Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/10571
DOI URL: http://dx.doi.org/10.21474/IJAR01/10571

RESEARCH ARTICLE

FORMS OF PRODUCTION RESEARCH OF HARDWARE AND SOFTWARE OF A COMPUTER SYSTEM

Kadirova Mokhigul

Manuscript Info

Manuscript History
Received: 22 December 2019
Final Accepted: 25 January 2020
Published: February 2020

Key words:-
Evidence, Examination, Expert, Expert, Information, Interrogation, Conclusion, Interrogation, Traces

Abstract

This article analyzes the concept and significance of information technologies, forms of information use, the role of networks, electronic communication services and expertise in combating crime. The author defines concepts and classification of forensic computer expertise as computer-programming expertise, computer-network expertise, computer-information expertise, computer-technical expertise and computer-digital expertise. The article analyzes the classification of technical means as computers, laptops, smartphones, printers, scanners, cameras, mobile phones, GPS navigators, media, cash equipment with fiscal memory and determines the features of their traces. The analysis resulted in proposals for improving the norms of the national criminal procedure legislation in the field of detection, fixing of evidentiary information stored on the Internet resources or in other technical means and conducting forensic computer examinations.

Introduction:-

The development of modern technologies in the field of telecommunications allows criminals to commit serious and especially felonies with impunity, to obtain profits, but it is sometimes impossible to collect sufficient evidence to bring them to criminal responsibility. The practice of combating transnational crime requires not only improved means and methods of combating it, but also the creation of new procedural mechanisms for providing legal assistance in criminal cases[1]. The analysis of investigative and judicial practices shows that new technical developments are being successfully used in the system of means and methods of evidence in criminal cases. In spite of the law enforcement difficulties, there is considerable experience in the field of criminal justice in the application of audio, video and other technical means that allow to objectively and accurately record the entire process of evidence and evidence in the criminal case. Scientific and technological progress is not stopping, and today scientists and legislators predict the prospects for the early normative consolidation of the order of using such new technical developments as video conferencing (video communication), a strain-gauge platform for assessing the stress psychophysical state of man, systems for conducting "electronic" criminal cases, video protocols, an electronic judge and conducting forensic computer expertise.

Forensic computer examination refers to the section of engineering and technical expertise. The purpose of this examination is to determine the status of the computer, its functioning as an information medium. The examination

[1] Sabine De Moora, Christophe Vandevivera,b, Tom Vander Bekena. Assessing the missing data problem in criminal network analysis using forensic DNA data. Social Networks. https://doi.org/10.1016/j.socnet.2019.09.003.

Corresponding Author:- Kadirova Mokhigul

is conducted including the computer and performing inspection of the content in the presence of a specialist, understandable, investigator, investigator or court. If the investigative action (inspection) is executed without violations of the criminal procedure code, the computer can be used as material evidence in the criminal case.

Methods:-

Several important points are taken into account when conducting the examination, so the procedure is carried out in several stages. In the first stage, only a visual inspection is applied: The system unit, the monitor and other components. In the second stage of the computer's examination, technical means are used to detect hidden defects. In this case, electrical, mechanical systems, units, instruments and devices are studied. The timing of the computer's examination usually depends on the type of examination. If the range of questions for the study is not outlined, then the expert conducts a comprehensive examination. In the course of the study, the expert is sure to identify the fact that the computer's operating time and intensity are the same. Depending on this, you can identify all the questions you are interested in. Only a person with qualifications corresponding to the status of an expert can conduct forensic computer examination. The progress and results are recorded in a special document called the expert's conclusion. The Code of Criminal Procedure allowed the appointment and production of studies before the initiation of a criminal case, which allows more rapid study of carriers and the capture of evidence information.

Discussion:-

Forensic computer examination is divided into the following types:
1. Computer-programming expertise;
2. Computer-network expertise;
3. Computer-information expertise;
4. Computer-technical expertise;
5. Computer-digital expertise.

Forensic computer examination may concern its program part. That is, computer-software expertise considers the software development that was used in it. Software testing identifies the following information:
1) software components;
2) access protection;
3) formation of functional problems;
4) a single algorithm of programming products;
5) evidence of counterfeit products;
6) use of devices in project research;
7) availability of the initial files in the media;
8) program name and type.

The computer-network expertise includes testing of network technologies. For this study, the expert will need data such as the telecommunications and network technologies used. Internet technologies should be mentioned separately. Research into this aspect can examine the computer connected to the Internet and the network of computers. What kind of services the network used when using the Internet is also an important question. This expertise is more extensive and requires attention to several issues, such as:
1) international network security;
2) sent and received messages;
3) characteristics and significance of networks;
4) bookmarks;
5) bans;
6) indecent;
7) configuration changes;
8) use of hardware;
9) annexes;
10) all users.

The computer and information expertise considers the information development used in it and identifies the following information:
1) type of record of information;

2) peculiarities of use;
3) access to information;
4) types and characteristics of information;
5) user information;
6) information security features;
7) preliminary information;
8) changes and place of information;
9) attempt to information;
10) historical file movement
11) observance of operating rules;
12) saved files;
13) integrity of information;
14) changes to the media.

Unlike forensic studies, computer and technical expertise is a subtype of forensic expertise that answers questions relevant to the case within the strict framework of legislation:
(1) computer system installation;
2) chronological order of use;
3) damage;
4) technical characteristics;
5) model;
6) time limits;
7) value in the computer system.

The objects of computer and technical expertise can be:
1. hardware: computers, laptops, mobile phones, equipment, servers, workstations, etc., as well as their peripherals and accessories;
2. software, including its source code;
3. information objects (data): text, graphics, audio and video files, electronic documents, databases, log files, etc.

Digital and computer expertise is a subset of forensic expertise that answers questions based on digital accounting. The objects of computer and digital expertise can be computers, laptops, smartphones, printers, scanners, cameras, mobile phones, GPS navigators, media, cash equipment with fiscal memory[2].

Questions for forensic computer examination are asked by the person or body appointing the forensic examination, but for drafting questions a specialist may be involved. The involvement of a specialist guarantees that no questions that are not within the competence of the expert will be raised to the permission. This is extremely important, since it may result in the recognition of such an answer or of the entire conclusion being invalid if the answer to a question is not within the competence of the competent authority. In some cases, the expert institution is indicated when the examination is performed. In the Expert Center, experts divide the work on specialization, and then summarize the information obtained. Thus, the examination includes a rather specific concept, which includes a lot of requirements and factors.

The expert is obliged to ensure the safety of the submitted objects of investigation and materials of the case. However, there are currently storage media that cannot be accessed without modifying their content. For example, mobile devices, etc. In this case, the investigator, investigator or court must be authorized to make changes that do not cause damage or destruction of the object or part of the study. The relevant authorization may be specified in the order of appointment of forensic computer examination or obtained by the court or investigator, the investigator of the special application.

[2] Polakov V.V., Shebalin A.V. To the question of the appointment of computer and technical expertise, the object of which is a smartphone, on crimes in the field of computer information // Collection of materials of forensic readings / ed. Yu.Boiko. - Barnaul, 2013. - 53-70.

The second examination on the same issues is appointed in cases of doubt about the validity of the expert's conclusion or the existence of contradictions in the conclusions of the expert (or expert Commission). Such examination shall be appointed by another expert or expert Commission.

Additional examination is appointed in case of insufficient clarity or completeness of the expert's conclusion, as well as in case of new questions regarding the previously investigated circumstances of the case. The examination is assigned to the same or another expert. The previous participation of an expert in the proceedings as an expert or specialist is not a reason for his withdrawal. The question of involving a person as an expert, if it had previously conducted a contract study from one of the parties, should be decided in the light of legality. Very often, a specialist is interrogated as a witness, which excludes his further participation in the case as an expert on formal grounds. The Commission examination is performed by two or more experts of one specialty. A complex examination is appointed if it requires experts of different specialties.

At present, the disclosure and investigation of computer-related crimes cannot be carried out without the use of special knowledge in the field of modern information technology. Computer means - modern means of providing automated information systems and information technologies - software, technical, information, etc., used or created during 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 the collection and study of evidence. The peculiarities of the detection and research of criminally significant computer information are connected, first of all, with the fact that this area of special knowledge includes a number of sufficiently diverse science-intensive directions (electronics, electrical engineering, information systems and processes, radio engineering and communication, computer technology (programming) and automation). The crimes in question are often patentless, leave no visible traces and are complex in terms of disclosure and collection of evidentiary information in connection with the widespread use of remote access and data protection.

The main procedural form of the use of special knowledge in these cases is forensic computer examination. It is expert research that provides the results with the greatest evidentiary value in the study of hardware, software and computer information[3].

R. S. Belkin, divides the traces into: Material (in material evidence) and ideal (in the memory of the victim or witness)[4].

V.A.Meshcheryakova and A.N.Kolychev define virtual traces, "electron-digital trace" as criminally significant information expressed by means of electromagnetic interactions or signals in a form suitable for processing with the use of computer technology, as a result of creation of a certain set of binary machine code or its transformation, expressed in modification, copying, removal or blocking, fixed on a material carrier, without which it cannot exist[5]. The basis of the mechanism for the formation of traces of the category under consideration is their electronic-digital display, which occurs in artificially created environments: The memory of electronic media, information-telecommunication networks, communication channels, information systems. The main objects of the fixation from the point of view of the evidentiary value are IP address, MAC address, log files, cached application data, history or logs of the users' work contained in the computer system, on the server of the organization and provider, files, their physical addresses, names, details of connections. The record of evidence stored on the Internet 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 examination of the scene of the incident).

Taking into account the positions of D.A. Ilyushin and A.L. Osipenko[6], the provisions included in the doctrine of the fixation of evidence information, as well as the features of the functioning of the Internet network, identified the

[3] Michael Welnera, Kate Y. O'Malleya, James Gonidakisa, Alisha Saxenab,1, Jada Stewart-Willisa. The Depravity Standard III: Validating an evidence-based guide. Journal of Criminal Justice 55 (2018) 12–24.

4 Белкин Р.С.Курс криминалистики. –М., 1997. –Т. 2. (Belkin R.S. Forensics course. –M., 1997. –T.2). - С. 61.

[5] Meshcheryakova V.A. Computer crimes: The Basics of the Theory and Practice of Investigation. - Voronezh, 2002. - 102. Kolycheva A.N. Fixation of evidentiary information stored on the resources of the Internet network. Auto DICS. …. legal science. - M. 2019. - 10.

[6] Ilyushin D.A. Peculiarities of investigation of crimes committed in the sphere of provision of Internet services: Dis. ... the channel of law. sciences. - Moscow, 2008; Osipenko, A. L. Networking computer crime: Theory and

main objects of fixing evidence information placed on the resources of the Internet, which are recorded in a certain way, including:

a 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 technical-criminally component containing graphic (plans, schemes, drawings, graphics, drawings), subject (removal of objects in full or their parts, making of casts, layouts, prints) and visual-like (photography and video, screenshots) forms of fixation[7].

The analysis of the theoretical aspects of the fixation of evidence stored on the resources of the Internet made it possible to conclude that further recommendations on fixing the relevant information, which in the future can have evidentiary significance. One of the properties of electronic-digital traces is the possibility of their easy duplication without changing the original data source, as well as the possibility of creating an unlimited number of easily and quickly modified duplicates of information, and you can destroy a fairly large amount of information in a rather short time interval. It is believed that it is incorrect to divide electronic-digital traces into traces arising on electronic computers and traces found on the global Internet, since the Internet is, in fact, a system of communication networks and a set of technical means that unite various computer systems, and therefore it can be considered as a means of transmitting information. With ponoscopic and genomic traces, using technical means, the information located on a material medium is transformed in such a way that a person can perceive it visually, audial 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 (particulars of placement on the carrier), time (creation, modification, use, destruction), etc., as well as a number of other properties, such as objectivity, reliability, completeness, accuracy, relevance, utility, etc., traces can serve not only transformed objects, but also recorded information about the progress of their transformations, and often they will play an equally important role in the evidentiary process.

Without analyzing the information about the means of its modernization, the time, the subjects of reference to this file, it is impossible to get a full idea of the event and criminalally information. In turn, the mechanism of investigative education in information networks depends on a number of factors:

1. factors independent of the identity of the victim or the offender;
2. factors directly dependent on the identity of the victim or the offender.

Conclusion:-

Thus, unlike the criminally doctrine of follow-up education, where the main factor is the mechanical contact interaction of the following and the following objects having physical properties, when forming digital traces, due to the lack of the physical shape of the object, it is possible to fix only changes at the level of electromagnetic interactions of the digital signal, which can be revealed only by means of technical means, which transform the electronic-digital model of the object into a view accessible for human perception. In each case, it is necessary to identify the information environment, due to certain rules and algorithms, in which information was processed, where this information will be criminally information, and not a set of coded symbols that do not represent practical value, in order to identify traces.

The work on creation of mechanisms of investigation of evidence information in information networks through features of storage on the Internet resources, fixation of evidence information, reveal ways of fixing evidence in the materials of criminal case taking into account the capabilities of computer hardware and software, to classify electronic and digital traces of crime, To consider the peculiarities of carrying out separate investigative actions aimed at revealing and fixing of evidence stored on the Internet resources.

Traces by type are classified into:

1. system and application software files;

practice of struggle. Monograph. – Omsk: Omsk. Acad. Ministry of Internal Affairs of Russia, 2009. - 479; Osipenko A.L. Crime control in global computer networks: International experience. Monograph - Moscow: Norm, 2004. - 432.

[7] Litvin I.I. Modern technical means and problems of their application in proving at the pre-trial stages of criminal proceedings. Auto DICS. …. legal science. - E. 2018. - 31.

2. configuration files;
3. software and hardware log files;

files, sources of information generated during the user's activities, including their backups and deleted files to be restored;
1. files that provide authentication and confidentiality of users;
2. information stored in the ram or swap file;
3. information obtained through appropriate radio electronic or special equipment.

And by the location of electron-digital traces:
1. technical devices and channels of communication of the victim;
2. technical devices and channels of communication of criminals;
3. technical devices of communication operators.

And by the source of storage of electronic-digital traces:
1. traces on hard drives;
2. traces in the computer's RAM, peripherals and communications;
3. traces in wired, radio-fiber and other electromagnetic communication systems.

The classification of technical means on the basis of the purpose for the needs of criminal proceedings can be presented in the form of three groups of technical means:
1. technical means – physical evidence;
2. technical means of office equipment and telecommunications;
3. technical means used in the investigation and judicial proceedings for the formation, verification and investigation of evidence.

The need to appoint forensic computer examination during the proceedings in the court is substantially dependent on the procedural situation in which the matter is dealt with. The necessary cases are understood as the following:

conclusion of the examination is especially important as evidence in the case under investigation (for example, in the case of the discovery in the electronic notebook of a suspect in the murder of data with the address and telephone of the killed, the acquaintance with which the suspect categorically denies);

conclusion of the examination is not substantiated, contradicts other materials of the case, has other shortcomings, and doubts arise about its correctness (for example, as a result of inspection during the investigation and later, as a result of the examination, different computer information on the same data carriers is revealed);

In the preliminary investigation, two examinations were conducted to establish the same fact, and the experts reached the opposite conclusions; there were disagreements between the experts who were conducting the commission or the complex examination and each of them made its opinion;

Interested participants in the trial do not agree with the conclusions of the examination and have filed a request for the expert to be called to court (for example, files with evidence in the case prepared by a specialized package of programs were found on the accused's computer, while the accused claims that computer illiteracy and the possible accidental appearance of this data on the computer);

conclusion of the examination is based on the initial data taken from the testimony of the accused, the victim, the witness, and there are grounds to believe that they can be changed in the court hearing; new background data has appeared or there are reasons to believe that they will appear in court (for example, one of the participants of the process intends to present in court the carriers of computer information received in due time from the accused for storage), etc.

There may be other situations that are not so typical when an expert is required to be called in court to give an opinion. However, it is illegal to call an expert to court only to answer the question whether he confirms his conclusion given in the preliminary investigation, since the expert is summoned to court not to confirm the earlier conclusion, but to produce an examination and give an opinion on its results.

The examination in court is an independent procedural action. In the cognitive plan, it can be a continuation of the previous research of computer means[8]. In case of appointment of the examination, the presiding officer shall invite the parties to submit questions in writing to the expert. The questions raised should be read out and heard by the participants in the trial.

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

The written conclusion is announced by the expert in court and is attached to the case together with the court's decision on the appointment of an expert. On the request of the expert, his presence in the court may be limited to the time necessary for the study of evidence relevant to the subject. After the expert has given his or her opinion, and after hearing the opinions of the prosecutor, the defendant, the civil plaintiff, the civil defendant and their representatives, the court may free the expert from further presence in the court.

Interrogation of an expert in court, the court has the right to call for the interrogation of an expert who has given an opinion during the preliminary investigation, for clarification or addition of the given opinion. The Law of Criminal Procedure determines that after the conclusion of the expert is announced, he may be asked questions by the parties. At the same time, the first questions are asked by the party on whose initiative the examination was assigned. If an expert is required, the court may give him time to prepare answers to the questions of the court and the parties.

In some situations, the incomplete conclusion of an expert may serve as the basis for the appointment of additional examination, the production of which is entrusted to the same or another expert. If the court has doubts about the validity of the expert's conclusion, and also contradictions in the expert's conclusions, then a second examination may be appointed, the production of which is entrusted to another expert. In any case, all questions raised to the expert during the interrogation and his answers to them should be recorded in the minutes of the trial.

References:-

1. Belkin R.S. (1997): Forensics course. 2: 61.
2. Decree of the President of the Republic of Uzbekistan “On measures to improve forensic science activity”, ПП – 4125.
3. Decree of the President of the Republic of Uzbekistan “On the Strategy for the Further Development of the Republic of Uzbekistan” dated February 7, 2017, No.UP-4947 (Collection of Legislation of the Republic of Uzbekistan, 2017, No.6, Article 70)
4. Federal Criminal Code and Rules. (2014): West Group, St. Paul, Minn, 632-634. http://www.interpol.int. http://www.fraund.org
5. lyushin D.A. (2008): Features of the investigation of crimes committed in the provision of Internet services. Diss., Candidate of legal sciences, Moscow.
6. Kalinina E.V. (2016): Evaluation of the findings of computer forensics and their use in evidence of fraud. St. Petersburg, 18.
7. Kolycheva A.N. (2019): Fixation of evidence stored on Internet resources. Abstract. Disser., Candidate of Law, Moscow.
8. The Law of the Republic of Uzbekistan “On electronic digital signature” dated December 11, 2003 No. 562 – II.
9. The Law of the Republic of Uzbekistan “On Informatization” dated December 11, 2003 No. 560 – II.
10. The Law of the Republic of Uzbekistan “On Communications” dated January 13, 1992, dated No. 512-XII.
11. Litvin I.I. (2018): Modern technical means and problems of their application in proving at the pre-trial stages of criminal proceedings. Abstract. Diss. Candidate of Law, 31.
12. Mesheryakova V.A. (2002): Crimes in the field of computer information: the basics of the theory and practice of investigation. Voronezh, 102.
13. Osipenko A. L. (2009): Network computer crime: theory and practice of struggle. Monograph. Omsk. Academy of the Ministry of Internal Affairs of Russia, 479.

[8] Usov A.I. Forensic examination of computer tools and systems: Basic methodological support. - MOSCOW, 2003. - 15.

14. Osipenko A.L. (2004): The fight against crime in global computer networks: international experience. Monograph. Moscow: Norma, 432.
15. 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, 53-70.
16. Rasulev A.K. (2017): Some issues of improving criminal law and criminological measures to combat crimes in the field of information technology and security. Monograph. Tashkent State University of Law. Tashkent, 20.
17. Usov A.I. (2003): Forensic research of computer tools and systems: the basis of methodological support. Moscow, 15.