AJPDIS
GLOBAL RESEARCH NETWORK

AMERICAN Journal of Public Diplomacy and International Studies
Volume 02, Issue 04, 2024 ISSN (E):2993-2157

Problems in Organizing the Economic Security System of Enterprises

Shodmanova Zubayda Ubaydullayevna
SamISI is an assistant at the "Economic theory" department

Abstract: This article examines the main problems faced by enterprises in the organization of the economic security system. The conditions for achieving economic security are presented through a comprehensive risk assessment.

Keywords: Economic security, information security, outsourcing, globalization and international threats, scalability and flexibility.

Economic security is an important aspect for the stable operation and development of any enterprise. It includes the various measures and strategies that organizations implement to protect themselves from internal and external threats that may threaten their financial stability, reputation, and overall well-being. However, despite the importance of economic security, many businesses face difficulties in establishing and maintaining an effective economic security system. This article examines some of the main problems encountered in the organization of the economic security system of enterprises.

Failure to carry out a comprehensive risk assessment is considered one of the main issues of the organization of economic security systems, and this is the lack of a comprehensive assessment of risks. Businesses often fail to fully analyze the potential threats, vulnerabilities and risks they may face. This can lead to failure to identify critical areas that require attention and adequate protection. Without a comprehensive risk assessment, organizations can overlook potential risks, making them more susceptible to financial losses, fraud, cyber attacks and other security breaches.

Information security is an important component of economic security in today's digital age. However, many businesses struggle to implement appropriate information security measures. This problem can be caused by a lack of awareness of emerging cyber threats, limited resources dedicated to information security, or failure to implement robust security protocols. Inadequate information security measures can expose businesses to data breaches, intellectual property theft, and operational disruptions that can result in significant financial and reputational damage.

Improper internal control shows that effective internal control is important for ensuring economic security in the organization. However, some businesses have difficulty establishing and maintaining a robust internal control system. Issues such as poor division of duties, lack of control, and insufficient monitoring mechanisms can undermine the integrity of financial processes and increase the risk of fraud and embezzlement. Inadequate internal controls can also hinder the detection and prevention of operational inefficiencies and irregularities, further jeopardizing economic security.

Numerical errors and carelessness in informing and training employees can seriously threaten the economic security of the organization. Inadequate employee awareness and training on security

protocols and best practices can increase vulnerabilities within an enterprise. Employees may unknowingly engage in risky behavior, fall victim to social engineering attacks, or mishandle sensitive information. Businesses should invest in comprehensive training programs to educate employees about the importance of economic security, potential risks and necessary preventative measures.

Lack of cooperation and coordination Establishing economic security systems often requires cooperation and coordination between different departments and stakeholders within the enterprise. However, many organizations struggle with establishing effective communication channels and developing a collaborative culture. A lack of departmental and cross-functional cooperation can prevent timely information sharing, hinder risk mitigation efforts, and undermine the overall effectiveness of the economic security system.

There are several additional points to expand the problems in the organization of the economic security system of enterprises:

The rapid development of the rapidly evolving technological landscape creates opportunities and challenges for enterprises' economic security systems. New technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence (AI) will increase efficiency and productivity, but also create new vulnerabilities. Businesses can struggle to adapt to the evolving technology landscape and adequately protect their systems and data from emerging threats. Staying abreast of the latest security trends and adopting a proactive approach to implementing appropriate safeguards is critical to maintaining economic security.

In today's interconnected business environment, with the risks of outsourcing (giving a portion of your company's operations a service function to another organization) and supply chain risks, many businesses rely on outsourcing and have complex supply chains. While outsourcing can offer cost savings and specialized expertise, it also poses additional risks to economic security. Dependence on third-party vendors can expose businesses to data breaches, intellectual property theft, or supply chain disruptions. To mitigate these risks, it is critical to ensure that appropriate security measures are in place in outsourcing and supply chain processes. Exploring Regulatory Compliance Challenges Businesses must navigate the complex landscape of economic security-related regulations and compliance requirements. Complying with laws and industry standards, such as data protection regulations or financial reporting requirements, can be challenging for organizations, especially those operating in multiple jurisdictions. Failure to comply with applicable regulations may result in legal consequences, financial penalties, or damage to the organization's reputation. Businesses must allocate resources to ensure ongoing compliance and stay abreast of any changes in the regulatory framework.

Even with strict preventive measures, incidents and crises can still occur due to the lack of response and recovery plans. Businesses can experience natural disasters, cyber attacks or other unexpected events that disrupt their operations and undermine their economic security. However, many organizations lack comprehensive response and recovery plans to effectively deal with such incidents. Without pre-defined strategies and protocols in place, businesses can experience extended downtime, increased financial losses, and reputational damage. It is essential to develop and regularly test response and recovery plans to minimize the impact of impact events.

Inadequate budget allocations require economic security to invest in a variety of resources, including advanced technology, skilled personnel, training programs, and security infrastructure. However, some businesses struggle with budgeting enough to adequately support their financial security systems. Limited financial resources can lead to security breaches, inadequate preparation and outdated technology. Businesses should prioritize economic security in their budget planning to ensure they have the resources they need to effectively protect their assets. It is important for businesses to recognize these issues and take proactive steps to address them.

By prioritizing economic security, conducting regular assessments, implementing robust measures, fostering a culture of security awareness and adapting to evolving threats,

organizations can strengthen their economic security systems and protect their long-term success.

There are several additional points to further expand the problems in the organization of the economic security system of enterprises:

Lack of Continuous Monitoring and Evaluation Effective economic security requires continuous monitoring and evaluation of security measures to identify vulnerabilities and adapt to changing threats. However, many businesses struggle with implementing a robust monitoring and evaluation system. Without constant monitoring, organizations may miss early warning signs of a security breach or fail to identify new risks. Regular evaluation of the effectiveness of the economic security system is important to identify areas for improvement and to ensure that security measures remain relevant and relevant to the evolving threat landscape.

Cultural and Behavioral Issues Building a strong safety culture in an organization is critical to the success of an economic safety system. However, businesses often face cultural and behavioral challenges that prevent them from adopting security best practices. This includes resistance to change, complacency, or a lack of accountability. Overcoming these challenges requires leadership commitment, effective communication, and employee engagement initiatives to foster a safety-focused mindset and encourage responsible behavior within the organization.

Lack of cooperation with external entities Economic security is not only the responsibility of individual enterprises, but also requires cooperation with external organizations such as government agencies, industry associations and law enforcement agencies. However, some organizations struggle with establishing effective collaboration and information sharing mechanisms. Collaboration with external entities provides valuable insights, threat intelligence and regulatory support. Businesses should leverage external expertise and actively engage with relevant stakeholders to strengthen their economic security efforts.

Globalization and International Threats In a global economy that is interconnected, businesses are increasingly exposed to international threats that may affect their economic security. These include risks such as geopolitical instability, cross-border cyber attacks and economic espionage. Businesses operating in multiple countries must navigate different legal and regulatory frameworks and address regionally specific security challenges. Developing a comprehensive understanding of international threats and implementing mitigation strategies is critical to maintaining economic security in a globalized business environment.

Lack of scalability and flexibility Businesses experiencing rapid growth or significant changes in their operations may struggle to appropriately expand and adapt their economic security systems. Improper scalability can lead to a mismatch between an organization's expanding needs and the capabilities of its security infrastructure. Likewise, a lack of flexibility can make it difficult to respond quickly to emerging threats or changing business requirements. Businesses must ensure that their financial security systems are scalable and adaptable, capable of meeting growth and evolving security needs.

Addressing these additional challenges requires a holistic approach to economic security. Enterprises must develop a culture of continuous improvement, leverage technological advances, build strong partnerships, and prioritize flexibility and scalability in their security strategies.

In this way, organizations can increase the stability of economic security and effectively reduce risks to financial stability, reputation and general well-being.

In conclusion, the organization of the economic security system is a complex task that requires careful consideration of various factors. Businesses must address the issues discussed in this article to improve their financial security. Conduct comprehensive risk assessments, implement robust information security measures, strengthen internal controls, increase employee awareness and training, and collaborate. by developing, organizations can reduce risks, protect their assets and ensure long-term stability in an increasingly changing business environment.

List of used literature

1. Дрягунова, Д. М. Финансовоэ состояние предприятия и его анализ / Д. М. Дрягунова – Текст :непосредственний // Молодой учений. – 2018. – №43. – С. 218–220.
2. Погодина, Т. В. Финансовийменеджмент : учебник и практикум / Т. В. Погодина. – М.: Юрайт, 2018. – 351 [1] с.; 22 см. – 7000 экз. – ИСБН 978–5–534–00680–3. – Текст :непосредственний.
3. Шулс, В. Л. Безопасностпредпринимателскойдеятелности : учебник для вузов/ В. Л. Шулс, А. В. Юрченко, А. Д. Рудченко ; под редак-сией В. Л. Шулса. – 2-е изд., перераб. и доп. – М.: Юрайт, 2020. – 585 [1] с.; 22 см. – 5000 экз. – ИСБН 978–5–534–12368–5. – Текст :непосредственний.
4. Десятниченко, Д. Й. Угрози финансовой безопасности устойчи-вого функционирования предприятия / Д. Й. Десятниченко, О. Й. Десятни-ченко, В. В. Остапенко. – Текст :непосредственний // Экономика и бизнес: теория и практика. – 2018. – 4. – С. 75–81.
5. VechkanovG.S. ekonomicheskayabezopasnost: Uchebnikdlyavuzov. –SPb. Piter 2007