, taking into account the capabilities of hardware and software in computer

technology, to classify electronic digital traces of crime generated in a computer system and Internet space for various reasons, to consider characteristics of certain investigative actions aimed at identifying and fixing the evidentiary information stored on the Internet resources.

Traces by type are classified into: system and application software files; configuration files; log files of software and hardware; files, sources of information generated during the user's activity, including their backups and deleted files to be restored; files that provide authentication and user privacy; information in RAM or a swap file; information obtained by appropriate electronic or special technical means.

And at the location of the electronic-digital tracks: technical devices and communication channels of the victim; technical devices and communication channels of criminals; technical devices of telecom operators.
And according to the source of storage of electronic-digital tracks: tracks on hard drives; traces located in the main memory of computers, peripheral devices, and communications; traces in wired, radio-optical fiber and other electromagnetic communication systems.

The classification of technical means on the basis of their intended purpose for the needs of criminal proceedings can be represented in the form of three groups of technical means: technical means - material evidence; office and telecommunication equipment; technical means used in the production of investigative and judicial actions in order to form, verify and study evidence.

The need for a forensic computer expertise in the course of proceedings in a court essentially depends on the procedural situation under which this issue is being resolved. By necessary cases, the following are understood: the conclusion of the expertise is especially important as evidence in the case under investigation (for example, if a person suspected of murder is identified in the electronic notebook with the address and phone number of the murdered person, the suspect categorically denies familiarity with it); the expert opinion is not justified, contradicts other case materials, has other shortcomings, and doubts arise as to its correctness (for example, as a result of inspection during investigative actions and later, as a result of the expertise, different computer information was found on the same data carriers); in the course of the preliminary investigation, two expertises were carried out to establish the same fact, and the experts came to the opposite conclusions; disagreements arose between the experts performing the commission or complex expertise and each of them made his own conclusion; interested participants in the process do not agree with the conclusions of the expertise and filed a petition to summon the expert to court (for example, files on the case of evidence prepared by a specialized software package were found on the accused's computer, while the accused claims his computer illiteracy and possible accidental appearance of these data on the computer); the expert opinion is based on the initial data taken from the testimony of the accused, the victim, the witness, and there is reason to believe that they can be changed at the hearing; new source data have appeared or there is reason to believe that they will appear in court (for example, one of the participants in the process intends to present in the court computer information media received at one time from the accused for storage), etc.

There may be other not so typical situations when an expert is called in a trial to give an opinion. However, it is illegal to call an expert in court only to answer the question of whether she/he confirms his conclusion given at the preliminary investigation since the expert is not summoned to court to confirm this earlier conclusion but to conduct an expertise and give an opinion on its results.

Expertise in court is an independent procedural action. In the cognitive plan, it can be a continuation of earlier studies of computer tools. In the case of the appointment of an expertise, the chairperson invites the parties to submit written questions to the expert. The questions raised should be announced and the opinions of the participants in the trial heard.

Depending on the complexity of the questions posed and other circumstances, expert studies of computer tools can be carried out directly in court or elsewhere (for example, in an expert institution specializing in information technology, or in an information and computer center, or at the scene of an incident, in the premises of the information service security, etc.) [10].

The written opinion is announced by the expert in court and attached to the case together with the court ruling on the appointment of the expertise. At the request of the expert, his/her presence in court may be limited by the time required to examine evidence related to the subject. After giving an expert opinion, interrogating him/her, having heard the opinions of the prosecutor, defendant, civil plaintiff, civil defendant, and their representatives, the court may release the expert from further presence in court.

The interrogation of an expert in court, the court has the right to call for interrogation of the expert, who gave a conclusion during the preliminary investigation, to clarify or supplement the conclusion given to him/her. The Criminal Procedure Law determines that after the expert's opinion is announced, he may be asked questions by the parties. In this case, the first questions are asked by the party on whose initiative the expertise was appointed. If an expert needs it, the court can provide him/her time to prepare answers to questions from the court and the parties.

In some situations, the incompleteness of an expert's opinion may serve as the basis for the appointment of an additional expertise, the production of which is entrusted to the same or another expert. If the court has doubts about the validity of the expert's opinion, and also contradictions in the expert's conclusions have been identified, a second expertise may be appointed, the production of which is entrusted to another expert. In any case, all the questions posed to the expert during the interrogation, and his/her answers to them should be recorded in the minutes of the court session.

IV. CONCLUSION

In this way, analyzing the point of view of experts in the field of optimizing the use of evidence generated using specialized facts, we can list the following conclusions:

First of all, the conduct of expert research in various forms (preliminary studies and judicial expertise) should be improved.

Second of all, the equal status of the results of any expertise should be enshrined in law. Other forms of using special knowledge should be used in the process of proving along with the expert’s opinion as “other documents”. When evaluating, the essence of the document, the nature of the research conducted, and the reliability of the results should be taken into account in the first place.

In order to optimize the use of evidence generated as a result of direct perception (by observation method), it is necessary, firstly, to try to avoid placing the same cognitive operations in different procedural forms. The results of any type of law enforcement should not be excluded from the process of proof only on the basis of the

difference between the procedure and the criminal procedure. Especially, in cases where procedural guarantees in these types of activities are superior to criminal procedural ones.

Third of all, the current legislation does not prevent the involvement in the process of proof of any information submitted by participants in criminal proceedings and other entities, subject to the observance of the general requirements for evidence.

Fourth, a change in approaches to working with material evidence is required. The development of criteria is to highlight the unconditional signs of evidence. This is due to the fact that physical evidence and other types of evidence are categories of different orders. Material evidence is not a kind of procedural form; its information may be involved in the process of proof through other types of evidence. The optimal seems to be the universal procedure for handling seized objects and documents. One of the reasons for the competition of types of evidence is the distrust of information in a certain form that developed in law enforcement and is not based on law. In the process of proving, objects and documents can be recognized as material evidence or other documents if they were obtained using technical or electronic means, there is information about the applied technical and electronic means, permission (format) of the received electronic file, date of its creation and change and information about the author.

The consolidation in the criminal procedure law of the obligation to draw up a protocol in the case of using special technical means for publicly and secretly obtaining information that will reflect the information necessary to verify the results obtained, in the case of electronic information, reflect in this protocol information on the permission (format) of the received an electronic file, the date of its creation and change, as well as information about the electronic information carrier and its storage conditions; the obligation to provide the results of operational-search measures obtained using technical and electronic means, together with a protocol reflecting information about the means used and the results obtained, improves the quality of verification and evaluation of electronic information as evidence.

V. ACKNOWLEDGMENT

This scientific article was done within research in criminal procedure, and helped by Dr. U.Tukhtasheva. Authors also thank to teachers of Department of Criminal Procedure Law and Criminalistics of TSUL who gives scientific materials for writing our ariticle.

REFERENCES

1. Federal Criminal Code and Rules. West Group, St. Paul, Minn, 2014. –P. 632-634. http://www.interpol.int. http://www.fraund.org
2. Rasulev A. K. (2017). Some questions of improvement of criminal-legal and criminological measures of fight against crimes in the sphere of information technologies and security. Monograph. –T, University. - p. 20.
3. Kalinina, E.V. (2016). Evaluation of the findings of computer forensics and their use in evidence of fraud, St. Petersburg, p.18.
4. http://www.lex.uz
5. Polyakov, V.V., Shebalin, A.V. (2013). To the question of the appointment of computer-technical

expertise, the object of which is a smartphone, for crimes in the field of computer information, Collection of materials of forensic readings, ed. Yu.L. Boyko, Barnaul, pp. 53-70.

6. Belkin, R.S. (1997). Forensics course, Moscow, Vol.2, p. 61.
7. Mesheryakova, V.A. (2002) Crimes in the field of computer information: the basics of the theory and practice of investigation. Voronezh, p.102. Kolycheva, A.N. (2019). Fixation of evidence stored on Internet resources. Abstract of PhD thesis, Moscow, p.10.
8. Osipenko, A. L. (2009) Network computer crime: theory and practice of struggle. Monograph. - Omsk: Omsk. Acad. Ministry of internal Affairs of Russia. - p. 479
9. Litvin, I.I. (2018). Modern technical means and problems of their application in proving at the pre-trial stages of criminal proceedings. Abstract of PhD thesis, p. 31.
10. Usov, A.I. (2003). Forensic research of computer tools and systems: the basis of methodological support. Moscow, p.15.