Public Administration Mechanisms for Ensuring Cybersecurity in Modern Conditions of Socio-Economic Development

Myroslav Kryshtanovych [†], Viktoria Andriyash [††], Hanna Bondar [†††], Yuriy Kushnir [††††], Kateryna Ozarko [†††††]

[†] Lviv Polytechnic National University, Lviv, Ukraine
[††] Petro Mohyla Black Sea National University, Mykolaiv, Ukraine
[†††] Petro Mohyla Black Sea National University, Mykolaiv, Ukraine
[††††] Uzhhorod National University, Uzhhorod, Ukraine
[†††††] State University of Intellectual Technologies and Communications, Odessa, Ukraine

Abstract
The main purpose of the study is to identify key aspects of public administration mechanisms to ensure cybersecurity in the current conditions of socio-economic development. Considerable communication and coordination between different private and public structures of different countries and organizations is necessary to solve cybersecurity issues. The goal of cybersecurity is to achieve and ensure that both the organization and the user's assets remain in a state of security against security threats, risks in the cyber environment. Based on the results of the analysis, key aspects of public administration mechanisms for ensuring cybersecurity in the current conditions of socio-economic development were identified.

Keywords:
Public administration, cybersecurity, mechanisms, security, development.

1. Introduction

The massive use of computer and telecommunication technologies in various spheres of public life in recent decades, including Internet technologies and the acquisition of cybernetics, along with a large number of advantages, has contributed to the emergence of a large number of threats. The implementation of these threats causes significant damage both at the national level and in the international arena. This prompted an understanding of the need to solve an urgent problem in order to minimize, eliminate and prevent cyber threats.

Cybersecurity is a very important aspect in today's world. Information protection involves the achievement and preservation of security properties in user resources aimed at preventing relevant cyber threats.

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, an increase in the traffic of data streams have 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, but also the protection of the entire system in the information field and in the field of computer technology in general.

It should be noted that the penetration of modern technologies into everyday life requires new knowledge in a new environment - cyberspace, from which one should expect not only a large number of services and benefits, but also the development of existing and new threats. These threats are associated with the use of mechanisms of unauthorized interference in the operation of systems and violations of the security of information processed by them, the constant development of the development industry and the widespread use of various kinds of harmful and vulnerabilities in widely used software, the use of special operations in cyberspace on critical information infrastructure objects. . The close attention of society to the issues of introducing modern technologies into a wide range of social relations, the daily growing danger from their use makes the task of a systematic study of the national cybersecurity system, its shortcomings, substantiation of the directions and tasks of its modernization relevant.

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.79

The main purpose of the study is to identify key aspects of public administration mechanisms to ensure cybersecurity in the current conditions of socio-economic development.

2. Methodology

To fulfill the tasks of the study, general scientific and special methods were used that form our methodology: the dialectical method; empirical (observation, comparison, measurement) research methods; generalizing and comparative; subject-object method to reflect their own theses; methods of synthesis and generalization - in the formation of the main conclusions. The methodological basis of the research is the scientific works of domestic and foreign scientists.

3. Research Results

The rapid development of information and computer technologies observed in recent decades has led to the fact that in the 21st century the hallmarks of the world economy have become: informatization of all spheres of society, when almost all spheres of state and economic activity are IT-dependent and cannot exist and function without information systems; the formation of an information society, in which numerous online social networks began to play a key role; the development of the financial sector has become largely dependent on the reliable functioning of global information and communication technologies; the emergence of cyberspace, seen as a new “domain” for conducting state and military policy, as well as digital diplomacy (online foreign policy) [1-3].

Compliance of the cybersecurity system with modern challenges and threats, its balance based on the implementation of the principles of the minimum necessary regulation (proportionality and adequacy of cybersecurity measures), the maximum possible application of national and international law, non-interference in privacy and protection of personal data, equivalence of requirements for ensuring cybersecurity of critical infrastructure and others is the main task of public policy in the field of cybersecurity and cyber defense.

The growth in the number, scale, intensity, complexity of cyber incidents and cyber threats in the global cyberspace that no single state is able to effectively counteract is one of the main factors that necessitates their international cooperation in the field of cyber security and cyber defense, combining their forces and means to reduce the level of cyber threats for citizens, society and the state.

The comprehensive penetration of information technologies into the daily activities of the individual, society and the state, the ever-growing dependence of observance of fundamental human rights and freedoms on the constancy of the functioning of networks and information systems, the growing sensitivity of the consequences of security incidents for these cybersecurity subjects requires the implementation of operational measures to restore the capabilities of such systems and networks, and systemic measures to improve network and information security in general. A special place in solving this problem is occupied by the introduction of an effective, reliable and productive national system of cybersecurity and cyber defense [4-6].

The key elements of the public administration mechanism for ensuring cybersecurity are presented in Table 1.

Table 1: The key elements of the public administration mechanism for ensuring cybersecurity

№	***Elements***
1	Information security
2	Software protection
3	Network security
4	Internet security

The key elements of the public administration mechanism for ensuring cybersecurity are:

– information security concerns the protection of the confidentiality, integrity and availability of information in general, to meet the needs of the respective user of the information;

– software protection is a process applied to manage and measure software applications in an organization in order to manage the risk of their use;

– network security concerns the design, implementation and operation of networks to achieve the objectives of information security in networks within organizations, between organizations and between organizations and users;

– internet security refers to the protection of Internet-related services and associated ICT systems and networks as an extension of network security in organizations and

the home to achieve security goals. Internet security also ensures the availability and reliability of Internet services. Cybersecurity techniques can be used to ensure the availability, integrity, system authenticity, confidentiality, and non-repudiation of information actions. Cybersecurity can be used to ensure user privacy and establish user trust [7-10].

Cybersecurity focuses on the security of the cyber environment, a system that can involve stakeholders from many public and private organizations using different components and different approaches to security.

In the processes of public administration, there is a systematic need to make decisions on development problems: economic, social, humanitarian, environmental, technological, etc., on which the cultural, educational, scientific, technological level of the country (industry, region, territory), its place and role in the processes of world development Decision-making is preceded by the processing of large arrays of heterogeneous data, often under time constraints and lack of information. The decision-making process is a procedure that involves choosing the best option from a number of alternatives through the constant processing of data streams. Today it is impossible to imagine the decision-making process without the use of computer equipment and technologies. One of the areas of work with information received by public authorities is its generalization through the use of intelligent methods and technologies, in particular with the help of Decision Support Systems, which allow analyzing data and, based on its results, making motivated decisions and making long-term forecasts.

The rapid development of the information society, the development of the global information society, the introduction of electronic document management into the activities of public authorities, the exchange of information bases between authorities, the network of the public administration system requires the formation of protection of information flows from attacks and sources. Today, there is an acute problem of developing effective mechanisms for ensuring information security as the main system of national security.
Thus, the cybersecurity of the public administration system is the basis of national security, which forms the security of the state, society, the public administration system, the population of the country in cyberspace through the creation of legitimate mechanisms for ensuring the cybersecurity of public administration.
The main external threats to the public administration system to ensure cybersecurity are presented in Table 2.

Table 2: The main external threats to the public administration system to ensure cybersecurity

№	***Threats***
1	Targeted attacks
2	Cyberterrorism
3	Cyberwars
4	Hacktivism
5	Attacks on banking systems
6	Attacks on e-government

External threats to cybersecurity in the public administration system include:
- firstly, targeted attacks. Depending on the goals, two opposite tactics of attacks on computer systems can be distinguished. The first option is to use software (virus, trojan) to attack, with the goal of compromising as many systems as possible. The second option is to carry out a targeted attack (hence the name "targeted", that is, targeted), to compromise the computers of a particular institution or even specific users (as a rule, high-ranking officials or their assistants, scientists, in general, people dealing with a particularly valuable information);
- secondly, cyberterrorism (impact on control systems). What, in fact, is called cyberterrorism is the possibility of influencing through a computer network (in particular, the Internet) on the control systems of transport, industrial facilities, houses and any technological processes. ICTs provide terrorists with several tools: the use of computer networks to control, coordinate and prepare attacks; the ability for terrorists to directly contact a wide range of people using the services of the modern Internet; Potentially, any technological process controlled by a digital control system (or SCADA) can become an object of attack by cyberterrorists;

- thirdly, cyberwars. Stuxnet is the prototype of a cyber weapon for cyber warfare, used to carry out sabotage or disable systems (for example, air or missile defense systems);
- fourthly, hacktivism is the abuse of information in social networks (impact on society). As a rule, we are talking about exposing secret operations, conspiracies, corruption and other actions at the level of governments or individual political forces that are contrary to the law, the principles of democracy and other universal values;
- fifthly, attacks on banking systems (money theft);
- sixth, attacks on e-government. "Electronic government" - an information and communication system, or an association of information and communication systems that automates the information interaction of bodies; state authorities and local governments with citizens and business entities in order to increase the efficiency of the provision of public services.

Internal threats to cybersecurity include: corruption, hardware bugs in microcircuits and firmware of computer and network equipment, weak organization of the cyberspace management system, lack of corporate policy.

4. Discussions

Discussing the results of the study, one should pay attention to the main aspects of managerial decision-making in the field of public administration in the context of ensuring cybersecurity. First of all, the management measures include the formation of a security policy by the public authorities that 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 security service, the definition of job descriptions for employees, the organization of regime measures, the protection of premises, the control over the work of personnel with information, the determination of the procedure for storing, backing up, destroying confidential information) [11-15].

The level of cybersecurity depends on the environment in which the cybersecurity system operates. Engineering means include shielding of premises, organization of alarm systems, protection of premises with personal computers. Cybersecurity software and hardware includes hardware, software, cryptographic protection tools that complicate the possibility of an attack, help to identify the fact of its occurrence, and get rid of the consequences of an attack. Therefore, ensuring cybersecurity in decision-making by public authorities 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.

5. Conclusions

To summarize, based on the results of the analysis, we can say that the availability and reliability of cyberspace rely heavily on the availability and reliability of relevant critical infrastructure services, such as telecommunications network infrastructure. Cyberspace security is also closely related to the security of the Internet, corporate/home networks and information security in general. It should be noted that the security domains defined in this section have goals and scope. Therefore, to address cybersecurity issues, significant communication and coordination between different private and public structures of different countries and organizations is necessary. Critical infrastructure services are considered by some governments as services related to national security, so they cannot be discussed or disclosed openly. In addition, the knowledge of critical infrastructure deficiencies, if not properly exploited, can have a direct impact on national security. Thus, a basic model is needed to share information and coordinate issues or incidents to fill gaps and provide adequate assurance to stakeholders in cyberspace.

The rapid introduction of information technologies in all spheres of life, the globalization of information relations determine the global trend towards the transfer of illegal activities to cyberspace. Today, computer crime or cybercrime, for which there are no state borders, threatens not only the rights and property of citizens, but also infringes on national interests. There is a high vulnerability of cyberspace to cyber-attacks, the activities of criminal groups, hackers, industrial financial groups and persons admitted to work with systems in the course of their official activities (insiders). Incidents of negative cyber impact are becoming more frequent, more organized, easier and cheaper to prepare and implement.

In the future, further research is expected to analyze foreign experience in ensuring the cybersecurity of public authorities and highlight its main mechanisms.

References

[1] Vinska, O., & Tokar, V. 2021. Cluster analysis of the European Union gender equality and economic development. Business, Management and Economics Engineering, 19(2), 373-388. https://doi.org/10.3846/bmee.2021.15382 .

[2] Pyliavskyi, I., Martusenko, I., Molnar, O., Dzyana, H., & Kushniriuk, V. 2021. Modeling ways of improving Green economy and environmental protection in the context of governance. Business: Theory and Practice, 22(2), 310-317. https://doi.org/10.3846/btp.2021.13336

[3] 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. https://doi.org/10.3846/bme.2020.12177

[4] Dvoráková, Z. 2005. Encouraging ethical behaviour in public administration by human resource management. Journal of Business Economics and Management, 6(3), 171-178. https://doi.org/10.3846/16111699.2005.9636105

[5] Alshubiri, F. N. 2019. Public finance indicators and the value of investment project development: a comparative study of GCC countries. Journal of Business Economics and Management, 20(6), 1143-1167. https://doi.org/10.3846/jbem.2019.10783

[6] Afonso, A., Schuknecht, L., & Tanzi, V. 2006. Public sector efficiency: evidence for new EU member states and emerging markets, European Central Bank. Working Paper No. 581/January.

[7] Davidaviciene, V., Raudeliuniene, J., Vengriene, E., & Jakubavicius, A. 2018. Consolidation of the activities of regulatory institutions while implementing e-government solutions. Journal of Business Economics and Management, 19(2), 307-322. https://doi.org/10.3846/jbem.2018.5534

[8] Di Berardino, C., D'Ingiullo, C., & Sarra, A. 2017. Distributive trade and regional productivity growth. The Service Industries Journal, 37(13-14), 833-857. https://doi.org/10.1080/02642069.2017.1359261

[9] Johansson, Å. 2016. Public finance, economic growth and inequality: A survey of the evidence. OECD Economics Department Working Papers, No. 1346. OECD Publishing, Paris.

[10] Lovre, I., Ivanović, O., & Mitić, P. 2017. Analysis of public sector efficiency in developed. Economic Analysis, 50(1-2), 38-49.

[11] Gavurova, B., Belas, J., Valaskova, K., Rigelsky, M., & Ivankova, V. 2021. Relations between infrastructure innovations and tourism spending in developed countries: a macroeconomic perspective. Technological and Economic Development of Economy, 27(5), 1072-1094. https://doi.org/10.3846/tede.2021.15361

[12] Sylkin, O., Buhel, Y., Dombrovska, N., Martusenko, I., & Karaim, M. 2021. The Impact of the Crisis on the Socio-Economic System in a Post-Pandemic Society. Postmodern Openings, 12(1), 368-379. https://doi.org/10.18662/po/12.1/266

[13] Shtangret, A., Korogod, N., Bilous, S., Hoi, N., & Ratushniak, Y. 2021. Management of Economic Security in the High-Tech Sector in the Context of Post-Pandemic Modernization. *Postmodern Openings*, *12*(2), 535-552. https://doi.org/10.18662/po/12.2/323

[14] Sylkin, O., Kryshtanovych, M., Bekh, Y., & Riabeka, O. 2020. Methodology of forming model for assessing the level financial security . Management Theory and Studies for Rural Business and Infrastructure Development, 42(3), 391–398. https://doi.org/10.15544/mts.2020.39 .

[15] Kryshtanovych M., Dragan I., Chubinska N., Arkhireiska N., Storozhev R. 2022. Personnel Security System in the Context of Public Administration. IJCSNS International Journal of Computer Science and Network Security, Vol. 22 No. 1 pp. 248-254 https://doi.org/10.22937/IJCSNS.2022.22.1.34