CYBERCRIME AND ITS PREVENTION: MODERN METHODS AND LEGAL AND TECHNICAL PROTECTION

Uzakova Vasila Ilkhom qizi
Student, Faculty of Digital
Economy and Information Technologies,
Tashkent State University of Economics
E-mail: uzakovavasila2007@gmail.com
Tel: +998 99 054 36 08

Y.B. Eshmatova
Scientific supervisor (PhD):
https://doi.org/10.5281/zenodo.24021551

Abstract. This comprehensive scientific article provides an in-depth analysis of the concept of cybercrime, its main forms, the harm it causes, and the threat it poses to society and the digital economy amid the rapid development of digital transformation processes. In particular, it covers the technical mechanisms of cybercrime, phishing technologies, Trojan and ransomware programs, social engineering methods, and global cyber threats related to the unlawful acquisition of personal data. It also develops practical proposals and methodological recommendations aimed at comprehensively ensuring information security, improving the national and international legal framework, raising citizens' digital literacy, and preventing cybercrime.

Keywords:cybercrime, information security, phishing, digital literacy, cybersecurity, personal data, ransomware, social engineering, two-factor authentication.

Introduction and Relevance of the Topic

Today, digital technologies are penetrating all spheres of human life, including public administration, the financial and banking system, industrial enterprises, and education, broadly and rapidly. Under digital transformation, electronic payment systems, cloud technologies, mobile applications, and platforms based on artificial intelligence have brought information exchange and business processes to a qualitatively new level. Alongside increasing the speed of operations, these technological conveniences have made network security and information integrity pressing problems.

With globalization, the number of internet users keeps growing, which creates ground for the expansion of offences committed in cyberspace. Cybercrime is no longer a simple tool for damaging the computer equipment of individuals; it has become a complex global problem threatening the strategic infrastructure of states, the financial sector, and international security.

In recent years, extensive reforms have also been carried out in our country to develop the digital economy and digitalize all sectors. However, as the digital environment expands, the attack methods and technical tools used by cybercriminals are also steadily improving. Therefore, analyzing methods of preventing cybercrime from scientific and practical perspectives and developing effective protection mechanisms is of utmost importance.

The Concept of Cybercrime and Its Classification

Cybercrime (or computer crime) is a set of unlawful and dangerous acts committed using, or directed against, information technologies, computer systems, telecommunication networks, and digital devices. In international legal practice, in particular in the Council of Europe's Budapest Convention on Cybercrime, cybercrimes are divided into four main groups: crimes against the confidentiality, integrity, and availability of computer data and systems; computer-related forgery and fraud; offences related to prohibited content; and offences related to the infringement of copyright.

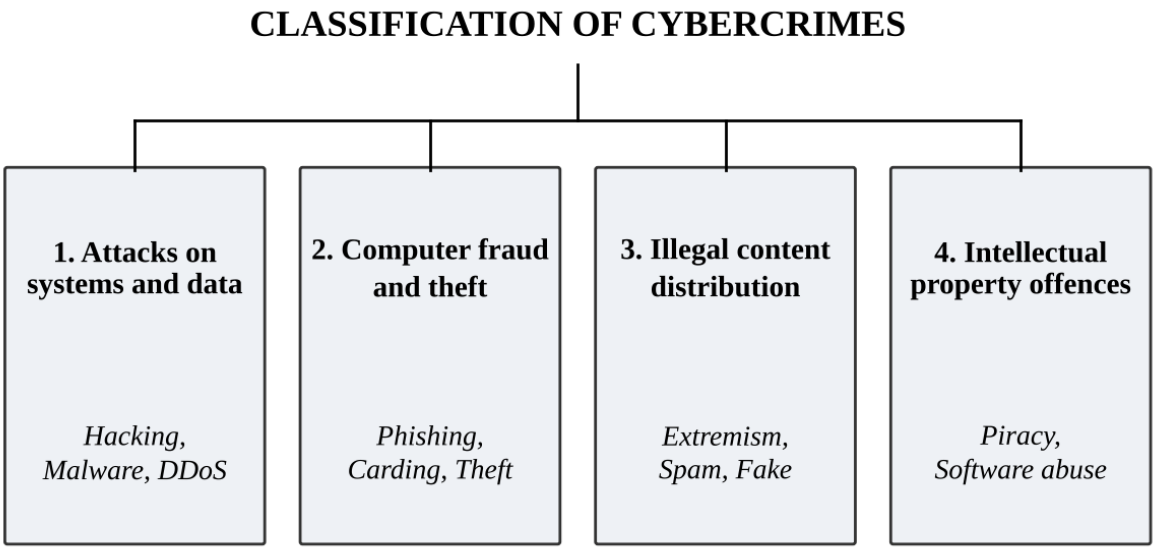

Fig. 1. Main classification groups of cybercrime.

The first group includes unlawful access to computer systems (hacking), unlawful interception of data, disrupting the operation of systems, and distributing malicious software. Such crimes are often committed to obtain confidential data or to paralyze the activity of organizations. Intruders who gain unauthorized access to a system may alter or delete databases or use them as a means of extortion.

The second group mainly includes computer fraud committed for financial gain. It is dominated by misappropriation of funds in electronic payment systems, theft of bank card details, and conclusion of fraudulent transactions. Such acts are in most cases carried out by gaining users' trust or deceiving them.

The third and fourth groups relate to the distribution of unlawful information in the digital space and the infringement of intellectual property rights. Examples include unlawful copying of intellectual property objects, causing material damage to copyright holders, and threatening information attacks on social networks.

The technical complexity of cybercrimes lies in their cross-border nature. An offender can sit in one country and attack an information system in another. This complicates investigations and requires international cooperation and rapid information exchange.

Analysis of Modern Cyber Threats and Attack Methods

Today, the attack methods used by cybercriminals are extremely diverse and growing more sophisticated. One of the most widespread and effective of them is social engineering. In social

engineering, the main target is not the technical system but the human factor. Attackers exploit human psychology, trust, and carelessness to obtain confidential data from users.

Table 1. Main types of modern cyber threats and their impact.

Threat type	Attack mechanism	Damage caused
Phishing	Deceiving users through fake websites and messages.	Loss of personal logins, passwords, and bank card details.
Ransomware	Encrypting files and demanding payment to unlock them.	Disruption of an organization's operations and financial losses.
DDoS attacks	Sending a large number of fake requests to a server simultaneously.	Temporary disruption of a system or website.
Trojan programs	Penetrating a system disguised as a useful program and spying.	Unlawful loss of confidential documents and files.
Man-in-the-Middle	Intercepting the data flow between a user and a server.	Transactions and private correspondence passing to a third party.

The best-known form of social engineering is phishing, in which criminals send fake e-mails, SMS messages, or links in the name of official state bodies, banks, or popular social networks. The moment a user enters their login and password or bank card details on the fake page, this information immediately falls into the attackers' hands.

In addition, the number of attacks involving ransomware has risen sharply in recent years. After entering a computer or server, ransomware encrypts all important files on it using complex cryptographic algorithms and demands a large payment in cryptocurrency to decrypt them. If the payment is not made, the files are destroyed completely or published on the internet.

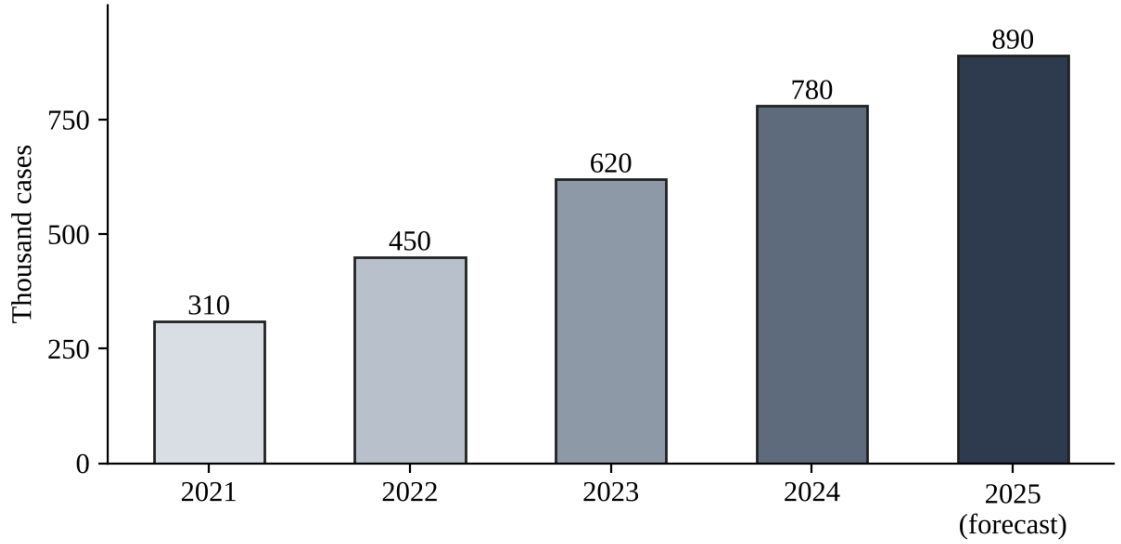

Fig. 2. Growth dynamics of phishing and ransomware attacks (thousands of cases).

Another serious threat is DDoS (Distributed Denial of Service) attacks. In them, thousands of computers around the world infected with malware (a botnet) send millions of requests to a single target server at the same time. As a result, the server's resources are exhausted and its ability to serve users stops completely.

In addition, through Man-in-the-Middle (MitM) attacks, programs that intercept data transmitted over unprotected Wi-Fi networks are actively used to monitor every character typed by users on the keyboard (keylogging).

Ensuring Information Security and Technical Protection Methods

To successfully counter cyber threats, technical protection measures must be properly organized and continuously improved. One of the main technical pillars of information security is complex passwords and authentication mechanisms. Using weak passwords allows cybercriminals to gain access easily by means of automated brute-force (password guessing).

Therefore, every user and organization employee needs to use unique passwords of at least 12–16 characters containing uppercase and lowercase letters, digits, and special characters. Using the same password for several accounts is strictly prohibited. It is advisable to use special secure password managers for managing passwords.

Table 2. Effectiveness and cost indicators of cybersecurity technical tools.

Protection component	Technical feature	Implementation cost	Level of effectiveness
Two-factor authentication (2FA)	SMS, OTP token, or biometrics	Low / Medium	Very high (99% protection)
Firewall and IDS/IPS	Filtering and monitoring network traffic	High	High (against external attacks)
Antivirus and EDR systems	Detecting and blocking malicious programs	Medium	Medium / High
Data encryption (SSL/TLS)	Cryptographic encryption and channels	Low	Very high (confidentiality)
Backup	Cloud and offline secure storage	Medium	Maximum (system recovery)

Introducing two-factor (2FA) and multi-factor (MFA) authentication systems raises the level of security several times over. To log in to an account, the user must enter not only the password but also a one-time code (OTP) sent to a mobile device or biometric data (fingerprint, face recognition). This prevents access to the account even if an attacker obtains the password.

Updating software in a timely manner (patch management) is another important factor of technical protection. Vulnerabilities identified in operating systems, browsers, and other programs serve as the main entry point for cybercriminals. Installing security updates released by developers without delay ensures the robustness of the system.

At the organizational level, it is necessary to use network security firewalls, intrusion detection and prevention systems (IDS/IPS), and licensed antivirus software. In addition, regular backup of all important data and storing these backups on servers isolated from the main network play a decisive role in reducing the negative consequences of ransomware attacks.

Digital Literacy and the Human Factor

According to leading world experts in cybersecurity, the weakest link in information security is the human factor. Even when the most modern and expensive technical protection systems are installed, the whole system remains at risk if an employee opens an attachment in a suspicious e-mail or follows a phishing link.



Fig. 3. Model of the balance between the human factor and technical protection in cybersecurity.

Therefore, forming a culture of cybersecurity and digital literacy in society and organizations is one of the important tasks. Digital literacy means not only the ability to use computers and the internet, but also knowledge of how to correctly assess the risks that may arise in the digital environment and how to protect oneself from them.

Awareness-raising on information security is necessary among all segments of the population, especially young and elderly people. Increasing special training courses and seminars on cybersecurity in educational institutions and universities, and showing students phishing and fraud methods through practical examples, yields high results.

In organizations, it is required to train employees on cybersecurity regularly and to conduct trainings. Testing employees' vigilance by sending simulated phishing messages and analyzing the mistakes made strengthens practical skills.

Legal and International Cooperation Foundations

Effective combating of cybercrime is impossible without an appropriate legislative framework and robust legal mechanisms. In recent years, important legal reforms have been carried out in the field of cybersecurity in the Republic of Uzbekistan. In particular, the adoption of the Law of the Republic of Uzbekistan “On Cybersecurity” became an important legal foundation for regulating relations in this area, protecting national cybersecurity infrastructure, and defining the powers of responsible bodies.

The Criminal Code of the Republic of Uzbekistan establishes the relevant articles and measures of liability for crimes in the field of information technologies. However, the rapid development of technologies requires constant improvement of legislative norms as well. Mechanisms for the legal assessment of new types of crimes related to artificial intelligence, the unlawful use of cryptocurrencies, and violations of personal data need to be further clarified.

Moreover, since cybercrime is international in nature, international cooperation plays a decisive role in investigating cross-border cybercrimes. It is necessary to expand bilateral and multilateral agreements with Interpol, Europol, other international organizations, and the law enforcement bodies of neighboring states on rapid information exchange, on apprehending cybercriminals, and on extradition.

Practical and Methodological Recommendations

The analyses and findings make it possible to define criteria for preventing cybercrime and ensuring information security in the future. Below is a set of practical recommendations for individual users and organizations:

Recommendations for individual users:

Do not open hyperlinks and e-mail attachments received from unknown sources, and do not download unlicensed software.

Do not disclose bank card details, CVC codes, and one-time SMS codes to anyone, even to persons who introduce themselves as bank employees.

Do not store highly confidential personal documents and photos openly on social networks and messengers, and use VPN services when using open Wi-Fi networks.

Recommendations for organizations and institutions:

Conduct security audits of information systems on a regular basis and eliminate vulnerabilities in a timely manner.

Develop internal regulations on information security and limit employees' access rights (access control) to the minimum necessary level.

Create periodic backups of data and prepare a plan for restoring systems in emergencies (Disaster Recovery Plan).

Conclusion

In conclusion, in a digital society the risk of cybercrime and cyber threats is constant and dynamic in nature. Combating this problem can be achieved not by individual efforts alone, but through a joint comprehensive approach of the state, the private sector, and society.

A safe and sustainable digital space will be built by improving technical protection tools, adapting the legal framework to modern requirements, strengthening international cooperation, and, most importantly, raising citizens' digital literacy. In this regard, the knowledge and skills of future specialists in the digital economy and information technologies are of great importance.

As digital technologies develop, their security infrastructure must also improve in parallel. The digital future, financial stability, and inviolability of the citizens of the Republic of Uzbekistan depend directly on the development of the cybersecurity sector and on putting the recommendations presented in this article into practice.

MAIN SCIENTIFIC RESULTS OF THE RESEARCH

- The socio-economic and technical classification of types of cybercrime has been improved.
- The effectiveness of multi-factor authentication and anti-fraud systems in preventing phishing and ransomware attacks has been substantiated.
- A three-stage practical methodology for raising national cybersecurity and digital literacy has been developed.

References

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, O'RQ-764-son, 2022-yil 15-aprel. Qonunchilik ma'lumotlari milliy bazasi.
2. ITU (International Telecommunication Union). (2024). Global Cybersecurity Index 2024 Report. Geneva: ITU Publications.

3. Kovtanyuk, M., & Savenko, O. (2023). Methods of Counteracting Phishing Attacks in Modern Information Systems. Journal of Computer Security and Information Protection, 11(2), 87-95.
4. Stallings, W. (2022). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson Education.
5. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash to'g'risidagi PF-6079-son Farmoni.
6. Aripov, M. M., & Muhammedov, D. A. (2021). Axborot xavfsizligi va kiberxujumlardan himoyalanish texnologiyalari. O'quv qo'llanma. Toshkent: "TDIU", 195 b.