West Pomeranian University of Technology in Szczecin
Faculty of Computer Science

Abstract of doctoral thesis entitled:

Security assessment of ICT systems that process classified information

Author: Damian Kacprowicz, M.Sc.
Supervisor: prof. zw. dr hab. dr h.c. mult. Brunon Hołyst
Auxiliary supervisor: dr inż. Witold Maćków

Advances in information and communications technology have resulted in the majority of organizational activities relying on information processing in ICT systems. On the one side, this makes it easier to collect and transmit information, but on the other, it poses additional risks related to the possibility of criminal copying and modification of data.

The nature of ICT systems requires the use of appropriate safeguards to protect system resources from the various threats to which they are exposed in their production environment. ICT system resources, particularly information resources, are extremely important assets of an organization and require adequate protection, regardless of their form. The security of electronically processed information is of fundamental importance, especially in the case of confidential information subject to statutory protection.

Many standards and recommendations specify the need to assess the level of security for a security perspective. Existing methods are characterized by high complexity and thus prone to error. The use of overly complex methods creates the risk of performing security assessments only at the stage of accreditation of systems and not according to the principles of the application periodically from time to time. Lack of systematicity understates the security level of protected systems.

The research concept includes a review of existing standards, security assessment methods to propose an effective procedure for assessing the security level of an ICT system.

The proposed assessment of security mechanisms will take into account the most important security attributes, i.e. confidentiality, integrity and availability of information content of ICT systems.

The work consists of four chapters.

The first chapter introduces the topic of information security, outlining the basic categories of information that need to be protected, the arguments for securing it, the classification of information, the

classification process and metadata content of digital files, the life cycle of an ICT system, and key aspects of information protection. It also includes highlighting the various factors and threats that can affect their security, as well as the need to focus on risk management and minimizing potential threats.

The second chapter focuses on assessing the level of information security in the system. It consists of several steps to determine the level of information protection and identify the threats and risks associated with it. The first step is to identify the protected information assets and determine their value. This is followed by identification of threats and assessment of their level, which enables identification and estimation of risks. The process is based on an analysis of the value of information, threats and vulnerabilities, and the resulting risk assessment is used to prioritize actions to ensure an adequate level of information security.

The third chapter presents a comprehensive information security assessment method. It consists of steps that include identification of information assets, threats, estimation of the consequences of loss of assets, and risk assessment. It highlights how important it is to maintain the confidentiality, integrity and availability of information, as well as to prevent damage through appropriate protection measures.

The fourth chapter discusses various activities to maintain the assumed level of information security. This includes risk reviews, supervision and control of compliance with security documentation, real-time security monitoring, reporting emerging risks and updating security, and employee awareness and training. The applicability of the proposed method will be determined. All these activities are important to ensure sustainable and effective information security in the system.

In the course of researching the proposed security assessment method, consultations were held with experts (System Accreditation Auditors), stakeholders (Managers of Organizational Units processing sensitive information, System Administrators, ICT Security Inspectors, Managers of Classified Offices and Cryptographic Offices, Users). This provided diverse perspectives and valuable experience.

Damian Kasprowicz

16.05.2024