SOME ISSUES CONCERNING THE SUSPENSION OF INVESTIGATION IN CRIMINAL CASES RELATED TO THEFT OFFENSES

Ashirboyev Akhrorjon Tirkash ugli
Internal affairs of the Republic of Uzbekistan
Academy of the Ministry of Investigation
the head of the cabinet of the department,
E-mail: ashirboyevaxrorjon@gmail.com

https://doi.org/10.5281/zenodo.14759996

Abstract: This article analyzes the institution of suspending inquiry and preliminary investigation in criminal cases, particularly focusing on cybertheft crimes as an example. It examines the legal grounds, conditions, and procedures for suspending investigations, as well as modern types of cybertheft crimes. The study highlights legal-normative, organizational-technical, forensic, operational-search, and preventive factors that contribute to these crimes remaining unsolved and investigations being suspended. Furthermore, the article proposes comprehensive recommendations to enhance the effectiveness of combating cybercrime, such as improving human resource capacity, strengthening technical capabilities, developing international cooperation, refining legislation, and reinforcing preventive measures.

Keywords: suspension of investigation, cyber theft, cybercrime, phishing, electronic evidence, cybersecurity, international cooperation.

During the preliminary investigation of criminal cases, the investigator and inquiry officer may be compelled to suspend the investigation for various reasons. In such instances, strict adherence to the legal grounds, procedures, and conditions for suspending the investigation is required.

According to criminal procedure legislation, there are several grounds for suspending inquiry and preliminary investigation. These include circumstances such as when the person who should be involved in the case as an accused has not been identified, the whereabouts of the accused are unknown, the accused has left the territory of the Republic of Uzbekistan and it is impossible to ensure their appearance for investigation, or the accused has a serious and prolonged but curable illness that precludes their participation in the proceedings of the case[1].

According to the first clause of part 1 of Article 364 of the Criminal Procedure Code, cases where the person who should be involved as an accused has not been identified constitute the majority of grounds for suspending an investigation. This situation indicates that there are serious deficiencies in the mechanisms for identifying individuals who have committed crimes.

According to the statistical data examined during our research, theft crimes constituted 28.8% of all crimes committed in 2024, and for 22.5% of crimes in this category, the inquiry and preliminary investigation procedures were suspended[2].

One of the main factors contributing to the failure to solve this type of crime and the suspension of investigations is theft committed through information technology (cybertheft), which is very widespread today. Let’s examine the main types:

Phishing (from the English word “fishing”) is a type of Internet theft aimed at gaining access to users’ confidential information - logins and passwords. This is achieved by sending mass emails impersonating popular brands, as well as direct messages within various services, such as on behalf of banks or within social networks. The message often contains a direct link to a website that appears indistinguishable from the genuine one, or a redirected website. Once a user accesses the fake page, the thieves employ various psychological techniques to persuade the user to enter their username and password into the counterfeit page, which they use to access a specific site. This allows the thieves to gain access to accounts and bank accounts[3].

Bank card information theft involves copying card data by installing special devices on ATMs or terminals.

Theft through malicious software:

Trojan programs secretly infiltrate computers and steal data. In the field of computer technology, the term “Trojan horse” is used as a general description for any malicious program that misleads users about its true intention while installing itself on their computers. This term is derived from the ancient Greek story of the famous Trojan horse that led to the destruction of the city of Troy[4].

Keyloggers record all keys pressed on a keyboard. What is a keylogger? It’s a malicious tool that carefully examines captured files in hopes of finding passwords or other valuable information[5].

The following scholars’ opinions can be cited regarding the main factors leading to unsolved cybertheft crimes and suspended investigations:

Professor A.V. Fedorov emphasizes: “One of the main problems in investigating cybercrimes is the high level of technological knowledge possessed by criminals and their use of modern methods to conceal their tracks. They often utilize cryptocurrencies, VPN services, and other anonymizers, which makes identifying them more challenging”[6].

In his research, I.S. Ivanov points out that one of the primary difficulties in investigating cybertheft crimes is the insufficient knowledge and skills of law enforcement officers in the IT field. Effective investigation of such crimes requires specialized technical knowledge and skills[7].

S.M. Petrov notes, “The lack of adequate international cooperation in investigating cybercrimes is a significant problem. Criminals often commit offenses against victims in one country while operating from another. In such cases, it is necessary to improve mechanisms for interstate cooperation to conduct investigative actions”[8].

In our opinion, based on the views of the aforementioned scholars and the cited statistical data, we deem it necessary to summarize the main factors leading to unsolved cybertheft crimes and suspended investigations as follows.

Firstly, there are legal and regulatory factors such as the absence of a special procedural framework for investigating cybertheft crimes, inadequately developed mechanisms for international cooperation, and the lack of clearly defined procedures for collecting and preserving electronic evidence.

The following scholars’ opinions can be cited regarding the main factors leading to unsolved cybertheft crimes and suspended investigations:

Professor A.V. Fedorov emphasizes: “One of the main problems in investigating cybercrimes is the high level of technological knowledge possessed by criminals and their use of modern methods to conceal their tracks. They often utilize cryptocurrencies, VPN services, and other anonymizers, which makes identifying them more challenging”[6].

In his research, I.S. Ivanov points out that one of the primary difficulties in investigating cybertheft crimes is the insufficient knowledge and skills of law enforcement officers in the IT field. Effective investigation of such crimes requires specialized technical knowledge and skills[7].

S.M. Petrov notes, “The lack of adequate international cooperation in investigating cybercrimes is a significant problem. Criminals often commit offenses against victims in one country while operating from another. In such cases, it is necessary to improve mechanisms for interstate cooperation to conduct investigative actions”[8].

In our opinion, based on the views of the aforementioned scholars and the cited statistical data, we find it necessary to summarize the main factors leading to unsolved cybertheft crimes and suspended investigations as follows.

Firstly, there are legal and regulatory factors such as the absence of a special procedural framework for investigating cybertheft crimes, inadequately developed mechanisms for international cooperation, and the lack of clearly defined procedures for collecting and securing electronic evidence.

The second direction involves implementing modern software and technical tools to enhance technical capabilities, establishing specialized laboratories for detecting and analyzing cybercrime, providing advanced equipment for collecting and analyzing digital evidence, improving cyberattack monitoring systems, as well as integrating databases and automating information exchange.

The third direction focuses on developing international cooperation by concluding international agreements on combating cybercrime, establishing rapid information exchange with law enforcement agencies of foreign countries, creating joint investigative teams for cross-border crimes, participating in international conferences and seminars, and strengthening regional cooperation in the fight against cybercrime.

The fourth direction requires aligning cybercrime legislation with international standards, simplifying procedures for collecting and presenting electronic evidence, clearly defining the procedural status of digital evidence, and enshrining international cooperation mechanisms in legislation.

The fifth direction involves implementing preventive measures such as conducting cybersecurity awareness campaigns among the population, providing cybersecurity consultations to enterprises and organizations, disseminating warning materials on social networks, and teaching cybersecurity basics in educational institutions.

The comprehensive implementation of the aforementioned measures will significantly enhance the effectiveness of cybercrime investigations. Additionally, it is crucial to thoroughly study international experience in improving the institution of inquiry and suspension of preliminary investigation, implement best practices from developed countries into national legislation, further strengthen international cooperation, and introduce modern approaches in this field.

References:

1. Criminal Procedure Code of the Republic of Uzbekistan. https://lex.uz/docs/111460 [Electronic source] Accessed on 12.01.2025. Date of appeal 12.01.2025.

2. Information note issued by the Investigative Department under the Ministry of Internal Affairs of the Republic of Uzbekistan dated January 9, 2025.

3. Mark Liberman "Fishing" (in English). UPenn Language Log (September 22, 2004). Archived from the original on August 23, 2011 https://ru.wikipedia.org/wiki [Electronic source.] Accessed on 12.01.2025.

4. Landwehr, Carl E.; Alan R. Bull; John P. McDermott; William S. Choi (1993). "A taxonomy of computer program security flaws, with examples." DTIC Document. Archived from the original on 2013-04-08. [Electronic source.] Accessed on 12.01.2025.

5. Researchers reconstruct typed text using keyboard acoustic emanations. Archived on December 24, 2013, at the Wayback Machine, berkeley. [Electronic source.] Accessed on 12.01.2025.

6. Fedorov A.V. "Cybercrime in the modern world: problems and solutions," Moscow, 2023.

7. Ivanov I.S. "Methodology of Investigation of Cybercrimes," Saint Petersburg, 2022

8. Petrov S.M. "International cooperation in the fight against cybercrime," Moscow, 2023.