UPHOLDING INFORMATION SECURITY IN THE ECONOMY

Kamalov Otabek Erkin o'g'li
Kamalov Ulug'bek Erkin o'g'li
Master of Karakalpak State University named after Berdakh

Annotation: *In this thesis, I will explore the critical role of information security in the economy, focusing on Uzbekistan's experience with cybercrimes in 2023. The thesis will examine the impact of cybercrimes on the economy, particularly in the context of e-commerce and digital transactions. It will also analyze the measures taken by Uzbekistan to ensure information security within the economy in response to the cybercrime challenges faced in 2023.*

Keywords: *Information security, data, cybercrimes, economy, cyber threats.*

THE ROLE OF INFORMATION SECURITY IN THE ECONOMY

Information security plays a critical role in the modern economy, influencing various aspects of businesses, governments, and individual consumers. Its impact extends across multiple dimensions, underpinning the stability, trust, and growth of economic systems. Here's an overview of the role of information security in the economy:

a) Safeguarding Sensitive Data and Intellectual Property

Information security measures are essential for protecting sensitive data, including financial records, customer information, and proprietary business data. By safeguarding this information, businesses can maintain trust and confidence among customers, partners, and stakeholders, thus fostering a healthy economic environment.

b) Enhancing Consumer Trust and Confidence

A secure information environment fosters consumer trust and confidence. When individuals feel assured that their data is protected, they are more likely to engage in economic activities, make purchases, share personal information, and participate in digital interactions, thus contributing to economic vibrancy.

c) Mitigating Cybersecurity Risks and Economic Threats

Information security measures help mitigate the risks associated with cyber threats, including financial fraud, data theft, and disruptions to critical infrastructure. By proactively managing these risks, information security contributes to economic stability and overall resilience in the face of potential threats.

Impact of Cybercrimes on the Economy

The proliferation of cybercrimes has far-reaching implications for economic growth and consumer trust. With the increasing reliance on digital platforms for commercial transactions, cybercrimes can erode consumer confidence and impede the growth of e-commerce. Moreover, the disruption caused by cybercrimes can lead to financial losses for businesses and individuals, thereby hampering overall economic progress.

Uzbekistan faced 5,500 cybercrimes in 2023

Currently, there are about 50 different payment systems in Uzbekistan. However, not all of them meet the necessary requirements for protection against cyber threats. Around 70% of cybercrimes in 2023 will be fraud and theft, mostly related to bank cards. Addressing this issue requires government ministries and agencies to create and implement strong cybersecurity regulations for all electronic payment systems.

Work done to ensure information security in the economy in 2023

In 2023, the work aimed at ensuring information security in the economy has involved a range of efforts and initiatives to address evolving cyber threats, protect sensitive data, and foster a secure digital environment. Here are some key areas of work that have been notable in the ongoing efforts to bolster information security in the economy:

1. Advancements in Cybersecurity Technologies: There has been a focus on investing in and adopting advanced cybersecurity technologies, including next-generation firewalls, threat intelligence platforms, and advanced endpoint security solutions, to enhance the overall resilience of digital systems and safeguard critical infrastructure.

2. Emphasis on Data Protection and Privacy Compliance: Organizations have continued to prioritize compliance with data protection regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other regional data privacy laws to ensure the lawful and ethical use of consumer data, thereby fortifying consumer trust and data integrity.

3. Cybersecurity Awareness and Training Programs: Efforts have been directed towards increasing cybersecurity awareness among employees and individuals, coupled with ongoing training programs to empower personnel with the knowledge and skills needed to identify, mitigate, and report potential cybersecurity threats and incidents.

4. Focus on Secure Digital Payments and Fintech Security: Given the increasing reliance on digital payment platforms and financial technology solutions, there has been a concerted effort to bolster the security of digital payment systems, enhance transaction security, and combat financial

cybercrime, thereby fortifying the trust and integrity of digital financial transactions.

5. Application Security and Secure Software Development: Emphasis has been placed on secure application development practices and secure coding methodologies to address vulnerabilities at the software level, aiming to reduce the risk of software exploits, data breaches, and systemic vulnerabilities in digital applications and platforms.

6. Artificial Intelligence and Machine Learning for Threat Detection: The utilization of artificial intelligence and machine learning for advanced threat detection, behavior analysis, and anomaly detection has gained momentum, enhancing the ability to identify and mitigate complex cyber threats in real time.

7. International Collaboration on Cybersecurity Standards and Best Practices: Continued efforts have been made to foster international collaboration and information sharing on cybersecurity standards, best practices, and threat intelligence to build a global defense against cyber threats and promote a unified approach to information security.

These ongoing multifaceted efforts underline the comprehensive approach taken to bolster information security in the economy in 2023, aiming to create a resilient, secure, and trustworthy digital environment conducive to economic growth and innovate

In summary, information security serves as a foundational element in fostering trust, stability, and growth within the economy. By safeguarding sensitive data, fostering innovation, enabling resilient business operations, and building consumer confidence, robust information security measures contribute to the overall health and prosperity of economic systems.

Information security plays a pivotal role in creating a safe, trustworthy, and resilient environment for e-commerce and digital transactions, safeguarding consumer data and fostering a conducive atmosphere for business expansion, consumer engagement, and global e-commerce growth.

REFERENCES:

1. Journal of Innovation in Economics
2. internet resources