World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-25, August -2023
ISSN: 2749-3601

SPECIFICS OF DETECTION AND INVESTIGATION OF CYBERCRIME AND HIGH TECHNOLOGY OFFENCES

Zokirov Sardorjon Karimjon ugli
Lecturer of the Criminal Procedure Law Department of
the Tashkent State Law University

Article history:

Received: June 20th 2023
Accepted: July 20th 2023
Published: August 24th 2023

Abstract:

The article examines the specifics of cybercrime and high technology offences, as well as methods and technologies for their detection and investigation. The focus is on the need for co-operation between different countries and law enforcement agencies to effectively combat these threats.

Keywords: Cybercrime, high technology offences, detection, investigation, cooperation, blockchain.

The modern world is facing the growing threat of cyber and high-tech crimes. Cybercriminals use various methods and technologies to achieve their goals, such as social engineering, malware, hacker attacks, and others. High-tech crimes can involve copyright infringement, software piracy, intellectual property theft, etc. Cybercriminals may utilize new technologies such as blockchain to protect their actions from law enforcement interference.

Detecting and investigating cybercrime and high-tech crime requires specialized knowledge and skills. It is necessary to use modern methods and technologies to gather evidence and analyze information. It is also important to take into account the peculiarities of these crimes in their detection and investigation.

Features of cybercrime. One of the features of cybercrime is that it can be committed from anywhere in the world. Cybercriminals can use anonymous communications and virtual private networks to conceal their identity and location. This makes the detection and investigation of cybercrime more difficult, as cooperation between different countries and law enforcement agencies is required.

In addition, cybercriminals use various methods and technologies to achieve their goals. For example, they may use social engineering to gain access to sensitive information. Social engineering is a method of manipulating people to gain access to protected information. Cybercriminals may also use malware, such as Trojan horses or spyware, to gain access to computers and networks. They may use hacking attacks to break into protected systems.

Features of high-tech crimes. High-tech crimes also have their own characteristics. They may involve copyright infringement, software piracy, intellectual property theft, etc. Criminals may use new technologies, such as blockchain, to protect their actions from interference by law enforcement.

For example, software piracy is a common high-tech crime. Criminals may use special programs to copy and distribute software without the permission of the copyright holder. They may use technologies such as torrents or file-sharing networks to distribute pirated software.

In addition, high-technology crimes may involve the theft of intellectual property. For example, criminals may use technology, such as hacking into e-mail or social networks, to gain access to confidential information. They may use this information to steal intellectual property such as patents, copyrights, or trademarks.

Detecting and investigating cyber and high-tech crimes. Identifying and investigating cybercrime and high-tech crime requires specialized knowledge and skills. It is necessary to use modern methods and technologies to gather evidence and analyze information.

One of the main methods of detecting cybercrime is monitoring network activity. This identifies unusual online activity that may indicate the presence of a cybercrime. For example, if someone is trying to access protected information from an unfamiliar device or country, this may indicate a cybercrime.

In addition, special malware or hacking detection programs can be used to detect cybercrime. These programs can scan computers and networks for malware or vulnerabilities that can be used for hacking attacks.

In order to investigate cyber and high-tech crimes, evidence must be collected. This may include collecting logs of network activity, hard drive images, copying emails, etc. It is important to maintain a chain of evidence to ensure that it is reliable and credible.

Investigations of cyber and high-tech crimes also need to take into account the characteristics of these crimes. For example, when investigating intellectual property theft, it is important to consider that criminals may use various methods to conceal their

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-25, August -2023
ISSN: 2749-3601

actions. They may use anonymous e-mail or virtual private networks to conceal their identity and location.

Cooperation between different countries and law enforcement agencies. Cooperation between different countries and law enforcement agencies is a key factor in combating cybercrime and high-tech crime. Only by joining forces can we effectively combat these threats and protect the interests of the state, businesses and ordinary citizens.

For example, in 2014, the International Group of Cyber Security Experts (IGCI) was established within INTERPOL. This group is dedicated to coordinating actions between law enforcement agencies of different countries in the fight against cybercrime. It also provides training to law enforcement agencies and develops recommendations to improve cyber security.

In addition, there are various international agreements and conventions aimed at combating cybercrime and high-tech crime. For example, the Convention on Cybercrime was adopted by the Council of Europe in 2001. This convention contains recommendations for improving legislation and cooperation between law enforcement agencies of different countries.

In general, cybercrime and high-tech crimes pose a serious threat to the modern world. However, with the help of modern methods and technologies, as well as cooperation between different countries and law enforcement agencies, it is possible to effectively combat these threats and protect the interests of society. It is necessary to take into account the peculiarities of cybercrime and high-tech crime in their detection and investigation. It is also important to train law enforcement agencies and develop recommendations to improve cyber security.

LIST OF REFERENCES

1. Convention on Cybercrime. Council of Europe. 2001.
2. International group of experts on cybersecurity (IGCI). Interpol.
3. Grigoriev A.V. Cybercrime: problems of detection and investigation // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2018. № 3.
4. Shishkin A.V. Crimes in the sphere of information technologies // Vestnik of the Academy of Law and Management. 2019. № 3.
5. Medvedev D.A. Cybercrimes: features, methods of detection and investigation // Legal Journal. 2017. № 2.