УДК 004.056.5

I. Yu. Makovskyi, Senior Research Fellow, Research Department
R. V. Netrebko, Senior Lecturer, Higher Education Institution
Korolov Zhytomyr Military Institute

ANALYSIS OF REGULATORY AND INTERNATIONAL STANDARDS FOR THE FORMATION OF SECURITY PROFILES FOR AUTOMATED SYSTEMS

In the context of military conflicts and hybrid confrontation of the 21st century, the systematic assessment of information security risks related to restricted-access information processed and stored in automated systems becomes particularly important for the formation of security profiles. Despite the existence of a regulatory framework in the field of technical information protection, one of the key challenges remains the practical implementation and compliance with the established procedures for information security risk assessment in order to further develop security profiles of different levels.

The main regulatory legal act governing the authorization procedure in the field of security is the Resolution of the Cabinet of Ministers of Ukraine dated June 18, 2025, No. 712. This document establishes unified rules for authorization for all entities operating relevant systems, regardless of their form of ownership or subordination [1]. The legal framework is also complemented by the Law of Ukraine "On Information", the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine", ND TZI 3.6-006-24, ND TZI 2.5-004-99, DSTU ISO/IEC 27001:2023, DSTU ISO/IEC 27002:2023 (adapted national versions), and other regulatory acts.

Let us consider international standards and methodologies for information security risk assessment. ISO 27005 is a standard from the ISO/IEC 2700x series that describes an approach to organizing the entire information security risk management process [2]. The NIST SP 800-30 standard presents approaches not only to risk assessment but also to organizing information security risk management activities at various levels [3]. The CRAMM methodology, developed by the UK Government Security Service, is based on the BS7799 information security management standards and describes an approach to qualitative risk assessment [4]. The OCTAVE method, developed at Carnegie Mellon University, provides for assessing the criticality of threats, assets, and vulnerabilities [5]. The COBIT for Risk methodology [6], developed by the ISACA association, is based on best practices in risk management (COSO ERM, ISO 31000, ISO/IEC 27xxx, etc.). This methodology considers information security risks in relation to the organization's core business risks and describes approaches to implementing information security risk management functions within an organization, as well as processes for qualitative risk analysis and risk management. The BSI

Standard 200-3 methodology (formerly known as IT-Grundschutz Risk Analysis) is a German standard that regulates the approach to information security risk assessment within the IT-Grundschutz framework [7]. This methodology enables effective evaluation and management of risks.

The analysis of most international methodologies has shown that they are often insufficiently productive and informative for practical application in current real-world conditions. The reviewed international standards and methodologies lack clear recommendations and guidelines for implementing a specific algorithm of actions; moreover, they are based on the standards of the countries in which they were developed and primarily determine compliance with a standard rather than the actual level of security. Considering the results of the analysis, it appears appropriate to apply an improved and adapted approach to determining the degree of risk. Such an approach would make it possible to obtain consistent results regardless of the experience and qualifications of the specialist conducting the risk assessment.

References

1. Cabinet of Ministers of Ukraine. Resolution No. 712 of 18 June 2025 "On Approval of the Procedure for Security Authorization of Information and Communication Systems".

2. DSTU ISO/IEC 27005:200.335. Information technology — Security techniques — Information security risk management. Kyiv: SE "UkrNDNC", 200.335. – 60 c.

3. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments [Electronic resource] : National Institute of Standards and Technology. — Gaithersburg, MD : U.S. Department of Commerce, 2012. — 95 p. — Mode of access: https://doi.org/10.6028/NIST.SP.800-30r1.

4. UK Government Commerce. CRAMM: Risk Analysis and Management Method. London : The Stationery Office. URL: https://www.cramm.com.

5. Alberts C., Dorofee A. OCTAVE® Method Implementation Guide (Version 2.0). Pittsburgh : Software Engineering Institute, Carnegie Mellon University, 2001. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419.

6. ISACA. COBIT 2019 Framework: Governance and Management Objectives. Rolling Meadows, IL: ISACA, 2018. URL: https://www.isaca.org/resources/cobit.

7. BSI-Standard 200-3. IT-Grundschutz Methodology: Risk Analysis [Electronic resource] : Federal Office for Information Security. — Bonn : BSI, 2017. — 64 p.