Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/10250
DOI URL: http://dx.doi.org/10.21474/IJAR01/10250

ISSN NO. 2320-5407

RESEARCH ARTICLE

FEATURES OF THE APPOINTMENT OF A FORENSIC COMPUTER - TECHNICAL EXAMINATION

Rakhimova Ulzana
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, Forensic Computer-Technical Examination, Comprehensive Examination, Additional Examination, Errors Arising During The Appointment Of An Examination

Abstract

Acquisition, decoding, and presentation of information from mobile devices are complex and challenging. Device memory is usually integrated into the device, making isolation prior to recovery difficult. In addition, manufacturers have adopted a variety of file systems and formats complicating decoding and presentation. A variety of tools and methods have been developed (both commercially and in the open-source community) to assist mobile forensics investigators. However, it is unclear to what extent these tools can present a complete view of the information held on a mobile device, or the extent the results produced by different tools are consistent. The article analyzes the features of the appointment of a forensic computer-technical examination, also addresses the issues of the appointment of a comprehensive and additional computer-technical examination. The errors arising at the appointment of the examination are considered.

Introduction:-

The world is actively growing indicators of terrorism, human trafficking, drug trafficking and crime in the field of information technology. According to reports, lately 13,759 people have died as a result of 1,787 acts of terrorism, 16,683 people have been injured [14], in 2021, due to an increase in the number of cyber crimes, US $ 6 trillion is planned to be fought against them [2], and 190,000 people die prematurely from exposure to drugs man [15]. In today's situation of combating such crimes due to the increased need, it is relevant to improve the institution of using special knowledge in criminal cases. A systematic analysis of the application of special knowledge in criminal matters requires expanding the application of the capabilities of new types of expertise, high technology (hi-tech), audits, and obtaining samples for expert research.

Discussion:-

In the world, there is a need to analyze the criminal procedural and criminalistic aspects of using special knowledge in criminal matters, using tactical methods to use the capabilities of experts and specialists, creating effective mechanisms to ensure the rights and freedoms of citizens in the process of examination, which requires deep scientific research.

Large-scale events are being held in our republic in order to guarantee the rights and freedoms of citizens, and to improve the process of detecting crimes. In particular, in accordance with the Strategy of Action for the five priority areas of development of the Republic of Uzbekistan in 2017–2021 [3], systematic measures are being taken to

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

prevent the use of evidence obtained in violation of procedural legislation and expert opinions; improvement of forensic activities based on international standards (implementation of the standard "ISO / IEC 17025"); developing an interdepartmental electronic system to track the timing and quality of forensic examinations [4]; strengthening the material and technical base of forensic examination; the introduction of new types of forensics; simplification of the procedure for carrying out procedural actions by electronic collection of evidence and expert examinations; the introduction of specific criteria and principles for the examination and audit in pre-trial and judicial proceedings; clarification of the procedural status of a specialist in pre-trial and judicial proceedings, giving his conclusion procedural significance [5]. This requires an inventory of legislation on the use of special knowledge in criminal matters, improvement of legal mechanisms for the use of special knowledge, the implementation of the provisions of international legal documents and the positive aspects of foreign legislation in the field of information technology in the national legislation of our country.

In accordance with the current legislation of the Republic of Uzbekistan, an expert examination is appointed if, when conducting judicial actions, it becomes necessary to resolve issues related to areas of special knowledge in science, technology, art or craft. In our case, this special knowledge may be contained, for example, in such branches of scientific knowledge as programming, system electronics, computer engineering, system engineering, etc.

The need for appointment is determined by the official of the body conducting the preliminary investigation, by the interrogating officer, investigator, court. At the same time, it is taken into account that the expert has the right to request, in addition to the objects presented, case materials related to the subject of the examination, and to submit a request for the provision of necessary additional materials to him. For the class of examinations under consideration, this is especially important, since the correct study of computer tools and systems requires a comprehensive study of the accompanying technical documentation, the use of certain auxiliary software and hardware that is used in a particular situation. Often there are cases when, when answering the questions posed, the expert requires an individually-defined hardware-software complex. This is typical for situations when the examination is carried out in cases involving the manufacture of counterfeit money (securities), with violations of copyright and related rights.

I would like to note that attracting experts to participate in the formulation of questions posed for expert research is today a necessary reality, due to both the rapid development of the field of information technology itself and the lack of established ideas about the possibilities of computer-technical expertise [10].

As expert practice shows, when assigning computer-technical expertise, there is currently a serious difficulty in determining the class and kind of appointed examinations. When conducting studies of court rulings on the appointment of the examination in question, it was found that there was great confusion on this issue. Unfortunately, it leads to the fact that the examination is appointed to state expert institutions that do not have specialists in the required field, or to experts who do not have the necessary qualifications. The need for the production of comprehensive examinations is not taken into account, questions are raised that are not related to the field of special knowledge of computer-technical expertise.

To date, the most developed of the new areas of SKTE in terms of methodological support can be considered an examination of cellular communications. It contains already developed methods for establishing the operability of hardware (RCFE named after Kh. Suleimanova under the Ministry of Justice of the Republic of Uzbekistan), as well as several instrumental techniques for researching information content: “XRY COMPLETE” (manufacturer - Swedish company Micro Systemation (MSAB)); “Mobile forensic scientist” (CJSC “Oxygen Software” (Russia)); “MOBILedit Forensic CONPELSON Labs” (CLUA); “Cellebrite’s UFED” (Cellebrite (USA)). In our opinion, it is in this direction that computer-technical expertise will develop in the near future. The remaining areas are under development.

According to the Code of Criminal Procedure of the Republic of Uzbekistan, experts are any natural person with special knowledge in the field of science, technology, art or craft, necessary to give an opinion. The questions posed to the expert and his conclusion should not go beyond the expert’s special knowledge.

The practice of disclosing and investigating crimes involving the use of computer tools shows that the interaction of the investigator with the expert in the appointment of the examination is most often carried out in the form of an appeal by the investigator for advice on the following issues:

1. determination of the kind (type) of examination;
2. expert selection;
3. formulation of questions to the expert;
4. preparation of materials for examination, including the selection of samples for comparative research;
5. resolving the issue of expediency of the appointment of additional, repeated, commission, comprehensive examinations [12].

If the expert is convinced that the questions raised cannot be resolved on the basis of his special knowledge or the objects of research presented to him or the materials are unsuitable or insufficient to give a conclusion and cannot be made up, or the state of science and forensic practice does not allow answering the questions raised, he draws up a motivated act on the impossibility of giving an opinion and sends it to the body (person) that appointed the examination.

The active introduction of modern information technologies in all spheres of human life more often objectively raises the question of the need for the appointment and production of complex computer-technical examinations and other types and types of forensic examinations. It is necessary to touch on the features of the appointment of a comprehensive and additional computer-technical examination. As you know, a comprehensive examination is a study conducted by specialists from different branches of knowledge to solve questions posed to an expert related to various kinds (types) of forensic examinations. Typically, the need for a comprehensive examination is caused by the inability to resolve the tasks of examination based on one branch of knowledge. When assigning a comprehensive examination, including forensic software and computer expertise, the question often arises about the production of one expert, equally well versed in several knowledge in the field of science and technology. Practice shows that today experts engaged in computer-technical expertise often own all its kinds. Therefore, this examination as a comprehensive examination today can be qualified to carry out one expert. In some cases, such an examination is the highest priority. An example of this is the examination of the hardware-software complex of a computer for the possibility of performing specific (defined) functions with its help [13].

An additional examination is appointed if there is insufficient clarity or incompleteness earlier than this conclusion, which may be the result of an expert narrowing the scope of the task, examining not all the properties and signs of the objects, and the incompleteness of some issues. An example of this is the situation when, when deciding on the presence of signs of counterfeit software product, experts examine only external features covering the description of the storage medium and file composition, and do not examine its functional characteristics, interface properties, and the technical documentation that came with it. Uncertainty can also be expressed in the fact that according to this conclusion it is impossible to judge specific facts, to establish whether the conclusions are positive or negative, categorical or probable. For example, when deciding whether the system software of a computer system was reinstalled, the expert answered: "The system software could be reinstalled in this computer system." An additional examination is also appointed in those cases when, after an expert study, new questions arise related to the study of the same object that were not previously raised by the expert. So, if after examining the software of the computer system that was attacked, it is established that at the time the incident was detected, the computer was not connected to the network, a second forensic software and computer examination is appointed. Its solution raises the question of finding possible undocumented software functions installed to activate and perform a given set of actions in a specific period of time. It is the last reason for the appointment of such expertise is most often found in practice. In court, an additional examination is appointed only after the expert gives a conclusion at the stage of the trial and if the ambiguity or incompleteness of the conclusion could not be eliminated by interrogating the expert. An additional examination is always an examination of the same kind, species and subspecies as the primary one. An additional one differs from a new examination in that the issues it resolves are related to previously resolved ones and the expert does not need to re-conduct a full study of the software - he can use some of the results previously conducted. Therefore, it is advisable, if possible, to commission the production of additional expertise to the same expert (s). If the newly appointed examination is in no way connected with the previous one, then it will not be additional, but a new, independent examination [13].

It should be noted that some of the errors that arise during the appointment of FKTE may not be related to a direct violation of the law, but rather because of the “stereotyped” actions of the investigator, which may negatively affect the effectiveness of the study. The most common mistake is incorrectly posed questions. Often, the investigator poses legal questions to the expert, for example, whether the software used to conduct gambling is present on the

provided computer. The expert is not obligated to answer such questions, since the resolution of legal issues, namely the determination of whether the characteristics of the studied software correspond to the characteristics corresponding to gambling, goes beyond the expert's competence and lies with the investigator, interrogator or court.

A person entitled to order a forensic examination may raise incorrect, incomplete, or with a large number of objects similar questions that are not necessary. Since no regulatory act establishes an expert's right to reformulate questions, the existence of such a situation can delay the process of conducting a study, understanding by an expert of a task, and also drawing up an expert opinion. So, A.I. Usov notes that currently the range of issues of FKTE as a new developing type of forensic examination is in constant development and is being specified. This is explained by the heterogeneity of the tasks of FKTE solved by the expert, the level of methodological and instrumental support for the study of FKTE objects and the wide and diverse classification of the objects of examination [9].

Conclusion:-

Existing crime trends in the field of information technology require an adequate response from the state. Moreover, the educational process must be built on the basis of modern mechanisms for the preparation of special knowledge and professional skills among law enforcement officials.

In addition, it is necessary to open the Department of Forensic-Computer-Technical Expertise at the Republican Center for Forensic Examination named after H. Suleymanova at the Ministry of Justice of the Republic of Uzbekistan.

References:-

1. Breeuwsma M., at el. (2007): Forensic data recovery from flashmemory. Small Scale Digital Device Forensics Journal, 1(1). www.ssddfj.org/papers/ssddfj_v1_1_breeuwsma_et_al.pdf.
2. 2.www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html.
3. 3. Decree of the President of the Republic of Uzbekistan. (February 7, 2017): No. UP-4947. "On an action strategy for the further development of the Republic of Uzbekistan". www.lex.uz.
4. 4. Decree of the President of the Republic of Uzbekistan. (January 22, 2018): No. UP-5308. "On the state program for implementing an action strategy in five priority areas for the development of the Republic of Uzbekistan in 2017-2021 in the Year of Support for Active Entrepreneurship, Innovative Ideas and Technologies". www.lex.uz.
5. 5. Decree of the President of the Republic of Uzbekistan. (May 14, 2018): No. PP-3723. "On measures to radically improve the system of criminal and criminal procedure legislation". www.lex.uz.
6. Emam K.E. and Koru A.G. (2008): A replicated survey of it software project failures. IEEE Software, 25(5):84-90.
7. 7. Jahankhani H. (2009): Criminal investigation and forensic tools for smartphones. International Journal of Electronic Security and Digital Forensics, 2(4): 387-406.
8. Kornblum J. (2006): Identifying almost identical files using context triggered piecewise hashing. Digital Investigation.
9. Pavlova A.A. (2005): Procedural and methodological foundations for the appointment of forensic computer-technical examination. MSTU named after N.E. Bauman. Polytechnic youth magazine, 5.
10. Polyakov V.V. (2014): Forensic computer-technical examination of mobile radio communications. J. News of the Altai district, S. 140-145.
11. Robinson B. (1996): Limited horizons, limited influence: information technology the London ambulance service: Proceedings of the international symposium on technology and society technical expertise and public decisions. IEEE Computer Society Press, p. 506-14.
12. https://studfiles.net/preview/6131517/page:2/
13. 13.https://stud.org/117912046811/legal/functions_of_forensic_computer_technical_examination
14. vawilon.ru/statistics-terrorism/# statistics-terrorism-in-the-world.
15. World Drug Report. (2017) www.unodc.org/wdr2017/field/WDR_Booklet1_Exsum_Russian.pdf.