E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

Current Issues in Digital Forensics

Sobirova Nasiba Avazovna

Namangan State Institute of Foreign Languages named after I. Ibrat

Abstract: This article discusses the main problems of digital forensics. At the same time, information is provided about the importance of social relations carried out using information technologies and telecommunications systems, the value of money and material flows involved in this area.

Keywords: information, telecommunications, technology, communication, program, microblock, perception, expert, problem, information.

Introduction

Human society is rapidly entering its digital stage of development. Traditional social relations are increasingly being carried out using new information technologies, and it is almost impossible not to use them.

Unfortunately, the modern legal regulation of this field lags behind the pace of technological development. Attempts to use existing legal mechanisms are ineffective and do not give the desired result.

At the same time, the importance of social relations carried out using information technologies and telecommunications systems, the value of money and material flows involved in this area, lead to their becoming objects of criminal aggression.

Crime information statistics confirm that crimes in the field of high technology (computer information), their detection rate is low, and the amount of damage caused to them is constantly growing. Based on these problems, the development of effective methods of detection and investigation of this category of crimes remains relevant.

The specific nature of this category of crimes, associated with the widespread use of the most advanced achievements of information technologies and telecommunications, further exacerbates this issue. First of all, the individuals who commit and organize such crimes are distinguished by their high level of education, non-standard creative approach, as well as deep theoretical knowledge and practical skills in using computer equipment and radio equipment. In the current environment, the fight against crime in the field of information and telecommunication technologies requires innovative approaches and significant changes. First of all, it is necessary to make changes in the current criminal procedural regulations for the detection and investigation of this category of crimes, to improve the forms of involvement of special knowledge, as well as to

sharply increase the level of special technical training of all participants in criminal prosecution. The current criminal-procedural legislation did not include not only information on the content of special knowledge necessary for detection and investigation of crimes in the field of information and telecommunication technologies, but also general definitions of the concept of special knowledge. At the same time, specialized literature provides a sufficient number of clear definitions of this category as a result of many years of scientific research by various scientists. Among the existing definitions, the most precise and concise one was provided by E.R. Rossinskaya, where she defines specialized knowledge as knowledge of a certain science or technology, art, acquired as a result of special training and professional experience necessary for resolving issues arising in the course of legal proceedings in criminal and civil cases, a system of theoretical knowledge and practical skills in the field of craftsmanship. In accordance with the field of information and telecommunications technologies, this definition should highlight a number of key features that an inquiry officer or investigator should take into account when deciding to independently perform certain procedural actions or when assessing the availability of the necessary specialized knowledge by an engaged specialist or expert. First, the field of special knowledge should be different from what is known and available in the field of informatics, and should be broader in general education and everyday experience of the common man. As has been repeatedly noted, the degree to which specialized knowledge differs from generally known knowledge is a very individual and highly subjective matter between people. Moreover, over time (according to the means of learning), specialized knowledge gradually becomes commonplace for the same person and does not cause any problems or difficulties. However, in our opinion, after the reform of local secondary education and the introduction of secondary (complete) education standards in informatics and information and communication technologies, as well as the Unified State Exam, a clear legal basis has emerged that allows us to assess the importance of this or that knowledge. A careful study of the above standard shows that an ordinary person with an average (complete) general education (meaning an investigator, investigator, lawyer, and judge) should not only have an idea of the basic concepts of computer science and information technologies, but also have the skills to apply them in practical everyday activities. As the text of the standard emphasizes, they "must have the ability to use automated information systems and communication activities in an information environment."

The content of specific examples from the 2012-2013 computer science exam shows that the level of preparation of a high school graduate should be sufficient to perform a set of very important actions that are encountered in the investigation of crimes in the field of information and telecommunications technologies. At the same time, it is noteworthy that almost no part of the standard (exam examples in the field of computer science and ICT) is practically related to operating systems, email clients, browsers, etc. However, in recent years, with the active development of digital forensics tools and technologies, the search and extraction of forensic data from digital media is being carried out using automatic or semi-automatic sets of specialized software and hardware tools. In this case, as a rule, no special skills or knowledge are required to enable / disable the standard operating mode of the device (program). Therefore, it is not necessary to involve a specialist or appoint an expert to perform such operations. The investigator can perform these actions independently. From a justice perspective, however, it is necessary to pay attention to several very important aspects: The existing device or program must be designed to solve forensic problems, that is, the developers of these devices and programs must have previously recorded the specific knowledge to be used in the hardware or software code. The ideal way to verify that a forensic tool has these features is to have it specifically certified before practical use. Unfortunately, there is currently no regulatory method for certifying digital forensic tools. The investigator must be familiar with these tools and understand the basics of using them. However, his actions should not go beyond the limits of simple standard operations. Secondly, theoretical knowledge about information technologies, computer hardware objects, and the

specific features of software systems must be accompanied by practical skills in working with specific technologies and software and hardware tools. Special scientific potential, even having a scientific degree and the title of a specialist in the field of information technology, does not guarantee that he is highly competent in the use of a certain information system. For example, a teacher or professor who teaches operating system theory and has a thorough understanding of all the features of their structure and operation may not know the details of implementing software on a particular operating system. Thus, even within a family of conceptually similar, POSIX-compliant operating system software, there are distinct variants (Linux, FreeBSD, Solaris, etc.) that have very different implementations of certain functions. Moreover, these differences can be a very important source of forensic information. Thus, "having special knowledge" in the field of information and telecommunication technologies means that the specialist has not only theoretical training, but also practical skills to work in a specific information system that appears in a specific criminal case. When selecting the necessary specialist (expert) to engage in certain procedural actions, the investigator or inquiry officer should not pay attention to the level of education and training. In addition, in some cases, the specifics of the training of an electrical engineer, radio engineer or electronics engineer are not clearly visible to him. A more difficult task for the investigator is to assess the practical skills of the specialist. A certain guiding value in this matter can be achieved by observing the experience (continuity) of using an information system and the chronicle of its actions in unusual situations.

Thirdly, a specialist (expert) involved in the investigation or other procedural actions in the investigation of crimes in the field of information or telecommunications technologies must have special training in the use of specialized hardware and software for the investigation of criminally significant data (digital forensics tools). When investigating crimes in the field of information and telecommunications technologies, everything that happens to the investigator is perceived through the prism of digital forensic tools: each of the special programs and technical tools is built on the basis of certain data (mathematical) models. The characteristics of these digital forensic tools are significantly different from the previous ones. For example, a magnifying glass used to study microblocks simply acts as an amplifier, without changing the characteristics of the object being studied or the information about the object. On the other hand, a program used for forensic examination of a digital image (for example, an image file) initially involves working with a certain data structure (image storage format - jpg, tiff, png, etc.). In addition, if the structure of the analyzed digital data corresponds to the idea of the used digital forensics tool, we will see the desired image on the monitor screen, and if it does not match, we will have a sequence of meaningless colored dots. Returning to the example of a magnifying glass in the analog version of forensic data perception, the work of a digital forensic tool can be described as follows. The light reflected from the object being examined passes through the magnifying glass and is divided into separate parts (spectrum). At the same time, they change places in a certain sequence. In addition, new elements are additionally introduced into them, obtained by adding / reducing (amplifying or suppressing) existing parts of the spectrum. Knowledge of the operation of digital forensic tools and the ability to use all their features is the most important condition for the qualitative solution of forensic tasks facing a specialist (expert). To summarize the above, we can offer the following option for determining the content of special knowledge used in digital forensics (in the investigation of crimes in the field of information and telecommunication technologies). Special knowledge in the field of digital forensics is a system of theoretical knowledge and practical skills in the field of computer science and information and telecommunication technologies, as well as criminal and civil cases on administrative offenses, is to know the criminalistic features of information systems and criminalistics technologies obtained as a result of special training and professional experience during the conduct of court cases. Unfortunately, from the perspective of information and telecommunications technologies, as in the classical definition of specialized

knowledge, it is no longer appropriate for us to talk about either craftsmanship or art. Because any activity that leads to perfection is art.

List of used literature:

1. Коджешау М.А. Подготовка будущего учителя информатики к pas- витию творческого мышления учащихся: дисс. … канд. пед. наук. – Май- коп, 2004. – 266 с.
2. Хуторской А.В. Дидактическая эвристика. Теория и технология кре-ативного обучения. – М.: Изд-во МГУ, 2003. – 416 с.
3. Sobirova N. A. Ta’lim jarayonini raqamlashtirishning metodologik asoslari. “Interpretation and researches”/ vol.1, 2023, p. 274-277
4. Собирова Н. А. (2024). Цифровизация учебного процесса. Educational Research in Universal Scienses, 3(4 SPECIAL), 58-62
5. Собирова Н. А. (2024). Опасности, которые таятся в интернете. Educational Research in Universal Scienses, 2(24).