



Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/10249

DOI URL: <http://dx.doi.org/10.21474/IJAR01/10249>



RESEARCH ARTICLE

MODERN POSSIBILITIES OF COMPUTER TECHNICAL EXAMINATION IN THE INVESTIGATION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGIES

Mamatkulova Khosiyat

Lecturer Department of the Criminal procedure and Criminalistics Tashkent State University of Law 100047, 35, Sayilgox str., Tashkent, Uzbekistan.

Manuscript Info

Manuscript History

Received: 14 October 2019

Final Accepted: 16 November 2019

Published: December 2019

Key words:-

Forensic Examination, Expert's Report,
Forensic Computer-Technical
Examination, Subject And Tasks, Errors,
Knowledge And Skills

Abstract

With the rapid growth of computer and network systems in recent years, there has also been a corresponding increase in cyber-crime. Cyber-crime takes many forms and has garnered much attention in the media, making information security a more urgent and important priority. In order to fight cyber-crime, criminal evidence must be gathered from these computer-based systems. This is quite different from the collection of conventional criminal evidence and can confuse investigators attempting to deal with the forensics of cyber-crime, highlighting the importance of computer forensics. In this paper, we offer solutions to guard against cyber-crime through the implementation of software toolkits for computer-based systems. In this way, those who engage in criminal acts in cyber-space can be more easily apprehended. The article analyzes the concept and significance of forensic computer-technical expertise, as well as analyzes the mistakes made in the appointment, production of forensic computer-technical expertise and provides ways to prevent and eliminate them. According to the results of the analysis, proposals were developed for improving the norms of the criminal procedure legislation.

Copy Right, IJAR, 2019,. All rights reserved.

Introduction:-

In the age of development of information and communication technologies, mobile radio communications, computer tools and other technological objects and the electronic information contained in them can be used as an object or means of committing crimes. Therefore, taking into account the features of the functioning of such tools and their correct expert research is the key to obtaining the necessary and meeting the admissibility requirements of evidence. Given the specifics of these objects, the role and need for the production of examinations of electronic evidence is increasingly increasing.

Discussion:-

According to Article 3 of the Law of the Republic of Uzbekistan "On forensic examination" [6], forensic examination is a procedural action in civil, economic, criminal and administrative legal proceedings aimed at establishing the circumstances of a case and consisting in conducting forensic research and giving an opinion by a forensic expert based on specialized knowledge in science, technology, art or craft. In turn, the opinion of a forensic expert is a written document drawn up by a forensic expert or a commission of forensic experts and reflecting the

Corresponding Author:- Mamatkulova Khosiyat

Address:- Lecturer Department of the Criminal procedure and Criminalistics Tashkent State University of Law 100047, 35, Sayilgox str., Tashkent, Uzbekistan.

progress and results of forensic research. Thus, it can be concluded that forensic examination is a special procedural action carried out in the event that issues arise that require special knowledge in the field of science, technology, art or craft.

The concept of forensics, as a means of evidence, is present in all processes. Forensic examination is a separate and independent type of evidence, which has the same evidentiary power before the law as other evidence. The subject of the examination is information about expert tasks, expert methods, methods for resolving issues, as well as information about objects and their properties. The subject of research in the framework of the examination is the subject of knowledge. The subject of cognition refers to information about objects, goals and conditions of research, obtained in experience and used in practice. Turning directly to the subject of research, it should be noted that forensic computer-technical examination is a relatively new and one of the most demanded examinations. This type of expertise is sometimes called computer expertise, software expertise, programme-technical expertise and other options.

There are various definitions of scientists regarding this type of expertise. Propastin S.V. [8] notes that a forensic computer examination is an independent study of information recorded in electronic form, as well as hardware and software of a computer system, carried out by an expert (specialist) in the manner established by the criminal procedure legislation, in order to give an opinion on facts that have significance for the criminal case.

Smolina A.R. [12] under the computer-technical expertise suggests to understand an independent kind of forensic examinations, belonging to the class of engineering-technical examinations, carried out in order to identify and study the trace in the investigated crime, through a comprehensive study of computer tools: the technical (hardware) part of computer tools; software; network information technology facilities; information contained in a computer system.

It should be noted that the moment of formation of computer-technical expertise as an independent kind can be considered 2001-2002, when the book of Rossinskaya E.R. and Usova A.I. "Forensic computer-technical examination", as well as A.I. Usov defended his doctoral dissertation "Conceptual Foundations of Forensic Computer-Technical Expertise".

The subject of forensic computer-technical examination (FCTE) is the facts and circumstances established on the basis of a study of the laws of development and operation of computer tools that ensure the implementation of information processes, which are recorded in the materials of a criminal, civil case, administrative case [13].

In 2000, Rossinskaya E.R. and Usov A.I. in the work "Classification of computer-technical expertise and its tasks" introduced the classification of FCTE, based on the supporting components of a computer tool. In accordance with this, the following types of forensic examinations were distinguished: hardware-computer, software-computer and information-computer examinations. Another type of expertise was also introduced - computer-network expertise. The appearance of this type of expertise was based on the allocation of knowledge into a separate industry and the rapid development of network technologies. [9] Sharing the position of Rossinskaya E.R., Averyanova T.V. proposes to supplement the examination with several more types - engineering-psychological and examination of the functioning of computers in the network [1].

The essence of hardware-computer expertise is to conduct research (mainly diagnostic) of technical (hardware) means of a computer system. Hardware includes: electrical, electronic and mechanical circuits, blocks, devices and devices that make up the material part of a computer system. The subject of this type of examination is facts and circumstances that are relevant to a criminal or civil case and are established on the basis of a study of the laws governing the development and operation of the hardware of a computer system – material carriers of information about the fact or event of a criminal or civil case.

To conduct expert research of software, this type of expertise is designed as software-computer expertise. Its specific subject is the laws of development (creation) and application (use) of the software of a computer system submitted for research in order to establish the truth in a criminal or civil case. The objectives of this type of examination is to study the functional purpose and characteristics of the implemented algorithm, structural features and the current state of the system and application software of a computer system.

Information-computer examination (of data) is a key type of forensic computer-technical examination, as it allows to complete the integrated construction of the evidence base by final resolution of most diagnostic and identification

issues related to computer information. The tasks of this type are the search, detection, analysis and evaluation of information prepared by the user or generated (created) by programs for organizing information processes in a computer system.

In addition, there is also another new type of forensic computer-technical examination - computer-network examination. This examination, unlike the previous ones, is based primarily on the functional purpose of computer tools that implement any kind of network information technology. Therefore, the facts and circumstances associated with the use of network and telecommunication technologies and established by order of the investigating and judicial authorities in order to establish the truth in a criminal or civil case constitute a specific subject of computer-network examination. This examination is highlighted in a separate form due to the fact that only the use of special knowledge in the field of network technologies allows you to combine the obtained objects, information about them and effectively solve the assigned expert tasks.

It should be noted that the issue of the production of this type of examination was resolved with the adoption of a resolution of the President of the Republic of Uzbekistan dated January 17, 2019 "On measures to further improve forensic science activity" [5]. One of the important innovations introduced in accordance with these acts is the permission to create non-governmental forensic organizations with the right to conduct certain types of forensic examinations. So one of these types of examinations is forensic-computer-technical expertise. Also, in accordance with this resolution, a laboratory of computer-technical expertise was established at the Tashkent University of Information Technologies named after Muhammad al-Kharizmi.

Among the possibilities of forensic computer-technical expertise, it should be noted that with the increase of information and communication and computer technologies in people's activities, there is an increasing risk of violating the security of these technologies and, accordingly, of committing various crimes. So, the list of crimes in this area is fixed in a special Chapter 20 of the Criminal Code of the Republic of Uzbekistan "Crimes in the field of information technology".

Depending on what crime in the field of information technology is committed, appropriate actions for this category are required: inspection, seizure, obtaining samples, appointment of expertise, etc.

As it has been already noted, forensic computer-technical expertise is a fairly new kind of forensic expertise. It is important to note that the priority area of development is to ensure the production process aimed at solving specific practical problems of forensic information-computer examination. Their weakness remains the flaw on the part of law and the theoretical foundations of forensic examinations. In addition, of great importance is the fact that today technological progress in the field of information and computer technologies is developing most intensively, which, in turn, does not allow experts to create step-by-step recommendations for solving problems of other types of forensic computer-technical expertise. [10]

Semikalenova A.I., Khatuntsev N.A. define errors in the production of forensic computer-technical examination based on the stage of production of the examination (preparatory, direct stage of production and in drawing up a conclusion), in addition, they highlight errors of a methodological nature, etc. For example, one of the errors is the discrepancy between the competence of the specialist who conducted the examination of the specialization of computer-technical examination. To conduct a forensic computer-technical examination, a specialist must have knowledge in the field of: electronics and electrical engineering; computer networks and telecommunications facilities; Internet technology methods and means of information protection; basics of algorithmization and programming; databases and data banks; peripheral devices; circuitry of telecommunication devices; methods and means of expert research of computer facilities and mobile devices.

In accordance with these main specialties of higher professional education, the knowledge that future specialists receive is the basis for the training of experts in forensic computer-technical expertise. Due to this, it is necessary to develop an appropriate system of training, retraining of specialists for this group of expertise. The specifics of expert training should take into account the development of information technology, the emergence of new methods of committing and concealing crimes. [7]

Speaking about expert errors, one cannot ignore the problem of obtaining samples for a comparative study of mainly software products. Often, when appointing such an examination, the courts do not have samples for a comparative study and do not know where to get them. In this case, the parties may submit samples for a comparative study.

However, it remains unknown how legitimate these samples are, since the source of their origin, the form and completeness of the presentation are not always clear, and the question of the parties' interest in the outcome of the case remains. Given these circumstances, we propose to fix a special rule, in accordance with which to establish the mandatory participation of a specialist in obtaining samples for the production of forensic computer-technical expertise. So, it is proposed to supplement article 189 of the Code of Criminal Procedure of the Republic of Uzbekistan with the third part as follows: "When receiving electronic and other samples for computer-technical research, the participation of a specialist is mandatory".

In addition, the questions posed in the determination or decision and submitted for permission by the expert also require special attention. So, the persons who appoint the expertise and do not speak well of the special terminology used in information and computer technologies incorrectly use it when formulating questions. This is due to the fact that modern computerization of society has led to the widespread use of various specialized terms in the media without reference to their true purpose and definition, which ultimately leads to the creation of a false sense of competence among people who do not specialize in computer technology. This fact, in turn, leads to a distortion of their interpretation by experts in the field of forensic computer-technical examination, which leads to confusion. In order to prevent such errors, we suggest increasing the degree of interaction between the person who appointed the examination and the expert. For example, an expert can clarify the essence of the issue and, with the permission of the person who appointed the examination, reformulate the question, indicating this in the expert opinion.

Conclusion:-

Based on the aforementioned, we can conclude that this type of examination, such as forensic computer-technical examination, is relatively new and requires the settlement of many issues mentioned in this work. It is proposed to amend the procedure for training and retraining of specialists in this type of examination. It is also proposed to make abovementioned changes and additions to the criminal procedure legislation of the country.

References:-

1. Averyanova T.V. (1998): Tasks of computer-technical expertise. Informatization of law enforcement systems: Abstracts of international reports. conf. Part 2.
2. Casey E. (2002): Handbook of Computer Crime Investigation: Forensic Tools and Technology. Academic Press, 1–16.
3. Casey E. (2000): Digital evidence and computer crime: forensic science, Computers and the Internet. Academic Press, 41–46.
4. Crankhite C., McCullough J.(2001): Access Denied: The Complete Guide to Protecting Your Business Online, Osborne/McGraw-Hill.
5. Decree of the President of the Republic of Uzbekistan "On measures to further improve forensic science activity". (January 17, 2019): <http://lex.uz/>
6. The Law of the Republic of Uzbekistan "On Forensic Expertise" on June 1, 2010. <http://lex.uz/docs/1633100>
7. Polyakov V.V. (2010): Features of the training of specialists for the investigation of crimes related to unlawful remote access to computer information. Izvestia Alt. state un-that., 2/1 (66): 96-97.
8. Propastin S.V. (2015): The state and development trends of technologies as the basis for the formation of the theory of investigation of Internet crimes. Modern Law, 11: 130-135.
9. Rossinskaya E.R. Ed. Forensic examination in civil proceedings. Scientific and practical manual. <https://www.labirint.ru/books/634670/>
10. Semikalenova A.I., Khatuntsev N.A. Ed. Rossinskaya E.R. (2012): Forensics: common mistakes. "Prospect", Mistakes made in the production of forensic computer-technical examinations. 259.
11. Shinder D.L., Ed. Tittel. (2002): Scene of the Cybercrime: Computer Forensics Handbook. Syngress Media, 558–566.
12. Smolina A.R. (2017): Methodological and algorithmic support for the production of computer-technical expertise. Diss. for the degree of candidate of jurisprudence, Tomsk., 19.
13. Usov A.I. (2008): Forensic computer-technical examination: formation, development, methodological support. Theory and practice of forensic examination. 3 (11): 10-22.
14. Wang S.J., Yang C.H. (2005): Gathering digital evidence in response to information security incidents, IEEE International Conference on Intelligence and Security Informatics, Lecture Notes in Computer Science (LNCS), Atlanta, Georgia, USA.
15. Wang X., Yu H. (2005): How to Break MD5 and Other Hash Functions, Advances in Cryptology. Eurocrypt'05.