

INFORMATION SOCIETY AND THE ESSENCE OF SOCIO-
PHILOSOPHICAL CONTENT OF CYBERSECURITY CONCEPTS**Khamidov Shukurullo Muqimjon oglu**

Researcher of Fergana State University

ORCID:0009-0005-4429-3188

shukurulloxamidov2695@gmail.com

<https://doi.org/10.5281/zenodo.21836193>

Abstract: The article analyzes the socio-philosophical aspects of the concepts of the information society and cybersecurity. Highlights the factors of the formation of the information society, its role in modern development, as well as the importance of cybersecurity in ensuring the security of the individual, society and the state.

Keywords: information society, cybersecurity, information security, digital transformation, information culture, digital literacy, cyber threats, social security.

In the 21st century, human progress is characterized by the rapid development of information and communication technologies. In modern society, information is not only a means of communication, but has become an important resource of economic, political and cultural development. The result is a process of transition from a traditional industrial society to an information society. This process covers all spheres of human activity and causes a radical change in the system of social relations.

Along with the formation of the information society, the issues of information security and cybersecurity also become relevant. This is because the widespread application of digital technologies has led to an increase in cybercrime, information manipulation, illegal dissemination of personal information and other types of threats. Therefore, cybersecurity today is being studied not only as a technological, but also as a socio-philosophical problem.

For the first time the concept of information society was introduced into scientific circulation in the second half of the twentieth century, it was used to denote a new stage of society's development. Scientists such as D. Bell, M. Castels, Y. Masuda, A. Toffler made an important contribution to the formation of the theory of the information society, analyzing the role of information and knowledge in social development. In particular, D. Bell in the concept of post-industrial society interpreted knowledge and information as the main factor of development[1].

In the information society, information acquires the status of a strategic resource. Knowledge and innovation come to the fore as the main source of economic development. In such a society, human capital, intellectual potential and



innovation activity become the decisive factor for development. As a result, information production, processing and distribution become an important branch of the economy[2].

M. Castels describes the information society as a "networked society". He considers that a special feature of modern society is the realization of social, economic and political relations through global information networks[3]. This approach shows that the information society is inextricably linked with the processes of globalization.

With the formation of the information society new opportunities have arisen, the risks associated with it also increase. Especially as a result of the expansion of cyberspace, cyber threats have a serious impact on the progress of modern society. Therefore, the concept of cybersecurity is gaining importance both scientifically and practically.

Cybersecurity concept means information systems, networks, software tools and a set of measures aimed at protecting data from malicious access, corruption, destruction or alteration[4]. However, modern research is interpreting cybersecurity not just as a technological phenomenon but as a complex system that is intertwined with social, political, and cultural factors.

From a socio-philosophical perspective, cybersecurity is a new form of security aimed at protecting the interests of people, society and state. It is closely linked to the individual's right to freedom of information, data integrity, social sustainability and safeguarding the national interest. It is therefore necessary to consider cybersecurity not only as a technical problem but also as a social institution.

One of the critical components of cybersecurity is information culture. Information culture expresses the skills of a person to work with information, select it, analyze it and use it rationally. Societies with developed information cultures tend to be highly immune to disinformation, moral manipulation, and other cyber threats[5].

Digital literacy is also one of the important social determinants of cybersecurity. In today's environment, most people use the internet and digital technologies. Therefore, the fact that users know and follow cybersecurity rules is becoming an important condition for ensuring information security.

In the context of globalization, cyber threats are acquiring a transnational character. Cybercrime, malware, phishing attacks, disinformation campaigns, and social engineering methods pose serious threats to international security. Such





threats have a negative impact not only on individuals, but also on the economic and political stability of entire states.

The effects of cyber threats on an individual are manifested in breach of his/her personal information, financial damage, and psychological pressures. At the community level, there is information manipulation, the spread of misinformation, and a decline in social trust. And at the state level, cyberattacks on strategic infrastructures pose a threat to national security.

In this context, the cooperation of the state, civil society and educational institutions is crucial in ensuring cybersecurity. The state will create a regulatory framework, civil society will develop an information culture, and the education system will develop the necessary knowledge and skills in cybersecurity. As a result of the interaction of these institutions, a secure digital environment is formed.

Digital transformation processes being implemented in the new Uzbekistan make the issue of cybersecurity one of the priority areas of state policy. The development of e-government, digital economy and artificial intelligence technologies require the development of new mechanisms for cybersecurity. In this regard, the importance of scientific approaches and socio-philosophical research in ensuring cybersecurity is increasing.

In conclusion it can be said that information society is the very important stage of modern development, where information and knowledge are manifested as the main strategic resource. The sustainable development of this society is directly related to the effective provision of cybersecurity. The socio-philosophical content of cybersecurity is that it serves not only to protect information systems, but also to ensure human interests, social stability and national security. Therefore, in the development of cybersecurity, along with technological approaches, special attention should be paid to such factors as information culture, digital literacy and social responsibility.

Adabiyotlar:

1. Bell D. The Coming of Post-Industrial Society. – New York: Basic Books, 1973.
2. Toffler A. The Third Wave. – New York: Bantam Books, 1980.
3. Castells M. The Rise of the Network Society. – Oxford: Blackwell Publishers, 2010.
4. Kaspersky E. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford University Press, 2018.
5. Назаров Қ. Ғ., Шермухамедова Н. А. Фалсафа асослари. – Тошкент: Ўзбекистон, 2018.
6. Туленов Ж. Т., Гофуров З. Фалсафа. – Тошкент: Ўқитувчи, 2016.



POLAND

CURRENT APPROACHES AND NEW RESEARCH IN MODERN SCIENCES

International scientific-online conference



POLAND

7.Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида” ги Қонуни. –
Тошкент, 2022.