ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

CYBERCRIME AND CYBERSECURITY

Naqibboyev G‘olibjon
Tashkent State University of Law.

https://doi.org/10.5281/zenodo.15425578

Abstract. *This article explores the concepts of cybercrime and cybersecurity, their significance in the present day, and their impact on society. Additionally, it discusses the main types of cybercrime, methods for their prevention, and approaches to ensuring information security.*

Keywords: *cybercrime, cybersecurity, information security, types of cybercrimes.*

Cybercrime refers to a set of criminal activities carried out in cyberspace using software and technical tools with the aim of seizing, altering, destroying information, or disrupting information systems and resources. The rise of cybercrime poses a threat not only to humanity but also to the security of nations worldwide. The development of internet technologies, the expansion of global networks, and the growth of the digital economy are giving rise to new forms of cybercrime. Cybercrimes manifest in various forms, including data theft, attacks on computer systems, financial fraud, and more. (Yusufjonovna, 2025).

The research results indicate that in today's information age, finding more modern and innovative ways to enhance the essence of information technologies, comprehensively supporting the informatization process, and widely implementing them in practice have become one of the key directions of state activity. It is important to emphasize that alongside the development of modern technologies, favorable conditions have emerged for the development of new forms of criminal activity.

The current trend of cybercrime is increasing day by day. Notably, according to a 2016 report by Cybersecurity Ventures, the global damages caused by cybercrime were predicted to reach $6 trillion annually by 2021 and rise to $10.5 trillion by 2025. In 2022, investment fraud was identified as the most costly form of cybercrime, with an average loss of $70,811 per victim.

(Measures to improve investigative actions in the investigation of crimes committed through information technologies).

Based on the above indicators, it is necessary to examine the cybercrime statistics in our country as well. Over the past three years, cybercrimes have increased by 8.3 times and accounted for 4.5% of total crime (Measures to improve investigative actions in the investigation of crimes committed through information technologies).

Cybercrimes primarily fall under the category of offenses committed through computer systems and networks. These crimes are divided into the following main types:

1) DDoS (Distributed Denial of Service) Attacks. Considered one type of cybercrime, these attacks overwhelm servers with internet traffic to prevent users from accessing online services or websites. Often, such cybercrimes are motivated by financial reasons, for example, a competitor may hire someone to disrupt or shut down another entrepreneur’s online operations. Another type involves extortion, where criminals attack a company, install ransomware or payment programs on their servers, and demand large sums of money to restore access. Currently, DDoS attacks are on the rise, and even some major global companies are not immune to being

"DDoS'ed." The largest recorded attack occurred in February 2020 against Amazon Web Services (AWS), surpassing the attack on GitHub three years prior. To address how a DDoS attack works: it primarily involves flooding targeted devices, services, or networks with fake internet traffic, rendering them unusable for users. Even knowing what a DDoS attack is, avoiding them remains challenging. This is because the signs of a DDoS attack may not significantly differ from typical service issues, such as slow-loading web pages (The Meaning of DDoS Attacks, Types, and Examples).

2) Malicious Software (Viruses, Trojans, Spyware, Ransomware, Malware). One of the most common cyber threats, malicious software is a program created by cybercriminals or hackers to compromise or damage a legitimate user's computer. Often spread through suspicious email attachments or seemingly legitimate downloads, malicious software can be used by cybercriminals for financial gain or political motives in cyberattacks.

3) Phishing Attacks. Phishing is a type of cybercrime where attackers target victims with seemingly legitimate emails that request sensitive information, posing as a reputable company. Phishing attacks are often used to trick individuals into providing credit card details and other personal information (Detection of Phishing Attacks, 2018).

Cybercrimes cause significant harm not only to individual users but also to businesses and government institutions. They can lead to economic losses, exposure of personal information, and threats to public safety. These crimes negatively impact society on various levels:

- **Economic Losses.** Companies and government institutions may suffer substantial financial damages due to cybercrimes. Fraud, extortion, and data theft result in large corporations losing billions of dollars.
- **Exposure of Personal Information**. As a result of cybercrimes, users' personal and financial information may fall into the hands of fraudsters, leading to credit fraud and threats to personal privacy.
- **Increased Social Distrust.** The rise of online fraud and misinformation increases distrust in society, causing people to view online services with skepticism.
- **Risk of Cyber Warfare.** Cyber espionage and cyberattacks between nations are intensifying, posing serious threats to national security and negatively affecting international relations.
- **Disruption of Reliable Systems.** Attacks on banking systems, government services, and major corporate networks can disrupt the functioning of entire societies.
- **Job Losses.** Due to the damages caused by cybercrimes, companies may face significant losses, forcing them to lay off employees.
- **Psychological and Legal Consequences**. Victims of cybercrimes may experience depression, stress, and other psychological issues. Additionally, the complexity of legal processes creates further challenges in combating cybercriminals (Crimes in Cyberspace and Measures to Prevent Them, 2025).

With the rapid development of information technologies, cybersecurity has become one of the most pressing issues today. While the widespread use of the internet and digital technologies has increased opportunities for information exchange, it has also brought about various cyber threats.

Cybercrimes are causing economic and social problems on a global scale.

Cybersecurity refers to a set of measures aimed at protecting information and preventing cyberattacks. It encompasses ensuring the confidentiality, integrity, and availability of information systems. Cybersecurity plays a crucial role in safeguarding personal data, corporate, and government information systems. Today, every organization and individual must have sufficient knowledge of cybersecurity measures, as threats continue to grow with the advancement of modern technologies.

Additionally, when we make online purchases, use internet banking services, or fill out tax declarations, we must protect our personal and financial information. To ensure the security of this data, we should use trusted websites, choose strong passwords and update them regularly, and avoid clicking on suspicious links.

Businesses and organizations must also pay serious attention to cybersecurity.

Vulnerabilities or security flaws in information systems can lead to significant financial losses, reputational damage, and loss of customer trust. Companies should install firewalls and antivirus software, train employees on cybersecurity, and regularly audit their systems to protect them.

Government institutions also play a vital role in ensuring cybersecurity. They safeguard citizens’ online security by developing cybersecurity laws, combating cybercrime, and raising public awareness about cybersecurity. In Uzbekistan, several measures have been taken in this regard. Notably, the "Law on Cybersecurity" was adopted in 2022. This law regulates relations in the field of information technologies and defines the rights and obligations of government bodies, legal entities, and individuals.

According to the law, government bodies and other organizations are required to ensure the security of their information systems, identify cyber threats, and take measures to counter them. Additionally, they must train their employees in cybersecurity and establish international cooperation in this area.

Individuals are also responsible for protecting their personal information. They are advised to share their personal data cautiously, use strong passwords, and update them regularly. Additionally, they should install antivirus software on their computers and mobile devices and keep it updated consistently.

Criminal and administrative liabilities have been established for cybersecurity violations.

Cybercrimes include unauthorized access to computer systems, data theft or destruction, distribution of computer viruses, fraud, and more.

Cybercrimes are currently a global issue, posing serious threats not only to individuals and organizations but also to the national security of states. In recent years, as modern technologies have advanced, the methods of cybercrime have also become more sophisticated.

Therefore, ensuring cybersecurity and information security requires a comprehensive approach that includes not only technical but also legal measures.

To effectively combat these cyber threats, it is essential to leverage advanced technologies and increase users’ awareness of cybersecurity. Cybersecurity is one of the most pressing issues today.

Everyone must take responsibility for protecting their personal information and financial resources, while government bodies and organizations should implement necessary measures in this regard.

Furthermore, fostering a culture of cybersecurity in society and enhancing the public's cybersecurity literacy are among the critical tasks. To achieve this, it is advisable to conduct cybersecurity classes and training in all educational institutions, publish programs and articles on the topic in mass media, and utilize social advertising. By doing so, we can instill cybersecurity skills in our youth and society, protecting them from various online threats.

It should not be forgotten that in an era of rapidly evolving digital technologies, the emergence of new cyber threats is inevitable. Therefore, we must develop new cybersecurity methods to prevent cybercrime and remain vigilant at all times. After all, awareness is the demand of the times!

REFERENCES

1. KIBERJINOYAT VA UNI OLDINI OLISH. (2025). *Лучшие интеллектуальные исследования*, *37*(3), 23-32. https://scientific-jl.com/luch/article/view/327
2. Fortinet. (n.d.). What is a DDoS attack? (2025) https://www.fortinet.com/resources/cyberglossary/ddos-attack
3. Detection of phishing attacks. (2018). 6th International Symposium on Digital Forensic and Security (ISDFS), 78 https://www.researchgate.net/publication/324999540_Detection_of_phishing_attacks
4. UzMarkaz. (n.d.). Kibermakondagi jinoyatlar va ularning oldini olish choralari [Cybercrime and measures to prevent it]. 2025, https://uzmarkaz.uz/ru/news/kibermakondagi-jinoyatlar-va-ularning-oldini-olish-choralari