Huo Feifei
1st year Master student
Specialty: Management
Academic supervisor: doctor of economics, prof. M. P. Chaikovska

THE INFORMATION SECURITY MANAGEMENT SYSTEM TO ADDRESS GLOBAL CHALLENGES

Given the swift proliferation and extensive utilization of information technology, the significance of safeguarding information security (IS) has ascended to the forefront of global priorities. IS encompasses not only the protection of personal privacy and assets but also intertwines with the economic and security imperatives of businesses and nations. Establishing robust IS frameworks is imperative for poised responses to global challenges.

As information technology becomes increasingly ubiquitous, the global landscape of IS threats manifests characteristics of diversification, complexity, and specialization. Instances of cyberattacks, data breaches, malware infiltration, and related security incidents are alarmingly frequent, resulting in substantial losses for enterprises.

To address the challenges posed by IS threats, governments worldwide have enacted pertinent legislation and regulations aimed at bolstering supervision and safeguarding of information assets. Examples include the European Union's General Data Protection Regulation (GDPR) and the United States' Cybersecurity Act. These legal frameworks impose elevated standards for Information Security Management (ISM) within enterprises and organizations, mandating proactive measures to mitigate risks and ensure compliance [1, p. 16].

As the frequency of IS threats continues to escalate, enterprises and organizations are increasingly prioritizing ISM. There is a growing trend among these entities to implement ISM systems, intensify ISM efforts, and enhance their capabilities for preventing IS incidents.

An ISM system capable of meeting global challenges needs to include the following components:

1. Systematic. The ISM system constitutes a comprehensive and systematic framework encompassing various facets of information security management, including but not limited to security strategy formulation, security organizational structuring, security technology deployment, and security governance mechanisms.

2. Prevention: The primary emphasis of the ISM system lies in prioritizing preventive measures, aiming to avert the occurrence of information security incidents through the establishment of robust security management systems and processes.

3. Dynamic: The ISM system operates as a dynamic management framework, necessitating ongoing adaptation and enhancement in response to evolving information security threats and the specific circumstances of enterprises.

Let's analyze the components of the ISM system.

1. Security policy. Is the core of ISM system, it clarifies the IS goals and policies of enterprises or organizations, and provides guidance for ISM.

2. Security organization. Is an important part of ISM system. It is responsible for establishing and managing ISM team, clarifying security responsibilities and authority, and formulating security management system and process.

3. Security technology is an important support for ISM system, which includes a variety of security technologies and tools, such as firewalls, intrusion detection systems, encryption technology, etc., to protect the security of information systems.

4. Security management is an important part of the ISM system, which includes various security management activities, such as security training, security audit, security monitoring, etc., to ensure the effectiveness and sustainability of ISM.

With the continuous development of artificial intelligence technology, ISM system will become more and more intelligent. For example, artificial intelligence technology is used for security threat warning and security incident analysis.

The ISM system will be more and more:

– visual, and the security data and information will be presented in an intuitive way through visualization technology to help security managers better understand and analyze the security situation;

– automated, through automation technology to achieve the automatic execution of security policies, automatic response to security incidents, improve the efficiency and accuracy of security management.

ISM demands continuous advancement through technological innovation, fostering the research and development of novel security technologies and tools to elevate the proficiency and efficacy of ISM practices. Moreover, addressing the need for a proficient workforce, substantial emphasis must be placed on bolstering personnel training initiatives, establishing comprehensive training frameworks, and augmenting the competence and expertise of ISM personnel.

Government bodies and pertinent institutions must intensify their oversight of IS and fortify efforts in legislating and regulating ISM. This entails enhancing the legal and regulatory infrastructure surrounding ISM to provide robust support and assurance for its effective implementation.

The ISM system serves as a pivotal mechanism for addressing the prevalent global challenges in IS, facilitating the establishment of robust ISM frameworks within enterprises and organizations, consequently enhancing their capabilities in IS management. As IS threats persistently evolve and ISM requirements undergo continuous refinement, the ISM system is poised for ongoing development and enhancement. To effectively confront these challenges on a global scale, it is imperative to bolster international cooperation, foster technological innovation, enhance personnel training initiatives, reinforce regulatory oversight, and continuously refine the legal framework governing ISM. Collaborative efforts aimed at perpetually refining the ISM system are essential for collectively addressing global IS challenges.

References

1. Chaikovska M., Azeev A. Management of information security risk in the protection of continuity of information and communication systems. *Proceedings Innovations – 2018*. 2018. Volume 1 (2). P. 15–19.