DOI: https://doi.org/10.34069/AI/2021.37.01.8

Tasks and powers of the National police of Ukraine in ensuring information security of the state

Завдання та повноваження Національної поліції України у забезпеченні інформаційної безпеки держави

Tareas y poderes de la Policía Nacional de Ucrania para garantizar la seguridad de la información del estado

Received: January 10, 2021 Accepted: February 21, 2021

Written by:
Makarchuk Vitalii[27]
https://orcid.org/0000-0002-1724-6918
Nikitenko Oleksandr[28]
https://orcid.org/0000-0002-0715-3873
Dotsenko Oleksandr[29]
https://orcid.org/0000-0001-7051-1656
Kopan Oleksii[30]
https://orcid.org/0000-0001-5322-1171
Kitsul Serhii[31]
https://orcid.org/0000-0002-0643-8463

Abstract

The purpose of the article is to examine the role of the National Police of Ukraine in ensuring the information security of Ukraine. The subject of the study: The subject of the study is the competence of the National Police of Ukraine in ensuring the information security of Ukraine. Methodology: Dialectical method, epistemological method, analytical method, formal and legal method, normative and dogmatic method, the methods of legal modeling and forecasting were used in the research. The results of the study: The definition of “information security” and “cyber security” is provided. The main factors that negatively affect the information space in Ukraine, as well as current threats to Ukraine’s national security in the information sphere are identified. Practical implications: It is established that the number of crimes in the information sphere is growing every year. In this regard, the task of the National Police is to combat crimes and other offenses in this area, as well as to protect relevant rights and freedoms of citizens, society and the State.

Анотація

Метою статті є дослідження ролі Національної поліції України у забезпеченні інформаційної безпеки України. Предмет дослідження: Предметом дослідження є повноваження Національної поліції України у забезпеченні інформаційної безпеки України. Методологія: У дослідженні використовувались діалектичний метод, гносеологічний метод, аналітичний метод, формально-правовий метод, нормативно-догматичний метод, методи юридичного моделювання та прогнозування. Результати дослідження: Надано визначення понять „інформаційна безпека” та „кібербезпека”. Визначено основні фактори, що негативно впливають на інформаційний простір в Україні, а також сучасні загрози національній безпеці України в інформаційній сфері. Практичні наслідки: Встановлено, що кількість злочинів в інформаційній сфері зростає з кожним роком. У зв'язку з цим завданням Національної поліції є боротьба зі злочинами та іншими

[27] PhD in Law, Assistant of the Department of Constitutional Law and Theoretical and Legal Disciplines of the Faculty of Law and Linguistics of Bila Tserkva National Agrarian University.

[28] Doctor of Law, Honored Lawyer of Ukraine, Professor of the Department of Public Law of the Faculty of Law and Linguistics of Bila Tserkva National Agrarian University.

[29] Doctor of Law, Associate Professor, Professor of the Department of Public Management and Administration of the National Academy of Internal Affairs.

[30] Doctor of Law, Professor, Leading Researcher of the Scientific Laboratory on Crime Prevention of the National Academy of Internal Affairs.

[31] PhD in Law, Senior Researcher of the Scientific Institute of Public Law.

Value/originality: The tasks and powers in the area of information security protection of the National Police in general and the Department of Cyber Security, in particular, are defined.

Key Words: National Police of Ukraine, economic security, powers, functions, investigative jurisdiction.

правопорушеннями у цій сфері, а також захист відповідних прав і свобод громадян, суспільства та держави. Цінність / оригінальність: Визначено завдання та повноваження Національної поліції загалом та Департаменту кібербезпеки зокрема у галузі захисту інформаційної безпеки.

Ключові слова: Національна поліція України, інформаційна безпека, повноваження, функції, підслідність.

Resumen

El propósito del artículo es examinar el papel de la Policía Nacional de Ucrania para garantizar la seguridad de la información de Ucrania. El tema del estudio: El tema del estudio es la competencia de la Policía Nacional de Ucrania para garantizar la seguridad de la información de Ucrania. Metodología: En la investigación se utilizaron el método dialéctico, el método epistemológico, el método analítico, el método formal y legal, el método normativo y dogmático, los métodos de modelización y previsión jurídica. Los resultados del estudio: Se proporciona la definición de "seguridad de la información" y "seguridad cibernética". Se identifican los principales factores que afectan negativamente el espacio de la información en Ucrania, así como las amenazas actuales a la seguridad nacional de Ucrania en la esfera de la información. Implicaciones prácticas: Se establece que el número de delitos en el ámbito de la información crece cada año. En este sentido, la labor de la Policía Nacional es combatir los delitos y otras infracciones en este ámbito, así como proteger los derechos y libertades relevantes de los ciudadanos, la sociedad y el Estado. Valor / originalidad: Se definen las funciones y competencias en el ámbito de la protección de la seguridad de la información de la Policía Nacional en general y del Departamento de Ciberseguridad en particular.

Palabras clave: Policía Nacional de Ucrania, seguridad económica, poderes, funciones, jurisdicción de investigación.

Introduction

According to Art. 17 of the Constitution of Ukraine “protection of the sovereignty and territorial indivisibility of Ukraine, and to ensure its economic and informational security are the most important functions of the State and a matter of concern for all the Ukrainian people (LAW No. 254k/96-VR, 1996). It follows that information security is one of the essential components of a country’s national security. Providing a well-formulated national information strategy greatly contributes to success in solving problems in political, military and political, military, social, economic and other spheres of State activity, as well as significantly influences the resolution of domestic, foreign and military conflicts.

The emergence of new information technologies and their active development in the 21st century has significantly increased the risk of violating the rights and interests of an individual, society and the State. This requires the search for new tools for the protection of confidential data, methods of collecting, processing and storing information, adoption of legislation that can effectively regulate the relations in this area. Ensuring the information security is a necessity, which becomes an attribute of modern life of any social entity, and requires a tireless work with the information that involves interaction with a variety of expert systems, the delocalization of actions, ensuring freedom and minimizing risks. That is why the protection of information security is a priority for the country as a whole and for specially authorized agencies in particular.

The National Police of Ukraine is one of the bodies that ensure the information security of our State. As Nehodchenko (2017) correctly points out, “The National Police, as the central executive body that serves society by ensuring the protection of human rights and freedoms, combating crime, maintaining public safety and order, cannot ignore problems related to the information sphere of our State as well. After all, the lack of adequate action on such threats is a factor that leads to the commission of many crimes against the integrity and inviolability of our State, property, the established order of activity of public authorities, etc.

Thus, the purpose of the article is to study the legal status of the National Police of Ukraine in ensuring information security of the State and determining its functions and powers in this process.

Methodology

Philosophical, general theoretical, special and intersectoral methods of scientific knowledge were used as the methodological basis for the research. In particular, dialectical method helped to study information security and cyber security as the components of national security of Ukraine, to determine actual threatens to this area as well as to identify the factors that affect its current state. Epistemological method was used to clarify the concepts of information security and cyber security of Ukraine and the legal status of the National Police of Ukraine in ensuring information security of Ukraine. The application of the analytical method contributed to the classification of threats to information security and cyber security of Ukraine, as well as the analysis of functioning of the National Police of Ukraine in ensuring information security of the State. Formal and legal method made it possible to study the competence of the National Police as the subject ensuring information security of Ukraine. Normative and dogmatic method helped to examine legal acts providing legal support for information security of the State and determining the powers of the National Police in this area. The use of methods of legal modeling and forecasting allowed to formulate the relevant conclusions.

Literature Review

The problem oh protection of information security of the State is the topic of consideration of a number of foreign and domestic scientist. For example, Tropina (2017) states that the development of information technology has greatly expanded the opportunities of people in various spheres of life, but at the same time allowed offenders to use these achievements to expand the areas of their illegal activities. She argues that the fight against cybercrime requires the adoption of an effective legal framework, as well as the provision of police with sufficient procedural tools to investigate such crimes. The author also examines the role of the police in combating cybercrime, the problems it faces during this process, and suggests possible solutions.

Elkins (2019) argues that the computer databases of relevant police departments can suffer from cyber-attacks as well. The author proposes the methods to protect police information systems, as well as the ways to recognize and report intrusions.

Woollacott (2019) examines the reasons that lead to the rapid development of cybercrime, as well as justifies the need to invest additional funds in the organization of special classes for police officers, during which they will learn to prevent and combat this problem.

Miralis (2020) considers 5 key challenges for law enforcement in fighting cybercrime, which are: loss of data, loss of location, challenges associated with national legal frameworks, obstacles to international cooperation, challenges of public-private partnerships.

The scientific and theoretical basis for the article is also the works of domestic scientists, who have considered the issue under investigation, such as: Cherniavskyi (2018) Demediuk (2018), Nehodchenko (2017), Zolotar (2018) and others. The normative basis for the research is the Constitution of Ukraine, Laws of Ukraine “On the National Police of Ukraine”, “On the National Security of Ukraine”, the Doctrine of Information Security of Ukraine, Cyber Security Strategy of Ukraine, etc.

Results and Discussion

The effective work of the police is closely related to the fundamental changes that are taking place in Ukraine today in connection with European integration processes, the improvement of the system for ensuring human rights and freedoms, the implementation of international legal standards in the domain of protection of the person etc. (Martselyak, Karelin, Koropatnik, & Kalyuzhnyi, 2020, p. 175). All this also applies to the protection of human rights in the area of information security, which is one the most vulnerable because of the events that are taking place in our country nowadays.

To begin with, let us provide a definition of “information security” to determine what should be protected by police officers in this area. The legislative definition of information security is enshrined in par. 13 of the Law of Ukraine “On the Basic Principles of Information Society Development in Ukraine for 2007–

2015" (LAW No. 537-V, 2007). According to this provision, information security is a state of protection of vital interests of a person, society and the State, which prevents damage due to: incompleteness, untimeliness and unreliability of the information used; negative information impact; negative consequences of the use of information technology; unauthorized dissemination, use and violation of the integrity, confidentiality and availability of information.

According to the Draft Doctrine of information security of Ukraine, developed pursuant to the decision of the National Security and Defense Council of Ukraine of April 28, 2014 "On the measures to improve the formation and implementation of State policy in the area of information security of Ukraine" (National Security and Defense Council of Ukraine, 2014) information security is an important independent area of guaranteeing national security, which characterizes the state of protection of national interests in the information sphere from external and internal threats and is a set of information and psychological (psychophysical) and information and technological security of the State.

The Draft Concept of Information Security of the State, developed by the Ministry of Information Policy of Ukraine (2015) also contain a definition of information security according to which it is a state of protection of vital interests of man and citizen, society and State, which prevents harm because of incompleteness, untimeliness and inaccuracy of disseminated information, violation of the integrity and availability of information, unauthorized circulation of information with limited access, as well as due to negative information and psychological impact and intentional causing of negative consequences of information technology.

Thus, information security is a complex, systemic, multilevel phenomenon, the state and prospects of development of which are directly influenced by external and internal factors, the most important of which are: 1) the political situation in the world; 2) the presence of potential external and internal threats; 3) the state and level of information and communication development of the country; 4) the domestic political situation in the country. At the same time, information security is a complex, dynamic, holistic social system, the components of which are the subsystems of security of the individual, State and society. It is the interdependent, systemic information unity of the latter is a qualitative certainty designed to protect the vital interests of man, society and the state, to ensure their competitive, progressive development (Zolotar, 2018).

Actual threats to the national security of Ukraine in the information sphere identified: the implementation of special information operations aimed at undermining defense capabilities, demoralization of personnel of the Armed Forces of Ukraine and other military formations, provoking extremist acts, panic, aggravation and destabilization socio-political and socio-economic situation, incitement of interethnic and interreligious conflicts in Ukraine; conducting by the aggressor State of special information operations in other States in order to create a negative image of Ukraine in the world; information expansion of the aggressor State and its controlled structures, in particular by expanding its own information infrastructure on the territory of Ukraine and in other States; information domination of the aggressor State in the temporarily occupied territories; insufficient development of the national information infrastructure, which limits Ukraine's ability to effectively counter information aggression; inefficiency of the State information policy, imperfection of the legislation concerning regulation of public relations in the information sphere, uncertainty of a strategic narrative, insufficient level of media culture of a society; spreading calls for radical action, propaganda of federalism and separatism in Ukraine (Decree of the President of Ukraine, No. 47/2017, 2017).

According to Kosohov and Siryk (2017), the main determining factors that negatively affect the information space in Ukraine should be considered: 1) constant losses among personnel (dead, captured, wounded), which lead to the formation of distrust in the Ukrainian military-political leadership that is allegedly unable to control the situation in Ukraine; 2) imperfect national information security system contributes to reducing the level of patriotism; 3) the activity of external information measures on the part of the Russian Federation influences the formation of the statement about the acceptability for Ukraine of the federal system of the State and the end of hostilities in Eastern Ukraine under the Kremlin regime.

Thus, as can be seen from the above, the state of information security in Ukraine is currently influenced by a number of negative factors that should be countered, including by the National Police. According to the Cyber Security Strategy of Ukraine (decree of the President of Ukraine No. 96/2016, 1996) to the

National Police of Ukraine is responsible for 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 citizens' awareness of cyber security.

Note that cyber security is an integral part of information security. When we talk about cyber security, we mean the state of protection of human rights, society and the State in the digital environment; information security means the prevention of violations of human rights, society and the State not only on the Internet, but also through other means of transmission, storage and reproduction of information (television, radio, etc.). According to the definition given in the Cyber Security Strategy, cyber security is a state of protection of vital interests of a person and a citizen, society and the State in cyberspace, which is achieved by integrated application of a set of legal, organizational and informational measures.

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 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 to commit fundamentally new types of crimes inherent in a society with a high level of informatization.

According to Demediuk (2018) "the number of detected crimes in the area of cyber security is increasing every year by an average of 2 500. In 2017, the National Police accompanied about 7 000 criminal proceedings, 4 500 of which are exclusively cybercrimes. In the eleven months of 2017, indictments were sent to courts against 726 people".

The Minister of Internal Affairs of Ukraine Arsen Avakov (2020), in turn, notes that over the past 5 years, the number of cybercrimes has increased by 2.5, and cyberspace has become the fifth area of hostilities. Ukraine was at the forefront of this new war. Aggression by the Russian Federation occurs not only in the form of hostilities, information campaigns and economic sabotage, but also in the form of brutal cyber war.

Due to this situation, the Cyber Police Department was established in 2015 in the system of the National Police (Order of the National Police of Ukraine, 2015). The Cyber Police Department of the National Police of Ukraine is an interregional territorial body of the National Police of Ukraine, which in accordance with the legislation of Ukraine ensures the implementation of State policy in combating cybercrime, provides information and analytical support to the National Police of Ukraine and public authorities on the issues within its competence.

The Department of Cyber Police participates in the formation and implementation of State policy to prevent and combat criminal offenses, the mechanism of preparation, commission or concealment of which involves the use of computers, systems and computer networks and telecommunications networks.

The Department in accordance with its tasks:

identifies, develops and ensures the implementation of a set of organizational and practical measures aimed at preventing and combating criminal offenses in the area of combating cybercrime;
takes the necessary operational and investigative measures to expose the causes and conditions that lead to the commission of criminal offenses in the area of combating cybercrime within the limits of its powers;
takes measures provided by the current legislation to collect and summarize information on facilities, including facilities in the area of telecommunications, Internet services, banking institutions and payment systems in order to prevent, detect and suppress criminal offenses;
ensures formation and filling of information arrays of data, automated information systems according to needs of office activity in the order provided by the legislation of Ukraine;
analyzes and systematizes data on criminal offenses committed in the area of combating cybercrime and using high technology from citizens through call centers, e-mails and feedback terminals, in the order provided by the legislation of Ukraine;

collects, summarizes, systematizes and analyzes information on criminogenic processes and the state of the fight against crime under service line of the Department at the national and regional levels, evaluates the results of individual performance indicators in accordance with current legislation, etc.

The powers of the National police in the area of information security are also filling and maintaining up-to-date databases (banks) of data included in the Unified Information System of the Ministry of Internal Affairs of Ukraine, as well as ensuring the entry of information into the Unified Register of Missing Persons in Special Circumstances, and keeping such information current within the limits set by law. The police also have direct operational access to information and information resources of other public authorities in compliance with the Law of Ukraine “On Personal Data Protection” (LAW No. 580-VIII, 2015).

When working with personal data, the police take all measures to prevent any violations of human rights and freedoms. To this end, authorized officials of the National Police monitor the state of technical protection of State information resources and information. Such control is implemented in the form of comprehensive, targeted and control inspections, which can be both scheduled and unscheduled.

The conformity of a complex of technical protection of the information to the requirements of regulatory legal acts and normative and technical documents of the system of technical protection of information is defined in the course of comprehensive inspection. During the target inspection, certain components of the technical information protection complex are checked for compliance of the authorized measures with the requirements of normative legal acts and normative and technical documents of the technical information protection system. During the control inspection, the completeness and sufficiency of the measures taken to eliminate the deficiencies that were identified during the previous comprehensive or targeted inspection are checked. Such verification is carried out after receiving a written notice of elimination of deficiencies (Cherniavskyi, 2018).

If a violation of human rights and freedoms was committed during the processing of information, the guilty police officer will be subject to disciplinary, administrative or criminal liability.

Conclusion

Thus, we have found out that information security in general and cyber security in particular is the object of protection of the National Police of Ukraine. This is provided by a number of domestic regulations, in particular, the Laws of Ukraine “On the National Police”, “On the National Security of Ukraine”, the Doctrine of Information Security of Ukraine, the Cyber Security Strategy of Ukraine and others.

The state of information security in Ukraine is currently affected by a number of negative factors, and the number of cybercrimes has increased by 2.5 over the past 5 years. Therefore, the National Police should counteract the current threats to Ukraine’s national security in the information sphere.

The main body of the National Police, which is directly related to ensuring information security, is the Department of Cyber Police, established to participate in the formation and implementation of State policy to prevent and combat criminal offenses, the mechanism of preparation, commission or concealment of which involves the use of computers, computer systems and computer networks and telecommunication networks. This Department performs a number of functions related to the prevention, detection and suppression of violations in the information sphere, preventive work among the population, participation in the development of legislation to regulate relations in this area.

Besides, the National Police carries out information and analytical activities to exercise its powers by forming and filling its own databases, as well as using the databases of other public authorities. Such activities are carried out exclusively within the legal field with respect for human rights and freedoms. To this end, the state of technical protection of State information resources and information is constantly monitored. In case of violation of human rights in the processing of personal data, the perpetrators are prosecuted.

References

Avakov, A. (2020). Cyber Police is moving to a new level of work and announces a large recruitment of specialists. Government portal. Available online. https://www.kmu.gov.ua/news/arsen-avakov-kiberpoliciya-perehodit-na-novij-riven-roboti-ta-ogoloshuye-velikij-nabir-specialistiv. Consultation date: 09/01/2021.

Cherniavskyi, S. ed. (2018). Law of Ukraine “On the National Police”: scientific and practical commentary as of September 07, 2018. Kyiv: Publishing House “Professional”.

Decree of the President of Ukraine. No. 47/2017. Doctrine of Information Security of Ukraine of February 25 of 2017. Available online. http://zakon.rada.gov.ua/laws/show/47/2017. Consultation date: 09/01/2021.

Decree of the President of Ukraine. No. 96/2016. On the decision of the National Security and Defense Council of Ukraine “On the Cyber Security Strategy of Ukraine” of January 27 of 2016. Available online. https://zakon.rada.gov.ua/laws/show/96/2016#n11. Consultation date: 09/01/2021.

Demediuk, S. (2018). The number of cybercrimes has risen two and a half times. EPravda. Available online. https://www.epravda.com.ua/news/2018/01/15/633010/. Consultation date: 09/01/2021.

Elkins, F. (2019). “Police are Victims Too: How to Protect Your Department from Cybercrime”. Community Policing Dispatch, 12(8). Available online. https://cops.usdoj.gov/html/dispatch/09-2019/cyber_crime.html. Consultation date: 09/01/2021.

Kosohov, O. and Siryk, A. (2017). The task of protecting the national information space based on the experience of the Russian Federation’s hybrid war in the Eastern Ukraine. Weapons Systems and Military Equipment, 1, pp. 38–41.

Law No. 254k/96-VR. The Constitution of Ukraine of June 28 of 1996. Available online. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. Consultation date: 09/01/2021.

Law No. 537-V. On the Basic Principles of Information Society Development in Ukraine for 2007–2015 of January 9 of 2007. Available online. https://zakon.rada.gov.ua/laws/show/537-16?#Text. Consultation date: 09/01/2021.

Law No. 580-VIII. On the National Police of Ukraine of July 15 of 2015. Available online. https://zakon.rada.gov.ua/laws/show/580-19#Text. Consultation date: 09/01/2021.

Martselyak, O., Karelin, V., Koropatnik, I. and Kalyuzhnyi, R. (2020). “Object and Subject of Staffing of the National Police of Ukraine at the Regional Level”. “Amazonia Investiga”, 9(26), pp. 174-180. https://doi.org/10.34069/AI/2020.26.02.19.
https://amazoniainvestiga.info/index.php/amazonia/article/view/1128

Ministry of information Policy of Ukraine. (2015). Draft Concept of Information Security of the State dated June 9, 2015. Available online. https://www.osce.org/files/f/documents/0/2/175056.pdf. Consultation date: 09/01/2021.

Miralis, D. (2020). “The 5 key challenges for law enforcement in fighting cybercrime”. Lexology. Available online. https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4. Consultation date: 09/01/2021.

National Security and Defense Council of Ukraine no. n0004525-14. On the measures to improve the formation and implementation of State policy in the area of information security of Ukraine of April 28, 2014. Available online. https://zakon.rada.gov.ua/laws/show/n0004525-14#Text. Consultation date: 09/01/2021.

Nehodchenko, V. (2017). The specifics of the activities of the National Police of Ukraine in ensuring information security. Scientific Bulletin of Kherson State University. Series: Legal Sciences, 2(1), pp. 40-45.

Order of the National Police of Ukraine. 2015. On approval of the Regulation on the Cyber Police Department of the National Police of Ukraine of October 11, 2015 no. 85. Available online. http://tranzit.ltd.ua/nakaz/. Consultation date: 09/01/2021.

Tropina, T. (2017). “Cyber-policing: the role of the police in fighting cybercrime”. In D. Nogala, J. Fehérváry, H.-G. Jaschke, & M. den Boer (Eds.), European Police Science and Research Bulletin – Police Science and Police Practice in Europe, Special Conference Edition Nr. 2 (pp. 287–294). European Union Agency for Law Enforcement Training (CEPOL), Luxembourg.

Woollacott, E. (2019). “Why police need the skills to counter cybercrime”. Raconteur Daily. Available online. In: https://www.raconteur.net/legal/crime/police-skills-cybercrime/. Consultation date: 09/01/2021.

Zolotar, O. (2018). Human information security: theory and practice: monograph. Kyiv: Artek Publishing House LLC.