DOI (Issue): https: //doi.org/10.36486/np.2022.1(55) Issue 1(55) 2022

АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС. ФІНАНСОВЕ ПРАВО

UDC 352.07:316(477)

Alieksieienko Iryna,
Doctor of Political Sciences, Professor,
Dnipropetrovsk State University of Internal Affairs Dnipro, Ukraine,
ORCID ID 0000-0002-6873-003X
Kobets Maryna,
Candidate of Juridical Sciences, Senior Researcher,
Co-Head of the Department, State Research
Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-6725-8469

POLITICAL AND LEGAL PROBLEMS OF INFORMATION SECURITY IN PUBLIC GOVERNANCE IN THE CONDITIONS OF GLOBALIZATION

The article examines the problems of information security management of local governments of Ukraine in the context of globalization threats. It is determined that optimization of internal processes and of personnel management of local administrations are the first priority measures to improve information security. In addition, the information openness of local governments and authorities, as an innovative factor in the development of management informatization, must also be taken into account. This is necessary for the effective organization of the entire sphere of public administration.

Keywords: *information security, local self-government, globalization threats, cybersecurity, risk factors.*

Globalization trends, along with the emergence of the new power centers and political characters, provoked an interest of the scientific community in the study of legal problems of ensuring information security of the political process, its prerequisites, and factors for ensuring.

The growing interdependence of countries and peoples is one of the most influential global political trends of the modern period. This is an external prerequisite for the development of information security of the political process. Information security is characterized by both the presence of positive factors and the growth of international information threats in the economic, military, and political spheres of the life of the state, which weakens the stability and cooperation of countries on the world stage.

These information threats are carried out through certain foreign policy characters. Their distinctive feature is the desire to dominate the information space through an informational impact on political associations, individuals and social groups. Along with the foreign policy component, threats are realized by using modern technologies

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).5

in the field of informatization, that are aimed at destroying the political system, destabilization traditional values, blurring the personality, violating the territorial integrity and sovereignty of states. These are the distinctive characteristics of the internal political component of information security [9, 67].

Obviously, the researchers put into focus the problems associated with the development of principles and new technologies of information manipulation in the political sphere, as well as identifying sources to combat emerging threats and implementation of information security at the global, regional, and national levels.

The theoretical aspect of the research topic, in general, is associated with showing the importance of foreign and domestic information security components.

Scientific cognition of the definition of the concept of "information security" is relevant both in theoretical terms and in practice. Some researchers consider this concept as the security of networks and information systems, which is interpreted as cybersecurity. Some researchers of this issue interpret information security as manipulation of information, the impact of information on the consciousness of society, propaganda on the Internet.

The study of security threats by using information and computer technologies in the implementation and implementation of socially dangerous crimes, the commission of terrorist acts, interference in the affairs of sovereign states, the unleashing of interstate conflicts, incitement of interethnic hatred is also relevant and very important in the study of information security. Information security is considered the most important component of national security in the conceptual and key regulatory documents of many states. Thereby, the study of goals, objectives, a comparative analysis of approaches, and key problems of ensuring the security of the political process, assessment of the effectiveness, and efficiency of these approaches seem to be an issue of topical interest. Ukrainian society has passed into a qualitatively new state in the process of social and political transformations of our time. Among other things, it is characterized by the merger of local government bodies with business structures, which brings to a revision of the goals and objectives of state bodies, bodies for ensuring national and regional security [10, 317].

The appearance of completely new threats to both national security as a whole and its main components namely to social and economic, public, and information security, causes the transition to a new condition of the state. The emergence of these threats today is dictated primarily by the inconsistency of the legislative framework, its slow and insufficient development, with the rapid development of market relations, Ukraine's integration into global world socio-political relations. All this requires rethinking and developing new mechanisms for organizing counteraction to national and transnational crime, as well as for neutralizing internal and external threats.

Ensuring the reduction of the crime rate is one of the important conditions for the social and political development of Ukraine. Currently, the existing levers and methods of combating crime do not fully correspond to the dynamics of the development of organized crime.

Moreover, they do not help to reduce drug trafficking, human trafficking, extremism, terrorism.

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).5

The revolution in the field of information technologies facilitates the creation and implementation of innovations in the social and political system, which is sufficient to effectively solve modern state and regional problems, to ensure the rational use of natural resources, political, social, spiritual, and cultural development of society, as well as its safety. It is notable that criminals also use these advances in information technology. They have unlimited opportunities regarding access to informational, technical, and economic resources, their increase, and adaptation to their activities. These circumstances call for a rethinking of current views and developing new conceptual approaches to information security issues, solving problems with such phenomena as cyber-terrorism and cybercrime to ensure both information security and national security in general [3].

The study of information security issues is carried out primarily with technical positions. This has been happening since 1816.

This is what affects the relevance of information security in the context of the integration of information systems and the study of various levers of its management. At that time, the main objective was the protection of fundamental information databases of the state and society. After 1816, electrical and radio communications appeared. This leads to the use of interference-resistant signal coding. The direction towards a combination of technical and organizational measures to improve the security of radar and hydro acoustic equipment has been recorded since 1935. The implantation of electronic computing technology into the activities of the society and the state, which focused information security on limiting access to equipment began in 1946. The year 1965 is characterized by the creation of information and communication networks. At that time, information security was faced with the task of transferring network resource management to the administrator. Since 1973, information security has been associated with the development of new security criteria. “Hackers” are a new community that was formed during that period. Their goal was to damage the information channels of individual users, organizations, and entire countries. Information has become the most important resource of the state, and ensuring its security has become the most important component of national security. A new branch of international law that called information law was formed at that time. In 1985, world information and communication networks are created in which space technologies are applied.

Such classics of the political thought of that time as David Easton, Gabriel A. Almond and G. Bingham Powell actively participated in the study of the political process. The information and communication model of the political system presented by Karl Wolfgang Deutsch is suitable for the study of information security

The theoretical and methodological basis of this study is based on the treatises of foreign and domestic researchers on information protection and information security, including Bryzhko V., Tsymbaliuk V., Oriekhov A., Halchenko O., Kaliuzhnyi R., Shamrai V., Mezentseva N., Oliinyk O., Savruk M., Teptiuk Ye., Topchii V., Shelomentsev V., Potrubach N., Sivakova O., Cherniak L.

The object of the research is an information security of the political process in the system of public administration and local self-government.

The subject of the research is a comprehensive analysis of ensuring information security of the political process, including the regional aspect.

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).5

The purpose of the study is to identify effective areas and mechanisms for ensuring the information security of state administration and local government.

Results

Global trends in the development of the information society dictate the conditions for the complete information transparency of public authorities. In this regard, standards that regulate the access of interested parties to the information resources of the state are being formed. The state power is also dependent on these information resources when developing management decisions. Especially this dependence is manifested in local government, as it is directly related to all spheres of human life and the accumulation of operational information. According to researchers the growth of informatization processes in the provision of services by public authorities and local governments with the help of electronic document management contributes to the strengthening of the need for self-government bodies to use information, timeliness, and reliability of its receipt. According to experts, many databases are exposed to threats of unauthorized access, which entails a negative impact on confidential information, as a result of which the regime for achieving information security is violated [1, 97]. The risk factors in ensuring the security of confidential information in local governments are not clearly identified in any sources. Therefore, we pay special attention to the identification of the risk factors in our study.

– Threats to the constitutional rights and freedoms of man and citizen in the field of information activities and spiritual life.

– Threats to the informatization of management of the development of the territory of the municipality.

– Threats to the development and formation of the local information industry, which include the industry of information technology, communications and telecommunications, the efficiency of using local information resources.

– Threats to the security of information systems on the territory of the municipality [7, 78].

The sphere of legal regulation of information support of local self-government should cover the entire life cycle of information support: "design – creation – running – replacement". The last stage is to maintain information support up to date. System replacement strategies based on integral operating costs or on a revaluation basis are possible.

There are factors that directly affect the implementation of information security. They were formed according to the results of a sociological survey of local self-government bodies of the regions of Ukraine:

1) Unqualified personnel responsible for providing information support. This is one of the main factors in the formation and enhancement of this type of activity.

2) Lack of resources is also a significant factor. This is due to the fact that it is he who is a prerequisite for the purchase and modernization of ICT and its software.

3) Lack of broadband Internet and lack of providing all local inhabitants with high-quality communications and the Internet

4) Deterioration of hardware and its support, etc [6, 75].

These areas will help guide the administration not only on the formation of systematic activities to ensure information security, but also on the development of

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).5

specific measures in these areas. This will increase the level of information security of local self-government bodies. rationalization of paper workflow is considered as a significant course of formation security improvement. The amount of information that is processed and transmitted in electronic form is growing significantly In the modern period, in the context of informatization of communication channels and the transition to electronic document flow [2, 103].

Large amounts of information contained on paper are stored stably and require archival storage in paper form. Moreover, local authorities use organizational and administrative documents, which should be drawn up in paper form. Government regulations or decisions require protection from unauthorized access. It is necessary to reduce the number of specialists in the administration departments involved in making managerial decisions. it is also necessary to guarantee the impersonality of the request, keeping the applicant's personal data only in the department where he applied for getting a permission [4, 177].

It is argued that effective methods of protecting information in subdivisions of local administrations can be implemented with intensive work on the implementation of electronic document management systems. It is necessary to configure the access restriction mode at the electronic document flow. Unlike paper workflow, it is recommended to grant editing access rights to responsible users for electronic archive folders. Other users can only read these documents. In this case, the information will be protected not only from distribution, but also from unauthorized copying. The protection of paper media can be supported by the obligatory prescription in the specialist's duty regulations of conditions on personal responsibility for the distribution or transfer to third parties of information related to confidential information or state secrets.

To date, such measures are provided for in specialist's duty regulations of the personnel department, which mainly concern information about state secrets, confidential information and information with limited access. These restrictions are associated with separate types of information, however, do not apply to other types, that reduces the level of security of local governments.

Thus, the above-mentioned directions for ensuring information security in the administration of local self-government bodies are associated with the formation of know-how and modern information technologies that have new methods of protecting automated systems and software in order to introduce electronic document management. Forms of personal responsibility and control over the use, distribution and unauthorized copying of information are required. This surveillance guarantees technical means, but, in our opinion, a combination of technical means with administrative control measures will be more effective. Restricting functions carried out with documents that contain confidential information will allow reducing the risk of information leaks. Optimization of internal processes and Optimization of personnel management of local administrations are the first priority measures to improve information security. In addition, the information openness of local governments and authorities, as an innovative factor in the development of management informatization, must also be taken into account. It is necessary for an effective organization of information security.

DOI (Issue): https: //doi.org/10.36486/np.2022.1(55) Issue 1(55) 2022

REFERENCES

1. *Bryzhko V.M, Tsymbaliuk V.S. Orekhov A.A, Halchenko O.N.* (2002) E-budushchee y ynformatsyonnoe pravo. "E-future and information law". Ed. R.A. Kaliuzhnoho, M.Ya. Shvetsa. K.: "Yntehral". 264 p. [in Russian].
2. *Vakulych V.* (2014) Derzhavna informatsiina polityka yak mekhanizm realizatsii informatsiinoi funktsii suchasnoi derzhavy. "State information policy as a mechanism for the implementation of the information function of the modern state". Public Administration: Theory and Practice. No. 1 (17), P. 97–107 [in Ukrainian].
3. Global Risks Report 2018. URL: http: www.weforum.org. (Date of Application: 01.09.2020) [in English].
4. Informatsiine zabezpechennia upravlinskoi diialnosti v umovakh informatyzatsii: orhanizatsiino-pravovi pytannia teorii ta praktyky: monohrafiia. "Information support of managerial activity in the conditions of informatization: organizational and legal issues of theory and practice. Monograph". Ed. R.A. Kaliuzhnoho ta V.O. Shamraia. Kyiv. 2002. 296 p. [in Ukrainian].
5. *Mezentseva N.B.* (2013) Pravovi zasady protydii zahrozam informatsiinii bezpetsi ta rozvytku informatsiinoho zakonodavstva.[Legal bases of counteraction to threats to information security and development of information legislation]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava.* No. 10. P. 214–216 [in Ukrainian].
6. *Oliinyk O.V.* (2016) Pryntsypy zabezpechennia informatsiinoi bezpeky Ukrainy. "Principles of information security of Ukraine". *Yurydychnyi visnyk povitriane i kosmichne pravo.* Vol. 4, No. 41. P. 72–78 [in Ukrainian].
7. *Savruk M.V.* (2010) Aktualnist problemy zabezpechennia informatsiinoi bezpeky Ukrainy ta shliakhy yii rozviazannia. "The urgency of the problem of information security of Ukraine and ways to solve it". Systemy obrobky informatsii. No. 3(84). P. 77–79 [in Ukrainian].
8. *Teptiuk YeP.* (2014) Konstytutsiino-pravove vyznachennia poniattia prava na dostup do publichnoi informatsii. "Constitutional and legal definition of the concept of the right to access public information". *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Ser. Yurysprudentsiia.* No. 7. P. 85–87 [in Ukrainian].
9. *Topchii V.V.* (2015) Kiberteroryzm v Ukraini: poniattia ta zapobihannia kryminalno-pravovym ta kryminolohichnymy zasobamy. "Cyberterrorism in Ukraine: the concept and prevention of criminal law and criminological means". Naukovi visnyk Khersonskoho universytetu. Ser. Yurydychni nauky. Iss. 6. Vol. 3 P. 65–68 [in Ukrainian].
10. *Shelomentsev V.P.* (2012) Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta osnovni napriamy yii udoskonalennia borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka). "Legal support of the cyber security system of Ukraine and the main directions of its improvement fight against organized crime and corruption (theory and practice)". Iss. 1 (27). P. 312–320 [in Ukrainian].

УДК 352.07:316(477)

Алєксєєнко Ірина Вікторівна,
доктор політичних наук, професор, Дніпропетровський державний університет внутрішніх справ м. Дніпро, Україна,
ORCID ID 0000-0002-6873-003X
Кобець Марина Петрівна,
кандидат юридичних наук, старший дослідник, заступник начальника відділу ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0001-6725-8469

ПОЛІТИКО-ПРАВОВІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПУБЛІЧНОМУ УПРАВЛІННІ В УМОВАХ ГЛОБАЛІЗАЦІЇ

У статті розглядаються проблеми управління інформаційною безпекою органів публічного управління в Україні у контексті загроз глобалізації. Визначено, що оптимізація внутрішніх процесів та управління персоналом місцевих

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).5

адміністрацій є першочерговими заходами для підвищення інформаційної безпеки. Акцентовано на необхідності враховувати й інформаційну відкритість органів місцевого самоврядування та влади як інноваційний чинник розвитку інформатизації управління. Це слід виконувати для ефективної організації діяльності всіх суб'єктів політичної системи суспільства.

На основі аналізу масиву наукових джерел доведено, що тенденції глобалізаційного розвитку разом із новими центрами влади та політичних акторів актуалізували інтерес наукової спільноти до аналізу політико-правових проблем забезпечення інформаційної безпеки публічного управління.

Зростання взаємозалежності країн і народів, проникність кордонів, розвиток IT-технологій, діджиталізація суспільства, впровадження блокчейн-технологій та використання Big Data у сфері публічного управління і адміністрування – всі ці фактори актуалізують процес формування дієвої політики із захисту сфери управління державою від кіберзагроз.

Установлено, що інформаційна безпека сфери публічного управління характеризується наявністю амбівалентних чинників як позитивного характеру, так і процесів накопичення інформаційних загроз в економічній, військовій та політичній сферах життєдіяльності держави, що послаблює зовнішню і внутрішню стабільність. Доведено, що вектор сучасних глобалізаційних загроз спрямований на руйнування політичної системи держави, дестабілізацію її традиційних цінностей, розмивання цілісності особистості, порушення територіальної цілісності та суверенітету держав, на дестабілізацію в цілому сфери державного управління.

Зауважено, що всі ці обставини вимагають переосмислення сучасних політико-правових підходів у забезпеченні інформаційної безпеки органів публічного управління в контексті боротьби з кібертероризмом та кіберзлочинністю, а також вироблення нових концепцій забезпечення як інформаційної безпеки, так і національної безпеки держави загалом.

Ключові слова: інформаційна безпека, місцеве самоврядування, загрози глобалізації, кібербезпека, фактори ризику.

Отримано 11.04.2022