International Journal of Safety and Security Engineering
Vol. 13, No. 1, February, 2023, pp. 81-88
Journal homepage: http://iieta.org/journals/ijsse

Modelling a Public Administration System for Ensuring Cybersecurity

Vladislav Yemanov[1*], Halyna Dzyana[2], Nazarii Dzyanyi[3], Olga Dolinchenko[4], Oleg Didych[2]

[1] First Defender of the Head of the national academy of the national guard of Ukraine, candidate of military sciences, senior researcher, Kharkiv 61000, Ukraine
[2] Department of Public Administration and Public Service of Institute of Public Administration, Lviv Polytechnic National University, Lviv 79000, Ukraine
[3] Department of Information Security, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv 79000, Ukraine
[4] Department of Public Administration, Interregional Academy of Personnel Management, Kyiv 59000, Ukraine

Corresponding Author Email: emanov.vlad.edu@gmail.com

https://doi.org/10.18280/ijsse.130109

Received: 23 December 2022
Accepted: 20 January 2023

Keywords:
public administration, cybersecurity, cyberspace, information and communication technologies, threats

ABSTRACT

The main purpose of the study is to model the process of public administration system for ensuring cybersecurity. The research methodology involves the use of method of decomposition modeling IDEF0 to the achievement of the goals. As a result of the use of this methodology, a model of the implementation of methods and measures of the public administration system was formed in the context of ensuring the cyber security of the information space of its functioning. The use of this methodology made it possible to fully graphically depict the process of achieving the final goal. A significant advantage of this model is the clarity and systematic display of stages, resources and results. The study has limitations, considering that this model was formed for a separate province of Canada, all elements of the model were selected in accordance with the specifics of the public administration of this country, as well as methods for ensuring cybersecurity. In subsequent studies, the authors plan to adapt this model to the realities of other public administration systems.

1. INTRODUCTION

The development of information technologies and artificial intelligence have led to the emergence of threats in cyberspace, because the modern technological level gives rise to new challenges, respectively, pushes the leading countries of the world to strengthen their security policy. The use of digital technologies in various fields of activity contributes to the spread of cybercrime, which negatively affects the public administration system, harms the country's vital activities and reduces confidence in the public administration system as a whole. It is these new information challenges that pose a threat to sovereignty and territorial integrity, because cybercrime increases the contradictions between states.

The efficiency of the activities of public administration bodies directly depends on the timely adoption of a competent management decision. The process of making managerial decisions is always based on the collection, selection and processing of the required information. Only its generalized analysis allows making an informed decision. This process is of particular importance in conditions of multivariance and uncertainty, which leads to the difficulties of fast and high-quality processing of large amounts of data and thus increased attention to the timeliness, accuracy and truthfulness of information.

Despite the obvious advantages, the rapid development of information technologies, devices, intelligent things, the increase in data traffic led to the fact that a person, society, the state began to transfer more and more to cyberspace and to the cloud (digital environment) different aspects of their lives, their activities, which gives rise to a number of problems, one of which is not only the protection of information itself, but also the protection of the entire system in the information field and in the field of computer technology as a whole.

Solutions to problems arising from the implementation of public administration mechanisms in the context of ensuring cybersecurity require an integrated approach. The system for ensuring counteraction to cybercrime should have a nationwide character. It should cover several areas of vigorous activity at once: legal (improvement of legislation), international (expansion of international cooperation), educational (enlightenment campaigns and related training programs in higher educational institutions), political (active actions by the state aimed at protecting its information space , values), organizational (provides for an active public-private partnership), scientific and technical (improvement of information technologies).

For this purpose, a number of different measures are applied in the public administration system. First of all, the management measures include the formation of a security policy by the public administration, which determine the general direction of the work.

Organizational and administrative support of cybersecurity consists of regulating the activities and relationships of subjects using cyberspace on a legal basis, which makes it impossible for disclosure, leakage and unauthorized access to information or creates significant difficulties in accessing it through organizational measures (for example, the creation of a special information service security, determination of job descriptions for employees, organization of security measures, security of premises, control over the work of personnel with information, determination of the procedure for storing, backing up, destroying confidential information, etc.) Engineering and technical (physical) measures are a set of special bodies, technical means and measures that work together to perform a specific task of protecting information. The level of cyber security assurance depends on the environment in which the cyber security system operates.

In the modern world, the prerequisites for the dynamic spread of cyber threats still remain: the imperfection of the regulatory framework in the field of cybersecurity, as well as its outdated in the field of information protection, the slow implementation of the provisions of world legislation into national legislation, the insufficient regulation of the digital component of the investigation of cybercrimes for violation of legal requirements in this area; the absence of relevant structural divisions in a significant part of state authorities, financing of cyber defense work on a residual principle with technological errors; the lack of an independent information security audit system and mechanisms for disclosing information about vulnerabilities in the context of dynamic digitalization of all areas of government and the life of the country, which requires strict adherence to relevant standards; incompleteness of measures to implement an organizational and technical model of cyber defense that meets modern threats, challenges in cyberspace and global trends in the development of the cybersecurity industry; lack of a system to improve the digital literacy of citizens and a culture of behavior in cyberspace, raising public awareness of cyber threats and cyber defense.

Thus, the main purpose of the study is to model the process of public administration system for ensuring cybersecurity. The study consists of the following structural parts: introduction, which defines all the theoretical elements and prerequisites for the study; review of specialized scientific literature; description of the methodology; direct presentation of research results and model formation; discussion of the obtained results and conclusions.

2. LITERATURE REVIEW

According to the interpretation of scientists [1, 2], public administration can be interpreted as the activity of public administration bodies, local governments, representatives of the private sector and civil society institutions within the powers and functional duties (planning, organization, leadership, coordination and control) defined by law to form and implement management decisions of public values, development policy of the state and its administrative-territorial units.

Some researchers believe [3-5] that we have entered the phase of cyberwars (cyber interventions), as the facts of dangerous actions in cyberspace are growing quantitatively and qualitatively. Cyber intervention is a complex of socially dangerous actions that harm important areas of existence of the state and society. Various sectors of state, economic and public life are becoming more vulnerable to such actions and require protection. Cybercrime has become transnational. Cyber groups and individual hackers are becoming more active, attacking government and private sites, disrupting information resources. Carding has spread - financial crimes in cyberspace. Among the consequences of cyber incidents of a different nature are striking the authority of the state, spreading false information, disorienting the population, collecting valuable information, disrupting the functioning of websites, computer systems, and critical infrastructure facilities.

If we consider the concept of "cybersecurity", then here most experts recognize this concept as - the protection of the vital interests of a person and a citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization real and potential threats to national security in cyberspace [6, 7].

Speaking about cybersecurity in the field of public administration, one cannot but agree with Kryshtanovych et al. [8], who noted that the cybersecurity of the public administration system is the basis of national security, which forms the security of the state, society, public administration system, the population of the country in cyberspace through the creation of legitimate mechanisms ensuring cybersecurity of public administration

Most scientists [9, 10] come to the conclusi that the effectiveness of the functioning of the cybersecurity system, first of all, depends on the perfection of the legal regulation of the activities of the relevant system of state and public bodies, as well as non-governmental organizations.

Considering the specifics of Canadian cyber legislation and the peculiarities of public administration in this area, most scientists agree that the Canadian public authorities are making great efforts to change the law, modernize the powers of law enforcement agencies and ensure such an order that makes it impossible to evade legislation by criminal actions in cyberspace [11, 12].

In exploring cybercrime and cybersecurity development, Lapinskienė, Coppolino et al. [13] identify that the Canadian federal government is strengthening the resilience of government systems, developing public-private partnerships to secure critical infrastructure, sharing information about cybersecurity with the public, and expanding the powers of the police.

Analyzing specialized scientific sources [14, 15], it is possible to single out the main elements of the public administration cybersecurity system, in particular: information, information and communication systems; threats; mechanisms for ensuring cybersecurity of the public administration system; subjects of ensuring cybersecurity of the public administration system

The scientific and practical literature on this subject includes many methods that can be applied to solve this problem, but not all of them are effective. That is why it is necessary to look for new methodological approaches.

Despite the active attention of the scientific community to the problem of organizing an effective public administration system in the context of ensuring cybersecurity, this issue is still relevant and important today. Due to the complexity and complexity of this process, in our opinion, this requires the use of modeling methods for a better understanding.

3. METHODOLOGY

Analyzing the structure of our chosen methodology, we can determine that the entire collection of methods is divided into two groups: general theoretical and modeling.

General theoretical research methods include methods of analysis, synthesis, generalization and systematization. These methods were used for a thorough analysis of specialized scientific literature, the systematized data on which formed the basis of the theoretical basis of the study.

The second group of methods is represented by the method of decomposition modeling, which includes the formation of context diagrams and decompositions of different levels.

The method of decomposition modeling IDEF0 allows you to depict functions systematically, designate their relationship between themselves and the external environment, designate material, intellectual flows that affect the movement of processes [16].

The IDEF0 decomposition modeling method for describing business processes consists in describing actions using diagrams.

The graphical representation of the process allows you to analyze the problem in more detail, analyze each element of the chain, and calculate the required resource. With the help of a graphical expression of the process, the relationship with the external environment is also depicted, which is important for achieving the result.

The main advantage in comparison with other methods is the creation of any systems, not only information systems, but also the creation of systems and indications of the impact on processes of external factors. The methodical approach proposed by us has undergone a number of qualitative and quantitative evaluations by other scientists who have applied it [17, 18].

For an illustrative example, we have chosen the Canadian province of Ontario. According to the parameters, it is suitable for applying our methodological approach. Of course, there are many more provinces that could become an example for the formation of our model, but this province has advantages in the form of openness of information about public administration and methods of dealing with risks and threats in the information space.

Generally, Canada became the first country in the world to recognize the importance of media education and make it a compulsory school subject. This allows you to form the necessary knowledge and skills in the fight against disinformation and manipulation, distinguish between reliable information from fake, and protect both private and public cyberspace. The formed level of media education has expanded to cyber literacy and awareness, which contributes to close interaction between citizens and law enforcement agencies.

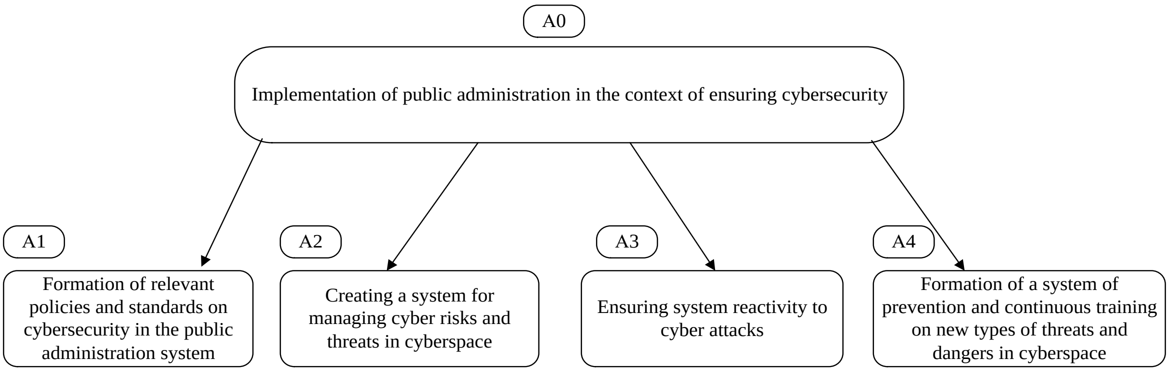
A0
Implementation of public administration in the context of ensuring cybersecurity
A1
Formation of relevant policies and standards on cybersecurity in the public administration system
A2
Creating a system for managing cyber risks and threats in cyberspace
A3
Ensuring system reactivity to cyber attacks
A4
Formation of a system of prevention and continuous training on new types of threats and dangers in cyberspace

Figure 1. Tree of goals of achieving the goal A_0 (implementation of public administration in the context of ensuring cybersecurity) for the public administration system of the province of Ontario

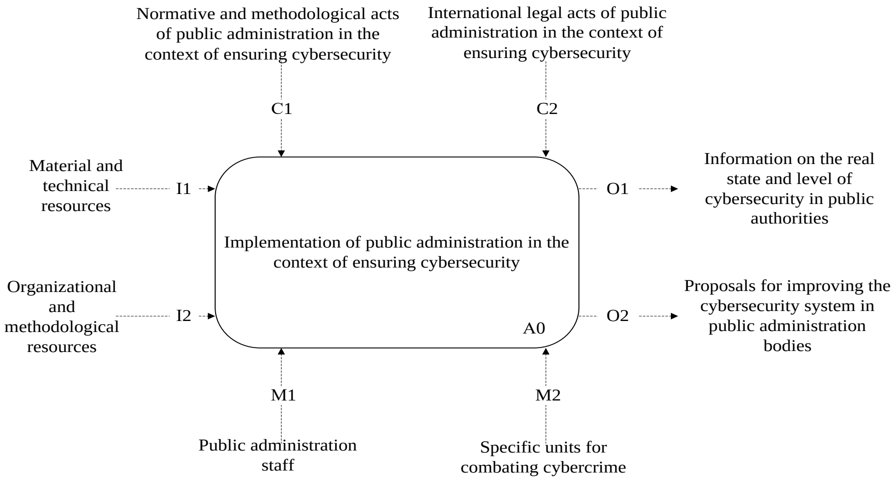
Normative and methodological acts of public administration in the context of ensuring cybersecurity
International legal acts of public administration in the context of ensuring cybersecurity
C1
C2
Material and technical resources
I1
Organizational and methodological resources
I2
Implementation of public administration in the context of ensuring cybersecurity
A0
O1
Information on the real state and level of cybersecurity in public authorities
O2
Proposals for improving the cybersecurity system in public administration bodies
M1
M2
Public administration staff
Specific units for combating cybercrime

Figure 2. Diagram of the main resources and results of the process of implementing the goal A_0

At the present stage, there is no doubt how strongly information technologies have integrated into our daily lives, because society has switched to a digital format. And while cyberspace brings significant benefits, continued reliance on it creates new threats and vulnerabilities. Analyzing the activity and mechanisms of public administration in the field of combating cyberpresence, one should pay attention to the fact that Canada is a world leader in the policy of protecting the information space, the legislation is distinguished by its flexibility, strict control over compliance with all norms and rules, as well as punishment of violators.

According to the rules for using decomposition modeling, the first step will be the formation of a tree of goals, in which the main stages of achieving the goal A_0 (implementation of public administration in the context of ensuring cybersecurity) will be graphically displayed in Figure 1.

As can be seen from Figure 1. four key elements need to be implemented for the public administration system of the province of Ontario to achieve the A_0 ultimate goal. In order to better understand the main resources, elements of organizational and methodological support, as well as the desired results, in Figure 2. diagram of the main resources and results is shown showing all of these key supply items. So A1, A2, A3, A4 represent the execution sequence of the main goal A0.

For a better understanding of all the inputs (denoted as I), outputs (denoted by O), controls (denoted by C), and mechanisms (denoted by M) of Ontario's government system, let's look at them in more detail:

I_1 - Material and technical resources. The structure of this element includes all material resources and technical equipment necessary for the implementation of all measures and public administration to ensure cybersecurity

I_2 - Organizational and methodological resources. This element represents the organizational and methodological support necessary for the implementation of public administration of cybersecurity.

M_1 - Public administration staff. Includes persons - employees of public authorities who are involved in the process of implementing measures and methods of public administration in the context of ensuring cybersecurity.

M_2 - Specific units for combating cybercrime. Includes all persons of special departments for combating cybercrime in the information space, both at the level of public authorities, and, if necessary, third-party cybersecurity specialists.

C_1 - Normative and methodological acts of public administration in the context of ensuring cybersecurity. This element includes all internal regulations governing the activities of public authorities in the context of ensuring cybersecurity and countering threats and risks in the public administration information environment.

C_2 - International legal acts of public administration in the context of ensuring cybersecurity. The structure of this element includes all international recommendations, regulations and norms of public administration in the context of ensuring cybersecurity and countering threats and risks in the information environment of public administration.

O_1 - Information on the real state and level of cybersecurity in public authorities. This information will be useful in the context of the analysis and correction of cybersecurity measures.

O_2 - The final result of the formed model. Proposals for improving the cybersecurity system in public administration bodies.

Thus, in the “Methodology” section, we have identified the main stages in the process of achieving the final goal A_0 for the public administration system of the province of Ontario, as well as the main elements that are necessary for the public administration system. Based on the two generated diagrams, in the Results section, we will form the final decomposition of achieving the final goal A_0 (implementation of public administration in the context of ensuring cybersecurity).

4. RESULTS OF RESEARCH

The next step in our study will be the formation of the main decomposition model of achieving the final goal A_0 (implementation of public administration in the context of ensuring cybersecurity) for the public administration system of the province of Ontario (Figure 3).

For a better understanding of all the elements of achieving the A_0 goal (implementation of public administration in the context of ensuring cybersecurity) for the public administration system of the province of Ontario., let's consider their essence in more detail:

A_1 - Formation of relevant policies and standards on cybersecurity in the public administration system. The public sector in a public administration system of the province of Ontario must first set standards, certify and test, and oversee procedures to ensure that sufficient cybersecurity is maintained to protect and promote the public interest, and take appropriate action when cybersecurity is not adequately maintained. Legal, technical and procedural arrangements and organizational structures for ensuring cybersecurity should be established at the level of public administration, as well as harmonized at the international level as follows: national laws should be adopted where they do not yet exist, and existing laws, as well as regional and international agreements should be based on a shared understanding of what cybersecurity threats are. Technical solutions must be defined and developed in accordance with accepted standards.

A_2 - Creating a system for managing cyber risks and threats in cyberspace. With the growing dependence on the use of information and communication technologies in public administration system of the province of Ontario, cyber risks and cyber threats grow accordingly, which requires a premature response to prevent or address them and awareness of the risk factors of all stakeholders. A cybersecurity system must work in the public interest for both service providers and service users. It is the state, as a guarantor of the rights and freedoms of citizens, that should take responsibility for ensuring access to a stable, secure digital space that all citizens can use, because ensuring an adequate level of cybersecurity is a necessary condition for the development of the information society. Cyber risk and threat management is the foundation for any public administration security activity, whether it is implementing systems or tools, or building processes and enforcing rules and policies. Risk management projects are often underestimated and not separated. Although the most competent definition and management of cyber risks and threats allows you to rationally distribute the budget for cybersecurity and competently prepare for attacks and threats in advance.

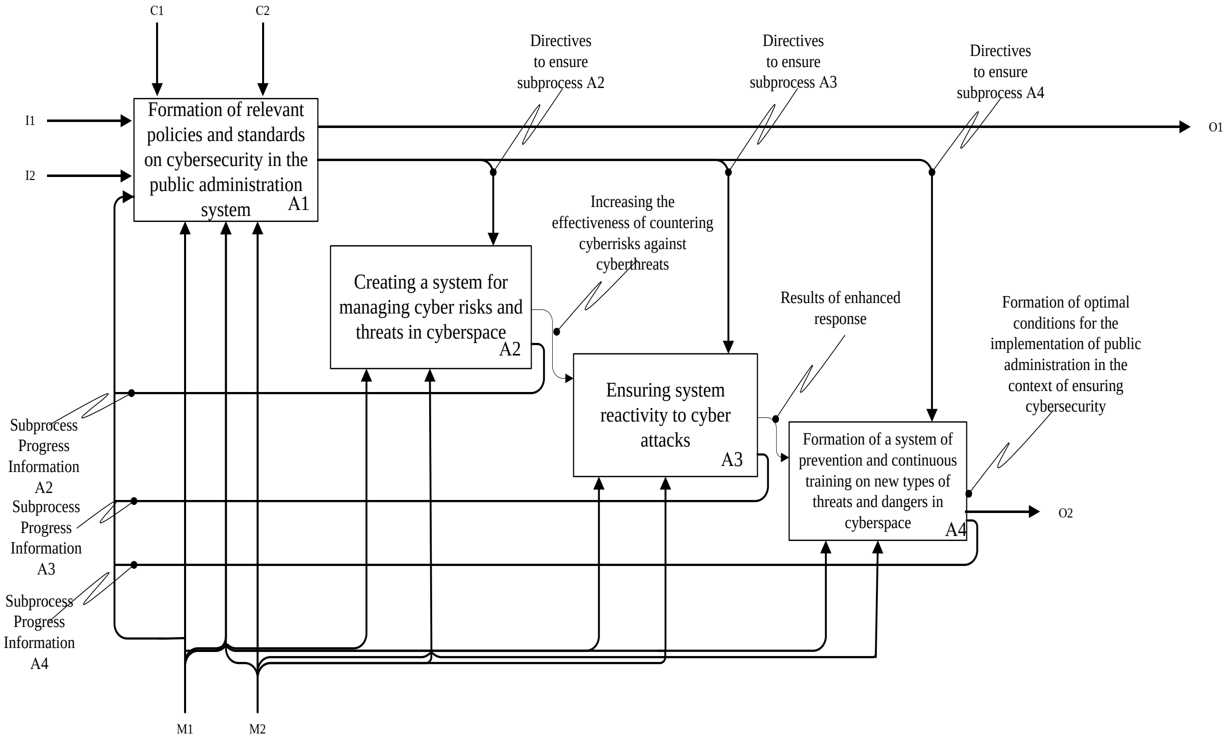
C1
C2
I1
I2
Formation of relevant policies and standards on cybersecurity in the public administration system
A1
Directives to ensure subprocess A2
Directives to ensure subprocess A3
Directives to ensure subprocess A4
O1
Creating a system for managing cyber risks and threats in cyberspace
A2
Increasing the effectiveness of countering cyberrisks against cyberthreats
Ensuring system reactivity to cyber attacks
A3
Results of enhanced response
Formation of optimal conditions for the implementation of public administration in the context of ensuring cybersecurity
Formation of a system of prevention and continuous training on new types of threats and dangers in cyberspace
A4
O2
Subprocess Progress Information A2
Subprocess Progress Information A3
Subprocess Progress Information A4
M1
M2

Figure 3. The main decomposition model of achieving the final goal A_0 (implementation of public administration in the context of ensuring cybersecurity) for the public administration system of the province of Ontario

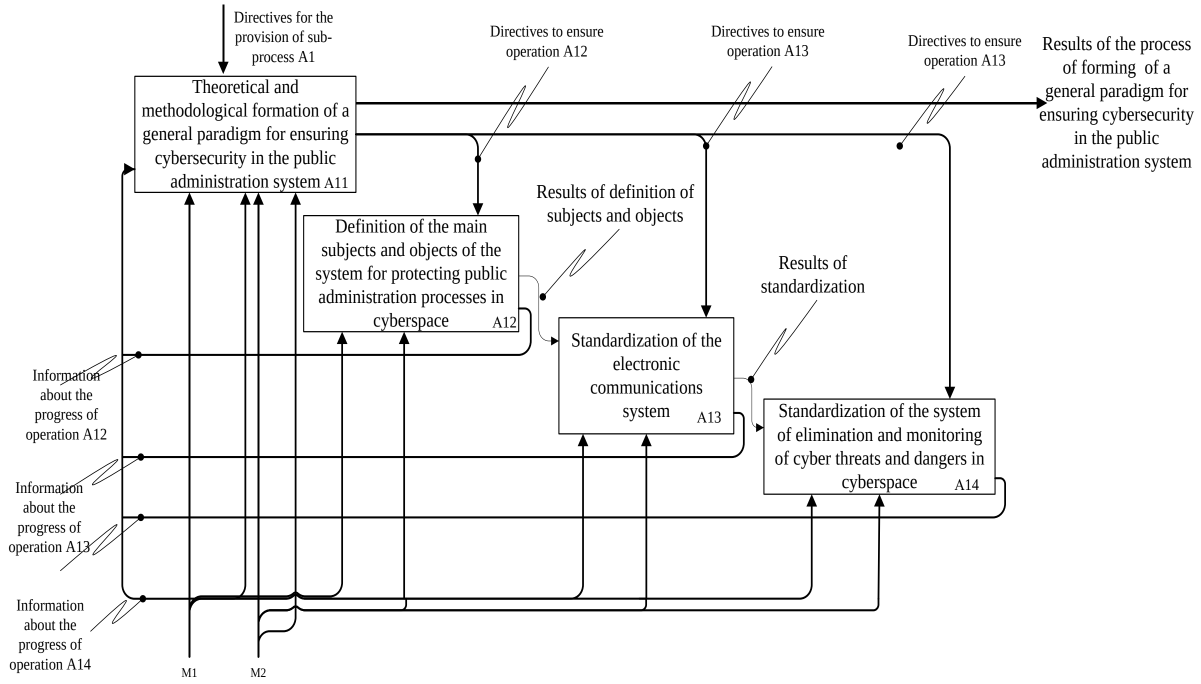
Directives for the provision of sub-process A1
Theoretical and methodological formation of a general paradigm for ensuring cybersecurity in the public administration system A11
Directives to ensure operation A12
Directives to ensure operation A13
Directives to ensure operation A13
Results of the process of forming of a general paradigm for ensuring cybersecurity in the public administration system
Definition of the main subjects and objects of the system for protecting public administration processes in cyberspace
A12
Results of definition of subjects and objects
Standardization of the electronic communications system
A13
Results of standardization
Standardization of the system of elimination and monitoring of cyber threats and dangers in cyberspace
A14
Information about the progress of operation A12
Information about the progress of operation A13
Information about the progress of operation A14
M1
M2

Figure 4. The decomposition model of achieving the second level of implementation of stage A_1 (Formation of relevant policies and standards on cybersecurity in the public administration system) for the public administration system of the province of Ontario

A_3 Ensuring system reactivity to cyber attacks. Cyber threats and influences are increasingly becoming an effective tool for achieving the goals of non-coercive control and management of both objects with a critical information infrastructure of the state, which may be subject to such influence, and individual citizens and their associations. They open up the possibility of achieving political goals, changing legitimate governments, as well as carrying out destructive changes in all spheres of the life of society and the state (economic, energy, spiritual, etc.), taking control and even enslaving entire peoples and countries with virtually no use of military strength in its classical sense. In this regard, the formation of a quick and effective response to all possible negative manifestations of cybersecurity is an important factor in the successful functioning of the public administration system of the province of Ontario.

A_4 - Formation of a system of prevention and continuous training on new types of threats and dangers in cyberspace. It is within the framework of public administration mechanisms in the field of preventing threats and risks in cyberspace that it is necessary to legally regulate the obligations of the subjects of the national cybersecurity system regarding the definition of cybersecurity risks. These risks may be limited only to technical risks, computer and telecommunication systems, should also include an analysis of risks of a strategic and operational nature, social, economic, infrastructural areas, etc. In addition, it is critically important to form a system of signal indicators that could group all possibly threatening elements of cybersecurity according to the level of threat or risk.

For a better understanding of the current model, we detail its individual stage. Given that the formation of a general paradigm for the policy of implementing public administration and its standards is a complex and complex process, in our opinion, it should be considered in more detail. Thus, Figure 4 shows the decomposition of the second level of implementation of stage A_1 (Formation of relevant policies and standards on cybersecurity in the public administration system) for the public administration system of the province of Ontario.

Thus, the main difference between Figure 3 and Figure 4 is that Figure 3. Represents the main stages of achieving the ultimate goal of modeling. While Figutr 4 provides for the specification of the achievement of one of the stages, namely A1, since this stage is complex and needed to be specified.

For a better understanding of all the elements of achieving the A_1 goal, let's consider their essence in more detail:

A_{11} Theoretical and methodological formation of a general paradigm for ensuring cybersecurity in the public administration system of the province of Ontario. The problem of effective cybersecurity requires a comprehensive solution and requires coordinated action at the national, regional and international levels to prevent, prepare, respond to and resume incidents by authorities, the private sector and civil society. Taking into account modern socio-political and informational challenges of determining political, scientific, technical, organizational and educational directions, designing an effective cyber defense system as part of a comprehensive response to cyber threats will contribute to the formation of an effective mechanism for countering threats in the cyber sphere, which is ahead of the response to dynamic changes taking place, development and implementation effective means and tools of a possible response to aggression in cyberspace. In this regard, the formation of an optimal paradigm for ensuring the cybersecurity of public administration is a critical parameter.

A_{12} Definition of the main subjects and objects of the system for protecting public administration processes in cyberspace. The definition of the main subjects and objects makes it possible to clearly define all the functional roles and responsibilities of all participants in the public administration system of the province of Ontario in the context of ensuring cybersecurity.

A_{13} Standardization of the electronic communications system. Communication is an indispensable component of management activities in general and public administration in particular. After all, the need to establish and maintain communications stems from the very essence of public administration as a targeted influence in order to achieve socially significant and socially defined goals and implies: the obligatory awareness of this need by the subjects of public administration, as well as the regulation and coordination of the communicative activities of these subjects. For the safe implementation of the communication system, an important element of proper public administration is the formation of clear standards and certifications of hardware and software for electronic communications.

A_{14} Standardization of the system of elimination and monitoring of cyber threats and dangers in cyberspace. The formation of a clear monitoring system and all possible threats and risks creates the preconditions for effective cybersecurity of the public administration system. This is due to the fact that the most effective systems and mechanisms for monitoring and elimination are selected during certification and standardization.

The presented models in Figure 3 and Figure 4 are a systematic result of all the modeling carried out, therefore they occupy a central place among the results of the study.

Thus, we have formed a model for the implementation of public administration of the province of Ontario in the context of ensuring cybersecurity. Such a model will be especially useful in the context of the fact that today the information space in which the sphere of public administration functions has expanded significantly, which has led to a proportional increase in dangers and threats in it. It should also be noted that this model is theoretical in nature and is the basis for further practical activities. In subsequent studies, the authors will adapt this theoretical model in accordance with practical results.

5. DISCUSSIONS

Discussing the results of our study, it should be noted that it is based on the use of graphical models. While most authors do not resort to the use of graphical methods, but only describe the measures they have proposed. This approach significantly reduces the level of understanding of the proposed mechanisms and methods.

Given the above, it is important to compare and highlight the key differences between our study and existing ones.

Min et al. [16] have explored the issue of forming an appropriate cybersecurity public administration strategy. In their work, they emphasized that the effectiveness of the system for combating cyber threats and cyber risks is the key to the formation of a secure information space and an urgent issue in many countries of the world. But, despite the emphasis on importance, this paper does not provide suggestions for improving this process. While in our work concrete steps have been formed to improve the system of public cybersecurity management.

Some scholars [17, 18], studying the issues of public administration in the context of ensuring cybersecurity, considered it only in the context of ensuring certain parts (security of the implementation of administrative services on the network, cybercrime, etc.). In our opinion, it is not correct to consider this issue separately, since most of the threats and dangers in cyberspace are interconnected and multifactorial, and therefore can affect various areas of the information space of public administration.

Another group of scientists [19, 20] in their research, taking the already existing scientific achievements about the features of public cybersecurity administration, created separate sets of mechanisms and measures to improve this process. But it should be noted that, despite the significant scientific achievements and high efficiency of the proposed measures, their presentation in the form of separate, unrelated and unsystematized methods is complex and difficult to implement. While in our study, all the proposed activities are presented in the form of a simple and understandable graphical model.

Thus, in our opinion, this study is relevant, given that the process of countering the methods of public administration of threats and risks of cybersecurity in the information space is a complex and complex process. That is why the use of a graphical methodology for this process is an important element of its understanding by ordinary employees of public authorities. It should also be noted that the methodology we used has a significant list of advantages that determine the following in the context of our study: the visibility of the display of results, the systematic and consistent implementation of the elements, a clear fixation of the place and role of resources and auxiliary elements. In addition, this model makes it possible, if it is necessary to detail a separate stage, to form more decomposition levels that would fully reveal the process of implementing a separate stage.

6. CONCLUSIONS

Cyberspace is a new channel for the creation and dissemination of various information, it has become a new engine of economic growth, a new platform for social management, a new way of international cooperation, and a completely new sphere of state sovereignty.

Therefore, ensuring cybersecurity in decision-making by public administration is an activity aimed at preventing, timely detection, termination or neutralization of real and potential threats in decision-making by public authorities when using cyberspace by applying legitimate mechanisms for ensuring cybersecurity.

This study has a close relationship with information and communication technologies involved in the process of ensuring cybersecurity.

In order to achieve the set goal it was used method of decomposition modeling IDEF0. As a result of the use of this methodology, a model of the implementation of methods and measures of the public administration system was formed in the context of ensuring the cyber security of the information space of its functioning. For a better understanding of this process, we have chosen the cybersecurity public administration system of Ontario in Canada.

The study has limitations, considering that this model was formed for a separate province of Canada, all elements of the model were selected in accordance with the specifics of the public administration of this country, as well as methods for ensuring cybersecurity. In subsequent studies, the authors plan to adapt this model to the realities of other public administration systems.

REFERENCES

[1] Zachosova, N. (2019). Innovative approach in the estimatology of financial institutions economic security: Possibilities of use in management and regulatory activity within the means of provision of the state financial security. Baltic Journal of Economic Studies, 5(2): 45-56. https://doi.org/10.30525/2256-0742/2019-5-2-45-56

[2] Hanna, N. (2018). A role for the state in the digital age. Journal of Innovation and Entrepreneurship, 7(1): 5. https://doi.org/10.1186/s13731-018-0086-3

[3] Pradhan, R.P., Mallik, G., Bagchi, T.P. (2018). Information communication technology (ICT) infrastructure and economic growth: A causality evinced by cross-country panel data. IIMB Management Review, 30(1): 91-103. https://doi.org/10.1016/j.iimb.2018.01.001

[4] Breznitz, D., Kenney, M., Rouvinen, P., Zysman, J., Ylä-Anttila, P. (2011). Value capture and policy design in a digital economy. Journal of Industry, Competition and Trade, 11: 203-207. https://doi.org/10.1007/s10842-011-0108-3

[5] Kohler, J.C., Dimancesco, D. (2020). The risk of corruption in public pharmaceutical procurement: how anti-corruption, transparency and accountability measures may reduce this risk. Global Health Action, 13(sup1): 1694745. https://doi.org/10.1080/16549716.2019.1694745

[6] Chałubińska–Jentkiewicz, K. (2022). Cybersecurity as a public task in administration. Cybersecurity in Poland, 191-513. https://doi.org/10.1007/978-3-030-78551-2_13

[7] Okewu, E., Okewu, J. (2015). E-government, e-Governance and e-Administration: A Typology of Corruption Management Using ICTs. In European Conference on e-Government, pp. 203-212.

[8] Kryshtanovych, M., Filippova, V., Huba, M., Kartashova, O., Molnar, O. (2020). Evaluation of the implementation of the circular economy in EU countries in the context of sustainable development. Business: Theory and Practice, 21(2): 704-712.

[9] Kryshtanovych, M., Antonova, L., Filippova, V., Dombrovska, S., Pidlisna, T. (2022). Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of ensuring security. International Journal of Safety and Security Engineering, 12(2): 193-199. https://doi.org/10.18280/ijsse.120207

[10] Kryshtanovych, M., Petrovskyi, P., Khomyshyn, I., Bezena, I., Serdechna, I. (2020). Peculiarities of implementing governance in the system of social security. Business, Management and Economics Engineering, 18(1): 142-156.

[11] Rachinger, M., Rauter, R., Müller, C., Vorraber, W., Schirgi, E. (2018). Digitalization and its influence on business model innovation. Journal of Manufacturing Technology Management, 30(8): 1143-1160. https://doi.org/10.1108/JMTM-01-2018-0020

[12] Heeks, R., Mathisen, H. (2012). Understanding success and failure of anti-corruption initiatives. Crime, Law and Social Change, 58: 533-549. https://doi.org/10.1007/s10611-011-9361-y

[13] Coppolino, L., D'Antonio, S., Mazzeo, G., Romano, L., Sgaglione, L. (2018). How to protect public administration from cybersecurity threats: The COMPACT project. In 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, pp. 573-578. https://doi.org/10.1109/WAINA.2018.00147

[14] Kostrubiec, J. (2021). The role of public order

regulations as acts of local law in the performance of tasks in the field of public security by local self-government in Poland. Lex Localis, 19(1): 111-129. https://doi.org/10.4335/19.1.111-129(2021

[15] Rodrigues, A.R.D., Ferreira, F.A., Teixeira, F.J., Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60: 101616. https://doi.org/10.1016/j.ribaf.2022.101616

[16] Min, K.S., Chai, S.W., Han, M. (2015). An international comparative study on cyber security strategy. International Journal of Security and Its Applications, 9(2): 13-20.

[17] Sylkin, O., Shtangret, A., Ogirko, O., Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: Practical aspect. Business and Economic Horizons (BEH), 14(4): 926-940. http://dx.doi.org/10.22004/ag.econ.287238

[18] Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. Verslas: Teorija ir praktika/Business: Theory and Practice, 20: 446-455. https://doi.org/10.3846/btp.2019.41

[19] Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. International Journal of Safety and Security Engineering, 11(4): 361-367. https://doi.org/10.18280/ijsse.110409

[20] Chowdhury, N., Nystad, E., Reegård, K., Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 12(3): 299-310. https://doi.org/10.18280/ijsse.120304