E- Global Congress
Hosted online from Dubai, U. A. E., E - Conference.
Date: 30th January 2024
Website: https://eglobalcongress.com/index.php/egc
ISSN (E): 2836-3612

THE ROLE AND NORMATIVE-LEGAL BASES OF CYBER SECURITY IN THE DIGITAL ECONOMY

Azizbek Hasanov
independent researcher, High School of Business and Entrepreneurship under the Cabinet of Ministers of the Republic of Uzbekistan, Republic of Uzbekistan, Tashkent
E-mail: ai.xasanov@gmail.com

.

Abstract

Accuracy and reliability of data are essential to data-driven decision making. Data authenticity plays a major role in this, and we adhere to legal norms and standards. Also, with the development of ICT, security in data storage and sharing (cyber security) is coming to the fore. These issues will be discussed below.

Keywords: cybersecurity; risk; analysis of the external environment; choice of strategy; strategy implementation; evaluation and control of implementation; team development; effectiveness of interaction; critical thinking.

In the digital economy, where information and communication technologies support almost all aspects of business and society, cybersecurity plays a major role in ICT management. As organizations increasingly rely on digital tools and interconnected systems, they become more vulnerable to cyber threats and attacks. Effective cybersecurity management is critical to protecting critical data, protecting critical infrastructure, and ensuring business continuity[1]. Ensuring cyber security in ICT management includes the following steps:

1. Assessing the extent of the threat

A key aspect of cybersecurity in ICT management involves assessing the evolving threat landscape. From traditional malware and phishing attacks to sophisticated nation-state cyber espionage, cyber threats are constantly evolving. Organizations should conduct thorough assessments to understand the specific threats that may be targeting their ICT infrastructure and data[2].

[1] Calderaro A., Craig A. J. S. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building //Third World Quarterly. – 2020. – Т. 41. – №. 6. – С. 917-938.
[2] Bhardwaj G. et al. Cyber Threat Landscape of G4 Nations: Analysis of Threat Incidents & Response Strategies //2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). – IEEE, 2021. – С. 75-79.

ISSN (E): 2836-3612

2. Risk management strategies

Once threats are identified, cybersecurity professionals work with IT management teams to develop robust risk management strategies. These strategies include assessing the potential impact of cyber threats, vulnerabilities, and vulnerabilities and prioritizing mitigation efforts accordingly.[3] Risk management security may include implementation of governance, encryption, access control, and incident response plans.

3. Eligibility and Regulation

Governments in many regions have adopted regulations and standards governing cybersecurity practices in various industries. Effective ICT governance involves ensuring compliance with these regulations, which may include requirements for data protection, incident reporting and cyber security audits[4].

4. Safety by design

A proactive approach to cyber security involves integrating security into ICT systems and processes from the outset. Known as "security by design", this principle emphasizes that security should be an integral part of system architecture and software development, rather than an afterthought. It includes secure coding practices, threat modeling, and secure software development lifecycles.[5]

5. Informing and training employees

The human element remains an important factor in cyber security. Employees can inadvertently expose organizations to risks through actions such as clicking on phishing emails or using weak passwords. Part of ICT governance includes employee awareness and training programs to increase cybersecurity literacy and encourage secure behavior.

6. Incident Response and Recovery

Despite preventive measures, cyber incidents can still happen. Effective ICT management includes developing robust incident response plans. These plans outline how organizations should respond when a cyber incident is detected, including prevention, mitigation and recovery measures.

[3] Sulistyowati D., Handayani F., Suryanto Y. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss //JOIV: International Journal on Informatics Visualization. – 2020. – Т. 4. – №. 4. – С. 225-230.

[4] Mirtsch M. et al. Information security management in ICT and non-ICT sector companies: A preventive innovation perspective //computers & security. – 2021. – Т. 109. – С. 102383.

[5] Стасюк К. А., Бойченко О. В., Акинина Л. Н. РОЛЬ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ //Теория и практика экономики и предпринимательства. – 2023. – С. 123-125.

7. Third Party Risk Management

In today's interconnected business environment, companies often partner with third-party vendors and service providers. ICT governance involves assessing and managing the cybersecurity posture of these third parties, ensuring that they meet cybersecurity standards and do not introduce vulnerabilities.[6]

8. Continuous monitoring and improvement

Cybersecurity is not a one-time effort, but an ongoing process. ICT management teams work to implement continuous monitoring solutions that assess the security of ICT systems in real time. This allows for early detection of anomalies and quick response.[7]

In conclusion, cybersecurity plays an important role in ICT governance in the digital economy. This includes threat assessment, risk management, regulatory compliance, design of secure systems, employee training, incident response planning, and continuous monitoring systems. An effective cybersecurity strategy integrated into ICT governance is essential to protect organizations from cyber threats and ensure the secure operation of digital systems.

The management of information and communication technologies in the digital economy is closely connected with the regulatory framework that regulates these technologies. In an interconnected and information-driven world, countries around the world have recognized the need for comprehensive legal guidelines and regulations to ensure the responsible and safe use of ICT. As Uzbekistan pursues digital transformation and economic growth, it has created a legal framework for managing ICT governance. In this section, we will study the international and local regulatory frameworks that play a decisive role in the formation of ICT management practices in Uzbekistan.

International norms and standards

The digital economy transcends borders and therefore international norms and standards have been established to facilitate global cooperation and harmonize ICT regulations. Uzbekistan has incorporated these norms and standards into the

[6] Alazab M. et al. Federated learning for cybersecurity: Concepts, challenges, and future directions //IEEE Transactions on Industrial Informatics. – 2021. – Т. 18. – №. 5. – С. 3501-3509.
[7] Gunduz M. Z., Das R. Cyber-security on smart grid: Threats and potential solutions //Computer networks. – 2020. – Т. 169. – С. 107094.

legal base in harmony with its peers in the world. Below are the main international documents and agreements that provide ICT management in Uzbekistan:

United Nations Consumer Protection Guidelines (1985): Adopted by the United Nations General Assembly, these guidelines set out the principles for consumer protection related to electronic commerce, data protection, and privacy.[8]

Budapest Convention on Cybercrime (2001): Also known as the Cybercrime Convention, this treaty provides a legal framework for combating cybercrime, including offenses involving computer systems, data, and content.

EU General Data Protection Regulation (2018): Although the regulation originated in the EU, it has influenced data protection standards around the world. It establishes rules for the processing of personal data, which provides more privacy and control for individuals.[9]

World Trade Organization (WTO) Agreements: Uzbekistan is a member of the WTO and adheres to its trade-related agreements, some of which relate to electronic commerce and intellectual property rights, which indirectly affect ICT governance.

International Telecommunication Union (ITU) standards: ITU sets global standards for telecommunications, including standards related to ICT infrastructure and network management, which Uzbekistan follows to ensure compatibility with global networks.

Compliance with international standards

The regulatory framework of ICT management in Uzbekistan has been developed in accordance with international norms and standards. This approach ensures that Uzbekistan's ICT governance practices are in line with global requirements, promotes international cooperation, trade and information exchange, while safeguarding national interests and security. We must emphasize that the regulatory framework of ICT management in Uzbekistan is firmly established in international norms and standards, and solves national needs and priority tasks. This balanced approach is essential in meeting the challenges and opportunities presented by the digital economy.

[8] Benöhr I. The United Nations guidelines for consumer protection: Legal implications and new frontiers //Journal of consumer policy. – 2020. – Т. 43. – №. 1. – С. 105-124.
[9] Штепура У. А. Общий регламент защиты данных: основные правовые идеи и проблемы реализации. – 2020.

In conclusion, Uzbekistan has developed a multifaceted legal framework that regulates various aspects of ICT management and digital transformation. These regulations are designed to protect consumers, ensure data privacy, strengthen cybersecurity, and encourage digital innovation. Uzbekistan aims to develop a safe and competitive digital economy, protecting the rights and interests of citizens and businesses through compliance with international standards and agreements. The dynamic nature of the digital economy is relevant in a rapidly changing environment and means the importance of constantly reviewing and adapting these rules to remain effective.

List of used literature:

I. Law and Code of the Republic of Uzbekistan

1. Decree of the President of the Republic of Uzbekistan dated January 28, 2022 No. PF-60 "On the development of the new development strategy of Uzbekistan for 2022-2026".
2. Decree of the President of the Republic of Uzbekistan dated July 15, 2008 No. PF-916 "Additional policy on the promotion of innovative projects and technology development".
3. Decision No. 253 dated June 30, 2000 of the Administrative Court of the Republic of Uzbekistan on the issue of establishing the activities of the joint-stock company "Uzbektelecom".
4. Measuring the Information Society Report Volume 1. 2018. ITUPublications. Statistical reports. International Telecommunication Union. Place des Nations. CH-1211 Geneva Switzerland.
5. Statistical information of the State Statistics Committee of the Republic of Uzbekistan.
6. Statistical information of the Republic of Uzbekistan on the promotion of information technology and communication.
7. Statistical information of "Uzbektelecom" JSC.