Management of financial and economic security of critical infrastructure objects in the conditions of risks of quarantine restrictions: strategic and personnel aspects

Nataliia Zachosova[1,*], *Dmytro* Kutsenko[1], *Oleksii* Koval[1], and *Andrii* Kovalenko[1]

[1]Department of Management and Economic Security, The Bohdan Khmelnytsky National University of Cherkasy, 81 Shevchenko Blvd., Cherkasy, 18031, Ukraine

Abstract. The purpose of the study was to develop theoretical and methodological background and to make practical offers for solving the problem of financial and economic security management of critical infrastructure in terms of personnel and strategic aspects. The list of reasons and circumstances of necessity of maintenance of financial and economic security of objects of critical infrastructure and its management is established. The definition of financial and economic security of a critical infrastructure object is offered. The peculiarities of the interpretation of the concept of financial and economic security for the needs of critical infrastructure are summarized. Two levels of financial and economic security management of critical infrastructure objects are distinguished – state (external) level and internal level – and an explanation of the differences in financial and economic security management at each of them is provided. The risks caused by quarantine restrictions for the state of financial and economic security of critical infrastructure objects have been identified. As a main result of the study the TARGET model for strategic management of financial and economic security of critical infrastructure objects is proposed. Practical value of the proposed in the study TARGET model for strategic management of financial and economic security of critical infrastructure objects – it will be the basis for developing strategic documents for stabilizing and further developing and maintaining high functionality of critical infrastructure of Ukraine. As an additional result of the study proposals on the basics of personnel policy formation for the need to ensure financial and economic security of critical infrastructure objects in a global pandemic and quarantine restrictions are made. The novelty of proposed personnel policy is in a fact that it contains such modern components as staff training; employee incentives; overcoming resistance to change; staff involvement in solving various issues; staff discipline; leadership, partnership and teamwork; time management and self-management; staff safety, staff digital literacy.

1 Financial and economic security of critical infrastructure as a management object

An important problem of national security and defense of the state is to ensure a high functional state of the critical infrastructure of the country, which is based on efficient and continuous operation of economic entities. Vectors of research of modern scientists and practitioners should be directed to the development of innovative management tools, new technologies of management solutions to ensure economic security of business structures to stabilize the critical infrastructure of the state in the transformation of classical business practices caused by Industry 4.0 and globalization. It is also necessary to take into account in this process the latest non-traditional risks posed by the epidemiological situation in Ukraine and in the world, in particular, and those of their species that are provoked by quarantine restrictions.

1.1 The need to manage the financial and economic security of critical infrastructure

According to the draft regulation acts, "the object of critical infrastructure defined in the manner prescribed by law, a component of critical infrastructure, functionality, continuity, integrity and stability of which ensure the realization of vital national interests" [1]. In the context of exacerbation of the epidemiological situation, the continuity of action of the critical infrastructure objects was threatened, which created risks not only for their financial and economic security, but also for the security of the state and the population as a whole

In order to target efforts to develop modern directions and concepts of financial and economic security management of critical infrastructure objects, in particular, at the state level, to establish opportunities for their financial support, etc., it is important to determine their list. At the legislative level, it is proposed to consider the objects of critical infrastructure as "enterprises, institutions, organizations, regardless of ownership, which:

*e-mail: natazachosova@gmail.com

1) carry out activities and provide services in the fields of energy, chemical industry, defense industry, transport, information and communication technologies, electronic communications, in the banking and financial sectors;

2) provide services in the spheres of life support of the population, in particular in the spheres of centralized water supply, centralized drainage, supply of thermal energy, hot water, electricity and gas, food production, health care;

3) included in the list of enterprises of strategic importance for the economy and security of the state;

4) are subject to protection and defense in a state of emergency and a special period;

5) are objects of increased danger;

6) are objects of national importance, extensive connections and significant impact on other infrastructure;

7) are objects, the dysfunction of which will lead to a crisis situation of regional importance" [1].

Thus, the list includes business structures of various sectors of the economy, those objects, the shutdown of which may actually destabilize the state of the national economic system or lead to increased social tensions, humanitarian or man-made disaster. Obviously, the quarantine restrictions, in particular regarding the temporary suspension of activities, will not directly apply to such facilities. At the same time, the efficiency of their operation is directly affected by the suspension of the rest of the business structures, the transport system, which ensure and mediate the performance of critical functions by objects of critical infrastructure. It is in this context that the issue of ensuring financial and economic security should be addressed, because it is the system tools that characterize risks and minimize the consequences of the impact of threats that should be used in such conditions in the first place.

Continuity of financial transactions and financial services plays an important role in maintaining the normal state of the financial system of the country, the functioning of business and the well-being of the population. Therefore, the regulatory acts specifically state that "critical infrastructure in the banking system of Ukraine includes banks, the sustainable operation of which ensures the stability of the banking system, is essential for the economy and security of the state, the functioning of society, and which are of significant public interest. In particular, these are: National Bank; banks that meet at least one of the following criteria: a bank that is included in the list of systemically important banks; a bank that is included in the list of banks of Ukraine authorized to operate (carry out operations) during a special period; a bank in which the state directly or indirectly owns a share of more than 75 percent of the authorized capital of the bank" [2].

Awareness of the importance of maintaining an adequate level of security of critical infrastructure objects is reflected in the specification of the definition of this concept at the level of government as such a state of "security of critical infrastructure, which ensures the functionality and continuity of its work and / or ability to provide basic services" [3].

Given the importance of continuous and efficient operation of economic entities belonging to the list of critical infrastructure objects, the state of their financial and economic security is a characteristic that requires close control, monitoring and maintenance at a high level through rational and timely management actions by the management of such companies, and by public authorities through the tools of legal regulation.

The need to manage the financial and economic security of critical infrastructure objects is explained by the following circumstances and reasons:

- influence – economic and financial stability of economic entities that form the structural framework of the national economic, industrial, defense systems determines the functional capacity of the national economy as a whole;
- strategic importance – the state of financial and economic security of the subject is the starting point, the zero hypothesis for determining the strategic guidelines of its development in the future; at the same time, the condition of critical infrastructure is crucial for economic foresight within the development of the national strategy of the state;
- autonomy – critical infrastructure must be economically and financially independent if not from public authorities, given their special status, but at least from market business structures in order for their activities to be fully aimed at meeting national interests and not the desires and needs of certain groups of stakeholders;
- specifics – critical infrastructure objects must demonstrate the peculiarities of building their own systems of financial and economic security, for example, in the context of organizing the protection of information resources, which often have the status of state secrets or information with limited access; for such objects, it may be inadmissible to disclose information about their own financial condition or sources of income, existing contracts, which may be necessary to obtain investments or loans; such specific aspects significantly reduce the capacity of some critical infrastructure facilities to attract additional financial resources, leaving them the only opportunity to rely on public funding for their activities;
- time constraints – given the need for continuous operation of critical infrastructure objects, they need to have a sufficient supply of resources, especially material and financial, to ensure the permanence of operational business processes, which in a low level of financial and economic security will be difficult guarantee.

Concretization at the normative level of the concept of security of a critical infrastructure object indicates the need to clarify the content and essence of the category of financial and economic security of such an object.

1.2 Principles of financial and economic security management of critical infrastructure objects

Scientists have long been discussing the problems of supporting the continuous operation of critical infrastructure. Thus, we find interest in the outlined issues in the publications of researchers such as Cristina Alcaraz and Sherali Zeadally [4], Razieh Mosadeghi, Russell Richards and Rodger Tomlinson [5], Georgios Giannopoulos, Roberto Filippini and Muriel Schimmer [6], David Rehak, Pavel Senovsky and Simona Slivkova [7], Grangeat Amélie, Bony Aurélia, Lapebie Emmanuel, Eid Mohamed and Dusserre Gilles [8], Christer Pursiainen [9]. Problems of financial and economic security management are solved by such scientists as Alina Ianioglo and Tatjana Polajeva [10], Lars Osberg and Andrew Sharpe [11], Valeriu Ioan-Franc and Marius Andrei Diamescu [12], Kurt Schimmel, Sifeng Liu, Jeananne Nicholls, Nicholas A Nechval and Jeffrey Yi-Lin Forrest [13], Emanuel Kopp, Lincoln Kaffenberger and Christopher Wilson [14], Marek Kośny and Maria Piotrowska [15], Jacob S. Hacker, Gregory A. Huber, Austin Nichols, Philipp Rehm, Mark Schlesinger, Rob Valletta and Stuart Craig [16], Jacob S. Hacker, Gregory A. Huber, Philipp Rhem, Mark Schlesinger and Rob Valetta [17], Stefano Bistarelli, Fabio Fioravanti, Pamela Peretti and Francesco Santini [18], Jacob S. Hacker, Gregory A. Huber, Austin Nichols, Philipp Rehm, Mark Schlesinger, Rob Valletta and Stuart Craig [19], M. Eric Johnson and Eric Goetz [20], Miles Kahler [21]. Ukrainian researchers are also making successful attempts to study the country's critical infrastructure management issues, in particular, [22]. As a separate area of research on financial and economic security at the micro and macro levels has become issues of risk management, which can be traced in the publications of such scientists as Brian J. Allen and Rachelle Loyear [23], Alison Wakefield [24], Ryan McCormack and Albert Lord [25], Matthias Dehmer, Silja Meyer-Nieberg, Goran Mihelcic, Stefan Pickl and Martin Zsifkovits [26].

If from the functional plane – the study of financial and economic security subsystems and their condition – to move to the species parameter, the field of view of scientists in the field of security often includes such critical infrastructure as financial institutions, especially banks. It should be noted that this study also began with the scientific interest of its authors to the problems of economic security of various types of financial institutions [27, 28].

Since the objects of critical infrastructure at the state level include strategically important enterprises of different types of economic activity, banking institutions, etc., the definition of financial and economic security, proposed for many years by researchers for different types of economic entities, may be more or less suitable for use for these specific objects. However, it is worth considering the question of clarifying the concept of financial and economic security through the prism of the definitions proposed for business structures, because for the latter the purpose of the economic security system is to form such an internal environment that can provide its competitive advantages with minimal risk and threats to the loss of economic viability in the long run, while the priority of critical infrastructure objects financial and economic security should be to ensure a high level of protection of resources of such structures and support their effective use to achieve the necessary social effect, ensuring the viability and activity of related industries, finance, social spheres, national defense. Making a profit for critical infrastructure should be a secondary task compared to meeting the needs of stakeholders related to their work.

Even those definitions of financial and economic security that we have found in the scientific sources and which can be used to assist in performing the tasks of this study have a large number of shortcomings. That's why we can not call them universal and give them the status of classical definitions and use them to explain the core of financial and economic security of critical infrastructure. For example, interpretations that explain the core of financial and economic security through a category of "state" are criticized because of the fact that in a changing, risky environment, maintaining a certain state of resources or economic opportunities or characteristics requires a number of dynamic action by company management, which makes such a state volatile, changeable, but not "fix" it. Therefore, some parameters should be added to the concept of financial and economic security in a "state", plane which characterize it at that particular moment in time, when the level of financial and economic security is assessed and experts conclude whether in the state of security or, conversely – danger – the business entity is.

We believe that the financial and economic security of critical infrastructure should be considered a set of financial and economic conditions that are created by making management decisions on the formation of economic resources of the entity, areas of their preservation and use within the main, financial, investment and other activities in order to ensure the continuity of the functioning of the structure and the timely implementation of the tasks of its existence in the architecture of the critical infrastructure of the state.

Given that the objects of critical infrastructure differ in the so-called level of criticality – that is, fall under a certain gradation of importance for the state of national security and sustainability of economic development, we propose to highlight certain characteristics of their financial and economic security table 1.

In the course of any enterprise, institution or organization, financial and economic security should be recognized as an object of management. Only in this case, the management of the entity will cease to consider financial and economic security as a result of external and internal environmental factors that partly determine and partly affect the results of its activities, and realize the need and ability to influence the results of economic and financial risks. Bobro offers to put the task of the object's security protection on the government forces or on the top-management of the business structure – depending on the level of "criticality" of this object for the national security [29]. Thus, it is advisable to distinguish two levels of management of financial and economic security of critical infrastructure objects – public, state, governmental (external) and internal.

Table 1. Features of the concept of financial and economic security of critical infrastructure

Level of importance	Core of financial and economic security essence
National level	Financial and economic security as a mandatory condition for stable functioning of the economic system of the country and for keeping of the proper state of national security
Industry level	Financial and economic security as a situation of supporting the proper level of financial and economic capabilities and the level of functionality of the object of critical infrastructure, giving the possibility to contribute to the stabilization and development of the industry through the mechanisms of efficient use of available resources in the face of external and internal risks, threats and challenges to this process performance
Regional level	Financial and economic security as a set of conditions for the continuous functioning of the economic system for achiving the goal of receiving economic or social effect in the surroundings, full of risks, for the purpose to ensure the sustainability of economic entities relations in the region
Local economic or social system level	Financial and economic security as an availability of the necessary amounts of financial and economic resources and opportunities for their effective use, taking into account the existing risks and threats and the possible consequences of their manifestation to maintain the viability and ensure the proper conditions for the future development of the system

Internal level – a set of management decisions aimed at maintaining financial and economic security through planning, organization, coordination and control of actions to form the resource provision of the business entity and prevent threats to the continuity of this process. External (state) level – a set of administrative, control and supervisory measures to maintain the state of financial and economic security, formed on the object of critical infrastructure or to initiate actions to improve it in the short and long term through advisory, support or enforcement actions in the direction of operation of the critical infrastructure object.

2 Risks caused by quarantine restrictions for the state of financial and economic security of critical infrastructure objects

The main risk posed by quarantine restrictions for all businesses without exception is the forced cessation of their operation, for example, during a period of lockdown announced in the country. At the same time, we should not forget that the concept of risk is dualistic, ie, in addition to a purely negative result that may have a risk to the enterprise, organization and institution, risk is also an opportunity for qualitative change, transformation, modernization of their organizational and business processes. Thus, the transformation of risks in the system of financial and economic security of economic entities into indicators and catalysts for qualitative change – is an important modern task of security professionals.

Ivanenko offers several stages of risk management that can be recommended for use in the context of financial and economic security management of critical infrastructure objects. These are such stages as: "identification of risks as a process of their recognition and description; risk analysis, which involves understanding the nature of risk and determining its level; risk assessment, which involves comparing the results of risk analysis with the criteria for determining whether the risk is acceptable or not acceptable" [30]. At the stage of this scientific study, we will try to identify the risks caused by quarantine restrictions, and currently have a negative impact, or in the future may cause it for the state of financial and economic security of critical infrastructure objects:

- diseases of employees (lack of replacement, downtime of equipment, shutdown of business processes, the need to involve outsiders to ensure the continuity of the work process);
- transport and logistics problems (supply disruptions, delayed delivery of necessary materials, personnel delays to the workplace, the need for additional costs for the organization of transportation of personnel to the place of work);
- non-fulfillment of contractual obligations (the need to cease operations during the lockdown causes a breach of contract by companies that must comply with government decisions and stop work; for critical infrastructure objects this may mean an increase in receivables and payables, breaks in chains supply, loss of customers and partners, the need to find financial and economic alternatives to maintain their own economic viability);
- reduction of the number of orders, refusal of previous agreements on the purchase of products or services due to their loss of relevance during the quarantine period;
- difficulty or inability to work with foreign partners and counterparties due to quarantine restrictions by both (or more) countries whose entities are involved in the process of such cooperation.

New risks, threats and challenges for critical infrastructure objects activities update the search for new approaches to managing their financial and economic security.

3 Features of financial and economic security management of critical infrastructure objects during quarantine restrictions

As already noted, the biggest risk of quarantine restrictions for critical infrastructure objects and for the state as

a whole is the termination of their activities, not due to the decision of the authorities, given the strategic importance of such facilities, but the impossibility of its continuation due to downtime of partners, contractors, etc. Given this, an important vector of financial and economic security management in such conditions should be strategic management, as to determine the potential goals and benchmarks of economic activity in force majeure, is a difficult but necessary management task. Management also needs close attention to the organization of the personnel security system, as most of the risks associated with the epidemiological situation or the source of its origin are connected with a person who can get sick, and this fact will affect the level of intellectual and, ultimately, economic security of the business entity, or the impact of other possible threats, intensified by quarantine and lockdown, will reduce staff efficiency (e.g., lower family budget incomes, higher health care costs, the need to spend time caring for children and elderly relatives, etc.).

3.1 Strategic management of financial and economic security of critical infrastructure objects during quarantine restrictions

Traditional approaches to strategic management of financial and economic security of economic entities are found in numerous publications, for example, [31, 32]. Deeply respecting the opinions of reputable scientists, however, we believe that the paradigms of strategic management in general and financial and economic security in particular in today's economy, given the trends of Industry 4.0 and the epidemiological situation in the world, require revision and modernization. In our opinion, strategic management should be organized according to the TARGET model figure 1.

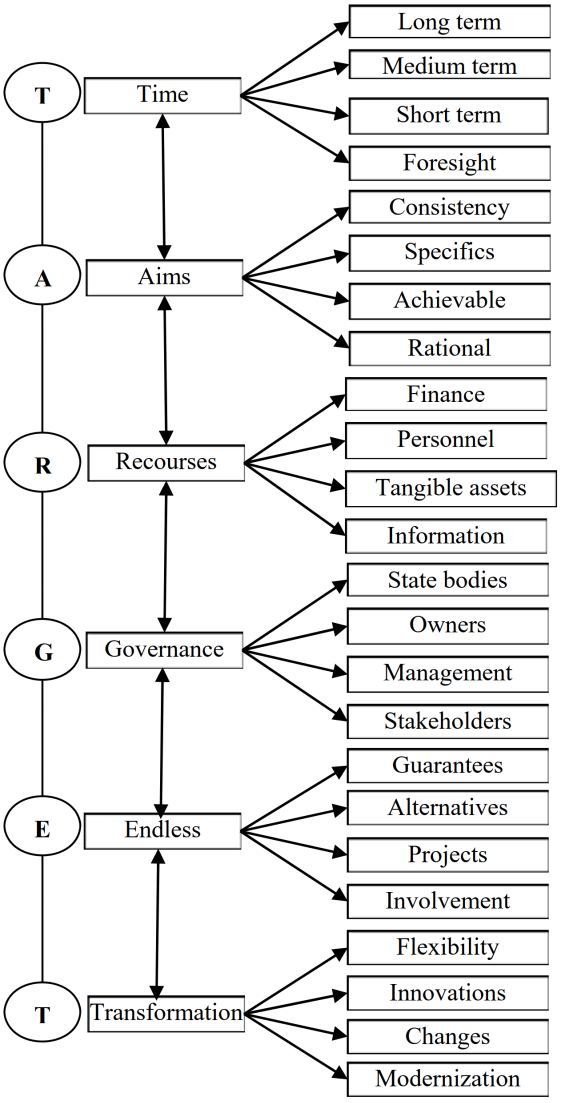

Figure 1. TARGET model for strategic management of financial and economic security of critical infrastructure objects

We will provide some explanations on the essence of the proposed model. Thus, in our opinion, it is necessary to reconsider the very essence of the strategic management process in the context of the time parameter. In the current conditions in Ukraine, to anticipate the company's actions even for one year is a strategy! Strategic management must be transferred from the plane of time, when strategy means one thing – a long-term vision of the company's development, into the plane of goals. That is, the strategy is the goal or goals to be achieved, the means and tools to achieve them, and the time interval for which it must be done may change depending on the factors and circumstances that accompany the activities of the enterprise. Thus, the strategic management of financial and economic security of critical infrastructure should be implemented not in terms of time, but in terms of objectives. However, if the factors and risks of the external and internal environment of the enterprise and their impact are sufficiently predictable, then the time parameter can be divided into short-term, long-term, medium-term. Foresight means the importance of trying to predict developments as one of the tasks of strategic management of financial and economic security.

The goals set by the financial and economic security system of the enterprise manager must be agreed with the interests of different categories of stakeholders, and also should be measurable, achievable and rational from the standpoint of available resources (primarily financial, human, material, informational). Governance (management (supervision, leadership, subordination)), as already mentioned, should be carried out at two levels – internal and external, but the proposed model is not a level one, it used a subjective approach – and identifies the main actors influencing the process of strategic management of financial economic security. For critical infrastructure objects, their list includes: state bodies (supervision, control, monitoring), owners (in the case of state-owned enterprises, these two groups coincide – coordination of strategies), enterprise management (planning, organization, implementation and control of strategic tasks), stakeholders (multifaceted influence on the formation and implementation of strategies for financial and economic security to meet their own interests and within available capabilities).

Endless (continuity, infinity) is a specific feature of financial and economic security management of critical infrastructure objects. We believe that the strategies of such entities should be based on the assumption that their activities will continue for at least a few more decades. To do this, they need to obtain guarantees from public authorities, have several alternatives for each existing partner or counterparty in the event of the possibility of termination of the partnership (such as during quarantine), make the transition to project management within individual business processes – that the completion of one project initiates the beginning of a new one – to expand, improve the results, maximize their effect on the company and introduce a policy of involvement of employees (if not all, then representatives of the workforce) in strategic planning and financial and economic security management.

The last parameter – transformation – means the desire and readiness to upgrade, modernize production, management and other processes in accordance with the requirements of the time and new challenges (eg, global pandemic, quarantine restrictions, lockdown). Characteristic features of such management will be flexibility in making management decisions, even at the strategic level, innovation, change management and modernization of business processes as needed.

3.2 Personnel security of critical infrastructure objects during the quarantine period

Personnel of critical infrastructure object are the most vulnerable to the risks posed by a global pandemic [33]. Stress factors can lead to the fact that the actions or inaction of employees, their temporary absence from work, inattention or concern about the situation in the country, will threaten the state of personnel security of the entity, and as a consequence – will have negative effect and for the state of financial and economic security. The main vectors of work with employees, given the possibility of the need to transfer them to part-time work, leave on schedule, savings on bonuses and other forms of financial incentives, etc., should be: constant channels of communication, maximum information openness, flexibility in the organization work process (where possible) and in the distribution of working time (also if possible), involvement of staff in making various decisions on the organization of the business entity in a pandemic, stimulating leadership and supporting the initiative, etc. table 2.

Thus, the rational management of personnel, support and assistance of people who face new challenges of the global pandemic and quarantine restrictions, are under constant stress, worry about their own well-being, and feel additional responsibility for employment in a strategically important for state needs entity, is important for maintaining the continuous operation of critical infrastructure and the state of their financial and economic security.

4 Conclusions

The updated approach to managing the economic security of business processes in various modifications, taking into account the risks of quarantine restrictions, will be used in all sectors of the national economy, will modernize the management systems of various economic activities, and thus have a positive effect on strategic development of financial system, national economy and achieving a high level of national security and financial and political sovereignty.

The practical importance of the result lies in the next plane. It is expected that the proposed in the study TARGET model for strategic management of financial and economic security of critical infrastructure objects will be the basis for developing strategic documents for stabilizing and further developing and maintaining high functionality of critical infrastructure of Ukraine. In particular, testing the objectives of critical infrastructure development strategies in terms of consistency, specificity, achievable and rationality will allow to adjust them in a timely manner in accordance with existing challenges and time requirements. Compliance of strategic guidelines with the parameters of flexibility, innovation, readiness for change and modernization at the application level will allow to make quickly and effectively restructure of the strategies of critical infrastructure, to change their direction in accordance with new opportunities and needs.

The implementation of the proposals developed within this study at the applied level will be impossible without supply this process with a proper staff. In fact, the personnel component is important for achieving and maintaining the level of financial and economic security in both tactical and strategic areas. Of practical importance is the proposed approach to the formation and implementation of personnel policy for critical infrastructure objects, which, in contrast to existing ones, contains such modern components as staff training; employee incentives; overcoming resistance to change; staff involvement in solving various issues; staff discipline; leadership, partnership and teamwork; time management and self-management; staff safety, staff digital literacy. The presence of personnel policy at the enterprise in the form of a document with the proposed structure will allow top-management to organize personnel work effectively and efficiently and to increase significantly the level of personnel security of critical infrastructure.

The need to update personnel policy appeared due to the risks to staff and to the state of enterprises financial and economic security, which were evident during the epidemic, quarantine measures and lockdown. In particular, it is the inability to organize and work remotely, low level of digital technology using skills, poor communication and other social skills, dishonest performance of duties, failure to meet deadlines for work and projects, and, at the same time, overload, excessive time at the computer, the need to acquire new skills, emotional and professional burnout, declining income, constant stress, etc.

Making timely management decisions will minimize the losses of critical infrastructure objects, prevent their financial instability, reduce the risk of bankruptcy and liquidation in the strategic perspective.

Prospects for further research lie in the plane of possibility of developing methods for assessing the level of

Table 2. Features of the concept of financial and economic security of critical infrastructure

Directions (sections) of personnel policy	Description (details)
Studing	Encouraging staff to take online courses, payment or partial payment for the required higher education, encouragement of various forms of distance learning, providing opportunities for training during the working day (in case of flexible schedule), organization of field training, inviting lecturers, mentors, organizing with them online conferences
Promotion	Performance bonuses, various forms of financial assistance, payment for babysitting services, tutors for children, bonuses for saving and rational use of enterprise resources, compensation for taxi services or fuel for own car, provided if it is used for work purposes
Overcoming resistance to change	Explanatory work on the need for certain changes in production processes or work organization, organization of psychological consultations, involvement of employees in the process of development and implementation of changes, demonstration of intermediate results from the introduction of changes, punishment for active and aggressive resistance to change
Involvement	Striving to achieve the maximum level of employee involvement in all business processes that fall within their field of responsibility
Discipline and organization	Control of discipline, quality of performance of the set tasks, efficiency of labor activity, level of the organization of working process (in case of use of the form of remote work in the conditions of quarantine)
Leadership, partnership and teamwork	Stimulating the manifestation of leadership qualities, periodic rotation of personnel, organization of permanent and temporary teams for the implementation of projects and current tasks of the enterprise
Time management and self-management	Explaining the need and methods of combating chronophages, incentives for efficient and rational use of time, its savings when participating in various business processes
Security	Establishing the priority of occupational safety, life and health of the employee over other production, financial, economic goals of the enterprise; popularization of safety norms and rules, penalties for their violation, introduction of a social package and health insurance
Digital literacy	Assistance to work with digital technologies, gadgets, assistance in organizing the workflow online, organizing and conducting group chats, consulting support for staff working remotely

financial and economic security of critical infrastructure objects and creating strategies for their further development in terms of extending quarantine restrictions or new lockdowns.

References

[1] *Proekt zakonu Ukrayiny Pro krytychnu infrastrukturu ta yiyi zakhyst (Draft Law of Ukraine on Critical Infrastructure and its Protection)* (2019), http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html

[2] National Bank of Ukraine, *Vyznacheno kryteriyi vidnesennya obyektiv bankivskoyi systemy do krytychnoyi infrastruktury (The criteria for assigning the objects of the banking system to the critical infrastructure are defined)* (2020), https://bit.ly/3doFp5A

[3] Verkhovna Rada of Ukraine, *Poryadok vnesennya obyektiv krytychnoyi informatsiynoyi infrastruktury do derzhavnoho reyestru obyektiv krytychnoyi informatsiynoyi infrastruktury, yoho formuvannya ta zabezpechennya funktsionuvannya (The procedure for entering critical information infrastructure facilities in the state register of critical information infrastructure facilities, its formation and operation)* (2020), https://cutt.ly/2vf0xTE

[4] C. Alcaraz, S. Zeadally, International Journal of Critical Infrastructure Protection **8**, 53 (2015)

[5] R. Mosadeghi, R. Richards, R. Tomlinson, *Critical Infrastructure Protection and Uncertainty Analysis* (2017), chap. Chapter 8, pp. 193–223, https://www.worldscientific.com/doi/abs/10.1142/9789813207950_0008

[6] G. Giannopoulos, R. Filippini, M. Schimmer, *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A state of the Art*, JRC Technical Notes (Publications Office of the European Union, Luxembourg, 2012), ISBN 978-92-79-23839-0, https://bit.ly/32jzHvu

[7] D. Rehak, P. Senovsky, S. Slivkova, Systems **6**, 21 (2018)

[8] G. Amélie, B. Aurélia, L. Emmanuel, E. Mohamed, D. Gilles, *The Challenge of Critical Infrastructure Dependency Modelling and Simulation for Emergency Management and Decision Making by the Civil Security Authorities*, in *Critical Information Infrastructures Security*, edited by E. Rome, M. Theocharidou, S. Wolthusen (Springer International Publishing, Cham, 2016), pp. 255–258, ISBN 978-3-319-33331-1

[9] C. Pursiainen, International Journal of Disaster Risk Reduction **27**, 632 (2018)

[10] A. Ianioglo, T. Polajeva, Journal of Business Economics and Management **18**, 1228 (2017)

[11] L. Osberg, A. Sharpe, *Economic Security in Nova Scotia* (2008), http://csls.ca/reports/csls2008-05.pdf

[12] V. Ioan-Franc, M.A. Diamescu, Revista Romana de Economie **31** (2010)

[13] K. Schimmel, S. Liu, J. Nicholls, N. Nechval, J. Forrest, Advances in Systems Science and Applications **17**, 14 (2017)

[14] E. Kopp, L. Kaffenberger, C. Wilson, *Cyber risk, market failures, and financial stability*, https://www.imf.org/-/media/Files/Publications/WP/2017/wp17185.ashx

[15] M. Kośny, M. Piotrowska, *Economic security of households: Assessment based on scenario analysis* (2019), http://www.ecineq.org/ecineq_bari13/FILESxBari13/CR2/p183.pdf

[16] J.S. Hacker, G.A. Huber, A. Nichols, P. Rehm, M. Schlesinger, R. Valletta, S. Craig, Review of Income and Wealth **60**, S5 (2014)

[17] J.S. Hacker, G.A. Huber, P. Rhem, M. Schlesinger, R. Valetta, *Economic Security at Risk: Findings from the Economic Security Index* (The Rockefeller Foundation, New York, NY, 2010), http://economicsecurityindex.org/upload/media/Economic_Security_Index_Full_Report.pdf

[18] S. Bistarelli, F. Fioravanti, P. Peretti, F. Santini, Journal of Experimental & Theoretical Artificial Intelligence **24**, 161 (2012)

[19] J.S. Hacker, G.A. Huber, A. Nichols, P. Rehm, M. Schlesinger, R. Valletta, S. Craig, Review of Income and Wealth **60**, S5 (2014)

[20] M.E. Johnson, E. Goetz, IEEE Security Privacy **5**, 16 (2007)

[21] M. Kahler, The Pacific Review **17**, 485 (2004)

[22] O. Sukhodolia, S. Kondratov, D. Bobro, V. Horbulin, *Developing The Critical Infrastructure Protection System in Ukraine* (NISS, Kyiv, 2017)

[23] R.L. B. J. Allen, *Enterprise Security Risk Management: Concepts and Applications* (Rothstein Publishing, Brookfield, Connecticut, 2017)

[24] A. Wakefield, *Corporate Security and Enterprise Risk Management*, in *Corporate Security in the 21st Century: Theory and Practice in International Perspective*, edited by K. Walby, R.K. Lippert (Palgrave Macmillan UK, London, 2014), pp. 235–253, ISBN 978-1-137-34607-0, https://doi.org/10.1057/9781137346070_13

[25] R. McCormack, A. Lord, *Risky business: Implementing risk management in national security decision-making* (2019)

[26] M. Dehmer, S. Meyer-Nieberg, G. Mihelcic, S. Pickl, M. Zsifkovits, EURO Journal on Decision Processes **3**, 305 (2015)

[27] N.V. Zachosova, Modern econ. pp. 14–25 (2011)

[28] N.V. Zachosova, Econ. Finan. Law pp. 7–13 (2010)

[29] D.B. Bobro, Strat. priorit. pp. 77–85 (2016)

[30] O.I. Ivanenko, Bul. of KNTU pp. 9–22 (2020)

[31] O.V. Cherevko, Efektyvna ekonomika (2014)

[32] I.O. Dotsenko, O.P. Melnychuk, SR pp. 79–84 (2018)

[33] M. Velykodna, Psychodynamic Practice **27**, 10 (2021)