

UDC 342.3 + 321.01
DOI:10.10.56215/01211214.46

State Policy of Human Rights in the Field of National Security in the context of Digitalization

Denis A. Chyzhov*

National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
Kyiv Regional Center of the National Academy of Legal Sciences of Ukraine
01024, 3 Pylyk Orlyk Str., Kyiv, Ukraine

■ **Abstract.** The purpose of the study is to determine the main principles of the state policy of promoting human rights in the national security sphere in the digital environment based on the analysis of scientific approaches, normative documents in the national security domain, human rights and digitalisation of the country. To meet this goal, the following tasks have been set: to provide arguments for the relevance of the chosen topic for research; to characterise the content of the identified areas; to substantiate the importance of ensuring state security and human rights in the context of digitalisation; to determine the relationship between information and cyber security at several levels – the security of the individual, society and the state. The methodological basis of the scientific article is a coherent and consistent system of methods that allowed analysing the subject of the study properly, in particular, scientific methods of analysis, synthesis, induction and deduction were used. The theoretical basis of this publication includes the writings of Ukrainian scholars on ensuring human rights in the national security sphere in the context of digitalisation and the reports of government officials delivered at special events dedicated to the chosen topic. The scientific novelty of the publication lies in the fact that, based on the analysis, two areas of human rights protection in the sphere of national security in the context of digitalisation have been identified: 1) ensuring information security as a component of national security in digitalisation; 2) implementation of digital transformation of the Armed Forces and ensuring information security. At the same time, it is substantiated that more such areas can be identified, however, given the limited scope of the study, other areas will be the subject of further scientific research. It is proved that information security should be considered in the context of cyber security. Their symbiosis can be represented at three levels: state security, public security, and individual security. The article emphasizes the importance of prioritising the information and cyber security of the individual: its provision will become the basis for the information security of society and the state as a whole. Cybersecurity is argued to reach a new level – the national level, moving from the civilian to the defense sphere

■ **Keywords:** digitalisation; ensuring human rights; national security; cyber security; cyber attack; security and defence; aggression

■ Introduction

Ensuring state security has become the central concern for representatives of the government, society and the international community. Human rights protection in the sphere of national security in the conditions of aggression of the Russian Federation

is of great importance. National security policy has always required increased attention from the state and civil society, and now this issue has become even more relevant. It is associated with the conflict in the East of the country, the development of digital technologies, the emergence of new information threats, the increased risk of cyber attacks, etc.

May 11-13, 2021 within the framework of the All-Ukrainian forum “Ukraine 30. Security of the Country” [1], a number of key issues in the national security sphere were discussed: conducting a socially significant dialogue on national security issues with representatives of strategic partners of

■ Suggested Citation:

Chyzhov, D.A. (2021). State policy of human rights in the field of national security in the context of digitalization. *Scientific Journal of the National Academy of Internal Affairs*, 26(4), 46-52. doi: 10.10.56215/01211214.46

■ *Corresponding author

■ Received: 26.08.2021; Revised: xx.xx.2021; Accepted: xx.xx.2021

the state; identifying priorities in reforming and developing forces, sectors and industries related to ensuring security in Ukraine; addressing the topic of information and cybersecurity, and the measures necessary to strengthen them, in particular the creation of cyber defence forces, etc.

The scientific relevance of the chosen subject is evidenced by a significant amount of scientific research that directly or indirectly covers the issues of state policy of ensuring human rights in the field of national security in the context of digitalisation. Three main areas of scientific research can be distinguished: 1) state policy in national security; 2) ensuring human rights as a factor in ensuring national security; 3) digitalisation and its impact on human rights and national security. At the same time, a detailed study on the state policy of ensuring human rights in the national security area in the context of the development of digitalisation has not yet been carried out. In particular, I. Doronin considered the issues of digital development and national security in the context of legal problems [2], and also devoted his dissertation thesis to the theoretical and legal study of the national security of Ukraine in the information age [3]. O. Pyshchulina analysed the current stage of world economic and social development, which is characterised by a significant impact of digitalisation, identified the main determinants and grounds for the development of the digital economy in Ukraine, and the country's readiness to introduce and use digital technologies (both from the point of view of suppliers and consumers of digital services), analysed the potential risks and threats of digitalisation in Ukraine and the world [4]. The study of the issue of national security is carried out by V. Smolyanyuk, who investigated the systemic principles of the national security of Ukraine [5]. S. Drobotov devoted his research to the constitutional and legal provision of national security in Ukraine [6]. O. Kubetska, T. Ostapenko, Ya. Paleshko defined the conditions for ensuring the national security of the state [7]. P. Bugutskyi studied the theoretical foundations of the formation and development of national security laws in Ukraine [1]. The analysis of these scientific works shows that a holistic, comprehensive study of the state policy of ensuring human rights in the field of national security in the context of the development of digitalisation has not yet been carried out. Some issues in this area of research are considered in this study.

The purpose of the publication is to determine the main areas of the state policy of ensuring human rights in the national security sphere in the context of digitalisation, based on the study of scientific approaches, normative documents in the sphere of national security, human rights and digitalisation of the country.

To achieve this goal, the following tasks are set:

- to present arguments on the relevance of the chosen research topic;
- to substantiate the importance of ensuring state security and human rights in the context of digitalisation;
- to describe the content of the outlined directions;
- to determine the interconnection of information and cyber security at several levels – security of the individual, society and state.

The study proves that the issue of ensuring state security has been the major one for Ukraine over the years. This is attributed to the conflict in the East of the country, the development of digital technologies and the increased risk of cyber-attacks, etc.

As a substantiation of the relevance of the study of the selected issues, the All-Ukrainian Forum “Ukraine 30. Security of the Country”, which discussed a number of key issues in the field of national security, the approval of the Strategic Defence Bulletin of Ukraine, one of the priorities of which is the digital transformation of the Armed Forces and information security, and a number of modern scientific developments in this area.

Based on the analysis, two areas of scientific research were identified to address the subject of the article:

- ensuring information security as a component of national security in the context of digitalisation;
- implementation of digital transformation of the Armed Forces and ensuring information security.

■ Results and Discussion

To begin with, the rights of every person can be considered protected and their interests secured only in conditions where the security of the country is not threatened. It is difficult to imagine a situation in which the state, whose security is constantly under threat, will be able to provide full protection of the rights of its citizens.

Article 3 of the Constitution of Ukraine defines a person, his life and health, honour and dignity, inviolability and security as the highest social value. Accordingly, this also includes ensuring security in general, i.e., national security.

Article 17 of the General Principles states that “to protect 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” [8].

During his speech at the All-Ukrainian forum “Ukraine 30. Security of the country” “President of Ukraine – Supreme Commander-in-Chief of the Armed Forces V. Zelenskyy [9] emphasised

the importance of security for the state. Along with freedom and justice, security is one of the most important values for Ukrainians. In the context of Russian aggression, society has no doubts: security is the main condition for the existence of the state and its independence. One of the main focuses of the programme is the security of the person and the country. Its provision as an integral element of a complex social system with all its needs, interests, and opportunities is the basis of the national security policy of Ukraine. This once again confirms the interconnection and interdependence of personal and state security.

As part of the study, it is also necessary to formulate a definition of the national security of Ukraine. The Law of Ukraine "On the National Security of Ukraine" interprets it as "the protection of state sovereignty, territorial integrity, democratic constitutional order and other national interests of Ukraine from real and potential threats" [10]. There is no exhaustive list of objects subject to protection as objects of national security. Thus, the objects of national security are all spheres of public life: vital interests of a person, society and the state, their protection from external and internal threats. Scientists claim that the triad of objects of national security of the state is the security of the individual, society and the state [11].

The examination of scientific and regulatory sources on the analysed topic made it possible to identify several areas of scientific research:

- ensuring information security as a component of national security in the context of digitalisation;
- implementation of digital transformation of the Armed Forces and ensuring information security.

There are many more such areas. However, given the limited scope of the study, they will be the subject of further scientific research.

The following areas should be considered thoroughly:

1) ensuring information security as a component of national security in the context of digitalisation. Digitalisation penetrates all spheres of human life. Ukraine became the first country in the world where digital passports in a smartphone became official legal analogues of ordinary documents. In September 2021, Ukraine started the process of introducing a "no-paper" approach: state authorities will not request paper documents if the necessary information is already in the registers [12]. Other digital

services should also be mentioned: eMalyatko is an integrated service for parents of newborns. With one application submitted online, it is possible to register the birth of a child and access up to 9 state services from various authorities needed immediately after the birth of a child; eCase – a system for optimising pre-trial investigations of anti-corruption agencies of Ukraine, which is integrated with the Unified Register of Pre-trial Investigations and judicial systems, which will allow NABU, SAP and HACC to interact online. Under such conditions, the issue of ensuring information security is becoming more and more relevant: databases of information about citizens, databases of holders of such data, the results of receiving certain services through internet requests, and so on should be reliably protected. Specially authorised officials direct their attention to these issues. In particular, within the framework of the All-Ukrainian forum "Ukraine 30. National Security" Deputy Head of the State Service for Special Communications and Information Protection of Ukraine noted that "information security in the context of national security is dual in nature. Firstly, information security aims to protect the balanced interest in the information sphere of a person, individual, citizen, state and society. There is a balance in the information sphere of all stakeholders. This balance must be protected and maintained. On the other hand, the object of information security is the information infrastructure that provides information resources, and technologies that form the digital state today, the digital economy, and the digital society. Relevant processes are also being implemented: digital democracy, digital voting. Thus, there is a duality: interests, in particular, protection of psychological and other influence on the consciousness of an individual citizen or society, and on the other hand – an object of a purely technical nature. On this basis, an appropriate pool or set of opportunities is formed, developing which, it is possible to assess the state of information security of the state" [13].

Information security should be considered together with cyber security. The draft Law of Ukraine "On Cyber Security of Ukraine" was submitted, so it is proposed to consider cyber security as the state of protection of vital interests of a person and a citizen, society and the state in cyberspace. Cyberspace is an environment formed by an organised set of information processes on the basis of the information,

telecommunication and information-telecommunication systems interconnected by common principles and rules [14].

Given the digitalisation process, it is believed that information security can be fully ensured only in the case of achieving cybersecurity. Their symbiosis can be represented at three levels: state security, public security, and individual security. It is believed that the security of the individual, society and state can be ensured at national, regional and international levels. The authors argue that the information and cyber security of an individual should be put at the highest level. Its provision will become the basis for ensuring the information security of society and the state as a whole.

The importance of ensuring cybersecurity can be supported by the following arguments. In particular, the Petya virus has affected more than 60 countries in the world. The damage from the virus attack was estimated at USD 8 billion. Ukraine lost UAH 10 billion in half an hour [15]. In 2017, Ukrposhta suffered UAH 100 million in losses due to the Petya virus [16].

It is also necessary to highlight the case of personal data leaks from the digital public service of the application "Diia". On May 12 last year, investigators of the Main Investigation Department of the National Police of Ukraine initiated criminal proceedings under Part 2 of Article 361 of the Criminal Code of Ukraine. The operation of the resource, which illegally distributed the personal data of citizens, was promptly blocked. Subsequently, information appeared on official websites that the data was not confirmed, and within the framework of the pre-trial investigation, it was established that the information disseminated in social networks, including Telegram channels, has signs of fragmented data sets compiled from various sources and resources, including open information from registers [17]. This demonstrates the importance of creating a reliable system of protection of citizens' information data and the high threat to national security in case of their unauthorised dissemination.

It seems that now, in the context of countering the aggression of the Russian Federation, it is extremely difficult to effectively ensure the information security of citizens. Therefore, it is important that information and cyber security is ensured at the state level, taking into account external threats;

2) Implementation of digital transformation of the Armed Forces and ensuring information security.

In September 2021, the President of Ukraine V. Zelenskyy [9] approved the Strategic Defense Bulletin of Ukraine, which identifies the digital transformation of the Armed Forces and information security as one of the priorities. As a result of the implementation of the military policy of Ukraine, the defence forces will meet the requirements of comprehensive defence of Ukraine and will be: built on national and Euro-Atlantic values; interoperable with the relevant structures of NATO member states; able to ensure the defence of the territory of Ukraine within the state border, confrontation in the information space, cyberspace as a component of the information space using the potential of the state and society, using all possible forms and methods to repel armed aggression. The above gives grounds to assert that cybersecurity is reaching a new level – the national level, and moving from the civilian to the defence sphere [18].

It should also be noted that this development is "new" for Ukraine and is currently at the stage of developing a regulatory framework. These normative acts, in turn, will become the basis for further development of the system of information and cyber security of the country as a whole and each citizen.

■ Conclusions

The article substantiates the position that in the current conditions of digital transformation, the issue of information security is becoming increasingly relevant: databases of information on citizens, databases of holders of such data, the results of obtaining certain services through Internet applications, etc. should be reliably protected. It is proved that information security should be considered in the context of cyber security. Their symbiosis can be represented at three levels: state security, public security, and individual security. The authors argue that the information and cyber security of an individual should be put at the highest level. Its provision will become the basis for ensuring the information security of society and the state as a whole. The conducted study gave grounds to assert that cyber security is reaching the general state level, moving the civilian to the defence sphere. This statement is based on the adoption of new normative legal acts in this area, in particular the Strategic Defense Bulletin of Ukraine, one of the priorities of which is the digital transformation of the Armed Forces and information security.

■ References

- [1] Country security. Site “All-Ukrainian Forum: Ukraine 30”. Retrieved from https://ukraine30.com/national_security/.
- [2] Buhutskyi, P.P. (2020). Theoretical bases of formation and development of the law of national security of Ukraine. Extended abstract of Doctor's thesis. Kyiv: National University.
- [3] Doronin, I.M. (2019). Digital development and national security in the context of legal issues. *Information and Law*, 1(28), 29-36. doi: 10.37750/2616-6798.2019.1(28).221305.
- [4] Doronin, I.M. (2020). National security of Ukraine in the information age: Theoretical and legal research. Extended abstract of Doctor's thesis. Kyiv: National University.
- [5] Dosenko, S.D., & Shevchenko, T.O. (2021). Rights and freedoms of man and citizen as an element of the system of national security. *Scientific Notes of Lviv University of Business and Law*, 29, 127-133. doi: 10.5281/zenodo.563641.
- [6] Drobotov, S.A. (2020). Constitutional and legal support of national security in Ukraine. *Science Rise: Juridical Science*, 2(12), 24-29. doi: 10.15587/2523-4153.2020.210858.
- [7] Fedorov, M. (2021). Ukraine is the first country in the world in which digital passports in smartphones have become complete legal analogues of ordinary documents. Retrieved from <https://thedigital.gov.ua/news/mikhaylo-fedorov-ukraina-persha-derzhava-svitu-v-yakiy-tsifrovi-pasporti-usmartfoni-stali-povnimi-yuridichnimi-analogami-zvichaynikh-dokumentiv>.
- [8] Information on the leakage of personal data of citizens from the digital state service of the application “Action” has not been confirmed. Retrieved from <https://www.kmu.gov.ua/news/informaciya-shchodo-vitoku-personalnih-danih-gromadyan-iz-cifrovogoderzhavnogo-servisu-dodatku-diya-nepidtvrdilasya-nacpoliciya>.
- [9] Constitution of Ukraine. No. 254k/96-VR (1996, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/254k/96-bp#Text>.
- [10] Kubetska, O., Ostapenko, T., & Paleshko, Ya. (2020). Conditions for ensuring national security of the state. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, 2, 321-327. doi: 10.31733/2078-3566-2020-2-321-327.
- [11] Draft Law of Ukraine “On Cyber Security of Ukraine”. No. 2207a. (2013, June). Retrieved from <https://ips.ligazakon.net/document/JG1PBA0A>.
- [12] Pyshchulina, O. (2020). *Digital economy: trends, risks and social determinants*. Retrieved from https://razumkov.org.ua/uploads/article/2020_digitalization.pdf.
- [13] Smolianiuk, V.F. (2018). Systemic principles of national security of Ukraine. *Bulletin of the National University “Yaroslav the Wise Law Academy of Ukraine”*, 2(37), 107-126.
- [14] In 2017 “Ukrposhta” suffered 100 million in losses due to the Petya virus. (2018). Retrieved from <https://www.epravda.com.ua/news/2018/04/24/636312/>.
- [15] Decree of the President of Ukraine from August 20, 2021 “On the decision of the National Security and Defense Council of Ukraine “On the Strategic Defense Bulletin of Ukraine”. No. 473/2021. (2021, September). Retrieved from <https://www.president.gov.ua/documents/4732021-40121>.
- [16] Volodymyr Zelensky opened the All-Ukrainian Forum “Ukraine 30. Country Security”. Retrieved from <https://drive.google.com/drive/u/1/folders/14shchqt3g6PfiUIvWhzCi9FmULvwIWw8>.
- [17] How Ukraine counteracts disinformation: the results of the third session of the All-Ukrainian Forum “Ukraine 30. Country Security”. Retrieved from <https://docs.google.com/document/d/100og15keak3HWfGAiNA2egRXU3R16xpjxsn6eKmQIN8/edit>.
- [18] The damage from the attack of the Petya. A virus in the world reaches 8 billion dollars – expert. (2020). Retrieved from <https://www.unian.ua/science/2003241-zbitkivid-ataki-virusu-petya-syagayut-8-milyardiv-dolariv-ekspert.html>.

■ Список використаних джерел

- [1] Безпека країни. “Всеукраїнський Форум: Україна 30”. URL: https://ukraine30.com/national_security.
- [2] Бугуцький П. П. Теоретичні основи становлення і розвитку права національної безпеки України: автореф. дис. ... д-ра юрид. наук: 12.00.01. Київ, 2020. 40 с.
- [3] Доронін І. М. Цифровий розвиток та національна безпека у контексті правових проблем. *Інформація і право*. 2019. Вип. 1. № 28. С. 29–36. doi: 10.37750/2616-6798.2019.1(28).221305.
- [4] Доронін І. М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження: автореф. дис. ... д-ра юрид. наук: 12.00.01. Київ, 2020. 39 с.
- [5] Досенко С. Д., Шевченко Т. О. Права та свободи людини і громадянина як елемент системи забезпечення національної безпеки. *Наукові записки Львівського університету бізнесу та права*. 2021. № 29. С. 127–133. doi: 10.5281/zenodo.563641.
- [6] Дроботов С. А. Конституційно-правове забезпечення національної безпеки в Україні. *Юридична наука*. 2020. Вип. 2. № 12. С. 24–29. doi: 10.15587/2523-4153.2020.210858.
- [7] Федоров М. Україна – перша держава світу, в якій цифрові паспорти у смартфоні стали повними юридичними аналогами звичайних документів. URL: <https://thedigital.gov.ua/news/mikhaylo-fedorov-ukraina-pershaderzhava-svitu-v-yakiy-tsifrovi-pasporti-u-smartfoni-stali-povnimi-yuridichnimi-analogami-zvichaynikh-dokumentiv>.
- [8] Інформація щодо витоку персональних даних громадян із цифрового державного сервісу додатку “Дія” не підтвердилася. URL: <https://www.kmu.gov.ua/news/informaciya-shchodovitoku-personalnih-danih-gromadyan-iz-cifrovogo-derzhavnogo-servisu-dodatku-diya-ne-pidtvrdilasyanacpoliciya>.
- [9] Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text>.
- [10] Кубецька О., Остапенко Т., Палешко Я. Умови забезпечення національної безпеки держави. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 2. С. 321–327. doi: 10.31733/2078-3566-2020-2-321-327.
- [11] Про кібернетичну безпеку України: проект Закону України від 4 черв. 2013 р. № 2207а. URL: <https://ips.ligazakon.net/document/JG1PBA0A>.
- [12] Пищуліна О. Цифрова економіка: тренди, ризики та соціальні детермінанти. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf.
- [13] Смолянчук В. Ф. Системні засади національної безпеки України. Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. 2018. Вип. 2. № 37. С. 107–126.
- [14] У 2017 році “Укрпошта” зазнала 100-мільйонних збитків через вірус Petya. URL: <https://www.erprava.com.ua/news/2018/04/24/636312/>.
- [15] Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України”: Указ Президента України від 17 верес. 2021 р. № 473/2021. URL: <https://www.president.gov.ua/documents/4732021-40121>.
- [16] Володимир Зеленський відкрив Всеукраїнський Форум “Україна 30. Безпека країни”. URL: <https://drive.google.com/drive/u/1/folders/14shchqt3g6PflUIvWhzCi9FmULvwIWw8>.
- [17] Як Україна протидіє дезінформації: підсумки третьої сесії Всеукраїнського Форуму “Україна 30. URL: <https://docs.google.com/document/d/100og15keak3HWfGAiNA2egRXU3R16xpjxsn6eKmQIN8/edit>.
- [18] Збитки від атаки вірусу Petya. А у світі сягають 8 мільярдів доларів – експерт. URL: <https://www.unian.ua/science/2003241-zbitki-vid-ataki-virusu-petya-syagayut-8-milyardiv-dolarivekspert.html>.

Державна політика забезпечення прав людини у сфері національної безпеки в умовах цифровізації

Денис Анатолійович Чижов

Національна академія внутрішніх справ
03035, Солом'янська площа, 1, м. Київ, Україна
Київський регіональний центр Національної академії правових наук України
01024, вул. Пилипа Орлика, 3, м. Київ, Україна

■ **Анотація.** Мета статті – на підставі дослідження наукових поглядів, нормативних документів у сфері національної безпеки, забезпечення прав людини, а також цифровізації країни визначити основні напрями державної політики забезпечення прав людини у сфері національної безпеки в умовах цифровізації. Для реалізації цієї мети поставлено такі завдання: навести аргументи щодо актуальності обраної теми для дослідження; схарактеризувати зміст визначених напрямів; обґрунтувати важливість забезпечення державної безпеки та прав людини в умовах цифровізації; визначити взаємозв'язок інформаційної та кібернетичної безпеки на декількох рівнях – безпека особи, суспільства й держави. Методологічне підґрунтя наукової статті становить цілісна й узгоджена система методів, що дала змогу належно проаналізувати предмет дослідження, зокрема використано наукові методи аналізу, синтезу, індукції та дедукції. Теоретичним підґрунтям цієї публікації стали праці вітчизняних вчених стосовно забезпечення прав людини у сфері національної безпеки в умовах розвитку цифровізації, а також виступи державних посадових осіб на спеціальних заходах, присвячених обраній тематиці. Наукова новизна публікації полягає в тому, що на підставі здійсненого аналізу ми виокремили два напрями забезпечення прав людини у сфері національної безпеки в умовах розвитку цифровізації: 1) забезпечення інформаційної безпеки як складової національної безпеки в умовах цифровізації; 2) впровадження цифрової трансформації Збройних сил і забезпечення інформаційної безпеки. Водночас обґрунтовано, що таких напрямів можна визначити більше, однак, з огляду на обмежений обсяг дослідження, інші напрями стануть предметом подальших наукових пошуків. Доведено, що інформаційну безпеку слід розглядати одночасно з кібернетичною. Їх симбіоз може бути представлено на трьох рівнях: безпека держави, безпека суспільства, безпека особи. У статті акцентовано, що слід поставити на найвищий щабель інформаційну й кібернетичну безпеку особи: її забезпечення стане підґрунтям для інформаційної безпеки суспільства та держави загалом. Обґрунтовано, що забезпечення кібербезпеки переходить на новий рівень – загальнодержавний, а також із цивільної сфери – в оборонну

■ **Ключові слова:** цифровізація; забезпечення прав людини; національна безпека; кібернетична безпека; кібератака; безпека й оборона; агресія