EXPERT PREVENTION OF INFORMATION TECHNOLOGY CRIMES

Gadjiyev Xagani Mokhubbat ogly
Law Enforcement Academy of the Republic of Uzbekistan
Head of the Specialized Center for Digital Research
xagani89@gmail.com
https://doi.org/10.5281/zenodo.13968779

ABSTRACT: This article examines the forms of participation of specialists and experts with specialized knowledge in the field of information technology in preventive activities. It focuses on expert measures aimed at identifying circumstances that contribute to the commission of crimes in the field of information technology, during the process of computer forensics of digital media and other activities.

KEYWORDS: preventive activities, specialized knowledge, forensically significant computer information, information technology, information security.

INTRODUCTION: The New Uzbekistan is a state whose main goal is to ensure a free, prosperous, and comfortable life for our multinational people. It is a state developing in strict accordance with universally recognized norms in the field of democracy, human rights, and freedoms, relying on the principles of friendship and cooperation with the international community [1].

Modern crime poses a threat to national security, exerting a destabilizing effect on all spheres of life of the state, society, and individuals [2].

The widespread development of information technologies and their active use in people's daily lives has provoked a rapid increase in the number of both traditional crimes and cybercrimes.

According to statistical data provided by the Ministry of Internal Affairs of the Republic of Uzbekistan, over a three-year period from 2021 to 2023, more than 17,500 crimes committed using information technologies were recorded and investigated. Analysis of the crime structure in the country revealed the following percentage ratio for the main types of crimes: the predominant type of illegal acts is theft (69.18% of the total number of registered cases), followed by fraudulent actions (27.81%), embezzlement through misappropriation or embezzlement (2.76%), illegal (unauthorized) access to the telecommunications network (0.37%), and unauthorized modification of computer information (0.10%).

These data indicate that more than 90% of registered crimes using information technologies were committed against property, with the vast majority being fraud and theft.

The increase in the number of registered crimes committed using information technologies indicates the need to organize preventive measures to counter the crimes under consideration.

This trend is observed on a global scale, affecting law enforcement systems in almost all countries of the world. Law enforcement agencies face a complex problem characterized not only by a sharp increase in the number of cybercrimes but also by a low level of their detection and insufficient effectiveness of investigation methods. This situation creates a

favorable environment for the further growth of cybercrime and requires the development of countermeasures.

According to expert estimates presented in the Global Digital Reports, the damage from cybercrime by the end of 2023 reached an unprecedented level of 8.5 trillion US dollars. Forecasts for 2024 indicate a further aggravation of the situation: an increase in the number of cases of extortion using the Internet is expected by 30-50%. At the same time, small and medium-sized businesses, as well as government structures, remain the most vulnerable to such illegal actions. Of particular concern is the fact that the regions of Central Asia, Oceania, and Africa are at the greatest risk of unauthorized interference in the operation of information systems, which may be due to the insufficient development of cybersecurity infrastructure in these regions [3].

In the Republic of Uzbekistan, programmatic measures are being implemented to ensure legal information security, prevent and combat offenses and crimes in the field of information technology. Issues of "improving criminal legislation, improving the system of ensuring information security and information protection" are envisaged [4].

If just a few years ago, the main efforts of law enforcement agencies were aimed at creating text databases on organized and street crime, now the situation has fundamentally changed. Already now, no less than 70% of data repositories on crime are occupied by video and photo files [5]. And this is absolutely true, as the analysis of expert practice shows that when appointing a decree for the production of computer technical expertise and examination of mobile devices, initiators are largely interested in information about previously deleted files, mainly video and photo files confirming the fact of the crime.

The participation of experts specializing in the field of digital forensics in preventive activities is not directly provided for by law. Nevertheless, experts with specialized knowledge in the field of information technology have opportunities to identify and disclose crimes in cyberspace through expert measures aimed at identifying circumstances that contributed to the commission of the crime.

Thus, Article 68 of the Criminal Procedure Code of the Republic of Uzbekistan states that if during the production of a forensic examination, an expert establishes circumstances that are relevant to the criminal case but about which no questions were posed to him, he has the right to indicate them in his conclusion. Such circumstances can undoubtedly include conditions that contributed to the commission of crimes in the field of information technology.

For example, when conducting a computer technical examination, digital traces that are important for identifying the circumstances of cybercrimes can be classified into the following groups:

- when registering accounts and accessing Internet resources;

- traces of Internet access through the use of a mobile device (subscriber number, IP address of Internet access, IMEI number of the device, cells, digital evidence in the device memory). SIM cards used in the phone;

- computer for access (Internet via Wi-Fi or traffic distribution through a mobile phone; traces are stored in the device memory);

- communication with the victim (online communication - phone call, IP telephony, messengers, offline - personal communication);

Based on the results of the analysis and generalization of the above-mentioned digital traces, the expert forms a conclusion with findings that can subsequently be used to identify circumstances contributing to the commission of crimes in the field of information technology.

It should be kept in mind that the expert only establishes facts related to causes and conditions; questions and the expert's conclusion cannot go beyond the expert's competence in the field of modern information technologies. The expert's conclusion should not contain an assessment of the legal content of the identified facts; their recognition as the cause of the crime is a legal issue and falls within the competence of the investigator.

In the process of implementing measures to organize preventive measures to counter crimes in the field of information technology, A.I. Usov put forward proposals for using the following methods: [6]

- Participation of employees of the forensic institution as specialists in the production of investigative actions in cases involving the use of computer tools and systems;
- Identifying circumstances that contributed to the commission of a computer crime;
- Reference and consulting activities of forensic institution employees on issues of special knowledge in the field of modern information technologies;
- Conducting theoretical and experimental research in the field of modern information technologies on problems of detecting and solving crimes in cyberspace involving the use of computer tools and systems;
- Participation of experts in operational-search activities and preventive measures conducted by law enforcement agencies (prosecutor's office, courts, internal affairs units, etc.), state bodies, public and other organizations;
- Conducting classes with officials of relevant ministries and departments to teach methods of identifying forensically significant computer information, solving other tasks of digital expertise (for example, establishing signs of unauthorized access to computer information, signs of using malicious programs, etc.).

In our opinion, it is also necessary to provide for the participation of experts in the field of digital forensics in legal propaganda (speeches to the public directly or using mass media with a demonstration of the possibilities of science and technology in the detection and prevention of crimes in cyberspace;

- Create a special laboratory at the Center for Information Security and Assistance in Ensuring Public Order for conducting testing and research work, as well as testing protection means in the field of information security. This laboratory will perform the functions of a kind of "testing ground" for testing the latest means of protection against computer viruses, malicious programs, hacks, etc. [7].
- Conducting comprehensive scientific research in the direction of expert prevention of crimes within the framework of implementing a unified state policy in the field of combating crimes in the sphere of information technology, which will result in the preparation of collections of scientific articles, monographs, specialized methodologies;

In conclusion, it should be noted that countering crimes in the field of information technology and security requires the state to conduct an effective and thoughtful policy, which indicates the need to systematize and concretize the foundations of state policy in the field of information security. Solving these issues will improve the quality of training for managers

and specialists, experts, and other employees of competent authorities, focusing their attention on practical activities to prevent offenses and crimes.

CONCLUSION: In conclusion, we note that the article analyzes the key aspects of expert prevention of crimes in the field of information technology, including forms of specialist participation, methods for identifying digital traces and circumstances contributing to the commission of crimes, and directions for scientific research. The implementation of the proposed recommendations will contribute to increasing the effectiveness of work on preventing cybercrime in the Republic of Uzbekistan. Prospects for further research on this issue are associated with an in-depth study of the possibilities of using big data technologies and machine learning to identify indicators of crime preparation, the development of specialized methodological support for expert preventive activities, and analysis of best international practices.

References:

1. Интервью Президента Республики Узбекистан Шавката Мирзиёева главному редактору газеты “Янги Ўзбекистон” Салиму Дониёрову [Электронныйресурс]. – Режим доступа: https://president.uz/ru/lists/view/4547. – Дата доступа: 28.06.2024 г.
2. Бабаева Э. У., Волохова О. В., Егоров Н. Н., Жижина М. В., Исютин-Федотков Д. В., Ищенко Е. П., Комиссарова Я. В., Корма В. Д., Кручинина Н. В., Милованова М. М., Паршиков В. И., Уваров В. Н., Харина Э. Н. Криминалистика: учебник для бакалавров и специалистов /отв. ред. д.ю.н., проф. Е. П. Ищенко. – Москва: 2020. – С. 353
3. Digital 2023: Global Overview Report [Электронный ресурс] – Режим доступа: https://datareportal.com/reports/digital-2023-global-overview-report– Дата доступа: 28.06.2024 г.
4. Расулев А. Преступления в сфере информационных технологий и информационной безопасности. профилактика и противодействие //Fuqarolik jamiyati. Гражданское общество. – 2019. – Т. 16. – №. 1. – С. 82-85.
5. Попова К. Профилактика правонарушений в условиях цифровизации мира //Противодействие правонарушениям в сфере цифровых технологий и вопросы организационно-правового обеспечения информационной безопасности. – 2022. – Т. 1. – №. 01. – С. 454-460.
6. Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: автореферат д-ра юрид. Наук (DSc). – М., 2002. – С.325.
7. Расулев А. Противодействие преступления в сфере информационных технологий и безопасности в Республике Узбекистанна современном этапе //in Library. – 2021. – Т. 21. – №. 1. – С. 46-53.