Turabboev Xusanbek Abdusalamovich
O'zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi Huquqbuzarliklar profilaktikasi va kriminologiya kafedrasi dotsenti yuridik fanlar nomzodi, dotsent
E-manzil: turabbaevkhusanbek@gmail.com

KIBERJINOYATLARNI TERGOV QILISHDA MAXSUS BILIMLARDAN FOYDALANISH

Turabbaev Khusanbek Abdusalamovich
Associate Professor of the Department of Prevention of Offenses and criminology of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan Candidate of Legal Sciences, Associate Professor
E-mail: turabbaevkhusanbek@gmail.com

USE OF SPECIAL KNOWLEDGE IN INVESTIGATING CYBERCRIMES

Тураббаев Хусанбек Абдусаламович
Доцент кафедры Предупреждение правонарушений и криминология Академии МВД Дела Республики Узбекистан Кандидат юридических наук, доцент
Эл. почта: turabbaevkhusanbek@gmail.com

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Cybercrime in the modern world has been declared a global international problem, as evidenced by international agreements that provide for joint steps to combat this high-tech evil. [1] The danger of cybercrime both for the world community as a whole and for Uzbekistan is also recognized by state law enforcement agencies. The means of information and telecommunication technologies have become frequently used in the commission of crimes, which have received the designation as cybercrimes. The successful investigation of this type of crime is hindered by a number of important factors, among which, one of the most important is the lack of an effective mechanism for attracting specialists in the field of information technology for the successful disclosure of cybercrimes. These specialist-empowered experts could be of significant help in solving cybercrimes.

In the rapidly changing conditions of the modern high-tech world, computer technology, machine information carriers used on the Internet and in other social networks have become widely used. This made it possible to create a fundamentally new virtual projection of the real world, into which they began to be involved in almost all aspects of our life. And this, in turn, created unprecedented conditions for the exchange of information, the improvement of information and communication technologies (ICT) in the innovative virtual space. Along with the positive aspects of

using the created ICT, there are also negative consequences of this reality, namely, the emergence of opportunities for illegal penetration into the created information and telecommunication network for the purpose of criminal enrichment ("cybercrimes"). These crimes are understood as offenses committed through the use of high-tech computer technology.

In essence, cybercrime is a socially dangerous act in the virtual space, which can be described as cybercrime modeled with the help of computer technology and other information, telecommunication means. Cybercrime includes any crime that can be committed using information and communication technologies within a computer system or network. In essence, this crime committed in cyberspace is illegal interference in the operation of computers, computer programs, computer networks, unauthorized modification of computer data, as well as other illegal socially dangerous actions committed with the help or through ICT, computer networks and programs.

The solution of one or another expert problem in the conduct of forensic examinations in full is associated with the investigation of cybercrimes, from the process of collecting evidence and ending with their research. Forensic expertise is the main form of cybercrime expertise. Depending on the circumstances of the case, the following types of computer-technical expertise can be assigned: hardware-computer; software and computer; information and computer; computer network expertise. So, for example, the quality and value of examinations in the field of information and communication technologies fully depend on the quality and professionalism of the work of a specialist in this area at the scene of an incident, aimed at finding and removing evidentiary information. As a rule, the evidence base for a specific crime depends on the quality of the detected and recorded traces seized from the scene.

A small percentage of identification examinations in conducting examinations in the field of information and communication technologies and a significant number of examinations of a classification and diagnostic nature in most cases are explained by the absence of the suspect at the beginning of the investigation. The problem is urgent, has scientific and practical interest, since today modern computer technologies affect almost all areas of human life.

In recent years, information, becoming one of the determining factors in the development of modern society, is being actively introduced into all social spheres and is gaining more and more importance.

It is natural that with the expansion of the sphere of using information technologies, the number of examinations in the field of information and communication technologies also increases. However, at the same time, the domestic practice of investigating such crimes is still small. At the stage of initiation of a criminal case, the examination appointed in the field of information and communication technologies can serve as the basis for making decisions on initiating a criminal case and the basis for the emergence of criminal procedural relations in general. Information and communication technologies and their carriers can be considered as information and sources, respectively, in the structure of

criminal procedural evidence, but only in such forms as material evidence and other documents.

Investigation of crimes in the field of computer technology differs significantly from the investigation of other "traditional" crimes.

Since there is a significant intensity of hacker attacks on critical infrastructure of the Republic and according to the data of criminal cases, mistakes are most often made, often explained by the lack of an appropriate level of theoretical and practical training of specialists whom the investigator attracts as experts. In addition, the investigators themselves, having only humanitarian education (lawyers), are poorly versed in the field of information technology and find it difficult to investigate cybercrimes.

The study of criminal cases in this category gives reason to believe that one of the significant reasons for the low quality of the investigation is the lack of involvement of relevant ICT specialists, the lack of systematic and approved methods for investigating computer crimes, as well as mistakes made during investigative actions in relation to information technologies. Having special knowledge in the field of computer technology, specialists (experts) are able to contribute to the activities of the investigator to establish the truth in the investigation of cybercrimes. Moreover, special knowledge can be used not only in the investigation of crimes in the field of computer technology, tk. when committing "traditional" crimes, ICT can be used to design and manufacture falsified documents, banknotes, to create and store a database containing information about the crime and for other purposes. Under these circumstances, an investigator cannot effectively work alone, relying only on his own knowledge and skills of a personal computer user. Even the knowledge of the involved expert or specialist may not be enough, because, depending on the circumstances of the case, knowledge in various areas of computer technology may be required. Despite the fact that the duty to search and consolidate evidence lies with the investigator, the effectiveness of such investigative actions as inspection of the scene (crime scene), search, seizure, etc., in the investigation of crimes related to the use of computer technology, becomes increasingly dependent on organization of interaction between the investigator and the specialists involved in carrying out these activities.

This circumstance entails the need for the active development and application of general organizational and tactical methods of using the assistance of persons with special knowledge in the investigation of cybercrimes, conducting research of these objects, as well as organizing the interaction of the investigator and specialists in the field of nanotechnologies in the investigation of cybercrimes, etc. [2, P. 32]

In the literature devoted to the investigation of cybercrimes, various authors have formed a forensic characteristic of illegal access to computer information, a classification of traces of illegal access to computer information, a classification of the methods of committing this crime, data on the methods of concealing it, tools and means of committing it, developed a methodology for research and search of funds computer technology [3. P. 290].

Due to the novelty of the methodology for investigating cybercrimes, studies of the peculiarities of using special knowledge in the field of computer information are

fragmentary, fragmented and most often come down to separate, private recommendations. Almost all works devoted to the investigation of crimes in the field of computer information indicate the advisability of attracting specialists, to one degree or another, but the content of their assistance is not disclosed. Also, the organization and tactics of using ICT experts, if analyzed, were rarely, fragmentary.

In this regard, it is relevant to study the problems of attracting experts in the field of computer technology, establishing interaction between them and the authorities carrying out the investigation. In 2018, A.K. Rasulev [4. P. 74], and I.R. Astanov [5. P. 75]. But if the first touched only on criminal law and criminological, then the second investigated the use of special knowledge in the investigation of crimes. 2020 A.U. Anorboev, considered the criminal legal aspects of cybercrimes [6, p.54]

Thus, at present, all over the world and Uzbekistan, including the appointment and production of expertise in the field of information technology, special attention is paid to the investigation of cybercrimes. However, the mechanism for attracting the necessary specialists and experts in this field to carry out the necessary examinations is not at a sufficient level and requires its own decision. It is necessary to conduct scientific research on the forensic aspects of attracting experts in the field of information technology and to develop an effective methodology and tactics for interaction of experts and specialists with the investigation, inquiry and pre-investigation authorities. An effective cybercrime investigation mechanism should be developed.

References:

1. "Convention on Cybercrime" (ETS N 185) [Russian, English] (concluded in Budapest on November 23, 2001) as amended on January 28, 2003 // http://www.coe.int/ru / web / conventions / full-list // conventions / treaty / 185 (date accessed: 15.10.2014); "Okinawa Charter of the Global Information Society" (adopted on Okinawa Island 22.07.2000) // Diplomatic Bulletin. 2000. No. 8. – PP. 51–56; Bangkok Declaration "Partnership for the Future" (adopted in Bangkok on October 21, 2003) // Diplomatic Bulletin and others.

2. Poleshchuk D.G. Criminal legal protection of information security (on the example of certain aspects of cybersecurity protection and protection of information of limited distribution): Author's abstract ... dis. Cand. jurid. sciences. – Minsk, 2020. – 32 – P. 3. Anorboev A.U. Cyberzhinoyatlarning zhinoy-ҳuқuқy zhiҳatlari: Legal. fan. bўyicha false. doc. (PhD). dis. – T., 2020. – P. 290.

3. Rasulev A.K. Improvement of criminal law and criminological measures to combat crimes in the field of information technology and security: Author's abstract. dis. ... Dr. jurid. Sciences (DSc). – T., 2018. – P. 74.

4. Astanov IR Procedural and criminalistic aspects of the use of special knowledge in criminal cases: Author. dis. ... Dr. jurid. Sciences (DSc). – T., 2018. – P. 75.

5. Anorboev A.U. Criminal and legal aspects of cybercrimes: Author's abstract. dis. … Doctor of Philosophy (PhD). – T., 2020. – P. 54.