Economic sciences

UDC 004.056.5:658

Obramych Orest
Postgraduate Student of the
Lviv Polytechnic National University

Ivanytskyi Igor
Postgraduate Student of the
Lviv Polytechnic National University

INFORMATION SUPPORT FOR DIAGNOSTICS OF THE LEVEL OF DIGITAL SECURITY AT THE ENTERPRISE

Summary. *The article addresses the issue of ensuring digital security for enterprises in the context of active digitalization of business processes. The author substantiates the need to develop a specialized model of information support for the digital security diagnostics process that meets the needs of Ukrainian enterprises, particularly small and medium-sized businesses. A structured approach to building such a model is proposed, comprising three key components: monitoring and data collection, analytical support, and information-based decision-making support. Special attention is given to the integration of technical and organizational indicators, as well as the development of a classification of digital security levels. The model enables timely risk detection, objective security assessment, and effective managerial decision-making aimed at minimizing digital threats. The article also outlines future research directions related to the automation of diagnostics and adaptation of the model to industry-specific features.*

Key words: *digital security, risk diagnostics, information support, digital transformation, automation, security management.*

In the current conditions of digitalization of economic activity, enterprises are becoming increasingly dependent on the reliable functioning of information systems and the secure circulation of digital data. A high level of automation, the use of cloud services, remote work, and the development of e-commerce are creating new risks for digital security. Digital threats such as cyberattacks, leakage of confidential information, or disruptions in IT infrastructure can have significant consequences for the financial stability, reputation, and competitiveness of enterprises. Therefore, the development of an effective system of information support for the diagnostics of digital security levels becomes an urgent scientific and practical task, as it allows timely identification of risks, prompt response to incidents, and ensures sustainable development.

The issues of enterprise digital security and information support for risk management are actively addressed in both international and domestic research. Andress (2021), in particular, emphasizes the importance of creating flexible security systems at the organizational level that integrate technical, administrative, and procedural controls. Significant contributions have been made by Whitman and Mattord (2022), who propose a multi-level model of information security management based on standardized approaches. González-Varona et al. (2021) underline the need to build digital competence within organizations as a means of increasing adaptability to digital environment risks, especially in small and medium-sized enterprises (SMEs). Moeuf et al. (2017) focus on the transformation of management practices in SMEs under the conditions of Industry 4.0. The authors point out the lack of a systemic approach to monitoring digital risks and the underestimated role of information flows in supporting security.

Ukrainian research also shows growing interest in digital security issues. For instance, Lysak (2024) proposes methodologies for assessing the level of digitalization and managing related risks at industrial enterprises, emphasizing the need for unified indicators to enable dynamic diagnostics of digital security. Special attention is also given to the study by Shandova, Senchyn, and Rybas (2024), which presents conceptual approaches to evaluating the effectiveness of

SME digitalization. The study highlights the importance of integrating technical and organizational aspects of digital transformation, as well as the need for decision-support tools in the field of digital security.

However, despite the availability of theoretical groundwork, several unresolved aspects remain: the lack of specialized models of information support specifically for the digital security diagnostics process; the absence of a clear system of indicators for evaluating the level of security tailored to Ukrainian enterprises; and an insufficient level of automation in collecting, processing, and visualizing data on digital threats.

These challenges underscore the need to further develop the toolkit for supporting digital security diagnostics in enterprises.

The aim of this article is to substantiate a conceptual model of information support for diagnosing the digital security level of enterprises, taking into account the specifics of risk management under conditions of digital transformation, and to develop proposals for forming a relevant decision-support information system.

Information support for a digital security diagnostics system should be understood as a comprehensive and structured set of methods, tools, indicators, information flows, and software-technical solutions that ensure completeness, timeliness, and reliability of the data necessary to assess the level of digital protection. This involves not only the availability of technical means for detecting threats, but also the creation of an information infrastructure that allows real-time monitoring of the digital security status, analysis of vulnerabilities, and informed managerial decision-making to strengthen protection.

Based on an analysis of international practices and standards (in particular, ISO/IEC 27001 and the NIST Cybersecurity Framework), three key components of information support for the diagnostics process are identified.

The first component is monitoring and data collection, which involves automatic logging of security incidents, vulnerability scanning, auditing access to critical resources, and network event logging. The use of specialized tools, such as SIEM systems, allows centralized processing of large volumes of information

and timely detection of potentially dangerous activity. It is especially important to integrate technical monitoring with business processes to reveal not only IT-related incidents, but also their operational impact.

The second component is analytical support, which transforms raw data into practical information for decision-making. This includes dashboards for displaying key security indicators, anomaly detection systems, risk evaluation algorithms, and aggregated digital security indexes. For example, enterprises may develop an overall security index that considers both technical aspects (e.g., number of successful attacks, frequency of software updates) and organizational factors (e.g., internal policies, employee awareness). Such analysis helps identify vulnerabilities and adjust security strategies in response to changes in the digital environment.

The third component is information-based decision support. Its function is to provide enterprise management with structured, relevant, and accessible information on the current state of digital security, emerging threats, and proposed mitigation measures. This support may take the form of regular reports, interactive dashboards, risk matrices, scenario modeling, and response plans. It is essential that the provided information is not only technically accurate but also aligned with strategic decision-making, considering financial, reputational, and legal implications of potential incidents.

The proposed model also integrates technical and organizational indicators. Technical indicators include the number of registered incidents, system update levels, detected vulnerabilities, and phishing attempt frequency. Organizational indicators include the existence of internal security policies, staff training, and incident response teams. The combination of these indicators offers a complete and objective picture of the enterprise's digital security level.

To ensure practical applicability, the model introduces a classification of digital security levels: low, medium, and high. Each level corresponds to specific technical and managerial characteristics, enabling comparative analysis between enterprises or departments, and facilitating the development of individualized

roadmaps for improving security in line with available resources, industry specifics, and the organization's level of digital maturity.

Thus, the proposed approach to information support for digital security diagnostics combines technical tools, analytical methods, and management decisions into a unified system, allowing enterprises to act proactively in a dynamic digital environment. Future research should focus on the development of diagnostic automation tools and the adaptation of the model to specific industry requirements.

The growing significance of digital risks necessitates a shift from reactive to proactive digital security management, with high-quality diagnostic information support at its core.

References

1. Andress, J. (2021). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (3rd ed.). Syngress.

2. ISO/IEC 27001:2022. (2022). Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. International Organization for Standardization.

3. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://doi.org/10.6028/NIST.CSWP.04162018

4. Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.

5. González-Varona, J. M., López-Paredes, A., Poza, D., & Acebes, F. (2021). Building and development of an organizational competence for digital transformation in SMEs. *Journal of Industrial Engineering and Management,* 14(1), 15–24. https://doi.org/10.3926/jiem.3279.

6. Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., & Barbaray, R. (2017). The industrial management of SMEs in the era of Industry 4.0.

International Journal of Production Research, 56(3), 1–19. https://doi.org/10.1080/00207543.2017.1372647.

7. Лисак, В. (2024). Цифровізація промислових підприємств: методики оцінювання та подолання ризиків. *Вісник Хмельницького національного університету,* 4, 499–509. https://doi.org/10.31891/2307-5740-2024-332-74.

8. Shandova, N., Senchyn, O., & Rybas, D. (2024). Концептуальні підходи до оцінювання ефективності цифровізації підприємств малого та середнього бізнесу. *Європейський науковий журнал економічних та фінансових інновацій,* 2(14), 389–398. https://doi.org/10.32750/2024-0235.