

ROLE OF CYBERSECURITY AND SOCIAL IMPORTANCE IN THE
DEVELOPMENT OF AN INFORMATION SOCIETY**Khamidov Shukurullo Muqimjon oglu**

Researcher at Fergana State University

ORCID:0009-0005-4429-3188

shukurulloxamidov2695@gmail.com

<https://doi.org/10.5281/zenodo.21836164>

Annotation: The role and social importance of cybersecurity in the development of the information society is analyzed from a socio-philosophical perspective. The importance of cybersecurity in ensuring the security of individuals, society and the state, its role in the sustainable development of the information society, and the social consequences of modern cyber threats are highlighted. Also, the moral, legal and institutional factors of strengthening cybersecurity are justified.

Keywords: cybersecurity, information society, information security, cyber threat, digital transformation, information culture, digital literacy, national security.

In the 21st century, the rapid development of information and communication technologies marked a new stage of human development. In the context of an information-ized society, information has become the main resource of economic, political and social development. Thanks to the widespread introduction of digital technologies in all spheres of society, the way people relations, management systems, economic activity and social institutions function is changing radically. However, the expansion of the digital space also introduces new types of risks.

Today, cybersecurity is emerging as an integral component of the information society. This is because the digitalization of strategic sectors such as public administration, banking and finance, education, healthcare, energy, and transport is increasing their vulnerability to cyber threats. As a result, the issue of cybersecurity is becoming an object of important research, which has not only technological, but also socio-philosophical, political and cultural relevance.

One of the main features of the development of an information-ized society is the emergence of information and knowledge as a strategic resource. D. Bell in the theory of post-industrial society evaluated knowledge and information as a decisive factor of progress [1]. This approach shows that the economic and social development of modern society is directly related to the efficiency of information flows.

M. Castels believes that modern society is formed as a "networked society", in which economic, political and cultural relations are carried out through global information networks [2]. This is leading to the expansion of the information space and an increasing role of cyberspace in social life. Consequently, cybersecurity is becoming an important mechanism ensuring the stable functioning of the information society.

The essence of cybersecurity is defined by the protection of information systems, computer networks and digital resources against various threats. In modern approaches, however, cybersecurity is not limited to technical defenses alone. It is interpreted as an integrated social system aimed at protecting the interests of the individual, society and the state [3].

The role of cybersecurity in an informationized society is manifested primarily in protecting the interests of the individual. Modern person in his daily life makes extensive use of electronic services, social networks, online payment systems and digital platforms. Therefore, protection of personal data, inviolability of information and ensuring digital rights is one of the main tasks of cybersecurity. As a result of cyber threats, cases of identity theft, financial fraud and mental health crisis can occur [4].

The social importance of cybersecurity is also related to ensuring the stability of society. Disinformation, disinformation and manipulative information disseminated in the information space can adversely affect public opinion. Such situations lead to a decrease in social trust, a weakening of moral values, and an increase in various social contradictions. Therefore, cybersecurity is manifested as an important factor ensuring the moral and information security of society [5].

The importance of cybersecurity in the life of the state is also increasing. In the context of digital transformation, the dependence of public administration, defence, energy, and transport systems on digital infrastructures is increasing. Cyberattacks on strategic information resources can seriously damage national security. Therefore, cybersecurity today is increasingly recognized as an essential component of national security [6].

The processes of globalization are expanding the scope of cyber threats even further. Threats such as cybercrime, malware, phishing attacks, social engineering, and information manipulation are gaining international character. The fact that they do not depend on geographical boundaries and spread over a wide area in a short period of time poses new challenges for modern security systems.

One of the most important conditions for ensuring cybersecurity in an information society is the development of an information culture. Information culture refers to a person's ability to work with information, critically analyze it and use it responsibly. The development of information culture strengthens social immunity against cyber threats and serves to form a secure information environment [7].

Digital literacy is also one of the important social determinants of cybersecurity. Ensuring that users can safely use internet resources, protect their personal information, and detect cyber threats can help reduce the number of cyber incidents. Therefore, special attention should be paid to the development of digital literacy and cybersecurity culture in the education system.

Cooperation of the state, civil society and educational institutions is essential in ensuring cybersecurity. The state creates a regulatory and legal framework, civil society develops an information culture, and the education system forms cybersecurity competencies. The interaction of these institutions allows creating a safe and stable digital environment.

Digital reforms in the new Uzbekistan make cybersecurity strategically important. Along with the development of e-government, digital economy, artificial intelligence and innovative technologies, cyber threats are also becoming more sophisticated. Therefore, strengthening cybersecurity is emerging as one of the priorities of state policy.

In conclusion, cybersecurity is an important prerequisite and an integral component of the progress of an information society. It manifests itself as a complex social institution that serves not only to protect information systems, but also to ensure the interests of the individual, society and the state. The increasing sophistication of modern cyber threats requires an integrated approach to the issue of cybersecurity. In this regard, along with technological tools, it is necessary to improve the socio-philosophical mechanisms for the development of cybersecurity, based on information culture, digital literacy, social responsibility and institutional cooperation.

References:

1. Bell D. The Coming of Post-Industrial Society. – New York: Basic Books, 1973.
2. Castells M. The Rise of the Network Society. – Oxford: Blackwell Publishers, 2010.
3. Kaspersky E. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford University Press, 2018.
4. Toffler A. The Third Wave. – New York: Bantam Books, 1980.

5. Назаров Қ. Ғ., Шермухамедова Н. А. Фалсафа асослари. – Тошкент: Ўзбекистон, 2018.
6. Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги Қонуни. – Тошкент, 2022.
7. Туленов Ж.Т., Гофуров З. Фалсафа. – Тошкент: Ўқитувчи, 2016.