THE ROLE OF CYBERSECURITY IN THE INFORMATION AGE. CHALLENGES OF THE INTERNET AND SOCIAL MEDIA

Boburjon Shokirov
Student of Fergana state university
https://doi.org/10.5281/zenodo.15474644

Annotation. The 21st century is known as the era of information technology. With the rapid growth of the internet, new opportunities for communication, education, and commerce have emerged, transforming all aspects of human life. However, alongside its advantages, the internet has introduced several social and legal challenges, such as addiction, misinformation, and cybercrime. This article analyzes the cultural and legal implications of internet use, the rise of cybercrime, and the growing threat of cyberterrorism. Furthermore, it explores preventive cybersecurity measures and the responsibilities of state authorities in combating cyberthreats in Uzbekistan.

Keywords: Cybercrime, cybersecurity, information technology, social networks, cyberterrorism, digital threats, internet addiction, legal regulation.

The Information Age and the Rise of Cyber Threats:

The 21st century is considered the age of information technology. It is almost impossible to imagine today's global progress without the internet. The internet, as is widely known, is an international system of interconnected computer networks that enables the exchange of information and documents. It has opened the door to vast possibilities: people can now access global libraries, attend virtual universities located on the other side of the globe, and perform freelance digital work (such as translation, content creation, and publishing) without leaving their homes.

One of the major attractions of the internet is social media and messaging platforms, which allow for cheap and fast communication, online training, and video conferencing. These advantages have made the internet more popular than television and radio. However, its negative effects are also increasingly evident. Many young people lack the skills to critically consume information, making them vulnerable to manipulation, disinformation, and even internet addiction. Notably, China has recognized internet addiction as a medical disorder and established rehabilitation centers for its treatment.

Unfortunately, many youths waste valuable time scrolling through social networks, forming opinions based on whatever information they encounter—regardless of its accuracy. It is common to see individuals posting opinions or literary works without considering their relevance or credibility, and often filled

with grammatical and spelling errors. Social networks are now filled with praise circles, public shaming, and baseless content, with gossip and personal attacks becoming normalized. Due to the lack of effective oversight, many users mistakenly believe they can do anything online. While some advocate for freedom of expression, their online behavior often reveals their lack of ethical and intellectual depth.

Despite these drawbacks, statistics indicate that 96% of young people globally interact through social media. Among them, Facebook remains the most popular platform, followed by Twitter, Instagram, LinkedIn, Google+, Pinterest, Snapchat, YouTube, Reddit, WhatsApp, Flickr, and Weibo. Social media platforms are also being actively used in Uzbekistan to promote the country's reforms and achievements in the global media space and to contribute to the spiritual development of society.

Cybercrime as a Global Challenge:

Among the major global challenges of our time is cybercrime, which has been steadily increasing. These crimes include the distribution of malware, password theft, bank fraud, the dissemination of illegal and morally corrupt information, and other forms of digital sabotage. The term "cybercrime" refers to a wide range of offenses conducted through information and communication technologies: spreading malicious software, phishing, hacking, illegal website access, identity theft, copyright infringement, and electronic fraud.

Another serious threat is cyberterrorism, whose danger to society continues to grow. A cyberterrorist act (cyberattack) involves using information technology to cause or threaten to cause serious harm to people, infrastructure, or public safety. The appeal of such attacks to terrorists lies in their low cost and high impact. Experts argue that such cyberattacks are often masked as efforts to promote democratic values in developing countries while in fact undermining their national sovereignty and public consciousness.

Efforts to exploit the internet for destabilizing countries are increasing. Social networks and their backers sometimes interfere in domestic affairs under the guise of freedom and openness. Consequently, experts are now suggesting transitioning to a new internet model that limits user anonymity, which would help curb online crimes. Countries like China and Russia are already developing or implementing closed, state-controlled network systems.

Cybersecurity Policy in Uzbekistan:

Uzbekistan, as part of the global information community, has adopted a consistent state policy on the effective use of information and communication

technologies. While digital technologies create new conveniences for citizens, they also raise the issue of cybersecurity. One of the most pressing tasks is to ensure protection against cybercrime and prevent its escalation.

Effective cybersecurity requires implementing the following key measures:

- Educating staff on the fundamentals of information security;
- Regular vulnerability testing of software systems;
- Using reliable antivirus software;
- Using licensed and official programs;
- Applying multi-factor authentication in information systems;
- Enforcing strong password policies;
- Encrypting data stored on hard drives.

In this regard, it is also essential to emphasize the responsibilities of authorized state agencies in Uzbekistan. These bodies are tasked with protecting the country and its citizens from internal and external cyber threats, ensuring national security, upholding the rule of law in cyberspace, preventing and investigating cybercrimes, and protecting public and private interests in the digital domain.

Conclusion

The internet and modern communication technologies, while enabling remarkable social and economic progress, also pose serious risks to individual users and society at large. Cybercrime, misinformation, and digital addiction are growing challenges that require coordinated legal, technical, and educational responses. Uzbekistan's commitment to cybersecurity and its implementation of proactive measures highlight the country's strategic vision in adapting to the digital age. Ensuring cybersecurity is no longer optional—it is a fundamental pillar of national security and social development in the information age.

References:

1. Otayev U.M. What is a cyberattack and how does it occur? In: Proceedings of the Scientific-Practical Conference on the Use of Digital Technologies in Combating Crime. Public Security University. – Tashkent, 2024.
2. Otayev U.M. Offenses committed in cyberspace. In: Proceedings of the National Scientific-Practical Conference "Prospects for Ensuring Cybersecurity and Improving the Fight Against Crimes in the Field of Information Technology". Academy of the Ministry of Internal Affairs. – Tashkent, 2023.
3. Iminov A. Cybersecurity against cybercrime. – Tashkent, 2020.
4. Musaev M. Social networks: How do you use them? – Tashkent, 2020.
5. Information attacks: Objectives and forms. Postda Newspaper. – Tashkent, 2018.