DEVELOPMENT OF CRITICAL INFRASTRUCTURE FROM THE POINT OF VIEW OF INFORMATION SECURITY

DEZVOLTAREA INFRASTRUCTURII CRITICE DIN PUNCT DE VEDERE AL SECURITĂȚII INFORMAȚIILOR

Viktoriia KHAUSTOVA[1]
Mariana Rodica TIRLEA[2]
Lilia DANDARA[3]
Nataliia TRUSHKINA[4]
Iulita BIRCA[5]

Abstract

The rapid transition to digital technologies contributes to the acceleration of the processes of digitization of the development of the ecosystem. This is due to the use of large databases, blockchain, hybrid (combination of online and offline) forms of work, formation of digital platforms and national information infrastructure, activation of electronic commerce, etc. However, this, in turn, leads to the appearance of information security threats and risks, including: the absence of a comprehensive information policy of states, information leakage, use of unlicensed software, data loss due to spyware, cyber crime, cyber attacks, cyber wars, cyber terrorism.

[1] *Doctor of Economic Sciences, Professor Director of the Research Center for Industrial Problems of Development of the National Academy of Sciences of Ukraine (Kharkiv, Ukraine), ORCID: https://orcid.org/0000-0002-5895-9287*
[2] *PhD, Associate Professor „Dimitrie Cantemir" Christian University, Bucharest (Romania) ORCID: https://orcid.org/0000-0002-0665-5839*
[3] *PhD, Associate Professo.r Moldova State University (Republic of Moldova), ORCID: https://orcid.org/0000-0001-7701-5356*
[4] *PhD in Economics, Senior Researcher, Research Center for Industrial Problems of Development of the NAS of Ukraine (Kharkiv, Ukraine) ORCID: https://orcid.org/0000-0002-6741-7738*
[5] *PhD Student University of Suceava "Stefan cel Mare" (Romania) ORCID: https://orcid.org/0000-0002-3910-8022*

Therefore, the article theoretically substantiates the need to form a qualitatively new concept of critical infrastructure development from the standpoint of information security, taking into account modern global challenges and threats.

On the basis of methods of grouping and classification, the approaches to the interpretation of "information security" proposed by various scientific schools are conditionally systematized, according to the following groups: the state of security; field of activity; guarantee system; property of functioning; function of the state; public relations; threat and danger management process. An authors' approach to formulating the meaning of the term „information security" is proposed, the novelty of which is that this definition is based on a comprehensive approach and reflects the continuous process of managing information flows of resources with the aim of increasing competitiveness, ensuring the sustainable development of critical infrastructure and national security. Critical infrastructure is proposed to be considered from the standpoint of ensuring information security in the system of national security of states and restructuring of national economies. From the point of view of information security, the development of critical infrastructure can be understood as the process of transformational changes in information systems and telecommunication networks through the transition of key infrastructure components to a qualitatively new level of functioning thanks to adaptation to the variability and instability of the digital environment, taking into account the impact of possible cyber threats, risks and modern challenges of the global economy.

It has been proven that in order to form a qualitatively new concept of critical infrastructure development from the standpoint of information security and its effective implementation, it is expedient to develop an organizational and economic mechanism, the essence of which is a set of principles, tools, functions, methods and means aimed at reducing the level of cyber risks, the costs of management of information flows and implementation of digital technologies and software.

Further directions of research consist in the theoretical substantiation and development of practical recommendations for the formation of a fundamentally new concept of the development of critical infrastructure from the standpoint of national security.

Key words: digital economy; critical infrastructure; National security; informational security; cyber risks; threats; concept; paradigm; tool kit; mechanisms; digital technologies; risk management; Industry competitiveness; sustainability;

Rezumat

Tranziția rapidă către tehnologiile digitale contribuie la accelerarea proceselor de digitalizare a dezvoltării ecosistemului. Acest lucru se datorează utilizării bazelor de date mari, blockchain, formelor hibride (combinație de online și offline) de lucru, formării platformelor digitale și infrastructurii naționale de informații, activării comerțului electronic etc. Cu toate acestea, acest lucru, la rândul său, duce la apariția unor amenințări și riscuri la adresa securității informațiilor, inclusiv: absența unei politici cuprinzătoare de informare a statelor, scurgeri de informații, utilizarea de software fără licență, pierderi de date din cauza programelor spyware, a criminalității cibernetice, a atacurilor cibernetice, a războaielor cibernetice, a terorismului cibernetic.

Prin urmare, articolul fundamentează teoretic necesitatea formării unui concept calitativ nou de dezvoltare a infrastructurii critice din punct de vedere al securității informațiilor, ținând cont de provocările și amenințările globale moderne.

Pe baza metodelor de grupare și clasificare, abordările de interpretare a „securității informaționale", propuse de diverse școli științifice, sunt sistematizate condiționat, în funcție de următoarele grupe: starea de securitate; domeniul de activitate; sistemul de garantare; proprietatea de funcționare; funcția statului; relații publice; procesul de gestionare a amenințărilor și a pericolelor. De asemenea, autorii propun o abordare în ceea ce privește semnificația termenului „securitatea informațiilor", a cărui noutate este că această definiție se bazează pe o abordare cuprinzătoare și reflectă procesul continuu de gestionare a fluxurilor informaționale de resurse cu scopul de a crește competitivitatea, de a asigura dezvoltarea durabilă a infrastructurii critice și a securității naționale. Astfel, se propune ca infrastructura critică să fie luată în considerare din punctul de vedere al asigurării securității informaționale în sistemul de securitate națională a statelor și al restructurării economiilor naționale. Din punct de vedere al securității informațiilor, dezvoltarea infrastructurii critice poate fi înțeleasă ca procesul de transformare a schimbărilor în sistemele informatice și rețelele de telecomunicații prin tranziția componentelor-cheie ale infrastructurii la un nivel calitativ nou de funcționare datorită adaptării la variabilitatea și instabilitatea mediului digital, ținând seama de impactul posibilelor amenințări cibernetice, riscurile și provocările moderne ale economiei globale.

Cuvinte-cheie: economia digitală; infrastructura critică; securitatea națională; securitatea informațională; riscurile cibernetice; amenințări; concept; paradigmă; instrumente; mecanisme; tehnologii digitale; gestionarea riscurilor; Industria 4.0; competitivitate; durabilitate.

JEL: D80, D81, H54, H56, L86

INTRODUCTION

In recent years, the role of critical infrastructure as an important component of national economies in terms of ensuring information security and minimizing cyber risks and threats has been growing in the world. This is due to the rapid development of the digital economy, a change in the information security paradigm of states in the direction of digital transformation of economic systems of various levels. This, in turn, requires the formation and functioning of the information infrastructure.

Specialists of the McKinsey Global Institute [7] claim that the scale of the development of the digital economy can be compared to the industrial revolution of the 18-19th centuries, which contributed to the radical transformation of the global world, giving many countries an impetus to economic growth, changing the very paradigm of their sustainable development. According to the calculations of the Boston Consulting Group [42], the volume of the digital economy by 2035 will amount to 16 trillion dollars USA.

According to an expert survey of 130 general, operational and technical directors of member companies of the European Business Association [17], it was established that 47% of respondents assessed the level of digital development of their business as moderate, and 39% believe that it is high. However, 9% of respondents claim that the level of digital transformation of their companies is low. At the same time, the vast majority (89% of respondents) indicated that their company's corporate strategy includes digital transformation goals.

According to expert estimates by Forbes [34], the global expenditure on information security increased in 2020 compared to 2015 by 2.3 times, or from 75 to 170 billion dollars USA. The annual growth of the global cyber security market was 9.8% in 2015-2020.

Therefore, the digital transformation observed in many sectors of the national economy has led to the emergence of new challenges and risks of information security, which should be given special attention in order to increase competitiveness and achieve sustainable infrastructure development.

In view of this, the need for theoretical and methodological justification of the development of critical infrastructure from the point of view of information security in the national security system determines the conduct of further research. Firstly, this concerns the clarification of the conceptual and categorical apparatus in the direction of defining the essence and content of the terms "development", "critical infrastructure", "cyber security", "information security", "national security", "development of critical infrastructure from the point of view of information security". This will make it possible to substantiate the conceptual provisions of strategic management of the development of critical infrastructure.

ANALYSIS OF LITERATURE

Critical analysis shows that to date, scientists have not developed a unified approach to understanding the essence of the concept of "development". This is due to the fact that many scientific schools have been formed at the moment, which have specific approaches to the formulation of the terminological apparatus. Some scientists equate the concept of development with evolution, growth, improvement, improvement, etc. But for the most part, leading scientists distinguish between these scientific categories, understanding development as a law, principle, system component, changes, phenomenon, action, process, result, property of system objects.

Based on the generalization of scientific literature, it was found that leading scientists (H. Dźwigoł [10-12]; A. Karbownik et al. [23]; A. Kwilinski [28]; H. Dźwigol et al. [13]; A. Ahadiat & Z. Dacko-Pikiewicz [1]; P. Saługa et al. [43]; R. Miśkiewicz et al. [33]; K. Szczepańska-Woszczyna & S. Gatnar [51] and others) consider development as a general scientific category or concept in economics.

A separate place in the economic area is given to various aspects of the development of the enterprise as an economic system; effective development of business entities; economic development; sustainable development.

At the same time, researchers interpret development as a process (a specific process of change; a process resulting in a change in the quality of a phenomenon; a process resulting in a transition from one qualitative state to another; a process of quantitative and qualitative changes in a phenomenon unfolding over time; an immanent process, the source of which contained in the developing object itself; the process of changing the structure of the system; a continuous process of various forms of interactions within the system; an irreversible, directed, regular and unique process of changes in an open system in space and time; the process of forming a new open system, which is expressed in qualitative changes in the composition, structure and way of functioning of the system; a closely interconnected process of quantitative and qualitative transformations); changes (a set of quantitative, qualitative and structural transformations); a component of the system (deepening the composition of something, adding something new to it, previously unknown).

However, in modern conditions, the concept of "development" should be considered from the perspective of transformational economics, taking into account the significant influence of exogenous and endogenous factors and the emergence of new challenges of the time. Among them, we can indicate such as the activation and deepening of the processes of globalization and European integration, transformation, digitalization, infrastructural support and the transition to network forms of interaction and partnership [24; 29], the use of the toolkit of green logistics [14; 15] and circular economy [19; 53], etc. Therefore, the concept of "development" is proposed to be interpreted as: (1) the process of transformation of economic systems [5] through the transition of key components (for example, critical infrastructure) to a qualitatively new

level of functioning due to adaptation to the variability and instability of external factors and internal institutional environment; (2) a dynamic process that leads to structural changes (economic, social, organizational, environmental, etc.) of objects and networks occurring in a multi-component spatial system.

The study of various aspects of the development of infrastructure as a multifunctional system that ensures the functioning of economic systems is given considerable attention in the works of leading scientists (D. Aschauer [2]; M. Blaiklock [6]; J. Clark [8]; B. Frischmann [18]; G. Hedtkamp [20]; A. Hirschman [21]; R. Jochimsen [22]; W. Lewis [31]; A. Marshall [32]; K. Murphy et al. [35]; P. Samuelson & W. Nordhaus [45]; R. Nurkse [36]; A. Pesenti [37]; P. Rosenstein-Rodan [40]; W. Rostow [41]; P. Samuelson [44]; U. Simonis [48]; H. Singer [49]; A. Youngson [58] and others).

Based on the generalization of the existing scientific approaches to the formulation of the term "infrastructure", they are conditionally systematized according to the following groups: system; resource; mechanism; systemic economic category; a component of the economic system; complex of types of economic activity; part of the economy; appropriate conditions (institutional, economic, social, environmental); a component of the environment; component of the spatial system.

In the scientific literature (R. Srinivasan & A. Parlikad [50]; C. Zhang et al. [59]; R. Wróbel [57]; B. Rathnayaka et al. [38]; D. Rehak et al. [39]; L. Shen et al. [47]; C. Scholz et al. [46] and others), many interpretations of the concept of "critical infrastructure" are used from different positions, including cyber security in the national security system.

Summarizing the existing scientific developments regarding the conceptual apparatus, it was established that scientists usually understand critical infrastructure as: a complex system; its key components or components; critical infrastructure facilities; network structure; physical structure; organizational structures; institutes; institutions; institutions; set of assets; object of administrative and legal protection; object of cyber protection; security direction; one of the security tasks of the state; a component of the national infrastructure; a set of objects, technologies, state and scientific structures; object of state administration; component of information security; an element of the national security system of the state or region.

The analysis of scientific sources shows that, to date, a single approach to the interpretation of information security [4; 26; 52] and cyber security has not yet been identified. This is due to the fact that scientists are representatives of various economic theories and schools with their own scientific approaches and features, as well as the ambiguity and multifacetedness of these concepts. It can be noted that most researchers under the concept of "information security" consider the state, sphere of activity, system of guarantees, property of functioning, ability, function of the state, social relations, the process of managing threats and dangers, etc.

In scientific sources, this concept is usually defined as: the priority function of the state; the state of legal norms and their corresponding security institutions; a

set of means of ensuring the information sovereignty of the state; security status; an integrated component of national security; a component of economic security; the state of information work of business entities; the state of legal norms and their corresponding security institutions; legislative formation of state information policy; creation and implementation of safe information technologies; multi-aspect system from the standpoint of a systemic approach; multidisciplinary field, etc.

Thus, this problem determined the purpose of this article, which consists in substantiating the conceptual provisions of the development of critical infrastructure from the standpoint of ensuring information security and restructuring the economy.

METHODS AND METHODOLOGY

The theoretical and methodological basis of the research is the provisions of the institutional theory, in particular paradigms of evolutionary development; theory of systems, globalization, clustering, transaction costs, infrastructure; concepts of transport logistics, strategic, marketing and logistics management, national and information security, sustainable development. The research is based on systemic, structural-functional, linguistic, synergistic and logical-semantic approaches.

The following general scientific methods were used in the research process: dialectical, historical, formal-logical, axiomatic, theory of logic and hypothetical-deductive, analysis and synthesis, induction and deduction, component analysis, comparison, analogy, classification, expert survey, structural-logical generalization.

According to the results of a survey of 600 top managers of large international companies conducted by Deloitte as part of the study "The Future of Cyberspace in 2021" [9], it was found that 69% of respondents note a significant increase in cyber threats and risks for their business since the beginning of 2020. Almost 75% of respondents who had an income of more than 30 billion dollars. The United States announced that it will spend more than 100 million dollars on cyber security.

The EY Global Information Security Survey [16] showed that the company's revenue in 2021 was approximately 11 billion dollars. While annual information security costs averaged only 5.28 million dollars. It was found that 56% of representatives of companies with insufficient budgets note the review of cybersecurity requirements. And 44% said they were forced to cut costs and focus on their legacy architecture and information systems.

At the same time, 39% of respondents noted that the costs of cyber security are not properly taken into account in the cost of strategic investments related to the digital transformation of supply chains. 36% of respondents believe that they could face a serious breach of information security, which can be avoided if the company increases the amount of investments in cyber protection tools.

In the Barracuda Networks State of Industrial Security 2022 Report [3], which

was prepared based on the results of a survey of 800 IT managers, senior IT security managers and project managers responsible for the Internet of Things (IoT) and operational technologies (OT) in their organizations, it is stated that critical infrastructure is at risk of cyber attacks. In the current threat environment, critical infrastructure is an attractive target for cybercriminals.

But IoT/OT security projects often lag behind other security initiatives or fail due to cost or complexity, exposing them to risk. Issues such as the lack of network segmentation and the number of organizations that do not require multifactor authentication (MFA) make networks vulnerable to attack and require immediate and special attention. Research shows that 94% of surveyed organizations have experienced security incidents in the past year.

All survey participants recognized the importance of further investment in IoT and OT security. At the same time, 96% of business leaders noted that their organizations need to increase investments in industrial security. 72% of companies reported that they have either already implemented or are in the process of implementing IoT/OT security projects.

However, many face significant challenges when it comes to implementation. 93% of companies have failed their IoT/OT security projects. Critical infrastructure organizations are leading the way in implementing cyber security solutions, and 50% of oil and gas companies have completed projects. Completed projects in production make up 24%, in the field of health care – 17%.

Multifactor authentication (MFA) is rarely used: only 18% of surveyed companies restrict network access and use multifactor authentication when it comes to remote access to OT networks. Low adoption of MFA prevails even in mission-critical industries, with critical verticals such as energy (47%) enabling full MFA-free remote access for external users. Only 49% of organizations can install security updates themselves. This suggests a lack of job skills to make informed cybersecurity decisions.

As stated in the World Economic Forum (WEF) Cyber Security Center Report "Global Outlook for Cyber Security to 2022" [56], 92% of surveyed business leaders agree that cyber resilience is integrated into risk management strategies.

However, only 55% of security-oriented respondents agree with this statement. 84% of respondents say that cyber resilience is considered a business priority in their organization, supported by management.

However, 68% of respondents see cyber resilience as a core part of overall risk management. According to the results of the survey, 59% of all respondents consider it difficult to adequately respond to a cyber security incident due to the lack of qualified specialists in their team.

In the KPMG Cyber trust insights 2022 survey (1881 CEOs from around the world) conducted by KPMG [25], it was found that more than 80% of respondents recognized the importance of improving cyber security and data protection, including increasing the transparency of data usage.

In particular, 51% considered protecting IT assets from attacks extremely important. As organizations engage in digital transformation, it will be necessary to budget for investments in cybersecurity and privacy.

And it will increasingly be seen as an integral part of these strategic initiatives. 31% of respondents are concerned about the growing requirements for critical infrastructure facilities, which are subject to increased regulation in Great Britain, the EU and the United States.

In the survey, 44% of respondents say that collaborating on cybersecurity issues within the broader ecosystem will help them, for example, predict attacks. In addition, 38% of surveyed company executives note that confidentiality issues stand in the way of external partnerships in the field of cybersecurity, and 36% fear that they will disclose too much information about their own security measures. Other challenges include regulatory constraints, lack of support from senior management, and insufficient resources.

A Global Cyber Security Survey [27] showed that 18% of respondents expect future cyberattacks on their organizations by state-sponsored hackers. And although 8% expressed the opinion that they do not expect an effective solution to this problem at all (this opinion is shared by respondents whose organization is on the list of critical infrastructure objects).

It is worth emphasizing that 10% of surveyed organizations still do not have a cyber security strategy.

Respondents indicated that limited skills, outdated network technologies and security tools increase vulnerability. Most respondents (over 90%) say they have shared information about attacks, but not always complete information about the attack or its consequences.

About 9 in 10 respondents believe their government should do more to support organizations (91%) and protect critical infrastructure (90%) from cyberattacks sponsored by a hostile state.

RESEARCH RESULTS

As a result of the study [30; 54; 55], it was proved that for the effective development of critical infrastructure, it is necessary to form an appropriate concept (*Fig. 1*), the constituent elements of which are resources; influencing factors; goals, principles, functions, methods, control levers; digital technologies and information systems; financial financing tools (crowdsourcing, crowdfunding, grants from European and international financial organizations, technical assistance from international financial organizations, financial resources of investment funds, etc.); public-private partnership mechanisms; performance criteria.

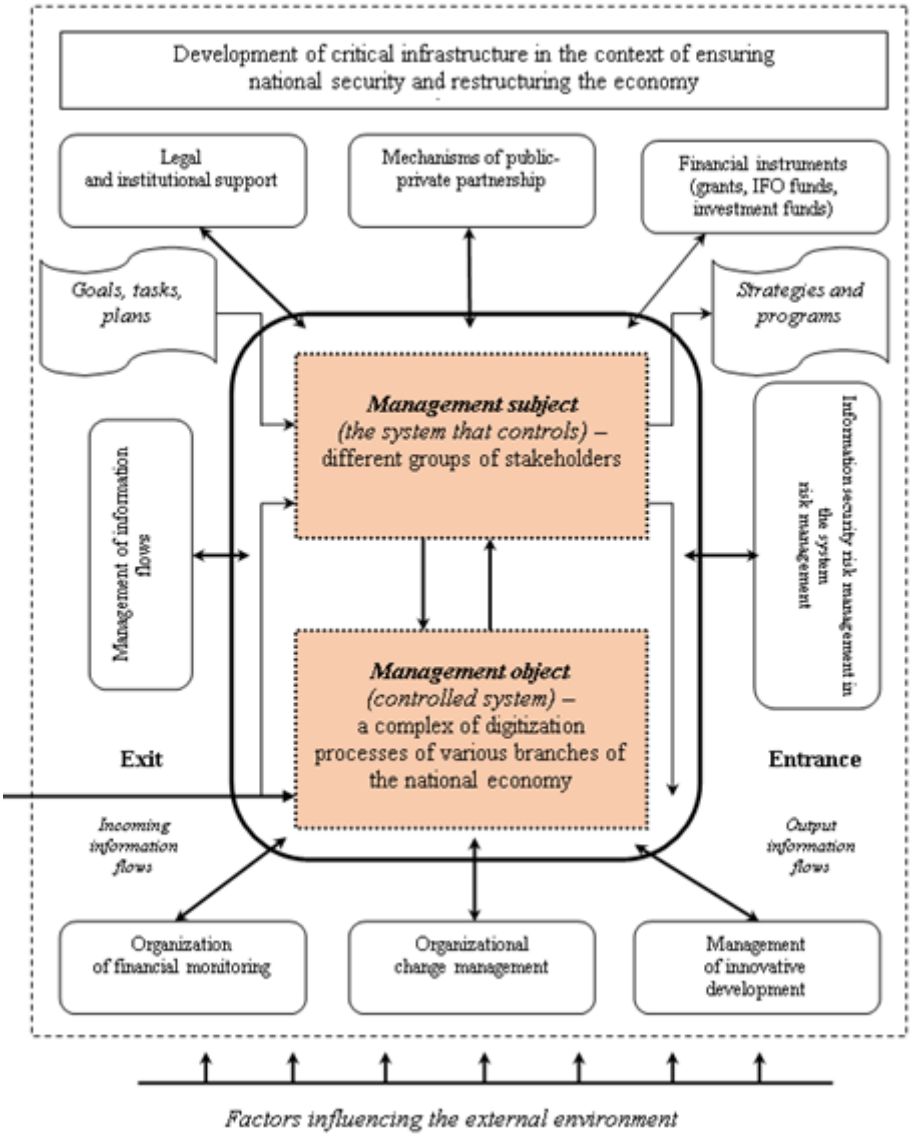
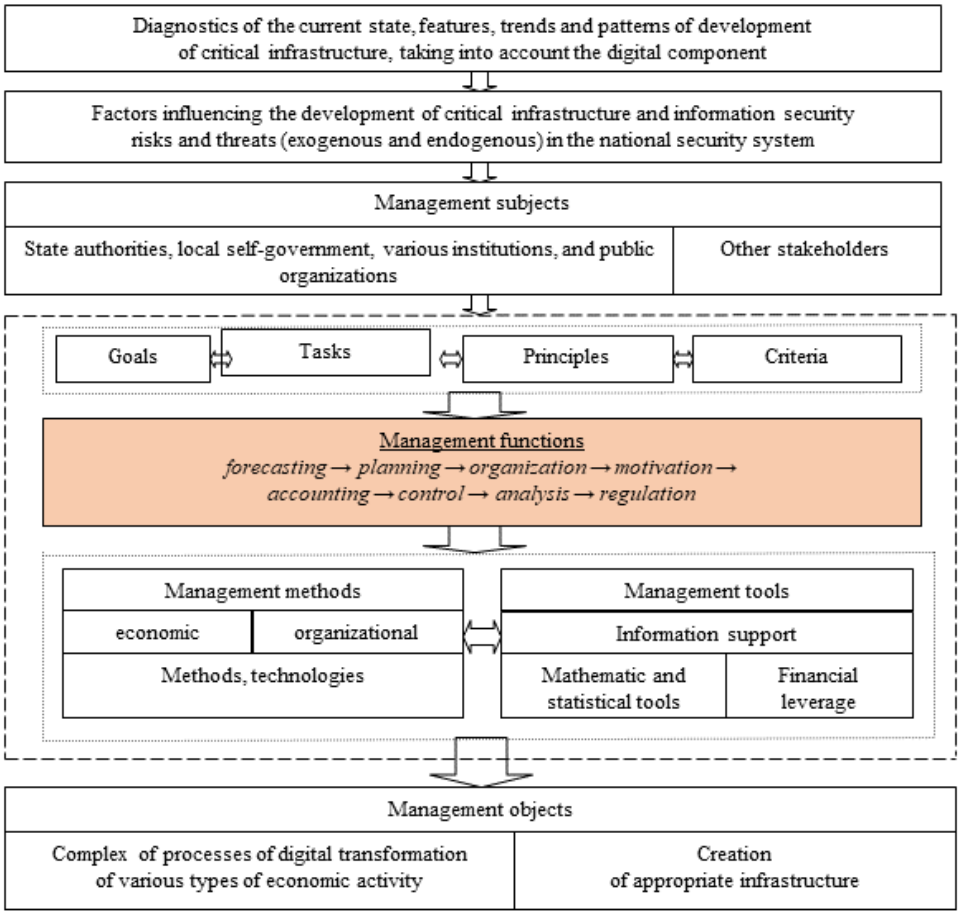


Figure 1. Structural and Logical Scheme of the Formation of the Concept of Development of Critical Infrastructure from the Point of View of Information Security

Source: development of authors.

In order to effectively implement the concept of the development of critical infrastructure in conditions of digitalization, it is advisable to develop an organizational and economic mechanism, the essence of which is a set of principles, tools, functions, methods and means aimed at reducing the level of cyber risks, costs of managing information flows and the introduction of digital technologies and software provision (*Fig. 2*).

Figure 2. The Main Elements of the Organizational and Economic



Mechanism of Implementing the Concept of Critical Infrastructure Development from the Point of View of Information Security

Source: development of authors.

Systematically, consistency, integration, reliability, complexity, presence of

connections, hierarchy, emergency, complexity, integrity, synergy (manifestation of synergistic effect), flexibility, dynamism, adaptability, targeting of complex efficiency can be attributed to the key principles of concept formation.

To minimize the negative consequences of possible cyber threats, it is necessary to pay attention to:

- levelling of information security risks;
- improvement of legislation on national and information security of the state;
- application of appropriate methodological tools;
- creation of a national model of the digital environment;
- formation of critical information infrastructure;
- implementation of a set of measures and relevant mechanisms of regulatory, institutional, financial, organizational and economic support for the development of critical infrastructure;
- implementation of the national cyber security strategy.

CONCLUSIONS

Based on the above, we can come to the following conclusion. At the moment, the concept of critical infrastructure development is being implemented in most countries of the world, which should reflect current problems, include ways to solve them, and also meet modern global challenges, especially from the point of view of security, stability, reliability, functionality, integrity. Therefore, the protection of critical infrastructure from numerous global cyber threats and information risks becomes a strategic task at the national level and is of crucial importance for maintaining the adequate functioning of ecosystems and ensuring their sustainable, inclusive and smart development.

At the same time, it is worth noting that in the transformational economy, the objects of the information infrastructure, which are heterogeneous in any state, play a huge role. And firstly, it is necessary to ensure the safety of "points", the failure of which can significantly affect the stability of the functioning of society and the state. These are nodes that ensure stable operation of the entire information infrastructure. Digitalization is impossible without maintaining the working condition of information infrastructure objects, which depend on the security of the state and society. Most often, such key "points" of the information infrastructure are called critical information infrastructure (information systems, information and telecommunication networks, automated control systems).

For example, in the People's Republic of China, security measures for critical information infrastructure are entrusted to the state. The country adopted the Law on Cybersecurity, in which Critical Information Infrastructure is interpreted as public communications and information services, public administration, water supply,

finance, public services, electronic management and other critical information infrastructure, which in case of its destruction, violation functionality or data loss may actually threaten national security, national welfare, people's livelihoods, or the public interest.

In India, there is an Information Technology Act (2008), according to which critical information infrastructure (Critical Information Infrastructure) computer resources, the failure or destruction of which will affect the national security, economy and social welfare of the nation (Article 70). The legislative document delineates the sector of telecommunications and information technologies. That is, information technologies are considered as an independent, critically important sector of the national infrastructure. According to the Information Technology Act, the National Critical Information Infrastructure Protection Center (NCIIPC) of India was established in 2014.

In international legislation, there is a lack of a unified approach to defining the criteria and features of critical information infrastructure. In many ways, the regulatory definition of critical information infrastructure is related to the concepts of national cyber security and its priorities. In some countries of the world, critical information infrastructure is considered as information infrastructure of traditional critical infrastructure. At the same time, the understanding is developing that nodes of the information infrastructure, which are not connected to any objects of the traditional critical infrastructure, can also be of critical importance in the conditions of the transition to the digital economy and the information society.

As a result of the conducted research, it was established that the concept of "critical infrastructure" is identified with such definitions as: infrastructure; life support systems; critical infrastructure facilities; vital social functions; products, goods, services and related processes.

With the use of the system approach and the classification method, the interpretation of the term "critical infrastructure" proposed by various scientific schools is conventionally systematized, according to such groups as: system; elements of the system; structure (network, physical, organizational); set of assets; security direction; the key security task of the state; object of protection (administrative-legal, cybernetic); a component of the national infrastructure; object of state administration; a component of information security, etc.

In this work, it is proposed to consider critical infrastructure from the standpoint of ensuring information security in the system of national security of states and restructuring of national economies.

Based on the generalization of conceptual provisions regarding this issue, it is proposed to interpret the term "information security" as an important factor in achieving stable and effective functioning of critical infrastructure objects in the system of the national economy, and "cyber security" (from two positions) as a practical activity aimed at protection of critical infrastructure (set of objects, systems,

networks) against cyber attacks and threats; an effective tool for protecting critical infrastructure in cyberspace.

From the point of view of information security, the development of critical infrastructure can be understood as the process of transformational changes in information systems and telecommunication networks through the transition of key infrastructure components to a qualitatively new level of functioning thanks to adaptation to the variability and instability of the digital environment, taking into account the impact of possible cyber threats, risks and modern challenges of the global economy.

It is worth noting that the scientific novelty of this research consists in the combination, symbiosis and integration of the categories "development", "infrastructure", "critical infrastructure", "security", "information security", "cyber security" taking into account the factors of the exogenous and endogenous environment, peculiarities, patterns, trends in the development of processes, qualitative transformations with the presence of interrelationships of organizational, digital, logistical, foreign economic, innovative and social transformations characterized by quantitative and qualitative changes. This makes it possible to achieve the set goals, to take into account various aspects of the development of critical infrastructure facilities in the conditions of the digital economy.

In further studies, it is planned to clarify the essence and content of the concepts "security of critical infrastructure", "protection of critical infrastructure", "sustainability of critical infrastructure".

BIBLIOGRAPHY

Ahadiat, A., Dacko-Pikiewicz, Z. (2020). Effects of ethical leadership and employee commitment on employees' work passion. *Polish Journal of Management Studies*, vol. 21, no. 2, pp. 24-35. http://dx.doi.org/10.17512/pjms.2020.21.2.02.

Aschauer, D. A. (1989). Is Public Expenditure Productive? *Journal of Monetary Economics*, vol. 23, no. 2, pp. 177-200. https://doi.org/10.1016/0304-3932(89)90047-0.

Barracuda (2022). Market Report. The state of industrial security in 2022. https://assets.barracuda.com/assets/docs/dms/NetSec_Report_The_State_of_IIoT_final.pdf.

Bezpartochna, O., Pushak, Ya., Trushkina, N. (2022). Current issues of information security management during the state of martial. *Current issues of security management during martial law*: scientific monograph. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, pp. 8-19.

Bezpartochnyi, M., Revenko, D., Dolha, H., Trushkina, N. (2022). Model Tools for Diagnosing the Stability and Survivability of Economic Systems. *Distributed*

Sensing and Intelligent Systems. Studies in Distributed Intelligence / Edited by M. Elhoseny, X. Yuan, Sd. Krit. Switzerland, Cham: Springer, pp. 275-288. https://doi.org/10.1007/978-3-030-64258-7_25.

Blaiklock, M. (2014). The infrastructure finance handbook: principles, practice and experience. London: Euromoney Books.

Boden, M., Cagnin, C., Carabias, V., Haegeman, K., Könnölä, T. (2010). *Facing the future: time for the EU to meet global challenges*. Luxembourg: Publications Office of the European Union.

Clark, J. M. (1923). Studies in the Economics of Overhead Costs. Chicago: University of Chicago Press.

Deloitte (2021). Deloitte Global 2021 Future of Cyber Survey finds rapid increase in cyberattacks driven by organisations' embrace of digital transformation. https://www2.deloitte.com/mm/en/pages/risk/articles/deloitte-global-2021-future-of-cyber-survey-finds-rapid-increase-in-cyberattacks.html.

Dźwigoł, H. (2008). Problemy zarządzania nowoczesnymi organizacjami gospodarczymi. *Czynniki kształtujące elementy systemu zarządzania współczesną organizacją*, nr. 158, ss. 57-69.

Dzwigol, H. (2016). Modelling of Restructuring Process. *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, nr. 99, ss. 89-106.

Dzwigol, H. (2021). Meta-analysis in management and quality sciences. *Marketing and Management of Innovations*, vol. 1, pp. 324-335. https://doi.org/10.21272/mmi.2021.1-25.

Dźwigol, H., Dźwigoł-Barosz, M., Zhyvko, Z., Miśkiewicz, R., Pushak, H. (2019). Evaluation of the energy security as a component of national security of the country. *Journal of Security and Sustainability Issues*, vol. 8, no. 3, pp. 307-317.

Dzwigol, H., Trushkina, N., Kwilinski, A. (2021). The Organizational and Economic Mechanism of Implementing the Concept of Green Logistics. *Virtual Economics*, vol. 4, no. 2, 74-108. https://doi.org/10.34021/ ve.2021.04.02(3).

Dźwigoł, H., Kwilinski, A., Trushkina, N. (2021). Green Logistics as a Sustainable Development Concept of Logistics Systems in a Circular Economy. *Proceedings of the 37th International Business Information Management Association (IBIMA)*, 1-2 April 2021 (pp. 10862-10874). Cordoba, Spain: IBIMA Publishing.

Ernst & Young (2021). Cybersecurity: how do you rise above the waves of a perfect storm? EY Global Information Security Survey 2021. https://www.ey.com/en_gl/ cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm.

European Business Association (2021). Digital Transformation Index 2021. https://eba.com.ua/wp-content/uploads/2021/05/digital-index_ukr1.pdf. (in Ukrainian)

Frischmann, B. M. (2013). *Infrastructure: the social value of shared resources*. New York: Oxford University Press.

Ganea, V., Trushkina, N., Ţîrlea, M. R., Birca, I. (2022). Economia circulară – un model de perspectivă pentru Republica Moldova [Circular Economy – a Perspective Model for the Republic of Moldova]. *UNIVERS STRATEGIC – Revistă de Studii Strategice Interdisciplinare şi de Securitate*, Anul XIII, nr. 4(52), pp. 52-68.

Hedtkamp, G. (1996). *Die Bedeutungder Infrastruktur in makrookonomischer Sicht*. Munchen: Osteuropa-Inst.

Hirschman, A. O. (1958). *The strategy of economic development*. New Haven, Conn: Yale University Press.

Jochimsen, R. (1966). *Theorie der Infrastruktur: Grundlagen der marktwirtschaftlichen Entwicklung*. Tübingen: J.C.B. Mohr.

Karbownik, A., Dźwigoł, H., Wodarski, K. (2012). System zarządzania ryzykiem uczelni wyższej. *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, nr. 60, ss. 125-139.

Khaustova, V. Ye., Trushkina, N. V. (2022). Teoretychni pidkhody do vyznachennia poniattia "merezheva struktura" [Theoretical approaches to defining the concept of "network structure"]. *Business Inform*, no. 8, pp. 12-19. https://doi.org/10.32983/2222-4459-2022-8-12-19. (in Ukrainian)

KPMG (2022). KPMG Cyber trust insights 2022. Building trust through cybersecurity and privacy. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/10/kpmg-cyber-trust-insights-2022.pdf.

Kryshtanovych, S., Prosovych, O., Panas, Y., Trushkina, N., Omelchenko, V. (2022). Features of the Socio-Economic Development of the Countries of the World under the influence of the Digital Economy and COVID-19. *International Journal of Computer Science and Network Security*, vol. 22, no. 1, pp. 9-14. https://doi.org/10.22937/IJCSNS.2022.22.2.2.

Kryvenko, P. (2022). Survey in the field of protection against cyber threats. https://www.newgeopolitics.org/2022/08/13/survey-in-the-field-of-protection-against-cyber-threats/.

Kwilinski, A. (2017). Development of industrial enterprise in the conditions of formation of information economics. *Thai Science Review*, Autumn, pp. 85-90.

Kyzym, M. O., Khaustova, V. Ye., Trushkina, N. V. (2022). Merezheva ekonomika: evoliutsiia rozvytku, peredumovy stanovlennia kontseptsii, kontseptualni pidkhody do vyznachennia [Network economy: evolution of development, prerequisites for the formation of the concept, conceptual approaches to definition]. *Business Inform*, no. 11, pp. 40-51. https://doi.org/10.32983/2222-4459-2022-11-40-51. (in Ukrainian)

Kyzym, M. O., Khaustova, V. Ye., Trushkina, N. V. (2022). Sutnist poniattia «krytychna infrastruktura» z pozytsii natsionalnoi bezpeky Ukrainy [The essence of the concept of "Critical Infrastructure" from the standpoint of national security of Ukraine]. *Business Inform*, no. 12, pp. 58-78. https://doi.org/10.32983/2222-4459-2022-12-58-78. (in Ukrainian)

Lewis, W. A. (1955). *The Theory of Economic Growth*. London: G. Allen & Unwin Ltd.

Marshall, A. (1920). *Principles of Economics* (Revised ed.). London: Macmillan; reprinted by Prometheus Books.

Miśkiewicz, R., Rzepka, A., Borowiecki, R., Olesińki, Z. (2021). Energy Efficiency in the Industry 4.0 Era: Attributes of Teal Organizations. *Energies*, vol. 14, iss. 20, 6776. https://doi.org/10.3390/en14206776.

Morgan, S. (2016). Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020. *Forbes*. March 9. https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/?sh=18e4e3366832.

Murphy, K., Schleifer, A., Vishny, R. W. (1989). Industrialization and the Big Push. *Journal of Political Economy*, vol. 97, no. 5, pp. 1003-1026.

Nurkse, R. (1966). *Problems of Capital Formation in Underdeveloped Countries*. Oxford: Oxford University Press.

Pesenti, A. (1970). *Manuale di economia politica*. Vol. primo. Roma: Editori Riuniti Nuova Biblioteca di Cultura.

Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D., Setunge, S. (2022). Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. *International Journal of Disaster Risk Reduction*, vol. 78, 103123. https://doi.org/10.1016/ j.ijdrr.2022.103123.

Rehak, D., Hromada, M., Onderkova, V., Walker, N., Fuggini, C. (2022). Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security. *International Journal of Electrical Power & Energy Systems*, vol. 136, 107700. https://doi.org/10.1016/ j.ijepes.2021.107700.

Rosenstein-Rodan, P. (1961). Notes on the Theory of the "Big Push". *Economic Development for Latin America. International Economic Association Series* / Edited by H. S. Ellis. London: Palgrave Macmillan, pp. 57-81. https://doi.org/10.1007/978-1-349-08449-4_3.

Rostow, W. W. (1962). *The Stages of Economic Growth*. London: Cambridge University Press.

Ruan, F., Tsai, R., Zhang, K., Zheng, T. (2017). Year 2035: 400 Million Job Opportunities in the Digital Age. *The Boston Consulting Group*. https://web-assets.bcg.com/img-src/BCG_Year-2035_400-Million-Job-Opportunities-Digital%20Age_ENG_Mar2017_tcm9-153963.pdf.

Saługa, P. W., Szczepańska-Woszczyna, K., Miśkiewicz, R., Chład, M. (2020). Cost of equity of coal-fired power generation projects in Poland: Its importance for the management of decision-making process. *Energies*, vol. 13, iss. 18, 4833. https://doi.org/10.3390/en13184833.

Samuelson, P. A. (1954). The Pure Theory of Public Expenditure. *The Review of Economics and Statistics*, vol. 36, no. 4, pp. 387-389.

Samuelson, P., Nordhaus, W. (2009). *Economics*. 19th ed. New York: McGraw Hill.

Scholz, C., Schauer, S., Latzenhofer, M. (2022). The emergence of new critical infrastructures. Is the COVID-19 pandemic shifting our perspective on what critical infrastructures are? *International Journal of Disaster Risk Reduction*, vol. 83, 103419. https://doi.org/10.1016/j.ijdrr.2022.103419.

Shen, L., Li, J., Suo, W. (2022). Risk response for critical infrastructures with multiple interdependent risks: A scenario-based extended CBR approach. *Computers & Industrial Engineering*, vol. 174, 108766. https://doi.org/10.1016/j.cie.2022.108766.

Simonis, U. E. (1989). Ecological Modernization of Industrial Society – Three Strategic Elements. *Economy and Ecology: Towards Sustainable Development. Volume 1: Economy & Environment* / Edited by F. Archibugi, P. Nijkamp. Dordrecht: Springer, pp. 119-137. https://doi.org/10.1007/978-94-015-7831-8_7.

Singer, H. W. (1964). *International Development: Growth and Change*. New York: McGraw-Hill.

Srinivasan, R., Parlikad, A. K. (2013). Value of condition monitoring in infrastructure maintenance. *Computers & Industrial Engineering*, vol. 66, iss. 2, pp. 233-241. https://doi.org/10.1016/j.cie.2013.05.022.

Szczepańska-Woszczyna, K., Gatnar, S. (2022). Key Competences of Research and Development Project Managers in High Technology Sector. *Forum Scientiae Oeconomia*, vol. 10, no. 3, pp. 107-130. https://doi.org/10.23762/ FSO_VOL10_NO3_6.

Trushkina, N. (2019). Development of the information economy under the conditions of global economic transformations: features, factors and prospects. *Virtual Economics*, vol. 2, no. 4, pp. 7-25. https://doi.org/10.34021/ve.2019.02.04(1).

Trushkina, N., Prokopyshyn, O. (2021). Circular economy as a new way of managing in the conditions of digital transformations. *Green, Blue & Digital Economy Journal*, vol. 2, no. 3, pp. 64-71. https://doi.org/10.30525/2661-5169/2021-3-10.

Trushkina, N. V. (2023). Rozvytok krytychnoi informatsiinoi infrastruktury z pozytsii kiberbezpeky: teoretychni aspekty [Development of critical information infrastructure from the point of view of cyber security: theoretical aspects]. *Upravlinnia sotsialno-ekonomichnymy systemamy na osnovi pidvyshchennia efektyvnosti marketynhovykh posluh v umovakh didzhytalizatsii [Management of socio-economic systems on the basis of increasing the effectiveness of marketing services in the conditions of digitalization]*: a collective monograph / Edited by V. I. Chobitok; Ukrainian Engineering and Pedagogical Academy. Kharkiv: I. S. Ivanchenko Publishing House, pp. 206-215. (in Ukrainian)

Trushkina, N. (2023). Sutnist poniattia "rozvytok krytychnoi infrastruktury" [The essence of the concept of "development of critical infrastructure"]. *Moderní aspekty vědy*: XXIX. Díl mezinárodní kolektivní monografie. Česká republika,

Jesenice: Mezinárodní Ekonomický Institut s.r.o., 2023. Str. 149-163. (in Ukrainian)

World Economic Forum (2022). Global Cybersecurity Outlook 2022. Insight Report. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

Wróbel, R. (2019). Dependencies of elements recognized as critical infrastructure of the state. *Transportation Research Procedia*, vol. 40, pp. 1625-1632. https://doi.org/10.1016/ j.trpro.2019.07.225.

Youngson, A. (1967). *Overhead Capital: Study Development Economics*. 1st ed. Edinburgh: Edinburgh University Press.

Zhang, C., Liu, X., Jiang, Y. P., Fan, B., Song, X. (2016). A two-stage resource allocation model for lifeline systems quick response with vulnerability analysis. *European Journal of Operational Research*, vol. 250, iss. 3, pp. 855-864. https://doi.org/10.1016/ j.ejor.2015.10.022.