DOI: https://doi.org/10.34069/AI/2021.39.03.24

The role of rule-of-law institutions in ensuring information security of Ukraine

Роль правоохоронних органів у забезпечення інформаційної безпеки України

Received: April 1, 2021 Accepted: May 1, 2021

Written by:
Serhii Bratel[91]
https://orcid.org/0000-0001-6826-2582
Nataliia Makarenko[92]
https://orcid.org/0000-0001-7354-5122
Valentyn Bortnyk[93]
https://orcid.org/0000-0002-1226-6215
Yurii Levchenko[94]
https://orcid.org/0000-0003-1124-9517
Andrii Mykytchyk[95]
https://orcid.org/0000-0002-9740-4348

Abstract

The purpose of the article: is to study the threats to the information security of Ukraine and to analyze the legislative acts that define the tasks and functions entrusted to rule-of-law institutions to ensure information security of the State. Research methods: Logical method, normative and dogmatic method, monographic method, system and structural method, grouping method, the method of generalization are applied in the course of the study. Results of the research. Scientific approaches to the concepts of "information security", "cyber security" and "rule-of-law institutions" are considered. The threats to legal relations in this area are identified. Practical meaning. The role, mission and powers of the rule-of-law institutions in ensuring information and cyber security of Ukraine are established. Scientific novelty. The normative and legal acts, which enshrine the tasks and powers of rule-of-law institutions in ensuring the information security of the State in general and cyber security in particular, are analyzed in detail.

Анотація

Метою статті: є вивчення загроз інформаційній безпеці України та аналіз законодавчих актів, які визначають завдання та функції, які покладаються на правоохоронні органи щодо забезпечення інформаційної безпеки держави. Методи дослідження: компаративний, метод аналогії, аналізу та синтезу, індукції та дедукції. Результати дослідження. Розглянуто наукові підходи до визначень понять «інформаційна безпека» та «кібербезпека» та «правоохоронні органи». Визначено загрози правовідносинам у цій сфері. Практичне значення. Встановлені роль, завдання та функції правоохоронних органів у забезпеченні інформаційної- та кібербезпеки України. Наукова новизна. Детально проаналізовано нормативно-правові акти, які закріплюють завдання та повноваження правоохоронних органів у забезпеченні інформаційної безпеки держави загалом та кібербезпеки зокрема.

[91] PhD in Law, Associate Professor, Professor of the Police Law Department of the National Academy of Internal Affairs, Ukraine.
[92] Doctor of Law, Associate Professor, Professor of the Department of Criminology and Penal Law of the National Academy of Internal Affairs, Ukraine.
[93] PhD in Law, Associate Professor, Deputy Head of the Department of Administrative, Financial and Banking Law of the Interregional Academy of Personnel Management, Ukraine.
[94] PhD in Law, Associate Professor, Head of the Department of Criminology and Penal Law of the National Academy of Internal Affairs, Ukraine.
[95] PhD in Law, Associate Professor of the Department of Criminology and Penal Law of the National Academy of Internal Affairs, Ukraine.

Key words: information security, cyber security, rule-of-law institutions, Security Service, National Police.

Ключові слова: інформаційна безпека, кібербезпека, правоохоронні органи, Служба безпеки України, Національна поліція.

Introduction

We live in an information age when the access to the necessary data can be obtained in the shortest possible time anywhere in the world. The information age has made possible rapid global communications and the existence of information networks, which has significantly changed the essence of modern society. However, this does not mean that we always have access to quality and truthful information; the large amount of data creates favorable conditions for abuse (spam, flood), and the use of the latest computer technology threatens the security of many governmental and non-governmental enterprises, institutions and organizations. The growing role of information as a resource has led to the emergence of a new type of war – information one, the purpose of which is not to destroy the enemy physically, but using information (information operations, psychological operations) to obtain and consolidate competitive advantage over him.

Thus, information security is an extremely important issue today. This is due to the rapid development of information technology, mass computerization of the population, the active use of Internet resources, the creation of new software products, the emergence of web storage for data (Dropbox, Icloud drive, etc.), etc. Nowadays everyone has the opportunity to become a participant in the information flow and disseminate information that can have both positive and negative content. Therefore, it is necessary to protect the interests of all participants in the information relationship and to prevent violations or restrictions of their rights.

Currently, each State is making efforts to protect the information space by adopting appropriate regulations, creating special institutions, etc. No less important role in this process is played by the coordinated work of rule-of-law institutions, whose main task is to protect the rights of citizens, society and the State, including in the information sphere.

That is why the purpose of the article is to study the threats to information security of Ukraine and the analysis of legislative acts that define the powers of rule-of-law institutions in ensuring information security of the State.

Methodology

Logical method is used to formulate the concepts of "information security", "cyber security" and "rule-of-law institutions". Normative and dogmatic method is applied to study the content of the normative acts regulating the problems of ensuring information security and cyber security in Ukraine. Monographic method is helpful in studying the relevant works of foreign and Ukrainian scientists, who examined the problem under consideration. System and structural method makes it possible to investigate the modern threats to information security and cyber security in Ukraine. With the help of grouping method we determine the powers of rule-of-law institutions in ensuring information security and cyber security of the State. The method of generalization is applied to formulate overall findings.

Literature Review

There are two main approaches to understanding the concept of "national security" in modern worldview and philosophical thought. The founder of the first one – realistic approach – is the American political scientist Morgenthau (1982), who defined national security as the inviolability of the territory and institutions of the State, emphasizing military and political security, which is a traditional understanding.

The second approach – Human Security – was developed within the idealist theory of international relations and was characterized by the analysis of military, political, economic, social, humanitarian, environmental, information problems (Blumenau, 1985).

The concept of "information security" appeared in the late 80's. There was an attempt in the work of the German scientist to consider security issues that are related to information threats in a comprehensive way. Since 1992 there was a tendency in Russian-language press to study of the problem of information security as a separate issue (Lipkan, 2006, pp. 16, 17).

Rossouw von Solms, Johan van Niekerk (2013, p. 97) tried to distinguish the concept of cybersecurity from information security. The authors argue that these two terms are not

similar; cybersecurity goes beyond the traditional concept of "information security", as it includes not only the protection of information, but also its carriers, as well as human rights, society and the State in this area.

Getman, Danilyan, Dzeban, Kalinovsky, & Hetman (2020, p. 8) stress that the issue of information security, which occupies one of the key places in the system of ensuring the vital interests of all countries without exception, is particularly relevant. This is primarily due to the fact that it is through the information environment the threats to national security in various spheres of activity of the individual, society and the state are more often realized.

According to Nimyshchenko (2016, p. 18), today, not to mention the future, computers are the most promising tool for committing mercenary crimes. The authors cite data from American experts that the direct economic damage caused by computer crimes can already be compared with the benefits of computer implementation, and social and moral losses cannot be assessed at all.

He also stresses that the most common computer crimes include theft of money, things, machine information, machine time, unauthorized use of the system, sabotage and blackmail, espionage, vandalism. He believes that the most common type of computer crime is the theft of funds in electronic banking systems. According to him, it accounts for about 45% of all computer-related crimes.

Results and Discussion

Considering the legislative definitions of this concept, Furashev (2012, p. 54) formulates his own definition of information security. In his opinion, this is a state of protection of vital interests of an individual, society and the State, in which damage is prevented through: Negative information impact through, first of all, unauthorized creation, use, deliberately directed for a specific purpose, of incomplete, untimely, unreliable and biased information; the negative impact of information technology; - unauthorized violation of the regime of access to information with its further dissemination and use.

Nashynets-Naumova, A (2017, p. 4) emphasizes that information security is a legal concept. It means the state of protection of national interests of Ukraine in the information sphere, which is determined by the set of balanced interests of the individual, society and the State.

Kravets (1992, p. 744) argues that information security means: - legislative formation of State information policy; - creating opportunities to achieve information sufficiency for decision-making by public authorities, citizens and associations of citizens, other legal entities in Ukraine in accordance with the laws of the State; - guaranteeing freedom of information activities and the right of access to information in the national information space of Ukraine; - comprehensive development of the information structure; - support for the development of national information resources of Ukraine, taking into account the achievements of science and technology and the peculiarities of the spiritual and cultural life of the people of Ukraine; - creation and implementation of secure information technologies; - protection of property rights of all participants in information activities in the national space of Ukraine; - preservation of the State's ownership to strategic objects of information infrastructure of Ukraine; - protection of the State secrets, as well as information with limited access, which is the object of the right to own or be possessed only by the possession, use or disposal of the State; - creation of a general system of information protection, in particular protection of State secrets, as well as other information with limited access; - protection of the national information space of Ukraine from the dissemination of distorted or prohibited information products; - establishment by legislation of the regime of access of foreign States or their representatives to the national information resources of Ukraine and the procedure for the use of these resources on the basis of agreements with foreign States; - legislative enshrinement of the order of distribution of information products of foreign production on the territory of Ukraine.

Studying the legislation of our State, we can conclude that information security is the state of protection of vital interests of an individual, society and the State, which prevents the infliction of harm through: incompleteness, untimeliness and unreliability of the used information; negative impact of information; negative consequences of using information technology; unauthorized dissemination, use and violation of the integrity, confidentiality and availability of information.

Information security of Ukraine is the protection of political, State, public interests of the country, universal and national values provided by the Constitution. It covers, first of all, compliance with existing law on inadmissibility of abuses of media freedom, prevention of calls for violent

changes in the constitutional order and the seizure of power, violation of the territorial integrity of the State, propaganda of war, violence, cruelty, incitement to racial, national, religious hatred, rights and freedoms of an individual, society, and secondly, preventing the disclosure of information constituting a State secret or information with limited access, as well as textual materials that move across the State border of Ukraine, information from all areas of society in documentary form (libraries, archives, funds, databases), as well as other forms of information organization, information threats – a set of factors that create a danger of violation of constitutional rights and freedoms, State secrets, preservation of important information through unauthorized dissemination (leakage, theft, copying), loss, distortion, forgery, destruction, modification, copying, blocking of information and other forms of unlawful interference with such resources.

The problem of information security is considered in three main aspects:

information protection,
control over the national information space,
sufficient information support of State and non-state bodies,
public and private organizations (Mochernyi, 2000).

The function of protecting the information security of the State is performed, among others, by its rule-of-law institutions. To begin with, let's define which state authorities of Ukraine are rule-of-law institutions. The Law of Ukraine “On State Protection of Court and Law Enforcement Employees” (Law No. 3781-XII, 1994) states that "rule-of-law institutions are the Prosecutor's Office, the National Police, the Security Service, the Military Law Enforcement Service in the Armed Forces of Ukraine, the National Anti-Corruption Bureau of Ukraine, State border guards, Revenue organs and assemblies, penal enforcement bodies and institutions, and remand centres, bodies of the State financial control, fish protection, the State forest protection, and other bodies which carry out law enforcement functions ".

Rule-of-law institutions are called to protect the rights and freedoms of an individual, society and the State from existing and potential threats in the information sphere. Threats in the information sphere are conditions and factors that may harm the above rights and interests, as well as hinder their implementation in whole or in part.

According to item 3.6. of the Strategy of the National Security of Ukraine (Decree No. 392, 2020) the threats to information security are: information war against Ukraine; absence of a coherent communication policy of the State, insufficient level of media culture of society.

According to item 3.7. of the Strategy the threats to cybersecurity and security of information resources are: vulnerability of critical infrastructure, government information resources to cyber attacks; physical and moral obsolescence of the system of protection of state secrets and other types of information with limited access. Paragraph 3.8. of the Strategy identifies the threats to the security of critical infrastructure, namely: critical depreciation of fixed assets of infrastructure of Ukraine and insufficient level of their physical protection; insufficient level of protection of critical infrastructure from terrorist attacks and sabotage; inefficient security management of critical infrastructure and life support systems.

Kukharska and Polotai (2019, p. 139) propose to identify the following problem areas of information security:

a) the impact of information threats on public information resources, information systems and information should be considered in the narrow sense of its understanding – as “information security ”;
b) the impact of information threats on public and private information technology and telecommunications systems - should be considered in the problematic area of cybersecurity;
c) informational impact on human consciousness, culture and psyche is expected to be considered in the theoretical area of information security in its broadest sense, or in the context of psychological and spiritual security, which in the theory of national security are studied according to the object of the information influence of threats and the object of protection – consciousness, psyche or culture.

With the development of the information society, mass computerization of the population, the transition to digital technology, convergence and globalization of computer networks, increasing the amount of data stored electronically, there was a need to protect information in the cyber environment. Thus, a new direction was singled out from information security – cybersecurity,

which is aimed directly at data protection in the digital environment.

According to the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" cybersecurity is the protection of vital interests of an individual and citizen, society and the State when using cyberspace, which ensures sustainable development of information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace"(Decree No. 96/2016).

The development of cybersecurity and the recognition of this concept in the scientific circles began with the adoption of the Okinawa Charter of the Global Information Society in 2000, which is considered the "constitution" of the information society. The Charter states that the international community's efforts to develop the global information society must be coordinated to ensure safe and crime-free cyberspace (Group of Eight (G-8) Summit, 2000).

In 2005, Ukraine ratified the Convention on Cybercrime (Council of Europe, 2001), which sets out a list of threats that arise directly in cyberspace. They are, in particular, offenses against the confidentiality, integrity and availability of computer data and systems, offenses related to computers, offenses related to content, offenses related to infringement of copyright and related rights.

The Cyber Security Strategy of Ukraine (Decree No. 96/2016) states that economic, scientific and technical, information sphere, the sphere of public administration, defense-industrial and transport complexes, electronic communications infrastructure, the security and defense sector of Ukraine are becoming increasingly vulnerable to intelligence and subversive activities of foreign intelligence services in cyberspace. This is facilitated by the wide, sometimes dominant, presence in the information infrastructure of Ukraine of organizations, groups, and individuals who are directly or indirectly connected with the Russian Federation.

Modern information and communication technologies can be used to commit terrorist acts, in particular by violating the regular modes of operation of automated process control systems at critical infrastructure. Politically motivated activities in cyberspace in the form of attacks on government and private websites on the Internet are becoming more widespread.

Increasingly, the objects of cyber attacks and cybercrimes are the information resources of financial institutions, transport and energy companies, government agencies that guarantee security, defense, protection from emergencies. The latest technologies are used not only to commit traditional types of crimes, but also fundamentally new types of offences inherent in a society with a high level of informatization.

Rule-of-law institutions of Ukraine are subjects of information security in general and cybersecurity in particular; they are designed to ensure the rights, freedoms and interests of citizens, society and the State in this area, to protect them from the adverse impact of threats and destabilizing factors, to prevent and detect offenses in this area.

So let's consider which rule-of-law institutions ensure the information security of the State, and what powers they have.

One of the main components of the national security system in the state mechanism is the Security Service of Ukraine, whose activities are regulated by the relevant Law (Law No. 2229-XII, 1992). Among the tasks assigned to the Security Service of Ukraine, we can highlight the protection of State secrets. In order to perform its functions, the Security Service of Ukraine, in accordance with its main tasks, is obliged to: carry out information and analytical work, perform counterintelligence activities, participate in the development and implementation of measures to protect State secrets and confidential information owned by the State, to contribute to the preservation of trade secrets of the enterprises, institutions, organizations and entrepreneurs, the disclosure of which may harm the vital interests of Ukraine, in the manner prescribed by law.

The National Police of Ukraine carries out information and analytical activities exclusively for the exercise of their powers. As part of this activity, it:

1) forms databases (banks) on matters within their competence;
2) uses databases (banks) of other public institutions;
3) carries out research, information and analysis;
4) performs information interaction with other State authorities of Ukraine, rule-of-law institutions of foreign States and international organizations.

The Police can also create their own databases necessary to ensure the daily activities of police agencies (institutions, establishments) in the area of labor, financial, management relations, documentation flow and inter-agency information and analysis systems necessary to perform their duties. Besides, the Police fills in and maintains up-to-date databases (banks) of data included in the Unified Information System of the Ministry of Internal Affairs of Ukraine (for example, in relation to persons against whom the Police perform preventive work, defendants whose indictment has been sent to court; search for suspects, accused persons (defendants) who evade serving their sentences, or a court sentence; search for missing persons, etc.) (Law No. 580-VIII, 2015).

The basis of the national cybersecurity system is, inter alia, the Security Service of Ukraine and the National Police of Ukraine, which are assigned in the prescribed manner the following main tasks:

to the Security Service of Ukraine - prevention, detection, cessation and disclosure of crimes against peace and security of mankind committed in cyberspace; implementation of counterintelligence and search measures aimed at combating cyberterrorism and cyber espionage, as well as the readiness of critical infrastructure for possible cyberattacks and cyber incidents; counteracting cybercrime, the possible consequences of which directly threaten the vital interests of Ukraine; investigation of cyber incidents and cyberattacks on State electronic information resources, information required to be protected by law, critical information infrastructure; ensuring response to computer incidents in the area of State security;

to the National Police of Ukraine – ensuring the protection of human and civil rights and freedoms, the interests of society and the State from criminal encroachments in cyberspace; prevention, detection, cessation and detection of cybercrime; raising public awareness of cyber security (Decree No. 96/2016).

It should be noted that in 2015 the Department of Cyberpolice was established in the National Police, which in accordance with the legislation of Ukraine ensures the implementation of State policy in the area of combating cybercrime, provides information and analytical support to the National Police of Ukraine and public authorities within its competence. The Department also participates in the formation and implementation of the State policy for the prevention and combating criminal offenses, the mechanism of preparation, commission or concealment of which involves the use of computers, systems and computer networks and telecommunications networks (Makarchuk, Nikitenko, Dotsenko, Kopan, & Kitsul, 2021, p. 90).

Conclusion

Thus, we have determined that rule-of-law institutions are public authorities designed to protect the rights and freedoms of an individual, society and the State from existing and potential threats, to prevent and detect offenses, including in the information sphere. Threats in the information sphere are conditions and factors that may harm the above rights and interests, as well as hinder their implementation in whole or in part. The list of such threats is provided in the National Security Strategy of Ukraine, as well as in the Doctrine of Information Security of Ukraine.

With the development of the information society, as well as the increase in the amount of data that is stored electronically, there was a need to protect information in the cyber environment, the threats of which are relevant due to such factors listed in the Cyber Security Strategy of Ukraine.

The legislation of Ukraine prescribes the functions and tasks of rule-of-law institutions to overcome these threats and ensure the rights and interests of the subjects of information relations. We have determined that the Security Service of Ukraine and the National Police of Ukraine have the greatest powers in this area; their status as subjects of information security, as well as the tasks assigned to them for this purpose are enshrined in the laws directly regulating the activities of these bodies, and in special regulations governing information and cybersecurity of the State.

However, unfortunately, the powers and functions of rule-of-law institutions to ensure information security are not clearly delineated, which allows for competition in such activities. In addition, in our opinion, it is necessary to clarify the content of some tasks related to cybersecurity protection, assigned to these bodies in accordance with the provisions of the Cyber Security Strategy of Ukraine, as their wording is somewhat vague and Inaccurate.

References

Blumenau, D. (1985). “Information: myth or reality?” NTI: Series 2. Information process and systems, Num. 2, pp. 1–4.

Council of Europe (2001). Convention on Cybercrime of November 23, 2001. No. 185. https://rm.coe.int/1680081561

Decree No. 392/2020. On the decision of the National Security and Defense Council of Ukraine “On the Strategy of the National Security of Ukraine” Office of the President of Ukraine, September 14, 2020. Retrieved December 12, 2020 from https://www.president.gov.ua/documents/39220 20-35037

Decree No. 96/2016. On the decision of the National Security and Defense Council of Ukraine. “On the Cyber Security Strategy of Ukraine”. Verkhovna Rada of Ukraine, January 27, 2016. Retrieved December 12, 2020 from https://zakon.rada.gov.ua/laws/show/96/2016#n 11

Furashev, V. (2012). “Essence of informative safety and determination of “informative safety” and “safety of information” concepts”. Legal Information, 2(34), pp. 51-59. http://ippi.org.ua/sites/default/files/12fvmbbi.pd f

Getman, A., Danilyan, O., Dzeban, A., Kalinovsky, Y., & Hetman, Y. (2020). Information security in modern society: Sociocultural aspects. Amazonia Investiga, 9(25), 6-14. Retrieved from https://amazoniainvestiga.info/index.php/amazo nia/article/view/1021

Group of Eight (G-8) Summit (2000). Okinawa Charter on the Global Information Society. https://www.mofa.go.jp/policy/economy/summi t/2000/documents/charter.html

Kravets, E. (1992). Information security of the State. Legal encyclopedia in 6 volumes. Kyiv: Ukrainian encyclopedia.

Kukharska, N. and Polotai, O. (2019). “Cyber security as a component of information security of Ukraine”. Information Technology and Security, Vol. 7, Issue 2(13), pp. 136-148. https://ela.kpi.ua/bitstream/123456789/33883/1/ ITS2019-7-2_03.pdf

Law of Ukraine No. 2163-VIII. On the Basic Principles of Cyber Security of Ukraine, Verkhovna Rada of Ukraine, October 5, 2017. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Law of Ukraine No. 2229-XII. On the Security Service of Ukraine. Verkhovna Rada of Ukraine, March 25, 1992. https://zakon.rada.gov.ua/laws/show/2229-12#Text

Law of Ukraine No. 3781-XII. On the State protection of employees of court and rule-of-law institutions, Verkhovna Rada of Ukraine, December 23, 1994. https://zakon.rada.gov.ua/laws/show/3781-12#Text

Law of Ukraine No. 580-VIII. On the National Police of Ukraine, Verkhovna Rada of Ukraine, July 15, 2015. Retrieved November 10, 2020 from https://zakon.rada.gov.ua/laws/show/580-19#Text

Lipkan, V. (2006). Information security of Ukraine in terms of European integration: textbook. Kyiv: KNT.

Makarchuk, V., Nikitenko, O., Dotsenko, O., Kopan, O. and Kitsul, S. (2021). “Tasks and Powers of the National Police of Ukraine in Ensuring Information Security of the State”. Amazonia Investiga, 10(37), 86-92. https://doi.org/10.34069/AI/2021.37.01.8. https://amazoniainvestiga.info/index.php/amazo nia/article/view/1523/1497

Mochernyi, V., ed. (2000). Economic Encyclopedia: in three volumes. Vol. 1. Kyiv: Publishing Center “Academy”. http://ukr.vipreshebnik.ru/entsiklopedia/55-i/1943-informatsija-bezpeka.html

Morgenthau, H. (1982). In Defense of the National Interest. USA: University Press Of America.

Nashynets-Naumova, A. (2017). Information security: issues of legal regulation: monograph. Kyiv: Helvetika.

Nimyshchenko, O.A (2016). Information security of Ukraine at the current stage of state and society development. Nashe Pravo, Num. 1, pp. 17 – 23. Retrieved December 12, 2020 from http://irbis-nbuv.gov.ua/cgi bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I2 1DBN=UJRN&P21DBN=UJRN&IMAGE_FIL E_DOWNLOAD=1&Image_file_name=PDF/N ashp_2016_1_6.pdf

Solms, R.V., & Niekerk, J.V. (2013). “From information security to cyber security”. Computers & Security, Vol. 38, pp. 97-102. https://doi.org/10.1016/j.cose.2013.04.004