

Administrative and legal mechanism of information security in Ukraine

Viktor Hryshchuk, Lviv State University of Internal Affairs

Oksana Hryshchuk, Ivan Franko National University of Lviv

Nataliya Fedina, Lviv State University of Internal Affairs

Vasyl Parasiuk, Lviv State University of Internal Affairs

Oleg Batiuk, 'Odessa Law Academy' National University

Abstract

The peculiarity of the organizational and legal support of the administrative and legal regime of information security determines the application of technical information security standards adopted in the EU and NATO, which are formulated as a result of identifying typical legal cases and unification of technical and legal norms governing the procedure for the activities of information security entities in the context of relations arising from administrative and other public legal relations in order to focus the provisions on the uniformity of the procedure for eliminating threats in information and telecommunication systems, in the national information space, which is interpreted as a special way of jurisdictional elimination of contradictions arising in the course of human activity and business entities of economic activity in the information sphere. The structure and nature of the administrative and legal regime for ensuring information security is still considered as a system of legal restrictions on the private interests of enterprises and organizations providing information services in favor of the public interest. The evidence from practice shows the shortcomings of the existing model as a basis for the legal model of information security regulation, which requires the construction of a new paradigm of administrative and legal management based on an open model of legal management.

Keywords

Administrative and Legal Regime, Legal Management Model, Information Security, Legal Restrictions.

JEL Classifications

M5, Q2

Introduction

The relevance of the research topic is due to social, legal, and economic factors, theoretical and practical problems of administrative and legal regulation and law enforcement practice in the information sphere. According to this reality, the state is looking for new methods and means of influencing the participants, which are in relations in the field of information security. The situation in it is constantly changing because institutional transformations are aimed at improving the legal institutions that ensure the implementation of rights in the information sphere, increasing the efficiency of the public administration system, developing human capital and civil society, sustainable functioning and development of the national economy, overcoming the technological and infrastructural gap in the field of application information and communication technologies.

The use of special forms and methods of public administration in ensuring information security is explained by the need for a timely response to emerging threats of a political, economic, and military nature since under such conditions the use of conventional traditional mechanisms does not always lead to the expected result.

The state is the main subject of information security. The main role in the effectiveness of information security should be played by administrative law as the law governing the management activities of subjects of information security. The norms of administrative law ensure the implementation of the management mechanism in various spheres of life, establish the appropriate legal regimes, which should become an effective instrument of public administration in the studied area.

Within the framework of European integration, the main goal of which is to correct the basic functions of the state, conditions for the development of information freedoms should be created, strategic guidelines for the implementation of NATO standards should be outlined, a policy of effective public administration should be implemented with the involvement of new organizational structures and the use of the mechanism for implementing the norms of administrative law by the subjects of information security.

The conceptual design of the information security system of Ukraine has a certain complexity in connection with many aspects and provides for the development of theoretical and methodological issues and legal (in particular, administrative and legal) mechanism, main directions, and forms and methods of implementation of relevant innovations. The main element of the administrative-legal mechanism for ensuring information security is the administrative-legal regime. Today there is a need to study the administrative and legal mechanism for ensuring information security, on which the effectiveness of the implementation of administrative and legal measures depends, and ultimately the degree of protection of protected state, public interests, and information rights of a person and a citizen.

The purpose of the research is to clarify and analyze the conceptual and organizational and legal foundations of administrative and legal support for information security by public authorities and other authorized bodies, to develop proposals and recommendations on this basis that will contribute to improving the efficiency of information security.

Review of Previous Studies

At the same time, as the researchers note, today the problem of "a person in the information society" is just beginning to be realized. There is an understanding that the interests of an individual in the information sphere are in the implementation of the constitutional rights of a person and a citizen to access information, to use information in the interests of exercising activities not prohibited by law, physical, spiritual, and intellectual development and in the protection of information that ensures personal safety (Spanos & Angelis, 2016).

First of all, information is now recognized as an important economic resource. The use of information resources, the effective organization of information processes can significantly increase the profitability of many types of productive activities, contribute to solving political, military-political, socio-economic, cultural, educational, and social problems (Reznik et al., 2017; Klochko et al., 2016). Information is becoming an economic commodity, which stimulates the growth of a new segment of the national economy - information services all over the world.

Like any product information of the owner, who has the right to dispose of information at its own discretion, and its unauthorized use entails material losses for its owner, unauthorized actions with information become the basis for harm to the state, citizens, business entities (Mengke et al., 2016).

At the same time, in developed countries, information has become the main subject of labor. That is, the industry, where physical work has traditionally prevailed, has switched to information bases, respectively, information becomes a means of production, also requires appropriate legal protection (Yang et al., 2020).

It should also be pointed out that in recent decades, information has acquired the properties of a powerful means of influencing socio-political, ideological and socio-economic processes, becoming a kind of weapon that requires the creation of a system of counteraction, protection of information resources belonging to state bodies, constitute the state, medical, personal and niche types of secrets (Dunlap et al., 2018).

In modern conditions, information becomes a strategic resource, the legal protection of which is dictated by the need to develop the economy, to form a civil society, and to ensure the security of the state and citizens. In this regard, information security is the most important component of national security in general, and the problem of ensuring information security is extremely urgent.

In this regard, the problem of legal regulation of processes in which information begins to act as the basis of public relations arising when the information needs of the state, individuals, and society is realized, that is, when creating, receiving, processing, accumulating, storing, searching, distributing, and consuming information, when creating and using information systems, information technologies, and information security tools.

Methodology

The methodological basis of the research is an interdisciplinary approach, a set of philosophical, general scientific (analysis, synthesis, induction, deduction, abstraction, modeling), and special scientific methods that provide an objective analysis of the subject under study. With the help of the dialectical method of cognition, research and substantiation of the basic concepts used in the work and study of legal phenomena in the context of their emergence, functioning, development, and interconnection were carried out. The comparative method was used to study measures of administrative and legal support of information security; historical method-to study the formation of legal views on the concept of information security; the systemic and structural method made it possible to determine the tasks and principles of the activities of the subjects of information security to protect the rights and freedoms of man and citizen; the special legal method was used to determine the legal nature of the phenomena under study and to formulate the corresponding legal concepts; the method of interpretation (understanding) was used to clarify the content of legal norms of the administrative and legal mechanism for ensuring information security.

The scientific and theoretical basis is the scientific development of specialists in the field of law, computer science, information and communication technologies, and other spheres of human life.

The regulatory and legal basis of the study is the Constitution of Ukraine, laws of Ukraine, decrees of the President of Ukraine, regulatory legal acts of the Cabinet of Ministers of Ukraine, departmental regulatory legal acts, and regulatory legal acts of the European Union, EU member states, European Court of Human Rights, USA and Japan.

The empirical basis of the study consists of official data and materials of the law enforcement practice of public authorities vested with powers in the field of information security and judicial practice.

Results and Discussion

The norms defined in the acts of international and supranational organizations of the EU and NATO play a crucial role in shaping the goals of legal regulation of information security, which have a transnational character. The goal of legal regulation, set in accordance with the principles of

development of the information society to achieve the desired result, requires an organic combination of public and private legal means in the structure of the legal regulation mechanism. This will take into account the entrepreneurial nature of information activities and information security.

The elements of the mechanism of legal regulation of information security are means of a regulatory nature, including the norms of law contained in the legislation, norms-principles, norms of "soft law", norms of self-regulation of owners of information systems, customs, rules of information security of information systems; ethical codes and rules: legal facts as the basis for the emergence of information legal relations in the field of information security; legal relations arising in information security systems (obligation, control, supervisory, and corporate legal relations); acts of application and implementation of the law.

The principles of information law and the principles of constructing an administrative legal mechanism for ensuring information security are correlated as a goal and a means of achieving it. The basic principles of building a legal mechanism for ensuring information security include the principle of economic efficiency; the principle of using legal means for the purposes of legal regulation; the principle of priority use of private law funds; the principle of using public legal means exclusively for the purposes of anti-crisis management of information systems.

State administration in the field of information security is to create conditions for the harmonious development of the national information infrastructure, for the implementation of constitutional rights and freedoms of man and citizen, the legitimate interests of the individual, society, and the state in the national information space, in obtaining information and using it by individuals and legal entities in order to ensure the inviolability of the constitutional order, sovereignty, and territorial integrity of Ukraine, political, economic, and social stability, in ensuring the rule of law and order, the development of equal and mutually beneficial international cooperation.

Administrative and legal regulation of information security is a system of legal acts regulating the stable functioning of national information and communication infrastructure, information resources, information space, the implementation of information rights and freedoms of a person and a citizen, the legitimate interests of society and the state, Ukraine's international obligations in the information sphere, counteraction to extremism, separatism, internal and external threats to national interests defined by the Constitution and legislation of Ukraine.

Administrative and legal regulation of information security is a set of measures and techniques enshrined in the legislation aimed at ensuring safe activities in the dynamically developing information space for individuals and legal entities, which are favorable for innovation, investment and provide the population with a high standard of living and economic progress. Therefore, the content of the administrative-legal regulation of information relations requires substantiation within the framework of the administrative-legal regime of information security.

The primary backbone element of ensuring information security is a legal entity that coexists with legal entities (individuals and legal entities), interacting with each other on the basis of subject-communicative relationships. The subject of information security is a multifaceted phenomenon. It is determined by the current law and other social norms to the extent that these social norms are completed in existing law, representing the set of legal qualities of protection of information rights and human freedoms and public administration in the field of information security enclosed in a special legal form.

The subject of information security is an individual or collective person, a potential participant in specific information relations, which possesses legal personality, which by its characteristics is the bearer of subjective legal rights and obligations, participates in legal relations, according to the goals and objectives of ensuring information security, making certain efforts to achieve a positive interest, and using the means and methods of administrative and legal regulation.

The system of subjects of information security is an integral and synergistic set of elements that are determined by the functions of ensuring information security of public relations, united by the sphere of interests and needs, which reflect the legal characteristics of administrative legal means of regulation, the content and elements of the legal status of subjects, which participate in relations regulated by the rules of information law, systemic in content.

To ensure information security, a multi-level system of subjects is characteristic, based on the principle of unity and differentiation. The first level includes three groups of subjects: individuals and legal entities, public law formations, which make up the subsystems of these subjects. Other levels (structural elements of these subsystems) are various kinds of special subjects of administrative law, the division of which is due to the differentiation of the subject of the corresponding legal regulation.

The administrative and legal regime for ensuring information security is a complex legal category, the study of which is advisable to be carried out on an interdisciplinary basis using the methodology of information law with an emphasis on information, communication and synergistic aspects, since, according to its intended purpose, the administrative legal regime for ensuring information security is complex, open, incomplete information and communication system, which provide legal regulation of procedural (including information) relations through a system of administrative procedures, which are characterized by a high degree of dynamism in regulation thanks to the latest software components and means of communication, including areas of various sizes - ensuring information security of the individual, society, and the state.

The peculiarities of the administrative and legal regimes for ensuring information security are revealed through the self-regulation mechanism with the participation of public legal entities, the establishment of a balance of interests in the context of legal regulation of the implementation of the legitimate interests of owners of critical information infrastructure, which follows from administrative and other public legal relations, forming a balance of public and private interests.

The peculiarity of the organizational and legal support of the administrative and legal regime of information security determines the application of technical information security standards adopted in the EU and NATO, which are formulated as a result of identifying typical legal cases and unification of technical and legal norms governing the procedure for the activities of information security entities in the context of relations arising from administrative and other public legal relations in order to focus the provisions on the uniformity of the procedure for eliminating threats in information and telecommunication systems, in the national information space, which is interpreted as a special way of jurisdictional elimination of contradictions arising in the course of human activity and business entities of economic activity in the information sphere.

The administrative and legal regime for ensuring information security should integrate the spheres of development and security, thereby ensuring a kind of fusion of security and development policies, which, as the experience of the United States and Great Britain shows, leads to a redistribution of financial flows for the needs of the development of information infrastructure and its technical and legal regulation. Information security involves not only protecting people from critical situations and common threats but also ensuring freedom, which is the essence of life and the ability to realize their aspirations.

Recommendations

The events of recent months related to the conduct of massive cyberattacks and blocking of the work of government agencies, commercial banks, and life support facilities have clearly demonstrated the vulnerability and insecurity of the information environment, the ineffectiveness of the legal basis of the information security system. The legislation on administrative responsibility frankly "*does not keep pace*" with the rapid development of the information society, which negatively affects the state of law and order in society.

In these conditions, the scientific understanding of the role and significance of administrative responsibility, which, along with other types of legal responsibility, is designed to ensure information security requirements in a functional sense and to carry out a preventive function, acquires special relevance.

To ensure information security, almost all types of administrative coercion measures (warning, suppression, penalties) and measures to ensure the proceedings in the case of an administrative offense are applied. Some scientists stand out as a special type of coercion of administrative and legal remedial measures of coercion, which are used to restore the original order, the former state of affairs, as well as to compensate for the damage.

However, in the mechanism of administrative-legal regulation of public relations in the information sphere, a special role belongs to measures of administrative suppression. Measures of administrative restraint are an independent type of measures of administrative coercion, they have all the features of the latter. Measures of administrative restraint are applied by a significantly larger number of government bodies and their officials than other measures of administrative coercion, by some public entities that have received these powers through outsourcing. In addition, these measures are very numerous and varied in terms of their functional (target) purpose.

Administrative preventive measures can be classified according to the purpose of their use into two categories: measures taken with the aim of preventing, suppressing, and punishing administrative offenses within the state, and measures taken in emergency circumstances (martial law) or with the aim of preventing external national threats, including the number of information security. At the same time, the measures taken to prevent offenses are of a preventive nature. In peacetime, the variety of measures of an administrative, legal, and informational nature allows one to respond flexibly and pointwise to illegal reality in the information sphere.

Conclusion

The study of ways to improve the efficiency of administrative and legal support for information security leads to the following conclusions:

Information security is considered as the normatively regulated state of security of the national information space, which is organizationally ensured with legal means and characterized by a set of legal indicators provided reflecting: the level of crime in general and certain types; quality and quantity of legal material; the level of legal consciousness and legal culture of various social groups; the presence of gaps, inconsistencies, or ineffectiveness of legal acts, which regulate information security, economic security, and social popularity of the application of legal norms; development of legal and non-legal trends; the quality and quantity of the criminalization of public relations; the level of arbitrariness of employees of law enforcement and other bodies, which are obliged to resolve a legal conflict that has arisen; shortcomings in the execution of court decisions; the level of protection of law enforcement officials who resolve legal conflicts and implement the decisions taken;

The effectiveness of the activities of bodies that ensure information security depends on the quality of the analysis of the general social situation (all factors and conditions of life); the timeliness and adequacy of measures taken to identify and prevent violations, monitoring (control) of the general state of information security, which is due to the nature of the threats arising from internal and external sources of danger, the choice of legal (legitimate) means of security;

It is advisable to carry out a comprehensive legal regulation of information security management processes by systematizing and unifying administrative legislation using a codified regulatory legal act that will establish the initial principles of administrative and legal information security in Ukraine;

Departmental legal tools form a specific legal regime that allows the most complete and consistent implementation of the powers defined by the competence, with due regard for public interests, creating a hierarchy of powers, from one point of view – their importance for information security, from another point of view - a kind of priority in their implementation;

The effectiveness of the organization and provision of information security by the National Police is determined by compliance with an objective social purpose, which is expressed in appropriate conditions and indicators, and all the rest, relatively independent cost-economic, technological, and technical efficiency criteria should be considered as subordinate to social goals, outside of which their application loses its meaning and may hinder their achievement;

The main criteria for assessing the activities of the National Police of Ukraine in the field of information security should include a balance of organizational, structural, and functional parameters; adequacy (quantitatively and qualitatively) of resource provision; professional training and readiness of the personnel corps; content filling of management functions, corresponding to the needs of organizational and law enforcement practice; the quality of organizational and law enforcement activities that meet the needs of society and meet the priorities of protecting human and civil rights and freedoms.

References

Dunlap, L., Cummings, J., & Janicki, T.N. (2018). Information security and privacy legislation: Current state and future direction. *Journal of Information Systems Applied Research*, 11(2), 24-39.

Klochko, A.N., Kulish, A.N., & Reznik, O.N. (2016). The social basis of criminal law protection of banking in Ukraine. *Russian Journal of Criminology*, 10(4), 790-800.

Mengke, Y., Xiaoguang, Z., Jianqiu, Z., & Jianjian, X. (2016). Challenges and solutions of information security issues in the age of big data. *China Communications*, 13(3), 193-202.

Reznik, O.M., Klochko, A.M., Pakhomov, V.V., & Kosytsia, O.O. (2017). International aspect of legal regulation of corruption offences commission on the example of law enforcement agencies and banking system of Ukraine. *Journal of Advanced Research in Law and Economics*, 8(1), 169-177.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58(1), 216-229.

Yang, A., Kwon, Y.J., & Lee, S.Y.T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, 120(9), 1-11.