DEPÓSITO LEGAL ZU2020000153
ISSN 0041-8811
E-ISSN 2665-0428

Revista de la Universidad del Zulia

Fundada en 1947
por el Dr. Jesús Enrique Lossada

Ciencias del Agro, Ingeniería y Tecnología

Año 15 N° 42
Enero - Abril 2024
Tercera Época
Maracaibo-Venezuela

DOI: https://doi.org/10.46925//rdluz.42.22

Mechanisms of State Management of the Development of Digital Technologies in the National Security System

Viktoriia Marhasova*
Olha Rudenko**
Olha Popelo***
Iryna Kosach****
Oleksandra Sakun*****
Tetiana Klymenko******

ABSTRACT

The relevance of the topic is due to the need to research the scientific aspects of reconciling the contradictions between the growing importance of the development of digital technologies and the formation of an information society, between the level of development of the information security of society and the readiness of state authorities to respond to strategic and tactical threats. The purpose of the article is to develop conceptual provisions for the formation of the mechanism of state management of the development of digital technologies in the country's national security system. To achieve the goal, general scientific methods of learning phenomena and processes were used: induction and deduction, system analysis and generalization, structuring, abstraction, formalization and graphic. It has been proven that the implementation of digital technologies in the process of state administration is an important element of the national security system. It is substantiated that the mechanism of state management of the development of digital technologies is a set of organizational, economic and legal measures, the interaction of which ensures the implementation of digital technologies in the national security system and the functioning of the structures that provide it, as well as the vital activities of society.

KEYWORDS: Mechanism of state administration, national security, national security policy, business entities, state authorities, local self-government, digital technologies, information economy.

*Chernihiv Polytechnic National University, Chernihiv, Ukraine. ORCID: https://orcid.org/0000-0001-8582-2158. E-mail: viktoriyamargasova@gmail.com
**Chernihiv Polytechnic National University, Chernihiv, Ukraine. ORCID: https://orcid.org/0000-0002-2807-1957. E-mail: olhamrudenko@gmail.com
***Chernihiv Polytechnic National University, Chernihiv, Ukraine. ORCID: https://orcid.or/0000-0002-4581-5129. E-mail: popelo.olha@gmail.com
****Chernihiv Polytechnic National University, Chernihiv, Ukraine. ORCID: https://orcid.org/0000-0003-1730-7140. E-mail: irish_kos@ukr.net
*****Chernihiv Polytechnic National University, Chernihiv, Ukraine. ORCID: https://orcid.org/0000-0001-9947-0210. E-mail: sakunalexandra@gmail.com
******Chernihiv Polytechnic National University, Chernihiv, Ukraine. ORCID: https://orcid.org/0000-0002-5852-6350. E-mail: klemenkotv79@gmail.com

Recibido:13/09/2023 Aceptado: 07/11/2023

DOI: https://doi.org/10.46925//rdluz.42.22

Mecanismos de gestión estatal del desarrollo de tecnologías digitales en el Sistema Nacional de Seguridad

RESUMEN

La relevancia del tema se debe a la necesidad de investigar los aspectos científicos de conciliar las contradicciones entre la creciente importancia del desarrollo de las tecnologías digitales y la formación de una sociedad de la información, entre el nivel de desarrollo de la seguridad de la información de la sociedad y la disposición de las autoridades estatales para responder a amenazas estratégicas y tácticas. El propósito del artículo es desarrollar disposiciones conceptuales para la formación del mecanismo de gestión estatal del desarrollo de las tecnologías digitales en el sistema de seguridad nacional del país. Para lograr el objetivo se utilizaron métodos científicos generales de aprendizaje de fenómenos y procesos: inducción y deducción, análisis y generalización de sistemas, estructuración, abstracción, formalización y gráfico. Está demostrado que la implementación de tecnologías digitales en el proceso de administración estatal es un elemento importante del sistema de seguridad nacional. Se fundamenta que el mecanismo de gestión estatal del desarrollo de las tecnologías digitales es un conjunto de medidas organizativas, económicas y legales, cuya interacción asegura la implementación de las tecnologías digitales en el sistema de seguridad nacional y el funcionamiento de las estructuras que la proporcionan, así como las actividades vitales de la sociedad.

PALABRAS CLAVE: Mecanismo de administración estatal, seguridad nacional, política de seguridad nacional, entidades comerciales, autoridades estatales, autogobierno local tecnologías digitales, economía de la información.

Introduction

Information technologies are an important element of the information security system of the state, which in turn is a component of the comprehensive national security system. The development of an appropriate mechanism for state management of the development of digital technologies is determined by the following factors: the formation of the information economy and the development of the processes of digitalization of society; the development of electronic governance and the transfer of a significant part of state administration functions to the information space; the formation of new national interests in the conditions of strengthening information communications; the impact of digitization processes on the functioning of the state power system, the activities of business entities, the interaction of state administration bodies and society.

DOI: https://doi.org/10.46925//rdluz.42.22

Therefore, the implementation of digital technologies in the process of public administration is an important element of the national security system, as well as the security of individual citizens and businesses in cyberspace. The above determines the need to develop and implement modern state management mechanisms aimed at the development of information technologies in the field of national security.

The purpose of the article is to develop conceptual provisions for the formation of the mechanism of state management of the development of digital technologies in the country's national security system.

1. Literature Review

Many publications by domestic and foreign authors are devoted to the study of various aspects of the national security system, especially in the modern conditions of the development of digital technologies. Studying the publishing activity of scientists and the subject of their research, it is appropriate to note that the topic under study is insufficiently studied. According to the scientific metric base of the Web of Science, only 29 articles were found in the titles of which the words "public administration, state management, digitalization, national security" are found (Fig. 1).

The first article was published in 1997. Further, the dynamics of publication activity was as follows: 2018 - 1 article, 2019-2 articles, 2020-3 articles, 2021 - 12 articles, 2022-7 articles, 2023 - 3 articles. Most of the articles (13) were published by Ukrainian scientists.

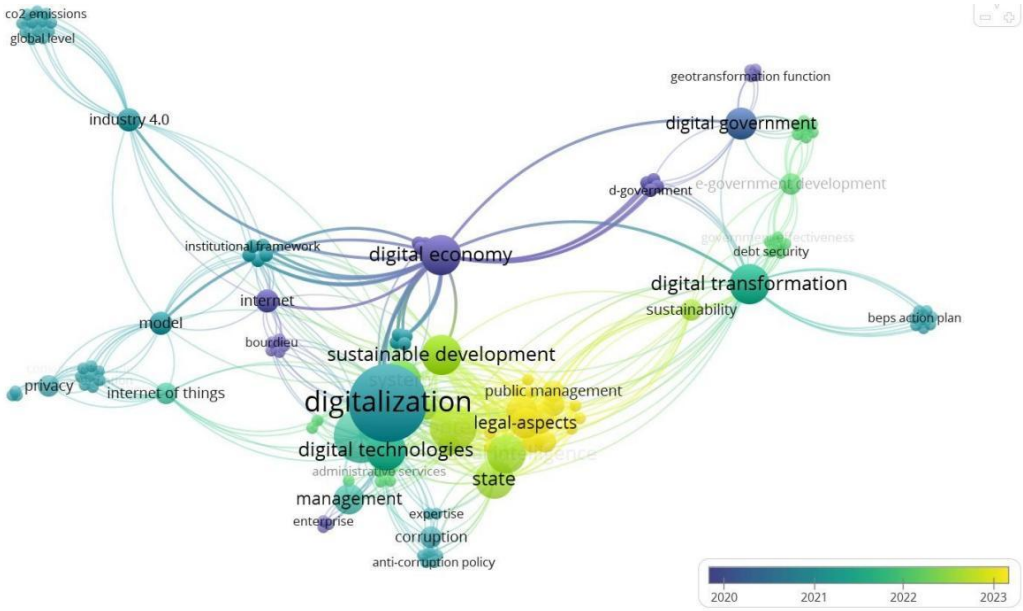
As part of the study (Samusevych Y.V. et al., 2021), the existence of dynamic convergent relations in the chains "national security - digitalization", "education - national security - digitalization" was confirmed, which indicates the need for further interstate integration of regulatory practices in the sphere of the impact of digitalization on national security. According to the results of the study, a significant level of convergence of the economy, education and digitalization of the studied countries was revealed, as well as the formation of sustainable convergent links of integrated development of the economy, education and national security.

The purpose of the authors' research (Hou Z. et al., 2023) is a comparative phraseological analysis of mass media representations related to the Hong Kong National Security Law. Based on the methodology, the authors identify four framing functions, i.e.

DOI: https://doi.org/10.46925//rdluz.42.22

politics and law, protest and crime, action and future, and evaluation, to suggest how legislation is viewed and understood in different press.

Figure 1. Cartographic analysis of the scientific works results by keywords «public administration, state management, digitalization, national security»



Source: compiled by the authors based on the analysis of the Web of Science database and using the tools of the VOSviewer program

The authors of the study (Kollabathini Siddhardha, 2023) claim that today cyberspace is a fact of everyday life, and the influence of cyberspace has not bypassed the national security of states. Because cyberspace is borderless, omnipresent in many domains, and anarchic, scholars are convinced that it attacks whenever disputes arise between two countries.

Within the framework of research (Stetsenko V. et al., 2023), scientists analyze the issue of determining the balance of private (individual) and public (state) interests regarding the admissibility of restricting human rights and freedoms in cases where it increases or prevents threats to national security. The authors are convinced that this topic has become especially relevant due to the growing number of hybrid threats to national security, which can be counteracted by the introduction of certain restrictions on human rights by the state.

Scholars (Rokvić V., 2023) examine the correlation between vaccination hesitancy and national security. On the one hand, the authors argue that health is a matter of special concern for the modern sovereign state and its security, and that the vaccine as an achievement of civilization is one of the most important mechanisms for protecting public health and, as a result, national security. On the other hand, the authors believe that vaccination indecision should also be seen as a threat to national security.

Article (Jing Chao, 2023) examines how the Court conducts the suitability test in national security cases according to two models, under which several representative testing criteria can be classified: the human rights priority model and the national security priority model. The scholar argues that, under the two models, the Court applies the fitness test in a consistent and predictable manner in national security case law.

According to the authors (Szyszlak T., 2023), the national security system is one of the main categories in the security sciences, which refers to a group of interrelated elements that generally pursue the goal of ensuring the security of the state. According to scientists, this is a system consisting of subsystems defined in different ways, but in the case of adopting a subjective perspective, the authors indicate the system of cultural security, the model of which is proposed in the article.

Scientific paper (Allison Abbe, 2023) argues that national security practitioners must understand the motivations, mindsets, and intentions of adversaries in order to anticipate and respond effectively to their actions. The authors summarize previous research on the development and application of forward-looking analysis and decision-making and recommend four ways that national security strategists and practitioners can improve their ability to gain understanding of adversaries.

Within the scope of the article (Tikk-Ringas Eneken, 2016), scientists prove the military benefit of the cyberspace related to the economic and social potential of information and communication technologies, while technologies with military and national security applications have become important for modern life. By summarizing the ways in which governments are addressing these challenges at a strategic level, the authors believe it helps prepare decision-makers and researchers involved in cybersecurity policy, strategy, and analysis.

Scientists (Kakeshov Bakyt D. et al., 2023) focused their research on identifying political and legal instruments of influence on persons who commit illegal actions against

DOI: https://doi.org/10.46925//rdluz.42.22

information security. According to the authors, the information sphere has acquired the character of a system-forming mechanism, on the basis of which the functioning of social life, its political, economic and defense components takes place. It has been established that the number of offenses in the field of information security is increasing, therefore there is a need to develop new legal tools to combat them in order to ensure national security.

Based on the results of the analysis of existing publications, it can be stated that the issue of developing a mechanism for state management of the development of digital technologies in the national security system is insufficiently studied and requires further research and analysis.

2. Methodology

The theoretical and methodological basis of the study was formed by the scientific works of leading scientists from the specified subject. The development of the theoretical foundations of the formation of the mechanism of state management of the development of digital technologies was built on the basis of systemic and synergistic approaches. To achieve the goal, general scientific methods of learning phenomena and processes were used: methods of induction and deduction - to clarify the relationship between the process of introducing digital technologies and the functioning of the national security system; methods of system analysis and generalization for systematization of existing scientific approaches, used theoretical sources and scientific literature; structuring method - to single out individual factors influencing the formation of the mechanism according to certain classification features; the method of system analysis, the method of abstraction and formalization - for the development of the conceptual foundations of the mechanism of public administration; graphic method - for displaying the theoretical and methodological material of the research.

3. Results

The multifaceted nature of the process of development of digital technologies and their further implementation in the functioning of society and the country's economic system requires the formation of an appropriate mechanism that could ensure the coordination of their effective use at the same time as ensuring the requirements of the national security system. The process of development and further implementation of

innovative technologies is the object of influence of state authorities and local self-government, as it is multi-level and involves the development of relevant directions both at the state level and at the regional level and at the level of a separate business entity. However, modern transformational processes, the increase in the level of cyber threats in the world, social instability require the development and application of new approaches to the formation of mechanisms for the implementation of state policy in the field of information innovations and the development of digital technologies. The system of state management mechanisms, according to the classification of many researchers, separates economic and regulatory-legal management mechanisms by functional feature. As a rule, their effective application is possible only under the conditions of constant interaction, which extends to the state management of the development of digital technologies, however, we consider it appropriate to take into account the requirements of national security of the state.

Management of digital technology development processes in the context of national security requires the development of appropriate state support measures, which are part of the state policy of innovative development on the one hand, and the country's national security policy on the other.

Using the principles of a systemic approach, we propose to consider the mechanism of state management of the development of digital technologies as an economic and political system, which makes it possible to single out the following general characteristics of its functioning:

- the implementation of the mechanism of the specified direction takes place on the basis of the formation of a goal common to all elements;

- the mechanism of state management of the development of digital technologies acts as a set of interconnected elements that form its internal structure and interact with the external environment, which has certain limitations due to national security requirements;

- it is advisable to group the elements of the mechanism into the following subsystems: institutional system (bodies of state power and local self-government, bodies of national security and defense), regulatory subsystem (laws and by-laws, state programs), material subsystem (tools for achieving the set goal, information resources, software, qualified personnel).

DOI: https://doi.org/10.46925//rdluz.42.22

Therefore, the specified characteristics indicate that the mechanism of public administration in the field of digital technology development in the management aspect is an element of the public administration system as a global system.

Accordingly, the mechanism of state management of the development of digital technologies should be considered as a set of organizational, economic and legal measures, the interaction of which ensures the implementation of digital technologies in the system of national security and the functioning of the structures that provide it, as well as the vital activities of society.

The key goal of the specified mechanism is the formation of a complex of optimal conditions for the life and development of an individual based on the use of digital technologies, the socio-economic and military-political stability of society in the conditions of digitalization of the economy, as well as the resistance to the influence of internal and external cyber threats in the sphere of life activities of the state administration system.

The mechanism of state management of the development of digital technologies in a narrow context should be considered as a system of special institutions and bodies that, in accordance with the interests of society, people and the state, perform the tasks of developing information technologies and establishing a digital economy and carry out state leadership in the field of ensuring the function of national security. The institutional approach makes it possible to single out economic and legal institutions as components of the mechanism. The role of economic institutions is to exert a regulatory influence on the processes of digital development. Legal institutes provide regulatory and legal regulation of the aforementioned economic institutes, as well as the use of tools and methods of state influence on the development of digital technologies.

A condition for promoting the development of digital technologies in the context of ensuring national security is the analysis of the adaptation of digitalization processes in a specific country to the requirements of the information economy. Therefore, timely forecasting of the state of informatization of society, the level of development of electronic management based on the research of cyber security trends, the state of protection of information flows is an important means of ensuring national security. On the basis of information from relevant monitoring, state authorities make decisions aimed at ensuring national interests, which is reflected in legal norms. Under these conditions, the balance of

the interests of the state, society and citizen in the field of digital technology development is possible only if national security requirements are taken into account.

Thus, it is expedient to distinguish the internal and external aspects of the mechanism of state management of the development of digital technologies. The internal aspect involves state control over the use of information resources, effective activity of state authorities and the implementation of state policy directions in the field of digital development and the formation of the information economy, as well as the implementation of measures to preserve and support the state's information potential.

The external aspect of the mechanism involves the presence of the following criteria for its effectiveness:

- the ability of the economy and society to counteract external cyber threats;

- the possibility of international integration in the field of cyber security;

- the possibility of control by state authorities on the level of implementation and further use of information technologies in all spheres of society and the economy;

- the quality level of information support for the functioning of the national security and defense system and its interaction with other countries and international organizations;

- the necessary degree of state regulation of international cooperation processes for the stable functioning of the state's cyber security system.

The effectiveness of the functioning of the mechanism of state management of the development of digital technologies depends on the chosen approaches and implementation tools, which should ensure:

- formation of the institutional environment on the basis of ensuring national security through the implementation of appropriate mechanisms, methods and tools;

- the orientation of state support for the development of digital technologies to solve problems in the field of economic, environmental, food, state and information security through the implementation of a monitoring tool.

The use of a system approach makes it possible to form the following principles of implementation of the specified mechanism:

- complexity, which is expressed in the development of directions for supporting the implementation of digital technologies in all spheres of society's life;

- integrity – implementation of the mechanism takes place on the basis of the formed feedback between its subsystems and elements;

DOI: https://doi.org/10.46925//rdluz.42.22

- the principle of sustainable development, which involves the interaction of economic, social and environmental tools for ensuring national security based on the implementation of digital economy tools;

- heterogeneity – means that the mechanism of state management of the development of digital technologies acts as an organized set and has a certain structure;

- openness – the functioning of the mechanism is under the influence of external and internal factors of national security;

- emergency – in the process of changing the external and internal environment, new qualities of the mechanism occur that are not characteristic of its individual components, that is, under the influence of national security requirements, the mechanism as a system acquires new qualities;

- purposefulness – formation of the goals of the state management mechanism based on the optimization of the structure of hierarchical relationships;

- efficiency, which involves the mobilization of resources in order to achieve the objective advantages of the development of digital technologies in the context of national security;

- relevance, which involves giving priority to those tools of the mechanism that solve urgent problems of national security.

The process of state management of the development of digital technologies is implemented on the basis of the interaction of state authorities, society and business entities. The interaction of the specified elements allows considering the action of the mechanism of state management of the development of digital technologies in the context of synergistic interaction. Thus, the emergence and dynamic development of the mentioned mechanism takes place on the basis of self-organization.

The use of a synergistic approach in the process of implementing the mechanism of state management of the development of digital technologies should take into account the balance of interests of business entities and state authorities, subject to compliance with the criteria of the country's national security policy. Depending on the level of cyber threats and the possibility of implementing appropriate countermeasures, the synergistic effect of implementing the mechanism can be both negative and positive. Thus, an objective necessity is the emergence of feedback between the components of the mechanism and the external environment in order to minimize the negative impact of threats. At the same time,

DOI: https://doi.org/10.46925//rdluz.42.22

state support in the field of digital technology development is not only a mandatory function of state administration, but a system of tools, levers and relationships that allows coordinating specific directions of state policy in accordance with the requirements of the national security system. This becomes possible under the conditions of the integration of state authorities and business entities to find optimal solutions in the field of information technology development and effective introduction of information resources into the national security system with the aim of obtaining a synergistic effect as the final result of the mechanism of state management of the development of digital technologies. The synergism of the interaction of the components of the mechanism involves the influence of the levers and tools of the mechanism directly on the operating environment, which will further contribute to changing the qualitative composition of the socio-economic environment and monitoring the effectiveness of the national security system in order to adapt it to possible cyber threats.

According to the synergistic methodology, the mechanism of state management of the development of digital technologies is a complex hierarchical system, the elements of which (state authorities, society, economic entities, levers, goals, tools) interact based on the principle of self-organization (Fig. 2).

Since the mechanism is in a state of dynamic equilibrium, it is gradually approaching the bifurcation point, where several scenarios of its further implementation are formed under the influence of threats and the corresponding reaction of the national security system. That is, under these conditions, the national security system acts as a corrective influence on the implementation of further directions of information development and digitization. Achieving a stable state and choosing one of the possible scenarios occurs after agreeing on the direction of the mechanism and the current tasks of the national security policy. The increase in threats to national security as a result of the action of the mechanism occurs in the absence of corrective influences as the distance from the steady state and the appearance of the next bifurcation point.

The state of the mechanism in which the system is at a certain moment in time t depends on its earlier state, the level of threats to national security, and the flows at the entrance that had an impact at the moment of time t-1.

The internal behavior of the mechanism as a system σ is a function of the change in the state of the system under the influence of the self-organization process. Accordingly,

DOI: https://doi.org/10.46925//rdluz.42.22

the state at the moment of time t is a function of time, the previous state and the input values X:

$$st, = f\ (t, st\text{-}1, x(t\text{-}1,t)), \quad (1)$$

where x(t-1,t) – incoming flows into the system.

Similarly, the external behavior ψ is a function of time, the previous state of the system and the output flows Y. The general state of the mechanism as a self-organizing system is influenced by the dialectical relationship between internal and external threats to national security, that is, the behavior of the mechanism as a set of elements is influenced by the action national security policy itself directly affects the state of external and internal threats (Fig. 3).

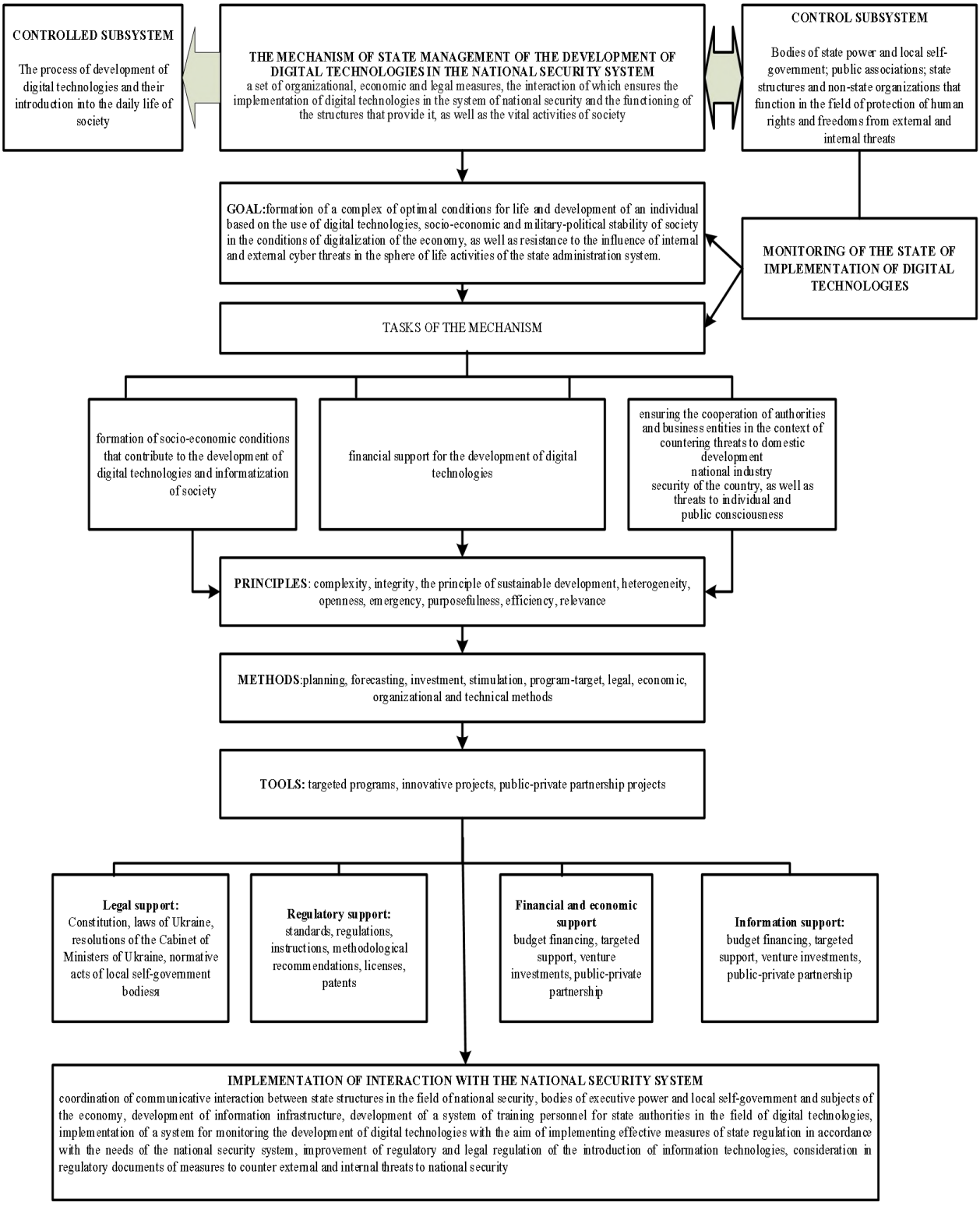
Then the set of elements of the external environment, from which the incoming flows are directed to the system of mechanism elements, will be denoted as EvS, and the set of elements of the internal environment will be defined as SEv. Accordingly, the mechanism of state management of the development of digital technologies is proposed to be considered in the form of a function (EvS, SEv, St, X(t-1,t), y (t-1,t),σ, ψ). The system of state management of the development of digital technologies under the influence of threats from the external and internal environment forms signals of influence (M1, M2... Mn).

Thus, in the process of self-organization of the specified mechanism, a stable interdependence is formed between the level of threats to the national security system, the level of development of digital technologies, and the behavior of the elements of the mechanism.

The use of a synergistic methodology for the study of the mechanism of state management of the development of digital technologies in the national security system makes it possible to single out the following conceptual principles of its functioning (Fig. 4).

DOI: https://doi.org/10.46925//rdluz.42.22

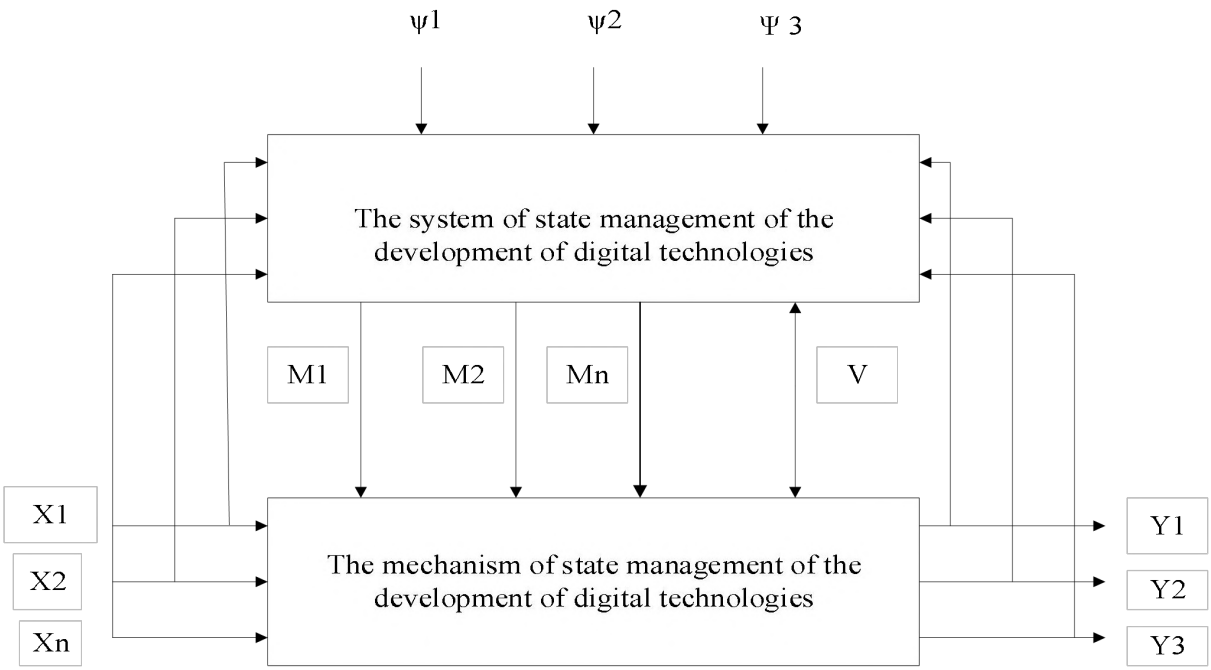
Figure 2. The structure of the mechanism of state management of the development of digital technologies in the national security system



Source: developed by the authors

DOI: https://doi.org/10.46925//rdluz.42.22

Figure 3. A model of the mechanism of state management of the development of digital technologies as a self-organized system



Source: developed by the authors

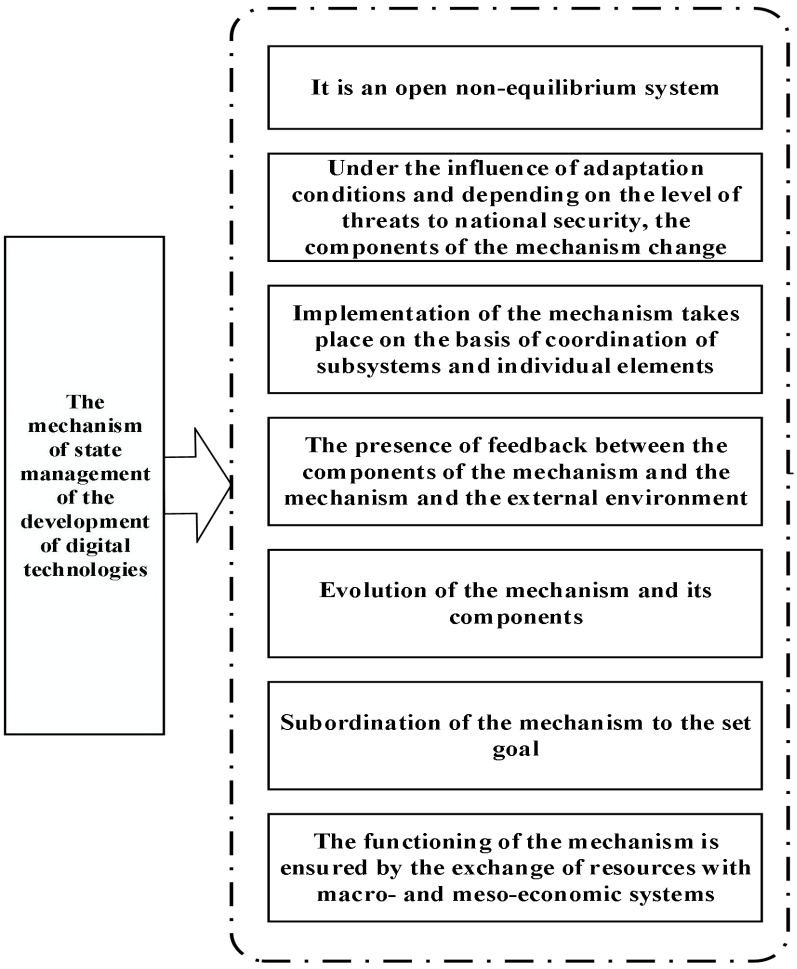
Therefore, the system-synergistic methodology makes it possible to ensure the effective implementation of measures of the state management mechanism by preventing and identifying threats to the national security system and to take into account alternative possible scenarios of its application.

4. Discussion

We consider the study (Criado J.I., 2021) relevant, which analyzed the digital government in Latin American countries from a comparative point of view. The authors studied a group of countries with a significant degree of economic diversity and heterogeneity of state administration. Scientists analyzed intersectional aspects of e-government, including national digital government programs, e-government websites, engagement initiatives, social media technologies, open data and open government strategies, and the future of technology in the region's public sector.

DOI: https://doi.org/10.46925//rdluz.42.22

Figure 4. Synergistic concept of the mechanism of state management of the development of digital technologies in the national security system



Source: developed by the authors

We support the results of a scientific study (Todoruț Amalia Venera et al., 2018), which examines the impact of information and communication technologies on the sphere of public administration, which lead to rapid and multiple transformations. The authors developed the concept of e-governance, which results in the modernization of central and local state administrations to provide public services to citizens and the business environment in an integrated, transparent and secure way, which is an urgent issue in modern conditions.

Considering it expedient in the modern realities of research (Peng Shin-yi, 2023), one should note the challenges of the digital economy in the context of cyber security threats, which have increasing implications for national security. The authors argue that

pre-digital trade exemptions are too narrow to address cybersecurity concerns, contrary to trends in a new generation of international trade agreements that create expansive security exemptions designed to rebalance international trade and national security.

Of practical interest is a study by the authors (Irwin D. et al., 2023) in which organizations in several domains, including national security intelligence, make judgments under uncertainty using verbal probabilities instead of numerical probabilities, despite research indicating that the former have different meaning for individuals. The results of the authors' study show that while most non-experts prefer the numerical format, the experts were about equally divided, and the majority of participants in both samples found the numerical format more informative.

Noting the practical significance of the study (Martinez Cortez et al., 2023), attention should be paid to the analysis of aerospace power as an instrument of the state and an important component of military power in the face of risks and threats that affect the security of Spain, both in the field of military operations and in the contribution of activities related to related to national security as a whole.

Taking into account the available research, it should be noted that the issue of formation and implementation of state management mechanisms for the development of digital technologies in the national security system is an extremely relevant and necessary research.

Conclusion

The article develops the mechanism of state management of the development of digital technologies as an economic and political system. The structure of the mechanism is considered in the context of the formation of an institutional subsystem, which includes bodies of state power and local self-government, bodies of national security and defense; regulatory subsystem, the elements of which are laws and by-laws, state programs; material subsystem, consisting of tools for achieving the set goal, information resources, software, available qualified personnel.

The implementation of the mechanism of state management of the development of digital technologies should include the following areas: the formation of the state concept of the development of digital technologies and the information economy, reflecting the impact of threats to the country's national security; improvement of normative and legal

regulation for the purpose of distribution of powers between state authorities and state structures in the national security system. In the process of functioning of the mentioned mechanism, it is advisable to take into account its purposefulness, however, under the influence of threats, the goals and tasks of the mechanism should be revised. The effective use of the specified mechanism has both theoretical and practical significance, taking into account the possibilities of adaptation to changes in the state of the national security system and the level of internal and external threats.

References

Allison, Abbe. (2023). Understanding the Adversary: Strategic Empathy and Perspective Taking in National Security. *Parameters*; *53*(2), 19-38. doi: 10.55540/0031-1723.3221.

Criado, J.I. (2021). Digital Public Administration in Latin America: Digitalization, Public Innovation, and the Future of Technologies in the Public Sector. In Peters, B.G., Tercedor, C.A. and Ramos, C. (Ed.) *The Emerald Handbook of Public Administration in Latin America*, *Emerald Publishing Limited*, *Bingley* (pp. 343-374). https://doi.org/10.1108/978-1-83982-676-420201014.

Hou, Z., Peng, Q. (2023). The national security law for Hong Kong: a corpus-driven comparative study of media representations between China's and Anglo-American English-language press. *Humanit Soc Sci Commun*, *10*, 207. https://doi.org/10.1057/s41599-023-01699-7.

Irwin, D., Mandel, D. (2023). Communicating uncertainty in national security intelligence: Expert and nonexpert interpretations of and preferences for verbal and numeric formats. *Risk Anal*, *43*(5), 943-957. https://doi.org/10.1111/risa.14009.

Jing, Chao. (2023). The ECtHR's suitability test in national security cases: Two models for balancing human rights and national security. *Leiden Journal of International Law*, *36*(2), 295-312. https://doi.org/10.1017/S0922156522000735.

Kakeshov, Bakyt D., Kanybekova, Baktygul K., Seidakmatov, Nurman A., Zheenalieva, Aida O., Kokoeva, Almagul M. (2023). Political and legal aspects of criminal and administrative responsibility for information security offences in the context of national security of the Kyrgyz Republic. *Economic Affairs*, *68*(Special Issue), 987-993. doi: 10.46852/0424-2513.2s.2023.48.

Kollabathini, Siddhardha. (2023). Dispute between Countries, a Corresponding Attack on Cyberspace: The New National Security Challenge. In *Advanced Computer Science Applications: Recent Trends in AI, Machine Learning, and Network Security* (pp. 365-373).

Martinez Cortez, Jose M. (2023). Air and space power – an essential instrument of national security. *Revista UNISCI*, *62*, 9-31.

Peng, Shin-yi. (2023). Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions. *AJIL Unbound*, *117*, 122-127. https://doi.org/10.1017/aju.2023.18.

Roković, V. (2023). Covid-19 Vaccine Hesitancy and National Security – A Serbian Case Study. *Politička misao: časopis za politologiju*, *60*(2), 122-148. https://doi.org/10.20901/pm.60.2.06

Roller, Robert J. (2023). National Security Competition or Cooperation Preparing for 21st Century Threats. *Homeland Security Affairs*, *19*(1), 1-18.

Samusevych, Y.V., Novikov, V.V., Artyukhov, A.Ye., Vasylieva, T.A. (2021). Convergence trends in the "economy - education - digitalization - national security" chain. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (6), 177–183. https://doi.org/10.33271/nvngu/2021-6/177.

Stetsenko, V., Havronska, T., Makarova, O., Konchakovska, V., Derkachova, N. (2023). Balance of Private and Public Interest Law in Matters of Restricting Human Rights for the Purposes of National Security. *Academic Journal of Interdisciplinary Studies*, *12*(4), 17-27. https://doi.org/10.36941/ajis-2023-0091.

Szyszlak, T. (2023). The system of cultural security as a subsystem of the national security system. *Cultural security: Theory – Selected Aspects – Case Studies*, 83-94.

Tikk-Ringas, Eneken. (2016). *Evolution of the Cyber Domain: The Implications for National and Global Security*. Routledge.

Todoruţ, Amalia Venera, Tselentis, Vasileios. (2018). Digital Technologies and the Modernization of Public Administration. *Quality: Access to Success*, *19*(165), 73-78.