УДК 004.056:006

RISK MANAGEMENT PROCESS AS PART OF INFORMATION SECURITY MANAGEMENT SYSTEM

Postgraduate Galina Kupreeva, student gr. 113530 Anna Sherbina
Professor Pavel S. Serenkov
Belarus National Technical University

The risk management process focuses on providing the business with an understanding of risks to allow effective decision-making to be applied to control the risks. The risk management process is an ongoing activity that aims to continuously improve the efficiency and effectiveness of the organization's ISMS implementation.

The risk management process should be applied to the whole ISMS (as specified in ISO/IEC 27001:2013 «Information technology - Security techniques - Information security management systems – Requirements») – that is, all elements of the ISMS. The process needs to be applied at the planning and design stages as well as the subsequent stages of operational deployment, monitoring and review of the risks, and the updating and improvement stages to ensure that any information security risks are always being appropriately managed.

An important part of the risk management process is the assessment of information security risks. This is necessary to understand the business information security requirements, and the risks to the organization's business assets. In ISO/IEC 27001:2013, the risk assessment includes the following actions and activities:

• identification of assets;

• identification of legal and business requirements that are relevant for the identified assets;

• valuation of the identified assets, taking account of the identified legal and business requirements and the impacts of a loss of confidentiality, integrity and availability;

• identification of significant threats to, and vulnerabilities of, the identified assets;

• assessment of the likelihood of the threats and vulnerabilities to occur;

• calculation of risk;

• evaluation of the risks against a predefined risk scale.

The next step in the risk management process is to identify the appropriate actions to be taken for the treatment of each of the risks that have been identified during the risk assessment. Risks can be managed through a combination of prevention and detection controls, avoidance tactics, insurance and/or simple acceptance.