CYBERCRIME. THREATS, CHALLENGES AND SOLUTIONS IN THE ERA OF GLOBAL DIGITALIZATION

Boburjon Shokirov
Student of Fergana state university
https://doi.org/10.5281/zenodo.15474493

Annotation. Cybercrime refers to a complex of crimes committed using information technologies and the Internet. It poses a serious threat to information security, manifesting in the theft of personal data, financial fraud, attacks on state information systems, and various other risks. In today's era of globalization and digitalization, cybercrime presents significant dangers not only to individuals but also to entire nations. This article analyzes the main types of cybercrime, the challenges in combating it, and possible solutions. A multifaceted approach involving legal, organizational, financial, and technological measures is proposed to ensure effective cybersecurity and minimize the impact of cybercrime on society and state infrastructure.

Keywords: Cybercrime, cybersecurity, personal data theft, cyberattacks, digital blackmail, legal framework, transnational crime, ransomware, information security, artificial intelligence.

Cybercrime is a set of crimes committed through information technologies and the Internet. It threatens information security and is manifested in the theft of personal data, financial fraud, attacks on state information systems, and many other threats. In today's era of globalization and digitalization, cybercrime poses a significant danger not only to individuals but also to entire nations. This article analyzes the main types of cybercrime, the challenges in combating it, and possible solutions.

Cybercrime involves crimes committed using information technology. Its key characteristic is the use of tools such as computers, smartphones, servers, or the Internet to commit the crime. Types of cybercrime can be classified as follows:

- **Theft of personal data**. Cybercriminals illegally obtain and use personal or financial data. This includes stolen bank card information, passwords, or personal identification data.
- **Cyberattacks**. These attacks target state, private sector, or personal information systems, aiming to damage, steal data, or disable systems. This category includes DDoS attacks, hacking, and the spread of malicious software.
- **Financial fraud**. Fraudulent activities conducted through online payment systems, cryptocurrency trading, and e-commerce platforms are among the most widespread forms of cybercrime.

• **Digital blackmail**. Cybercriminals encrypt (ransomware) or steal data and demand a ransom for its return.

• **Attacks on state information systems and strategic infrastructure**. This type of cybercrime threatens national security and affects the functionality of government institutions and critical infrastructure.

Challenges in combating cybercrime include legal, organizational, financial, and technological issues:

Legal Challenges: Many countries lack specialized laws to address cybercrime, or such laws are underdeveloped. Cybercrime is often transnational—it may be committed in one country but cause harm in another—making legal cooperation complex. Technology evolves rapidly, while the development and updating of legal frameworks often lags behind.

Organizational Challenges: There is insufficient information sharing between the public and private sectors regarding threats. Additionally, there is a serious lack of highly qualified specialists in the field of cybersecurity.

Financial Challenges: Insufficient funding for cybersecurity hinders effective crime prevention. Moreover, cybercrimes often result in significant financial losses, and mechanisms for compensating such damages are underdeveloped.

Technological Challenges: Many information systems are poorly protected, and most organizations lack modern technologies to defend against sophisticated cyberattacks.

To effectively combat cybercrime, the following measures must be implemented:

Legal Measures:

• **Adoption of specialized laws**: Each country should strengthen its legal framework to combat cybercrime, including data protection laws and stricter penalties for cyberattacks.

• **International cooperation**: Countries should enhance mechanisms for information exchange, extradition of criminals, and joint cybersecurity initiatives.

• **Legislative updates**: Laws must be regularly revised to address new threats.

Organizational Measures:

• **Creation of cybersecurity centers**: National and regional centers should be established to ensure rapid response to threats.

• **Specialist training**: Dedicated training programs and courses should be implemented to prepare cybersecurity experts.

Conclusion. Cybercrime is one of the most serious threats facing modern society, states, and the private sector. Combating it requires a comprehensive approach that includes legal, organizational, financial, and technological solutions. By strengthening international cooperation, increasing investments in cybersecurity, and implementing modern technologies, effective resistance to cybercrime is achievable. This not only reduces crime rates but also contributes to the overall security and stability of society.

References:

1. Shmelev, V.V. Cyber Law: Legal Approaches to Ensuring Information Security. Moscow, 2022.
2. Golovanov, S.A., et al. Malicious Software and Protection Technologies Against It. Saint Petersburg, 2021.
3. Abdurakhmonov, Sh.A. Legal Measures for Cybersecurity in Uzbekistan. Tashkent, 2022.
4. Decree of the President of the Republic of Uzbekistan. On Measures to Ensure Information Security and Combat Cyberattacks. 2022.
5. Ahmedov, B.K. The Economic Consequences of Cybercrime and Ways to Eliminate Them. Tashkent, 2021.
6. Methods and Tools for Ensuring Cybersecurity in Telecommunication and Information-Communication Technologies: Proceedings of the International Scientific-Practical Conference. Tashkent: University of Public Safety of the Republic of Uzbekistan, 2022.