CHAPTER 1

ENSURING CYBER RESILIENCE TRANSFORMATION OF PERSONNEL MANAGEMENT PROCESSES IN A MULTI-PROJECT ENVIRONMENT

Dotsenko N. V., Chumachenko I. V., Nekrasov I. B.

DOI https://doi.org/10.30525/978-9934-26-653-9-1

INTRODUCTION

In the era of digitalization, HR management requires a review of classic approaches to management to ensure the effective functioning of the company. The increasing speed of transformation and the lack of consideration of the specifics and needs of the organization make this process chaotic and sometimes lead to the opposite effect:

- loss of stability of functioning;
- information leaks;
- disruption of established business processes[1].

The analysis of the impact of digital technologies on the transformation of strategic management, described in the work of Donchak L., Pogryshchuk O., Sysoeva I., showed the need to implement innovative cyber defense systems, which in turn requires improving the digital infrastructure, increasing its accessibility, and revising the organization's corporate culture[2].

The implementation of projects in a multi-project environment of the company makes the issue of developing a policy for ensuring cyber resilience of processes relevant and requiring an urgent solution. Personnel management of portfolio projects involves the exchange of a large amount of data between elements of a multi-project environment, which leads to the need to take cybersecurity requirements into account.

Developing and implementing a comprehensive approach to increasing cyber resilience will ensure the resilience of the organization through preparedness

[1] Дворник О. Стратегії, виклики та успішні практики в епоху цифрової трансформації бізнесу. Develop-ment Service Industry Management. 2023. No 4. C. 107-111. URL: https://dsim.khmnu.edu.ua/index.php/dsim/article/view/68

[2] Дончак Л., Погріщук О., Сисоєва І. Стратегічний менеджмент у цифрову епоху: виклики та можливості. *Економіка та суспільство*. 2024. No 70. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5237

for cyber threats, cyber risk management, and the development of recovery mechanisms after cyber attacks.

1. Analysis of existing methods for solving the problem of transforming human resource management processes and formulating the task

Transformation of HR processes in a multi-project environment occurs under constraints of time and cost of implementation. The speed of implementation of transformation processes leads to the fact that the audit process of the existing state of organizational and digital systems does not always take place. At the same time, transformation and implementation of new processes at critical infrastructure facilities are carried out in real time, ensuring configuration management of resources[3].

Among the regulatory framework that regulates data security issues, this should be noted:

– standard ISO / IEC 27001 "Information security management systems";

– standard ISO / IEC 27701 "Privacy Information Management System";

– standard ISO / IEC 27005 "Information security risk management";

– standard ISO / IEC 270 17 "Cloud security controls";

– standard ISO / IEC 2 2301 "Business Continuity management";

– General Data Protection Regulation (GDPR);

– the Network and Information Security Directive NIS2;

– Law of Ukraine "On Protection of Personal Data";

– Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine";

– Resolution of the Cabinet of Ministers of Ukraine "On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities" [4].

When working with transnational companies, the issue of ensuring the protection of personal data in accordance with the GDPR standard arises, which is not always considered during the accelerated transformation of human resources management processes[5].

[3] Dotsenko , N., Chumachenko , I., Galkin , A., Kuchuk , H., Chumachenko , D. Modeling the Transformation of Configuration Management Processes in a Multi -Project Environment. ***Sustainability*** 2023. No. *15* (19), 14308. DOI: https://doi.org/10.3390/su151914308 .

[4] Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

[5] Загальний регламент про захист даних (GDPR) URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf https://gdpr-text.com/uk/

Implementing existing project management systems in a multi-project environment, in particular SAP, involves distributing access rights and working with many projects, but does not eliminate the risks associated with the influence of the human factor on the emergence of cyber risks[6].

The conducted analysis of cyber threats identified typical risks that arise when transforming human resource management processes into a multi-project environment:

- risks of personal data confidentiality;
- risks of access management in a multi-project environment;
- the complexity of the security audit;
- risks of integrating digital platforms;
- risks of cyber incidents related to remote work;
- risks of using AI.

The issue of integrating human resource management processes with cyber management was considered in the works of N. Tyukhtenko, M. Navrotska[7], T. Dluhopolska, and Huk. Yu.[8], Mat N.H.N. & al[9], Kiselak M.[10].

By cyber resilience of human resource management processes in a multi-project environment, we mean the ability of project HR processes to anticipate, withstand, adapt, and recover from cyber incidents, while maintaining the continuity of personnel management and the reliability of resource provision for the needs of a multi-project environment.

Key HR processes from the perspective of ensuring cyber resilience are presented in Table 1.

The purpose of the study is to develop a model of the process of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment.

The objectives of the study are:

- to analyse the approaches to ensuring cyber resilience of the organization and processes;

[6] Створіть бізнес із більшою відповідністю, стійкістю та потужнішим сталим розвитком URL: https://www.sap.com/ukraine/products/sustainability.html?url_id=banner-ua-homepage-row3-suite-pos8-sustainability-250520

[7] Актуальні питання інноваційного управління людськими ресурсами в умовах адаптації бізнес-середовища до трансформаційних змін. (2025). *Серія: Економіка*, *29*, 85-97. https://doi.org/10.34079/2518-1394-2025-15-29-85-97

[8] Длугопольська Т.І., Гук Ю.В. Цифрова трансформація у сфері HR: напрями, проблеми та можливості. *Причорноморські економічні студії*. Вип. 62. 2021. С. 13-18.URL: https://doi.org/10.32843/bses.62-2

[9] Mat , N.H.N, Jaafar , SM, Kamalbatcha , Z., & Derani , NES (2025). HRM Implementation , gig work , and the love framework : A systematic review of evolving dynamics in the modern digital workplace . *Multidisciplinary Reviews* , *9* (3), 2026113. https://doi.org/10.31893/multirev.2026113

[10] Kiselak , M., Žižek , S.Š. (2026). The Impact of Digitalization on Human Resources Management . In : Mulej , M., Hrast , A., Štrukelj , T., Likar , B., Šarotar Žižek , S. (eds) Bases for an Innovative Sustainable Socially Responsible Society Volume II. Palgrave Studies in Governance , Leadership and Responsibility . Palgrave Macmillan , Cham . https://doi.org/10.1007/978-3-031-96891-4_6

– to analyse the impact of cyber risks on project management resource provision processes in a multi-project environment;

– to develop a model for the process of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment;

– to develop the recommendations for the implementation of the model.

Table 1

Key HR processes

HR – process	Criticality
Access management	Critical
Allocation of resources between projects	Critical
Personnel planning	High
Evaluation and KPIs	High
Competency management	High
Recruitment and selection	Medium/high
Training and development	Medium
Engagement management	Medium

2. Main research material

For recovery programs and critical infrastructure projects it is advisable to use the Zero principle Trust Architecture[11], contributing to increase cybersecurity in information structures. This becomes extremely important in conditions of war and post-war restoration of critical infrastructure facilities because it contributes to increasing the level of security of the facility.

According to NIST Cybersecurity Framework with the main elements of Improving Critical Infrastructure Cybersecurity is a Function and Category[12]:

– Identify (Asset Management ID.AM; Business Environment ID.BE; Governance ID.GV; Risk Assessment ID.RA; Risk Management Strategy ID.RM; Supply Chain Risk Management ID.SC);

– Protect (Identity Management and Access Control PR.AC; Awareness and Training PR.AT; Data Security PR.DS; Information Protection Processes and Procedures PR.IP; Maintenance PR.MA; Protective Technology PR.PT);

– Detect (Anomalies and Events DE.AE; Security Continuous Monitoring DE.CM; Detection Processes DE.DP);

[11] Zero Trust Architecture URL: https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

[12] NIST Cybersecurity Framework v.1.1, Framework for Improving Critical Infrastructure Cybersecurity https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- Respond (Response Planning RS.RP; Communications RS.CO; Analysis RS.AN; Mitigation RS.MI; Improvements RS.IM);
- Recover (Recovery Planning RC.RP; Improvements RC.IM; Communications RC.CO).

Resource management according to the PMI PMBoK standard involves the following processes:

- Resources Management Planning (RMP);
- Operations Resources Estimation (ORE);
- Resources Acquisition (RA);
- Project Team Development (PTD);
- Team Management (TM);
- Resources Control (RC).

NIST Cybersecurity Element Projection The framework for resource management processes in projects is given in Table 2.

Functional identification ensures strategic alignment of human resource management processes with cyber risks implementation of projects in a multi-project environment. As a result of the analysis of the categories Governance, Risk Assessment, Business Environment in the context of Resource Management Planning, Operations Resources Estimation forms a matrix of critical project roles, Cyber-HR Risk Register, a team cyber resilience competency map. Human risk assessment will identify competency gaps, key role overload, and single point of failure in the team, outsourcing risks (in the process of acquiring resources) and risks associated with the functioning of geographically distributed teams.

The next stage is to form a team capable of functioning resiliently, adaptively, ensuring a certain level of cyber resilience. Based on the implementation of Identity Management and Access Control; Awareness and Training; Information Protection Processes and Procedures; Maintenance within processes Resources Acquisition and Project Team Development is forming a model for distributing access by roles, a plan for developing competencies and Cyber-aware onboarding / offboarding.

Understanding that a team functions as an organizational system makes it possible to provide both technical and organizational support for management processes.

Incident management allows for rapid response to anomalies and ensures reliable operation of the human resources management system. Incident response protection should be built into HR processes and safe default scenarios and automatic response scenarios should be defined.

A contextual model of the process of ensuring cyber resilience of the transformation of personnel management processes in a multi-project environment is presented on Figer 1.

Table 2

NIST Cybersecurity Element Projection Framework for resource management processes in projects

NIST CF	RMP	ORE	RA	PTD	TM	RC
ID.AM	+	+	+	+	+	+
ID.BE	+	+	+	+		+
ID.GV	+	+	+	+	+	+
ID.RA	+	+		+		+
ID.RM	+			+	+	
ID.SC					+	+
PR.AC	+	+	+	+	+	+
PR.AT				+	+	+
PR.DS	+			+	+	+
PR.IP	+	+	+	+	+	+
PR.MA	+			+	+	+
PR.PT	+	+		+	+	
DE.AE	+	+	+	+	+	+
DE.CM	+				+	+
DE.DP					+	+
RS.RP	+				+	+
RS.CO	+				+	+
RS.AN	+	+		+	+	+
RS.MI	+			+	+	+
RS.IM	+	+	+	+	+	+
RC.RP	+			+	+	+
RC.IM	+			+	+	+
RC.CO					+	+

The inputs to the context model are:

- project information;
- process cybersecurity requirements;
- cyber resilience requirements;
- resource provision.

The outputs of the contextual model are:

- cyber risk management plan;
- incident recovery plan;
- recommendations for developing a cyber-resilient team.

When decomposing the model, tunneled outputs were added:

- cyberrisk register;
- incident response.

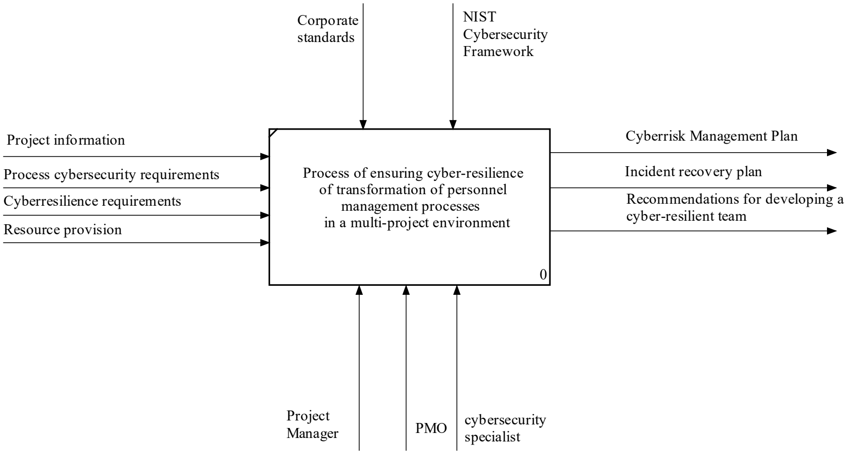
Corporate standards
NIST Cybersecurity Framework
Project information
Process cybersecurity requirements
Cyberresilience requirements
Resource provision
Process of ensuring cyber-resilience of transformation of personnel management processes in a multi-project environment
0
Cyberrisk Management Plan
Incident recovery plan
Recommendations for developing a cyber-resilient team
Project Manager
PMO
cybersecurity specialist

Fig. 1. Context model of the process of ensuring cyber resilience of transformation of personnel management processes in a multi-project environment

Project Manager, PMO, cybersecurity are involved in the process specialist, who act on the basis of regulatory documentation, corporate standards, NIST Cybersecurity Framework.

As a result of the decomposition of the contextual model, taking into account the requirements for cyber resilience, a decomposition model of the process of ensuring cyber resilience of the transformation of personnel management processes in a multi-project environment was built (Figure 2).

The Identify (ID) process involves identifying/understanding the resources, risks, and context associated with managing project human resources in a multi-project environment.

Protect (PR) process is designed to create safeguards to maintain the security of human resource management processes.

Detect (DE) process is designed to identify anomalies and events that may indicate incidents related to the implementation of human resource management processes.

The Respond (RS) process implements a response to identified incidents in accordance with the cyber risk management plan. The Recover (RC) process ensures recovery from events and improves human resource management processes from the perspective of ensuring cyber resilience of processes.

To analyze the effectiveness of the model, the proposed system of metrics is given in Table 3.

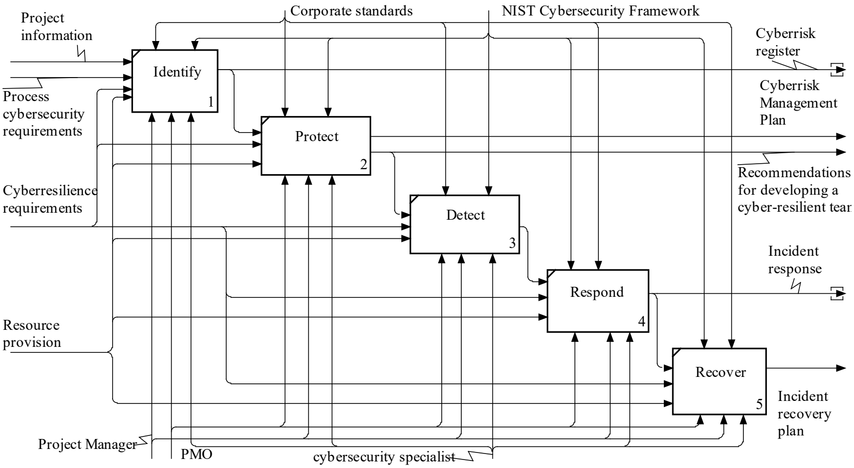

Fig. 2. Decomposition model of the process of ensuring cyber resilience of transformation of personnel management processes in a multi-project environment

Table 3

Metrics for ensuring cyber resilience of HR management processes

Metrics	**Description**
Detection Effectiveness	
MTTD-HR Mean time to detect HR incident	Average time from appearances incident before it detection
Incident detection rate	HR incidents detected before escalation
Proactive detection ratio	Fraction incidents detected preventively
Analysis Quality	
Root cause coverage	% of incidents from formalized RCA
Role-level analysis	Role-Level Analysis Index
Systemic cause ratio	% of causes that are systemic rather than individual
Response Effectiveness	
Decision latency	Time from analysis to management decision
Corrective action rate	% of incidents from implemented corrective actions
Role frequency adjustment	Frequency of role correction after incidents. Indicator adaptability
Learning Effectiveness	
Lessons learned utilization rate	% lessons learned , actually used in new projects

Continuation of table 3

Training alignment index	Fraction exercises related to real incidents
Competency update rate	Update frequency competency models
Organizational Memory Metrics	
Incident reuse index	How many times incident reused
Knowledge formalization rate	% of incidents converted to knowledge
Cross-project transfer ratio	Using knowledge between projects
Impact Metrics	
Incident recurrence rate	Frequency similar incidents
Human risk exposure index	Integral indicator human risks
Project disruption reduction	Reduction influence incidents per project

The cyber resilience contours of human resource management processes are presented in Table 4.

Table 4

Contours of cyber resilience

Contour	Elements
Protection	Zero Trust; RBAC/ABAC; data encryption, segmentation and prioritization of projects
Continuity	HR-BCP/HR-DRP; backup HR scenarios; alternative HR management channels
Adaptation	AI audit, process audit, human in the loop, role and access updates

When implementing the model, project documents are formed, which reflect measures to ensure cyber resilience of human resources management processes:

– cyber risk management plan;
– incident recovery plan;
– recommendations for developing a cyber-resilient team;
– cyberrisk register;
– incident response.

CONCLUSIONS

The issue of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment is considered. It is determined that despite the advantages, the digital transformation of management processes has significant challenges related to cybersecurity issues and ensuring cyber resilience of management processes.

For human resource management processes in a multi-project environment, ensuring cyber resilience and responding to cyber threats is most relevant, since the level of cyber threats increases in a multi-project environment, which can lead to the loss or leakage of confidential information. Based on the analysis of cyber threats, the most critical processes from the point of view of ensuring cyber resilience were identified.

The concept of cyber resilience of human resource management processes in a multi-project environment has been introduced. A projection of NIST Cybersecurity elements has been developed Framework for resource management processes in projects, which became the basis for developing a model of the process of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment.

Models of the process of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment (context model and process decomposition model) have been developed. The contours of cyber resilience of processes have been identified: protection contour, continuity contour, adaptation contour. The proposed models can be applied to formalize transformation processes in terms of ensuring cyber resilience.

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".

SUMMARY

Digital transformation of management processes promotes the development of companies, but requires the development of approaches to ensure the cyber resilience of human resource management processes.

The purpose of the study is to develop a model of the process of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment.

The concept of cyber resilience of human resource management processes in a multi-project environment is considered. An analysis of approaches to ensuring cyber resilience of the organization and processes is carried out, the regulatory framework governing data security issues is considered. An analysis of the impact of cyber risks on the processes of resource provision of project management in a multi-project environment was carried out, which allowed to identify processes with a high level of criticality of cyber resilience. A projection of NIST Cybersecurity elements is constructed Framework for resource management processes in projects. Models of the process of ensuring cyber resilience of the transformation of human resource management processes in a multi-project environment (contextual model and process decomposition model) have been developed. Recommendations for the implementation of the developed models are provided.

Bibliography

1. Дворник О. Стратегії, виклики та успішні практики в епоху цифрової трансформації бізнесу. *Development Service Industry Management*. 2023. No 4. C. 107–111. URL: https://dsim.khmnu.edu.ua/index.php/dsim/article/view/68

2. Дончак Л., Погріщук О., Сисоєва І. Стратегічний менеджмент у цифрову епоху: виклики та можливості. *Економіка та суспільство*. 2024. No70. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5237

3. Dotsenko, N., Chumachenko, I., Galkin, A., Kuchuk, H., Chumachenko, D. (2023) "Modeling the Transformation of Configuration Management Processes in a Multi–Project Environment". ***Sustainability**, №15(19), 14308. DOI: https://doi.org/10.3390/su151914308.*

4. Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

5. Загальний регламент про захист даних (GDPR) URL: https://gdpr-text.com/uk/

6. Створіть бізнес із більшою відповідністю, стійкістю та потужнішим сталим розвитком URL: https://www.sap.com/ukraine/products/sustainability.html?url_id=banner-ua-homepage-row3-suite-pos8-sustainability-250520

7. Актуальні питання інноваційного управління людськими ресурсами в умовах адаптації бізнес-середовища до трансформаційних змін. *Серія: Економіка*, 2025. №*29*, 85-97. https://doi.org/10.34079/2518-1394-2025-15-29-85-97

8. Длугопольська Т.І., Гук Ю.В. Цифрова трансформація у сфері hr: напрями, проблеми та можливості. *Причорноморські економічні студії Вип. 62. 2021.* С. 13-18.URL: https://doi.org/10.32843/bses.62-2

9. Mat, N. H. N., Jaafar, S. M., Kamalbatcha, Z., & Derani, N. E. S. (2025). HRM Implementation, gig work, and the amo framework: A systematic review of evolving dynamics in the modern digital workplace. *Multidisciplinary Reviews*, *9*(3), 2026113. https://doi.org/10.31893/multirev.2026113

10. Kiselak, M., Žižek, S.Š. (2026). The Impact of Digitalization on Human Resources Management. In: Mulej, M., Hrast, A., Štrukelj, T., Likar, B., Šarotar Žižek, S. (eds) Bases for an Innovative Sustainable Socially Responsible Society Volume II. Palgrave Studies in Governance, Leadership and Responsibility. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-96891-4_6

11. Zero Trust Architecture URL: https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

12. NIST Cybersecurity Framework v.1.1, Framework for Improving Critical Infrastructure Cybersecurity URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Information about the authors:
Dotsenko Nataliia Volodymyrivna,
Doctor of Technical Sciences, Professor,
Professor at the Project Management in Urban Management and Construction Department,
O. M. Beketov National University of Urban Economy in Kharkiv,
17, Chornoglazivska str., Kharkiv, 61002, Ukraine

Chumachenko Igor Volodymyrovych,
Doctor of Technical Sciences, Professor,
Head of the Project Management in Urban Management and Construction Department,
O. M. Beketov National University of Urban Economy in Kharkiv,
17, Chornoglazivska str., Kharkiv, 61002, Ukraine

Nekrasov Ivan Borysovych,
Candidate of Technical Sciences, Research Fellow,
Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine,
28-B, Povitroflotskyi ave., Kyiv, 03049, Ukraine