**UDC 338.28**

**RISK MANAGEMENT OF CYBER PROTECTION PROGRAMS FOR CRITICAL INFRASTRUCTURE FACILITIES**

*Kovalchuk O.I., Ratushnyi R.T., Peretyatko L.A., Zhuk I.M.*

Department of Law and Management in Civil Protection, Lviv State University of Life Safety

Анотація. Зі стрімким впровадженням новітніх інформаційних технологій у всі сфери діяльності збільшується і кількість цінної інформації, від безпеки якої залежать об’єкти інфраструктури. Об’єкти критичної інфраструктури, такі як: електростанції, транспортні системи, медичні установи, банки та інші системи у своїй діяльності використовують різні системи підтримки прийняття рішень та інформаційні системи, в яких недостатня кібернетійкість може призвести до серйозних наслідків.

Ключові слова: інформаційна безпека, ризик менеджмент, інформаційні системи, інфраструктура.

Abstract. With the rapid implementation of the latest information technologies in all spheres of activity, the amount of valuable information on the security of which critical infrastructure facilities depend on is also increasing. Objects of critical infrastructure, such as: power plants, transport systems, medical institutions, banks and other systems in their operations require various decision support systems and information systems, in which a lack of cyber security can lead to serious consequences.

Keywords: information security, risk management, information systems, infrastructure.

Successful managers skillfully analyze risks and make informed decisions relying on competence and experience. Managers have to consider many external and internal organizational factors that influence uncertainty. Risk management is an iterative process, the purpose of which is to ensure the achievement of the organization's goals. The process of improving the management system of state critical facilities should take into account the best practices of risk management. To optimize these processes, managers use information technologies such as corporate information and ERP systems. They enable efficient management of infrastructure projects, programs and project portfolios.



Figure 1 A portfolio of critical infrastructure consisting of various components

Objects of critical infrastructure, such as: power plants, transport systems, medical institutions, banks and other systems in their activities use various decision support systems and information systems in which insufficient cyber resistance can lead to serious consequences. Ishikawa and BTA - Bow-Tie Analysis methods are used to analyze causal relationships in risk management. Managing risk is based on the principles, framework and process outlined in [6].



Figure 2 Principles, framework and process efficient risk management

The characteristics of risk management may differ significantly depending on the chosen strategy. For example, a proactive approach involves constant monitoring of risks and the development of preventive measures, while a reactive approach focuses on eliminating the consequences of problems that have already occurred. The choice of risk management strategy directly affects the structure and functions of risk management programs. Some strategies require the creation of dedicated units responsible for risk management, while others may involve the division of responsibilities among different divisions of the organization. The effectiveness of risk management depends on the extent to which the chosen strategy corresponds to the specifics of the organization and the nature of the risks it faces. There is no one-size-fits-all strategy that fits all organizations.

Table 1 Characteristics of risk management depending on strategic approaches to formation

risk management programs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Characteristics  risk-  management | A strategic approach to forming a risk management program | | | |
| Conservative | Maximizer | Manager | Pragmatist |
| Management goals  risks | Loss control.  Software  system security | Reward for  accepted risks.  Profit from  purchase or  sale of risks | Impact on risks  by means of  a series of measures. | Diversification.  Avoidance of large  risk concentrations |
| Strategic  orientation  risk-  management | Low risk-  appetite.  Minimization  risks with a goal  minimization  losses  Stabilization  results. | High risk-  appetite.  Maximization  increase  profit for  maximum  (accepted)  risks | Average risk-  appetite.  Strategic  decision,  aimed at  increase  cost | Strategic benefits  relate to receiving  benefits from the complex  different, maybe not  related risks. |
| Features  management  risks | Hard limits,  restrictions and  regulators.  Control over  commercial  bank operations  or insurance  companies | Flexible  opportunities | Formal  politicians and  standards. | Flexible options,  high degree  communications and  competencies.  Portfolio management  risks |
| Approaches to  analysis and  assessment  risks | Stress testing.  Analysis  sensitivity  Scenario analysis. | Models  pricing,  methods  rating  agencies.  Evaluation and  reservation  trade operations  banking and  insurance  activity | Economic  capital and added  cost.  Reward for  risk and  budgeting | Simplified  economic capital. |
| Reports from  management  risks | Compliance  limits  Impact on risks,  that arose | Correlation  profit and  risks that  related to him | Coefficient  profitability  equity,  risk budget | Concentration of risks:  arising losses  due to large positions in  one asset or on  a certain market.  Consolidated report  about risks |
| Environment  dominance  risk | Collapse | Lift | Discreet | Indeterminate |

Therefore, to increase the cyber security of the energy system, it is necessary to apply a comprehensive approach, which includes both technical measures (updating software, intrusion detection systems) and organizational measures (increasing staff awareness, developing incident response plans). International cooperation and exchange of experience also play an important role

**References**

1. Shipovsky Volodymyr System of indicators for assessing cyber resilience of information systems of critical infrastructure objects Information Protection, volume 25, number 1, January-March 2023, pp. 37-45 DOI: 10.18372/2410-7840.25.17597
2. Kovalchuk Oleh, Kobylkin Dmytro and Zachko Oleh: Graphodynamic modeling for a multi-agent support system for personnel decision-making in the field of human safety. Proceedings of the 4th International Workshop IT Project Management (ITPM 2023). Warsaw 2023. P. 149–159
3. O. Kovalchuk, D. Kobylkin and O. Zachko, "HR Decision-Making Support System Based On The CBR Method," 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT), Lviv, Ukraine, 2023, pp. 1-4, doi: 10.1109/CSIT61576.2023.10324169.
4. Kovalchuk Oleh, Zachko Oleg Models of the life cycle of forming project teams in a security-oriented system IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), [IWPM](https://sci.ldubgd.edu.ua/bitstream/123456789/7677/1/IWPM_2020_paper_33%20%281%29.pdf) 2020, 2, pp. 211–214, 9321932 DOI:[10.1109/CSIT49958.2020.9321932](http://dx.doi.org/10.1109/CSIT49958.2020.9321932)
5. ДСТУ ISO 21503:2022 “Project, programme and portfolio management — Guidance on programme management”
6. ISO 31000:2018 Risk management — Guidelines
7. IPMA Organisational Competence Baseline (IPMA OCB). IPMA, 2013, 67 p.