JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 4 Issue: 8 | Aug–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Requirements for a Specialist in the Investigation of Cybercrimes

B. Kh. Khamidov
Deputy Head of the Department of Criminalistics and Forensic Expertise,
Tashkent State University of Law, PhD

Annotation: The rapid expansion of digital technologies has not only created opportunities for societal development but also increased the risk of cybercrimes. Their investigation requires a high level of technical and legal expertise. This article analyzes the requirements for specialists involved in the investigation of cybercrimes, focusing on national legislation, international standards (ISO/IEC 27037:2012), and comparative practices. It is argued that only competent and retrained professionals in digital forensics can ensure effective investigative processes and reliable evidence handling.

Key words: cybercrime, investigation, digital forensics, specialist, evidence, ISO/IEC 27037:2012.

Introduction

The digitization of social life in Uzbekistan has been accelerated through state reforms in information and communication technologies. While this transformation increases efficiency, it also contributes to the rise of cybercrimes, which are highly complex offenses committed through the use of the internet, computers, and digital devices. Their detection, investigation, and prevention require interdisciplinary expertise and specialized training. Consequently, the role of the specialist in investigative procedures has become critically important.

The development of digital technologies, in turn, leads to the expansion and complication of relations in the digital environment. Today, as a result of reforms implemented in the country in this field, all spheres of social life are being digitized, and these processes are also creating various problems in the sphere of law enforcement. In particular, the improvement of legislation and law enforcement practices related to the investigation of cybercrimes has become increasingly urgent today.

It should be noted that in recent years, in order to regulate the practice of investigating cybercrimes, a number of legislative acts have been adopted by our government, in particular:

Presidential Decree of the Republic of Uzbekistan No. PQ–357 of August 22, 2022, “On measures to bring the information and communication technology sector to a new stage in 2022–2023”;

Presidential Decree of June 21, 2024, No. PQ–229, “On measures to organize scientific research activities in the field of digital forensics”;

Presidential Decree of January 22, 2025, No. PQ–17, “On measures to introduce a system of training professional personnel in the field of combating crimes committed using digital technologies”;

Presidential Decree of April 30, 2025, No. PQ–153, “On measures to further strengthen the fight against crimes committed with the help of information technologies”;

Presidential Decree of April 30, 2025, No. PQ–155, “On comprehensive measures for the digital transformation of the internal affairs system.”

Main body

The adoption of these resolutions has been one of the important steps in regulating this sphere.

Volume: 4 Issue: 8 | Aug–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

At present, digital technologies have deeply penetrated almost all aspects of our lives. On the one hand, this increases convenience and efficiency, but on the other hand, it brings new types of threats, particularly cybercrimes. Cybercrimes are offenses committed through the use of the internet, computers, and digital tools, and their detection, investigation, and prevention are highly complex and require a high level of expertise. Therefore, great responsibility and specific requirements are imposed on specialists involved in this field.

First of all, a specialist must have deep knowledge of the nature, mechanisms, and modern technical means of cybercrime. He or she should have sufficient expertise in computer networks, operating systems, cryptography, internet protocols, and database structures. In today's digital environment, a specialist must not only possess theoretical knowledge but also be able to prove his or her skills in practice.

In foreign countries, specialists (including from the private sector) are also authorized to conduct investigations. A specialist may perform the following tasks:

provide initial information on the condition of a digital device and information security;

provide preliminary and subsequent information about the system and network architecture (configuration);

give methodological recommendations on choosing tactics for investigative actions;

take measures to neutralize means of deleting or destroying digital data, as well as cyberattacks;

identify data stored in cloud services;

assist in identifying and documenting in protocols digital evidence (traces) relevant to the case;

identify digital evidence (traces) and their sources, and make copies of them;

provide practical assistance in documenting the sequence of actions carried out on a digital device;

analyze and study evidence relevant to the case;

give scientifically grounded conclusions based on research results;

provide clarifications on his or her conclusions during investigation and trial.

At the same time, involving a specialist during the interrogation of a suspect or accused person also helps to quickly and fully solve the crime, as well as to identify the method and mechanism of its commission.

It should be emphasized that collecting, verifying, and evaluating traces in the digital environment requires knowledge, skills, and competencies in a narrow field of expertise. Therefore, ensuring the participation of a specialist in the investigative process is of fundamental importance. Article 204¹ of the current Criminal Procedural Code of the Republic of Uzbekistan also stipulates that electronic data submitted must be received in the presence of a specialist by an official of the pre-investigation body, an inquirer, an investigator, a prosecutor, or a court.

However, a reasonable question arises: what kind of specialist should be involved in the investigative process? Since the field has a technical character, directly involving any specialist may lead to methodological errors. The investigator must take into account the specialist's professional competence and experience in resolving this issue.

In this regard, researchers D.I. Chukova, D.A. Medvedev, and M.V. Litvinenko suggested the following:

Volume: 4 Issue: 8 | Aug–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

a) a specialist should have skills in detecting and investigating crimes and other offenses committed using computer technologies;

b) a specialist should be able to use modern software, tools, programming languages, and systems to solve professional tasks;

c) a specialist should have skills in collecting, analyzing, and evaluating relevant information in order to apply legal norms in the field of computer information.

According to the international standard ISO/IEC 27037:2012, a specialist must have appropriate technical and legal qualifications. Under this standard, a specialist should have sufficient preparation in processing digital evidence to perform investigative tasks and demonstrate his or her skills and competence in processing information presented in digital form (identification, collection, acquisition, storage, preservation, destruction, etc.) in relevant fields. In other words, he or she should understand and be able to apply appropriate processes and methods for handling evidence from digital sources.

Conclusion

The competence criterion also provides a specialist with the ability to effectively use digital forensic tools. Conversely, even the best digital forensic tools cannot guarantee the quality of digital information (evidence) obtained if the specialist lacks competence.

In general, taking into account the above and based on the nature of the criminal case, it is advisable to involve as specialists those who have undergone retraining in the field of digital forensics, hold higher education, have previously participated as specialists in similar cases, have experience, and are familiar with current legislation.

References

1. Presidential Decree of the Republic of Uzbekistan No. PQ–357 (August 22, 2022). *On measures to bring the information and communication technology sector to a new stage in 2022–2023*. Tashkent.
2. Presidential Decree of the Republic of Uzbekistan No. PQ–229 (June 21, 2024). *On measures to organize scientific research activities in the field of digital forensics*. Tashkent.
3. Presidential Decree of the Republic of Uzbekistan No. PQ–17 (January 22, 2025). *On measures to introduce a system of professional training in the field of combating crimes committed using digital technologies*. Tashkent.
4. Presidential Decree of the Republic of Uzbekistan No. PQ–153 (April 30, 2025). *On measures to further strengthen the fight against crimes committed with the help of information technologies*. Tashkent.
5. Presidential Decree of the Republic of Uzbekistan No. PQ–155 (April 30, 2025). *On comprehensive measures for the digital transformation of the internal affairs system*. Tashkent.
6. Criminal Procedural Code of the Republic of Uzbekistan (as amended). Article 204¹.
7. ISO/IEC 27037:2012. *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. International Organization for Standardization (ISO), Geneva.
8. Chukova, D.I., Medvedev, D.A., & Litvinenko, M.V. (2019). *Problems of involving specialists in the investigation of computer crimes*. Moscow: Moscow State Law University Press.
9. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press, Elsevier.
10. Baryamureeba, V., & Tushabe, F. (2004). *The Enhanced Digital Investigation Process Model*. Proceedings of the Digital Forensics Research Workshop (DFRWS).