CYBER RISK MANAGEMENT FOR SUSTAINABLE DEVELOPMENT OF HUMAN RESOURCE MANAGEMENT PROCESSES

N. Dotsenko[1], I. Nekrasov[2], Y. Lutsiv[1]

[1]O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv

[2]Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine, Kyiv

Digitalization of management processes has made it possible to increase the efficiency of management decision-making, which is important for ensuring the sustainable development of the organization. But along with the numerous advantages of using a single information space, creating a project portal and using artificial intelligence tools, the question of ensuring cyber resilience of management processes arises [1].

Human resource management in a multi-project environment is associated with the use of a large amount of data from different projects [2]. The use of a single information environment involves simultaneous work with data (in particular, corporate templates) in several projects and the need to implement roles related to ensuring the cybersecurity of the multi-project environment [3].

Among the potential cyber threats in a multi-project environment, the most influential are:

- technical, related to cyberattacks, hacks and malicious injections;
- organizational, caused by the influence of the human factor;
- project, arising as a result of project management problems in a multi-project environment, access conflicts between projects;
- legal, caused by violation of legislation;
- biased or uncontrolled AI solutions.

Since machine learning systems within a single corporate system were trained according to the same rules, there is a risk of information leakage, training data leakage, data poisoning, which will affect the predictability of forecasting results, on the basis of which management decisions are made.

Human resources, especially top management, are becoming nodes of data, access and management decisions.

The use of shared platforms, corporate control over correspondence, reuse of accounts and unauthorized access to information between projects can cause critical cyber risks in human resources management in projects and programs. Integration of project management systems with HR management systems must be secure from the point of view of Sensitive HR Data.

A typical problem is the availability of access to redundant resources, in particular to the personnel database, the level of competencies (including information with limited access) at the level of the entire multi-project environment. Privilege Creep as a result of the accumulation of excessive access rights, in particular in top management, reduces the cyber resilience of the system.

A low level of information management development or excessive decentralization leads to an insufficient level of monitoring of changes related to information flows. For example, when changing roles in a project, the levels of

access to information change, which requires reviewing the employee's information profile.

Monitoring the relevance of access to corporate mail, inclusion in mailing lists, auditing permissions and rights will allow you to respond to changes in the employee's status:

- removed from the project;
- accepted into the project;
- transferred to the bench;
- dismissed from the organization.

Transferring an employee to a resource pool, with the possibility of further involvement, and leaving them in the system, as well as information about contractors and stakeholders with whom they collaborated in past projects, are also potential causes of information leakage.

Auditing inter-project resource intersections that arise when applying the donor-acceptor approach to resource redistribution and program management, from the point of view of information flows and access rights, will reduce the risk of unauthorized data distribution.

Thus, cyber resilience of management processes is a critical factor of sustainability, as it reflects the trust and effectiveness of digitalization processes. Ensuring cyber resilience should combine technical protection mechanisms, organizational policies and ethical principles of using artificial intelligence, which should ensure compliance with modern cybersecurity standards.

Comprehensive cyber risk management should be integrated both into elements of a multi-project environment and at the PMO level, which should contribute to the prediction of the emergence of cyber risks, response to them, adaptation and recovery of management processes after cyber incidents.

The study is being conducted within the framework of the research project 2025.07/0038 of the National Fund of Ukraine on the topic «Scientific Foundations for the Formation and Management of Human Capital in a Multi-Project Environment to Support the Sustainable Development of Ukraine’s Recovery Programs».

References: 1. Camacho, J.M., Couce-Vieira, A., Arroyo, D. and Insua, D.R. (2026), A cybersecurity risk analysis framework for systems with artificial intelligence components. Intl. Trans. in Op. Res., 33: 798-825. https://doi.org/10.1111/itor.70049. **2.** Bushuyev, S., Chumachenko, I., Galkin, A., Bushuiev, D., & Dotsenko, N. (2025). Sustainable Development Projects Implementing in BANI Environment Based on AI Tools. Sustainability, 17(6), 2607. https://doi.org/10.3390/su17062607. **3**. Mizrak, K. C. (2025). Secure Remote Work: HR's Role in Managing Cyber Risks in Hybrid Work Environments. In F. Mızrak (Ed.), Utilizing Cybersecurity to Foster Business Innovation and Resiliency (pp. 169-188). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6417-8.ch008.