http://uzresearchers.com

XALQARO ANIQ FANLAR TAHLILI

The importance of cybersecurity interpretation in ensuring the development of digital Uzbekistan

Axmedov Umidjon Sadriddin o'g'li
Senior Lecturer of the Department of Information Technology of Samarkand Institute of Economics and services
umidjonaxmedov888@gmail.com

Abstract: *The article "The importance of cybersecurity interpretation in ensuring the development of digital Uzbekistan" examines the importance of cybersecurity interpretation for ensuring the secure development of Uzbekistan in the context of digital transformation. Introducing the problems of digital development of Uzbekistan and the growth of cybersecurity threats, the article draws attention to the importance of interpretation in understanding and analyzing threats, developing strategies and making decisions.*

The article examines the role of cybersecurity in the development of digital Uzbekistan, including an overview of the current state of digital infrastructure and the level of cybersecurity. The main threats that Uzbekistan faces, including cybercrime, information system vulnerabilities and cyber attacks on critical infrastructure, are indicated.

Further, the article draws attention to the concept of interpretation in the context of cybersecurity, defining it as the process of analyzing and understanding threats, events, and data related to cybersecurity. It is explained that interpretation includes not only technical analysis, but also analysis of social, economic and political aspects of cybersecurity.

The article goes on to provide examples of successful applications of the cybersecurity interpretation in other countries, such as the United States, Estonia, and Israel. The advantages of developing a national cybersecurity interpretation strategy for Uzbekistan, including coordination of efforts, setting priorities, developing the human resources base and international cooperation, are presented.

The article concludes with an emphasis on the need to develop a national strategy for interpreting cybersecurity for Uzbekistan in order to ensure the country's safe development in the digital age. The authors call for awareness of the importance of interpreting cybersecurity and taking appropriate measures for the development of cybersecurity in Uzbekistan.

Keywords: *interpretation, cybersecurity, development, digital Uzbekistan, digital transformation, threats, information technologies, security, strategy, vulnerabilities, analysis, coordination, education, cooperation, resources.*

Introduction: The modern development of Uzbekistan is closely linked to the use of information technologies and digital solutions. More and more sectors of the economy and public services are moving to the digital format of work, which brings significant benefits, but also causes an increase in cybersecurity threats. In this context, it is necessary to ensure the safe functioning of the digital space, which makes the interpretation of cybersecurity an important factor for the development of Uzbekistan. The gradual transition to a digital economy and digital government leads to an increase in the volume of digital data, the processing and transmission of which requires reliable protection. However, along with progress, new types of threats are emerging, such as hacker attacks, viruses, cyber espionage, and much more. These threats can lead to major information losses, disruption of critical infrastructure, and negative consequences for the economy and society as a whole.

Effective measures are required to ensure security in the digital space. However, technical and software solutions are not effective enough without a proper interpretation of cybersecurity. Interpretation in this context means understanding and analyzing cybersecurity threats, as well as making appropriate decisions and recommendations to ensure the security of information systems and data.

The significance of the interpretation of cybersecurity in ensuring the development of Uzbekistan is as follows:

1. Understanding threats: Interpretation helps to understand and assess potential threats that Uzbekistan may face. This includes both general threats and specific vulnerabilities specific to the country and region.
2. Strategic decision-making: Through interpretation, governments and organizations can develop effective cybersecurity strategies and policiesкибербезопасности. This allows you to identify priority areas for protection and resource allocation.
3. Competence development: Interpreting cybersecurity requires specialized knowledge and skills. Training and professional development of specialists in this field help to create a human resource base for effective protection of information systems.
4. Collaboration and information exchange: The interpretation of cybersecurity allows you to create networks of cooperation between organizations, government agencies, and international partners. The exchange of experience and information helps to improve the effectiveness of protection against cyberthreats.

In general, the interpretation of cybersecurity plays a key role in ensuring the safe and sustainable development of digital Uzbekistan. Proper understanding of threats, development of appropriate strategies and development of competencies in this area are integral components of creating a reliable digital space that can support the stability and development of the country.

The role of cybersecurity in the development of digital Uzbekistan:

Overview of the current state of digital infrastructure in Uzbekistan and the level of cybersecurity:

1. Digital Infrastructure Overview: Analyze the current state of digital infrastructure in Uzbekistan, including assessing the level of information technology development, broadband Internet availability, the level of digitalization of government and business sectors, and the level of digital literacy of the population.
2. Оценка уровня Cybersecurity Assessment: Examine the current level of cybersecurity in Uzbekistan, including cybersecurity regulation and legislationкибербезопасности, the availability of a national cybersecurity and incident response strategy, critical information infrastructure protection mechanisms, the availability of a cybersecurity incident monitoring and detection systemкибербезопасности, and the level of cybersecurity awareness and training of personnelкибербезопасности.

Threats that Uzbekistan faces in the field of cybersecurity:

- Cybercrime and hacker attacks: Consider the various types of cybercrimethat Uzbekistan faces, including hacking, phishing, fraud, malware, and others. Study the impact of these attacks on government organizations, the business sector, and the public.
- Information System Vulnerabilities: Describe the main vulnerabilities faced by information systems in Uzbekistan, including software flaws, incorrect system configuration, insufficient network protection, etc. Pay attention to vulnerabilities related to the digitalization of public services, banking systems, e-commerce, and other sectors.
- Cyber Espionage and Cyber attacks on critical infrastructure: Consider the threats associated with cyber espionage and possible cyber attacks on critical infrastructure, such as energy systems, transportation networks, banking systems, and communications networks. Study the potential consequences of such attacks and their impact on the country's development.
- Social engineering and human factor attacks: Pay attention to the role of social engineering in cyber attacks and threats related to the human factor. Consider examples of phishing attacks, identity theft, social media fraud, and other types of attacks that can target users in Uzbekistan.
- Cyber threats in the field of education and research: Consider the threats associated with the digitalization of educational and scientific organizations, including cyber

attacks on universities, theft of intellectual property, violation of privacy, etc. Explore the implications of these threats for the development of education and research in Uzbekistan.

It is important to conduct a comprehensive analysis of the current state of digital infrastructure and cybersecurity threats in Uzbekistan in order to identify the necessary measures to improve cybersecurity and ensure the country's safe development in the digital age.

The concept of interpretation in the context of cybersecurity refers to the process of analyzing and understanding threats, events, and data related to cybersecurityin order to identify their significance, potential consequences, and develop appropriate strategies and solutions.

Interpretation in cybersecurity includes not only technical analysis of computer systems and networks, but also broader analysis of social, economic and political aspects related to cybersecurity. It is based on the collection and analysis of various data and information about potential threats, their sources, methods and goals, as well as vulnerabilities in systems and methods of their operation.

In the process of interpreting cybersecurity, experts and analysts evaluate, analyze and compare data about the current situation, previous incidents, threat signals, and information about new vulnerabilities. They seek to identify the nature of the threat, its potential consequences, and possible ways to prevent or mitigate the threat.

Interpretation in cybersecurity requires a wide range of knowledge and skills, including understanding different types of attacks, methods for detecting and preventing incidents, analyzing logs and data, as well as the ability to assess risks and make decisions based on the information received.

An important aspect of cybersecurity interpretation is the ability to distinguish critical threats from minor incidents, as well as the ability to adapt to a changing угрознойthreat environment and quickly respond to new types of attacks and vulnerabilities.

As a result, interpretation in the context of cybersecurity allows you to assess threats, analyze their impact on target systems, and develop appropriate strategies and measures to ensure the security of information systems and data.

Applying the interpretation of cybersecurity in the context of Uzbekistan can have a number of important advantages and bring significant benefits for ensuring the secure development of the country's digital space. The following are examples of successful applications of cybersecurity interpretation in other countries, as well as the need to develop a national cybersecurity interpretation strategy for Uzbekistan.

Examples of successful implementation of the cybersecurity interpretation in other countries:

1. USA: The United States has a well-developed system of cybersecurity interpretationthat includes government agencies, the private sector, and academia. The use of cybersecurity interpretation has enabled the United States to develop and adopt effective strategies to ensure the security of information systems and data, as well as coordinate responses to cyberattacks.
2. Estonia: Estonia is an example of a country that has invested heavily in cybersecurity and developed a national strategy for interpreting cybersecurity. Thanks to this, Estonia was able to create reliable information security systems and develop the cybersecurity sector as a key sector of the economy.
3. Israel: Israel is one of the leading countries in the field of cybersecurity. The application of the cybersecurity interpretation has enabled Israel to develop advanced technologies and innovative solutions to protect information and combat cyberthreats. The interpretation helped the country actively analyze threats and develop appropriate countermeasures.

   The need to develop a national cybersecurity interpretation strategy for Uzbekistan:

- Coordination of efforts: The development of a national cybersecurity interpretation strategy will allow coordination of actions of government agencies, the private sector and educational institutions in the field of cybersecurity. This facilitates efficient use of resources and synchronization of actions of all stakeholders.
- Prioritization: The National Cybersecurity Interpretation Strategy will help identify priority areas for protecting and developing cybersecurity in Uzbekistan. It will help you identify the main threats, the most important facilities and infrastructure, and improve your understanding of risks and vulnerabilities.
- Human resource development: The development of a national strategy for interpreting cybersecurity encourages the development of educational programs and advanced training of specialists in the field of cybersecurity. This will create a human resource base that can effectively deal with cybersecurity threats and develop innovative solutions.
- International cooperation: The National Cybersecurity Interpretation Strategy promotes international cooperation in the field of cybersecurity. Uzbekistan can

strengthen its partnerships with other countries and international organizations, share experiences and information on new threats and best protection practices.

The development of a national cybersecurity interpretation strategy for Uzbekistan is an important step in ensuring the country's secure development in the digital age. It will allow efficient use of resources, identify priorities, develop the human resources base, and develop strategies that meet the specific threats and needs of Uzbekistan.

Licture:

1. Шодиевич, Ш. Ҳ., Эрматов, Н. Ж., Расулова, М. Р., Шодиев, Ж. Х., & Хожаназарова, С. Ж. (2023). MICROSOFT EXCEL ЭЛЕКТРОН ЖАДВАЛИДАН ФОЙДАЛАНИБ ИЛМИЙ ТАДҚИҚОТ НАТИЖАЛАРИНИ СТАТИСТИК ҲИСОБЛАШ. INTERNATIONAL JOURNAL OF RECENTLY SCIENTIFIC RESEARCHER'S THEORY, 1(4), 67-75.
2. Валентин Пашинцев**.** Кибербезопасность. Основные угрозы и их нейтрализация Internet Society – общемировая общественная организация под управлением широкого попечительского совета [Электронный ресурс]. http://www. internetsociety.org/sites/default/files/bpdeconstructing-cybersecurity-16nov-update. doc.doc_RU_121712.pdf «Взгляды на кибербезопасность: 2012г.» CNews – [электронный ресурс]. http://www. cnews.ru/top/2013/03/13/android_zahvatil_kitay_vlasti_byut_trevogu_522278 – «Android захватил Китай. Власти бьют тревогу»
3. CNews|безопасность – [электронный ресурс] Сергей Попсулин – http:// safe.cnews.ru/news/top/index. shtml?2013/08/02/537614&utm_ source=twitterfeed&utm_medium=twitter «ФБР способна удаленно включать микрофоны в смартфонах Android»
4. Гарнаева М.А., Функ К. Kaspersky security bulletin 2013 // Вопросы кибербезопасности. 2014. №3. С.65-68