INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 8.854 Volume 13, issue 03 (2026)

UDK 004.056

THREATS AND PROTECTION METHODS IN CYBERSECURITY

K.S. Khaydarov
PhD (t.f.f.d) Namangan State Technical University
(e-mail: kamoliddin1506@gmail.com)

Abstract

This article analyzes the main threats in the field of cybersecurity and modern methods of their prevention. In addition, effective mechanisms for protecting information systems and computer networks are considered.

Keywords

cybersecurity, malware, phishing, encryption, firewall, authentication.

In recent years, the rapid development of information and communication technologies has deeply penetrated all spheres of society. Digital technologies are widely used in public administration, the banking and financial system, education, healthcare, industry, and transportation. Although the process of digitalization increases efficiency and improves the quality of services, it also creates new cybersecurity-related threats.

In the Republic of Uzbekistan, special attention is being paid to cybersecurity issues at the level of state policy. In particular, the “Digital Uzbekistan – 2030” strategy, approved by the Presidential Decree No. PF–6079 of October 5, 2020, identifies ensuring information security, developing the cybersecurity system, and introducing modern protection mechanisms as priority tasks [1].

Additionally, the Presidential Resolution No. PQ–5053 dated March 26, 2021 emphasizes strengthening information security, enhancing cyber protection of state bodies and critical infrastructure facilities, and training qualified specialists. These documents play an important role in establishing the legal and organizational foundations for ensuring cybersecurity in the country [2].

Today, information resources have strategic importance, and their protection is one of the key factors of national and societal security. The expansion of internet networks, cloud technologies, mobile devices, and the widespread use of IoT systems create new opportunities for cyberattacks. As a result, the number of cybercrimes aimed at spreading malware, phishing attacks, network attacks, data theft, and system disruption is increasing.

Cybersecurity is not only a technical issue but also a complex problem that includes organizational, legal, and social aspects. Vulnerabilities in information systems may lead to financial losses, loss of confidential data, and damage to the reputation of organizations. Therefore, ensuring cybersecurity has become an important task for every state, organization, and user under modern conditions.

The main goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information. These principles form the foundation of the information security system. This article analyzes the main threats in cybersecurity and effective methods for preventing them [3–4].

Cybersecurity threats are a set of actions aimed at unauthorized access to information systems, computer networks, and data, as well as their disruption, theft, or destruction. In modern information society, along with the widespread use of digital technologies, the scope of

cyber threats is expanding and their complexity is increasing. These threats cause not only technical problems but also economic, social, and legal consequences.

One of the most common cyber threats is malicious software (malware). Malware refers to programs that secretly infiltrate a user's computer or network and cause damage to system operations. They often spread through unknown files downloaded from the internet or malicious links. Viruses corrupt files, Trojan programs disguise themselves as legitimate software, ransomware encrypts data and demands payment, while spyware monitors and tracks user activities.

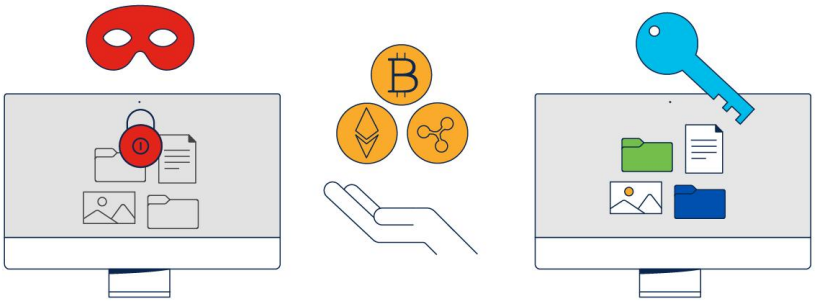

Figure 1. Malware

Network attacks are also one of the important categories of cyber threats. Through such attacks, hackers attempt to influence computer networks and disrupt their normal functioning. Examples of network threats include Distributed Denial of Service (DDoS) attacks, the Man-in-the-Middle (MitM) method, brute force attacks based on password guessing, and SQL injection attacks against web applications. As a result of these attacks, server operations may stop, data may be corrupted, or unauthorized access to systems may occur.

Internal threats also pose a serious risk to cybersecurity. They arise due to the negligence, lack of skills, or intentional actions of employees within an organization. For example, the use of weak passwords, insecure storage of confidential data, or incorrect system configurations are among the main causes of internal threats.

In addition, attacks carried out through social engineering techniques are becoming increasingly widespread. In this method, attackers exploit human psychology to obtain confidential information from users. Deception through phone calls, fake technical support services, or posing as a trusted person are examples of such methods.

Phishing is a type of cyberattack aimed at obtaining confidential information by deceiving users. In this case, attackers use fake email messages, fraudulent websites, or fake pages on social networks. When a user trusts these sources and enters their login credentials and password, the information is transmitted to the attacker.

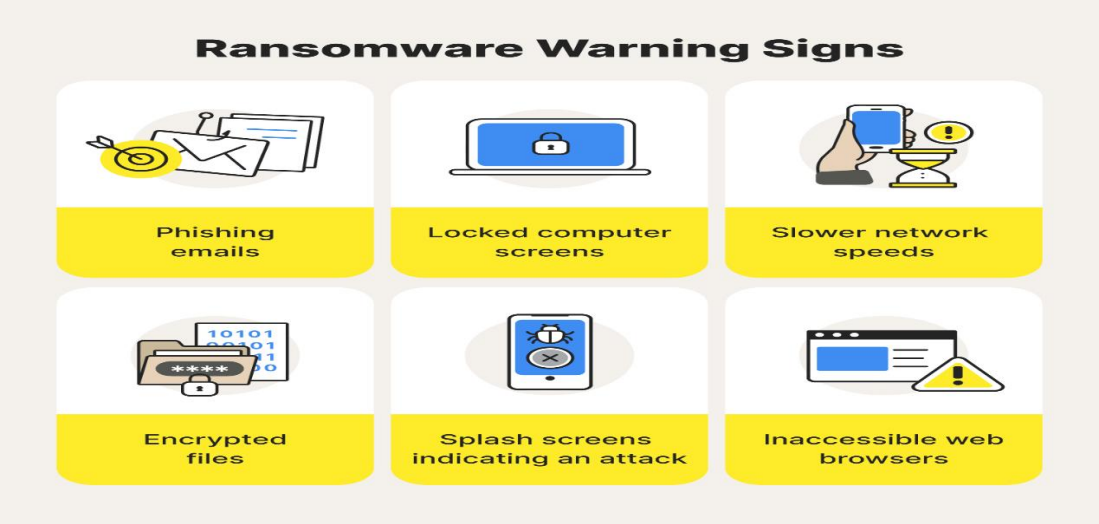

Figure 2. Example of a Phishing Attack

Cybersecurity protection requires the implementation of modern security technologies and management mechanisms. One of the most effective methods is the use of antivirus software that detects and removes malicious programs from computer systems. Regular updates of antivirus databases allow systems to be protected against newly emerging threats.

Another important protection method is the use of firewalls. Firewalls monitor incoming and outgoing network traffic and block unauthorized access to systems. They play a key role in protecting computer networks from external attacks.

Encryption technologies are also widely used to protect sensitive information. Encryption converts data into a coded format so that unauthorized users cannot read it. Modern encryption algorithms such as AES and RSA are commonly used to ensure data confidentiality.

In addition, strong authentication mechanisms help prevent unauthorized access. Multi-factor authentication (MFA), biometric verification, and secure password policies significantly improve system security.

Risk assessment is an important component of cybersecurity management. It involves identifying potential threats, analyzing system vulnerabilities, and evaluating the possible impact of cyberattacks. Organizations can prioritize security measures by assessing the likelihood and severity of different threats.

Effective risk management allows institutions to allocate resources efficiently and implement preventive security strategies.

Human awareness plays a crucial role in ensuring cybersecurity. Many cyber incidents occur due to a lack of user knowledge and security awareness. Therefore, organizations should regularly conduct cybersecurity training programs for employees.

These programs help users recognize phishing emails, suspicious links, and other forms of social engineering attacks. Educated users become the first line of defense against cyber threats.

Future cybersecurity challenges are expected to increase with the rapid growth of artificial intelligence, cloud computing, and the Internet of Things. Cybercriminals are also adopting advanced technologies to develop more sophisticated attack methods.

Therefore, continuous research, development of innovative security technologies, and international cooperation are essential to address future cyber threats.

Table: Types of Cyber Threats and Protection Methods

Threat Type	Description	Protection Method

Malware	Malicious software that damages systems	Antivirus software
Phishing	Fraudulent attempts to obtain sensitive information	User awareness
DDoS	Overloading servers with requests	Firewall and traffic filtering
SQL Injection	Attacks on databases through web applications	Secure coding

Network attacks are carried out through computer networks. DDoS attacks overwhelm a server by sending a large number of requests, which causes the server to become unavailable. In a Man-in-the-Middle (MitM) attack, the data transmission process is secretly intercepted and monitored. In the Brute Force method, passwords are automatically guessed through repeated attempts, while SQL Injection attacks are used to damage or manipulate databases by inserting malicious SQL queries into web applications [5].

Figure 3. Illustration of a Network Attack (DDoS)

Internal threats arise from employees or users within an organization. They may occur due to negligence, the use of weak passwords, insecure storage of data, or the use of unauthorized external devices. It has been observed that many information security incidents are related to the human factor.

Social engineering is a method of obtaining information by exploiting human psychology. In this type of attack, attackers introduce themselves as technical support staff or representatives of an organization and request passwords or confidential information from users. In such attacks, the main target is not technical systems but the trust and vulnerability of people.

Figure 4. Model of Internal Threats

With the development of technology, new threats are also emerging. Attacks on cloud services, vulnerabilities of IoT devices, artificial intelligence–based malware, and data leaks are among the major problems of modern cybersecurity.

Today, along with the rapid development of digital technologies, cybersecurity issues are becoming increasingly important. The widespread use of information systems and computer networks has led to the emergence of various cyber threats. Malware, phishing attacks, network attacks, internal threats, and social engineering techniques pose serious risks to information security. These threats can lead not only to technical failures but also to financial losses, leakage of confidential data, and disruption of organizational operations.

The article analyzes the main types of cybersecurity threats and describes their mechanisms and levels of risk. In addition, the importance of a **comprehensive approach** to protecting modern information systems—combining technical, organizational, and legal measures—is substantiated. Measures such as antivirus tools, network security firewalls, encryption methods, authentication mechanisms, and user awareness are shown to play an important role in preventing cyber threats.

In conclusion, it can be stated that ensuring cybersecurity is a continuous process that requires constant improvement. Effective results can be achieved through the joint efforts of government institutions, organizations, and ordinary users. Increasing knowledge and skills in information security and implementing modern protection technologies are key factors in combating future cyber threats.

REFERENCES

1. **President of the Republic of Uzbekistan.** (2020). Decree No. PF–6079: *Digital Uzbekistan – 2030 Strategy*. Tashkent, Collection of Legislative Acts of the Republic of Uzbekistan.

2. **President of the Republic of Uzbekistan.** (2021). Resolution No. PQ–5053: *Measures to Ensure Information Security*. Tashkent, Collection of Legislative Acts of the Republic of Uzbekistan.

3. **Stallings, W.** (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.

4. **Kurose, J. F., & Ross, K. W.** (2021). *Computer Networking: A Top-Down Approach*. Pearson.

5. **Xaydarov, K. S., & A. H. R. Qizi.** (2024). *Configuration of Cisco Router and Verification of Its Operation Process*. **Mechanics and Technology**, 4(17), 260–263.

6. **International Organization for Standardization.** (2022). *ISO/IEC 27001:2022 Information Security Management Systems (ISMS)*. Geneva, Switzerland.

7. **Xaydarov, K. S.** (2025). *Capabilities of Cisco Packet Tracer Software in Ensuring Modern Network Security*. **Economics and Society**, (1–2 (128)), 509–512.

8. **Zoidova, O., Inamova, G., & Imamnazarov, E.** (2025). THE ADVANTAGES OF USING DIGITAL TECHNOLOGY TOOLS IN TEACHING DIGITAL CIRCUITRY. ***Journal of Applied Science and Social Science***, *1*(3), 475-478.