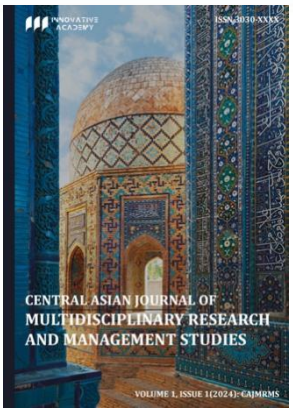

CYBERCRIME: THE LETTERS BEHIND MODERN TECHNOLOGY

Vokhidov Shaxriyor
Cadet of the Academy of MIA
Aminova N.Sh.
Senior teacher of the Academy of MIA (PhD)
https://doi.org/10.5281/зенодо.15684733

ARTICLE INFO

Received: 11th June 2025
Accepted:15th June 2025
Published: 17th June 2025

KEYWORDS

ABSTRACT

Cybercrime is a type of crime committed under the combined influence of a computer and a network. The computer acts as a targeted weapon during the crime. Cybercrime is committed with the aim of harming someone's security and financial well-being.

There are many crimes related to cybercrime that occur when confidential information is legally protected. Internationally, both governments and non-state actors engage in cybercrime, including espionage, financial theft, and other transborder crimes. Cybercrime that crosses international borders and involves the actions of at least one nation-state is sometimes called cyberwarfare. Warren Buffett describes cybercrime as "the number one problem of humanity" and adds that it "poses a real threat to humanity."

Today, digital technologies are developing rapidly and are playing an important role in people's daily lives. As a result of the development of the Internet and information technologies, new opportunities have been created for people, business processes have been optimized, government services have been digitized, and global communication has become easier. However, along with technological progress, new risks have also emerged.

Cybercrimes cause great harm not only to individual users, but also to businesses and government institutions. These crimes include cases such as theft of personal information, financial fraud, network attacks, and damage to information systems. Their widespread prevalence increases the importance of cybersecurity measures.

Cybercrimes manifest themselves in various forms, and their prevention is gaining global importance. Countries around the world are developing new strategies against these threats and strengthening international cooperation on cybersecurity. Education and awareness play an important role in this. The increase in information about fraud, phishing, malware and other cybercrimes in the media and social networks helps to increase user vigilance. Therefore, studying the main types of cybercrimes, understanding their scope and taking measures to protect against them is an urgent issue for every user, organization and state. In this article, we will talk about the main types of cybercrimes, their impact on society and the economy, as well as effective protection measures against them. With the development of the Internet and information technologies, human life has become more convenient, but at the same time, new threats have emerged. Cybercrimes cause great harm not only to individual users, but also to businesses and government institutions. Through them, personal information is stolen, financial fraud is committed, network attacks are carried out and damage is caused to important information systems.

In addition, modern digital technologies being introduced in our country are opening the door to a number of conveniences for our citizens. In this process, of course, there is also the problem of ensuring the security of digital technologies and information systems being

created. This is one of the most urgent issues, namely, ensuring cybersecurity, preventing and combating possible cybercrime and cyberterrorism.

In ensuring cybersecurity against cybercrime, which is improving day by day, we can protect ourselves from them, that is, ensure cybersecurity, by fulfilling the following requirements;

– use a reliable antivirus program,

– constantly monitor the vulnerabilities of the software products used,

– train employees in the basics of information security,

– adhere to a strong password policy when using passwords,

– use licensed official programs,

– use multi-factor authentication to protect information systems,

– regularly encrypt data on computer hard drives,

In this regard, it should be noted that the authorized state agencies responsible for combating and preventing cybercrime in our country also have certain tasks.

In particular, in the fight against cybercrime, the Republic of Uzbekistan and its people, which are implemented and made possible by information technologies and communications, should ensure the protection of the security of individuals, society and the state and their interests from external and internal cyber threats, strengthen legality and the rule of law in this area, prevent cybercrimes and cyber offenses, identify and eliminate them.

In addition, a recent study by the Association of Certified Fraud Examiners shows that digital information security is a pressing issue for organizations, and directors and executives expect the problem to worsen in the future: “Cyber fraud is the highest risk area for businesses, e-mail hacking, hacking, ransomware and malware, with 85% of respondents already seeing an increase in these schemes and 88% expecting them to increase in the future.”

Indeed, there is no international legal basis for holding social media owners accountable for incitement to overthrow the state on their pages. However, not every criminal act or omission should go unpunished, given its nature.

It is also worth noting that cyberterrorism and the threat it poses to society are also growing. A cyberterrorist act (cyberattack) is a political motive that is carried out using computers and information and communication technologies, which directly threatens the health of people or can potentially threaten their lives, and has the purpose or purpose of causing socially dangerous consequences. The attractiveness of using cyberspace for modern terrorists is due to the fact that carrying out a cyberattack does not require large financial costs.

In addition, modern digital technologies introduced in our country are opening the door to a number of conveniences for our citizens. In this process, of course, there is also the problem of ensuring the security of digital technologies and information systems being created.

This is one of the most urgent issues, namely the issue of ensuring cybersecurity, preventing and combating possible cybercrimes and cyberterrorism.

Cybercrime is a type of crime committed under the combined influence of a computer and a network. The computer acts as a targeted weapon during the crime. Cybercrime is committed with the aim of harming someone's security and financial well-being.

There are many crimes related to cybercrime that occur when confidential information is legally protected. Internationally, both governments and non-state actors engage in cybercrime, including espionage, financial theft, and other transborder crimes. Cybercrime that crosses international borders and involves the actions of at least one nation-state is sometimes called cyberwarfare. Warren Buffett describes cybercrime as "the number one problem of humanity" and adds that it "poses a real threat to humanity."

Today, digital technologies are developing rapidly and are playing an important role in people's daily lives. As a result of the development of the Internet and information technologies, new opportunities have been created for people, business processes have been optimized, government services have been digitized, and global communication has become easier. However, along with technological progress, new risks have also emerged.

Cybercrimes cause great harm not only to individual users, but also to businesses and government institutions. These crimes include cases such as theft of personal information, financial fraud, network attacks, and damage to information systems. Their widespread prevalence increases the importance of cybersecurity measures.

Cybercrimes manifest themselves in various forms, and their prevention is gaining global importance. Countries around the world are developing new strategies against these threats and strengthening international cooperation on cybersecurity. Education and awareness play an important role in this. The increase in information about fraud, phishing, malware and other cybercrimes in the media and social networks helps to increase user caution. Therefore, studying the main types of cybercrimes, understanding their scope and taking measures to protect against them is an urgent issue for every user, organization and state. In this article, we will talk about the main types of cybercrimes, their impact on society and the economy, as well as effective protection measures against them. With the development of the Internet and information technologies, human life has become more convenient, but at the same time, new threats have emerged. Cybercrimes cause great harm not only to individual users, but also to businesses and government institutions. Through them, personal data is stolen, financial fraud is committed, network attacks are carried out and damage is caused to important information systems. In addition, modern digital technologies introduced in our country are opening the door to a number of conveniences for our citizens. In this process, of course, there is also the problem of ensuring the security of digital technologies and information systems being created. This is one of the most urgent issues, namely, ensuring cybersecurity, preventing and combating possible cybercrime and cyberterrorism.

In particular, in the fight against cybercrime, the Republic of Uzbekistan and its people, which are implemented and made possible by information technologies and communications, should ensure the protection of the security of individuals, society and the state and their interests from external and internal cyber threats, strengthen legality and the rule of law in this area, prevent cybercrimes and cyber offenses, identify and eliminate them.

List of Reference:

1. Talwant Singh, CYBER LAW & INFORMATION TECHNOLOGY, Online Available at: http://delhicourts.nic.in/CYBER%20LAW.pdf

2. Carey Goldberg, Federal Charges for Juvenile In a Case of Computer Crime, 1998, Online Available at: http://www.nytimes.com/1998/03/19/us/federal-charges-for-juvenile-in-a-case-of-computer-crime.html

3. Misbah Saboohi , Collecting Digital Evidence Of Cyber Crime, Online Available at: http://www.supremecourt.gov.pk/ijc/Articles/10/2.pdf

4. UNDP, CyberCrime: Regional Conference Booklet, 2007, Online Available at: http://www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf