SÉRIE “Veřejná správa”

[https://doi.org/10.52058/2695-1592-2021-3\(3\)-7-18](https://doi.org/10.52058/2695-1592-2021-3(3)-7-18)

Nataliia Varenia

*Candidate of Juridical Sciences / P.h.D., Leading Researcher,
National Academy of Security Service of Ukraine,
Kyiv, Ukraine. e-mail: varenii@ukr.net,
<https://orcid.org/0000-0002-5471-280X>*

INFORMATION SECURITY OF THE PUBLIC GOVERNANCE SYSTEM IN THE CONDITIONS OF DIGITALIZATION

Abstract. At present, Ukraine is faced with an urgent need for broad-scale digitalization of various spheres of public life. The digitalization policy is in line with European and global development trends; it is supported at the state level, being in the competence of, in particular, the Ministry of Digital Transformation of Ukraine, established two years ago. The accelerated pace of digitalization highlights the need for management decisions to ensure information security. Experts predict that both the Ukrainian citizens individually of Ukraine and business entirely as well as the whole public governance paradigm will increasingly suffer from the cybercrime growth. Therefore, responsible government agencies pursue a comprehensive policy aimed at preventing and combating cybercrime. The system of these measures partially fulfills the information policy in the field of public governance on a national scale and fully implements the official line of information security in the context of digitalization. In general, the strategy “Ukraine 2030E – a country with a developed digital economy”, developed by the Ukrainian Institute of the Future, identifies the following industries as priority cybersecurity vectors, namely: energy supply, transport management, banking and telecommunications, health care, water supply. Balanced cyber policy in the public governance sphere means a system of technical and organizational solutions that would not limit the state’s transition to the digital technology platform and at the same time ensure a sufficient level of trust and guarantee the security of all users of the digital environment. In the context outlined, the purpose of the academic paper was as follows: (1) to analyze the current directions of development of public governance on information security issues in the context of digitalization; (2) to identify the basic tendencies of further development on the basis of the analysis conducted and (3) to determine the priority vectors for the development of the cybersecurity system at the state level. Implementation of the purpose outlined provided thorough elaboration of legislative and regulatory framework concerning issues of information security public management in the conditions of digitalization and documents on strategic planning of sphere. It also involved studying and analytical interpretation of a network activity of

cybersecurity subjects defined by the Law of Ukraine “On Basic Principles of Cyber Security of Ukraine”, elaboration of domestic and foreign scientific works, revealing insights into the relationship between information security and cybersecurity, as well as the development of public governance in the field of prevention (through risk-oriented approach) and countering cyber threats. Public management on information security issues in the context of digitalization is being implemented in the areas of developing a new and adapting the existing regulatory framework, ratification of international documents on cybersecurity, educational and research work among the population, popularizing digital hygiene, as well as in the direction of systematic counteraction to existing cyber threats and elimination of cybersecurity incidents. The set of measures is especially carefully implemented in order to achieve the children’s safety in a digitalized society.

Keywords: information security, national security, information threats, cybersecurity, risk-oriented approach.

Problem Statement. The digitalization issues are currently out of the debate on the importance, necessity and priority. Special mention in this regard should be made of Elon Musk’s popular statement that people have already become cyborgs, implementing the Hollywood movie idea and becoming related to their gadgets, especially phones and computers so much so that they are like a bodily extension of people: forgetting a phone is like forgetting one’s limb [1]. However, the challenges connected with the dominance of devices and the transformation of human life’s numerous areas to adapted by cyberspace have always been massive - due to the very nature of the phenomenon, and, therefore, requiring comprehensive management decisions [2]. The full-fledged functioning of the state mechanism of the XXI century is possible only in the conditions of consistent implementation towards various life spheres of the society, in particular, to the public governance sphere as well as digital technologies. Only this can ensure the sustainability and quality of the society. Thus, digitalization is directly related to the implementation of the following goals of 17 Sustainable Development Goals (SDG 17), namely: № 8 “Decent Work and Economic Growth”, № 9 “Industrialization, Innovation and Infrastructure”, № 11 “Sustainable Cities and Settlements”, etc. [3; 4].

The digitalization issue is inextricably linked to security, in particular cybersecurity, as a process of implementing security measures aimed at ensuring the confidentiality, integrity and availability of data. Cybersecurity provides proper protection of IT resources: the information itself and its media, which are individuals, computers, servers, enterprises. Actually, the information security concept is broader in terms of cybersecurity, forasmuch as it covers the full range of measures in order to ensure the security of any information. Cybersecurity is presented as a new structural element of information security, specifically targeted at the digital environment. Cybersecurity is conceptualized not only as the protection of information itself, but as a holistic and full protection of the full-fledged system in the information field (computer technology field) in general. In the modern discourse on cybersecurity and information security, we are talking about changes in terminological relations towards the fact that

the very concept of information security is superimposed on the cybersecurity concept; moreover, the latter displaces its etymological predecessor, which is facilitated by the intensive digitalization process. Under these conditions, the understanding of any information through the prism of digital space is deepened and expanded [5; 6, c. 2-9]. Thus, from the same perspective, the public governance system concerning information security is developing.

The Ukrainian state is pursuing a forced policy towards the digitalization of various public governance spheres. All reforms in the outlined direction in one way or another relate to the security of the digital environment. For instance, at the recent forum “Ukraine 30. Digitalization”, which was held on May 17-19, 2021, one of the strategic issues was “cybersecurity and development of the Ukrainians’ personal data system protection” [4]. Thus, in the context of influencing comprehensive digitalization, we are currently talking about the transformed technological structure of the whole social-economic system and at the same time the public governance system, in particular, concerning security issues.

Analysis of recent studies and publications. While investigating the issue of updating the public governance sphere in Ukraine in accordance with the modern requirements, researchers often use the Europeanization concept to denote the principle of reforming the public management and administration sphere of the post-Soviet countries of Central and Eastern Europe in the context of an information society [7, p. 24]. In general, in Ukraine, the information security sphere, in particular, cybersecurity is marked by the influence of such global cyber giants as France, Great Britain, Germany, the USA, China, Japan, etc. On a global scale, leading UN countries have agreed for the first time on a common policy to limit action in the information space as a result of the signing the report on advances in information and telecommunications in the context of international information security. However, while the scientific conference abstracts on the regulation of security issues under the influence of digitalization are in the nature of recommendations, and not a legislative norm for all UN countries, that is, they are not legally binding; responsibility for ensuring information security in the context of digitalization is assigned to national public governance systems [8].

The relationship between cybersecurity and information security has been clearly defined in the work of Besy von Solms, Ross von Solms [6, p. 2-9], especially from a governance perspective. Herein, the cybersecurity niche is characterized as such, where the number of consequences and impacts is growing [6, p. 3]. That is, emphasis is made as follows: on the one hand, the rapid development of security in the digital space, and on the other hand, there is an urgent need for public governance systems to respond quickly to challenges related to security breaches in the digital space, as well as the necessity to categorize the concept of what the limits of security are and at what stage cyber freedom ends, becoming a cyber threat.

Interpreting the information security concept of the public governance system in the context of digitalization, we rely primarily on the definition specified in the Law № 2163-VIII as of 05.10.2017 “On the basic principles of cybersecurity of Ukraine” [9], which states that cybersecurity is a state of protection vital interests of a person and a

citizen, the society and the state when using o cyberspace. Along with this, the system of state management measures is conceptualized through the concept of cybersecurity towards ensuring the sustainable development of the information society and the digital communication environment. A range of actions is implemented to timely identify, prevent (based on a risk-oriented approach) and neutralize real and potential threats towards the Ukrainian national security in the cyber environment. At the same time, the Presidential Decree “On the decision of the National Security and Defense Council of Ukraine” as of December 29, 2016 “On the Doctrine of Information Security of Ukraine” states the necessity to develop a system in order to combat current threats towards national security in the information sphere. By the way, the necessity is also identified to elaborate innovative approaches that would form a reliable system of protection and development of the information space, which is significantly influenced by globalization processes and the free information circulation [10]. It also mentions the systematization of the fundamental positions of the state on cybersecurity as the digital environment security in a separate document, namely the aforementioned Law [9], which once again testifies to the adaptation of the public governance system at the legislative level in the context of full-fledged digitalization — so deep and broad-scale that requires a separate management discourse.

Thus, in the context of interpretation of the Ukrainian public governance sphere, cybersecurity is also a subset of information security; consequently, cybersecurity management is a subset of information security management, as it is typical of leading foreign works on the differentiation of two terms outlined.

International documents ratified by Ukraine are also a resource for the development of national algorithms in the cybersecurity sphere. In particular, we are talking about “ISO / IEC 27032: 2016 Information technology — Security techniques — Guidelines for cybersecurity (ISO / IEC 27032: 2012, IDT)”, which was adopted by Order No. 448 as of December 27, 2016 “On the adoption of national regulatory documents harmonized with international regulatory documents, and the abolition of national regulatory documents” [11] and entered into force on January 1, 2018.

V.H. Voronkova characterizes modern administrative state activity as a process of evolution of the society from the information one to the smart society. In particular, information security is a natural movement based on using certain software products, hardware along with the smart information security system, which is the nomen of the smart society [7, p. 24]. O.O. Fursin defines the core function of public governance as providing the state apparatus with integral integrity, unity, security and well-being of its citizens, based on the principles of skillful leadership and effective management. In general, the investigator defends the idea of noosphere-spiritual concept of the public sphere (integration of economic, social and political spheres). Along with this, speaking about the holistic adaptation of the public governance system to current conditions, the scholar appeals to dissipative structures as the ability of the system to self-organization, which is actualized whenever there is a need to organize the management space in order to “survive” under various factors. O.O. Fursin also takes security, especially information security, as a basis for achieving sustainable development during the noosphere formation. The investigator sees rational measures, the latest information

and intellectual technologies as security tools [12, p. 53].

O.V. Karpenko attributes creating access to public cyber literacy tools as an effective instrument in the fight against cyber threats, for instance, in order to avoid manipulation of consciousness. According to the scholar's viewpoint, having mastered effective security arrangements means against manipulation, every citizen will be protected from the harmful effects of information and psychological weapons [13, p. 48].

O.V. Sosnin, addressing the issues of the growing role of the state's information and communication function and ways to solve national security problems, identifies the necessity to ensure the information sovereignty of Ukraine as well as to improve state regulation of the information sphere development through the measures as follows: (1) regulated legal and economic preconditions for the development of national information infrastructure and information resources; (2) integration of the latest technologies in the outlined public governance spheres; (3) enrichment of domestic and global information space with reliable information about Ukraine in order to create its positive information image; (4) active involvement of mass media to counter current information threats; (5) observance of the constitutional right in a niche of information freedom and protection of the citizen; (6) comprehensive measures towards protecting the national information space and counteracting the monopolization of the information sphere, which would violate the information security of the whole public governance system [14, p. 288]. What it involves is an extremely complex configuration of the Ukrainian information and communication system due to the fact that social-political transformations and technological development of recent decades have resulted in the appropriation of the information and communication state structure, including authoritative resources in cyberspace. Thus, the consequence was the information withdrawal as a resource for the development of the nation and all the technical means of its dissemination to new owners, mostly from private entities that can potentially implement tactics of destructive influence on the public governance system in general [14, p. 297], which can be particularly easily implemented in the conditions of total digitalization.

According to researchers' viewpoint, information security can be ensured only by an integrated systemic comprehensive political and legal approach: in this case, the modern information and communication environment is a set of digital technologies and information in electronic format [15].

The purpose of the academic paper is as follows: to analyze the development directions of public governance concerning information security issues in the context of digitalization and, on this basis, to reveal the basic tendencies of further development of the cyber security system at the state level.

Statement of basic materials. To start with, the adaptation of the state apparatus structure to the operating environment in the conditions of digitalization bears evidence of the public governance system's reform under the influence of digitalization. Consequently, a separate Ministry of Digital Transformation of Ukraine was established in 2019. The government's provision on its establishment refers to the dominant function of formulating and implementing public policy in the following

spheres, namely: digitalization, digital economy, digital innovation, e-government and e-democracy, development of the information society, etc. All activity spheres of the Ministry of Digital Transformation in one way or another intersect with the issues of security field during the implementation of these options.

The purposes of the Ministry comprise the goal towards ensuring the availability of 100% of public services to citizens and businesses in the online format by 2024. Coordination of cybersecurity measures as a component of Ukraine's national security is the competence sphere of the President of Ukraine and the National Security and Defense Council of Ukraine headed by him (in particular, the National Cybersecurity Coordination Center).

The development of the information security system of the public governance system, therefore, is taking place against the background of a broad-scale possible involvement of Ukrainians into the digital environment. By 2024, it is planned that 95% of the population of Ukraine, social facilities and major highways will have coverage with faster Internet; also, 6 million Ukrainians, which currently make up one-eighth of the country's population, are planned to be involved in the digital skills' development program [16]. There are also plans to achieve the share of IT in the country's GDP to 10% [16]. This volume and accelerated format of transformations requires a serious and forward-looking approach towards ensuring the digital space security.

The modern cybersecurity system is implemented in two directions, namely:

- information and technical;
- information - psychological (psychophysical).

The system of cybersecurity facilities, established at the legislative level, determines the priority implementation directions of the public governance system (Figure 1).

Fig. 1. *Cybersecurity objects.*

Source: summarized by the author on the basis [9]

In October 2020, at the initiative of the Ministry of Digital Transformation of Ukraine, the government approved technical regulations for cryptographic information security, which sets requirements in the information security sphere.

For the purpose of digitalization, the Unified State Web Portal of Electronic Services “Portal Diia” was launched, which is steadily expanding the range of priority public services in electronic form. Optimization of public services, as discussed in the

plans of the Ministry for 2021, also applies towards improving the information security of users when receiving public services in the format of remote access, in particular:

(1) paragraph 40 states the necessity to ensure the adaptation of Ukrainian legislation to the requirements of European Union legislation in the field of information security during 2021. This requires appropriate approval of relevant acts in the information security sphere, developed by the State Service for Special Communications and Information Protection of Ukraine;

(2) furthermore, it is planned to create an online platform with Internet security in the direction of ensuring information security with access to educational materials, created tools for prevention and response and cyber threats (paragraph 58);

(3) holding an annual international online conference on digital security (paragraph 59);

(4) conducting research on risks and threats in the digital environment (paragraph 60);

(5) development of a draft order of the Cabinet of Ministers of Ukraine on the approval of the Concept of a safe cyberspace for children for the period up to 2025 as well as an Action Plan for this concept and other measures towards ensuring the safety of children in the digital environment (paragraphs 61-63), etc. [17].

The Ministry of Digital Transformation implements the information security system quite comprehensively and deeply, providing the necessary information materials for the population on the nature of cybersecurity and cyber threats. For instance, in October 2020, the Ministry launched an educational campaign on the interpretation of online security terms, which resulted in the conclusion of a dictionary of special profile terms. It will ensure the unification of the discourse on cybersecurity, thus, accelerating consensus productive solutions. The security of users' personal data of the "Diia" service as a conceptual project of the Ministry of Digital Transformation is a matter of constant careful control conducted by employees of the Ministry. Developments in this direction have been confirmed by the ombudsman. Previously, in December 2020, Bug Bounties were launched in order to verify the security of Ukrainian data in the digitization program with a prize fund of 1 million UAH or 35 000 USD for white hackers from around the world in order to find vulnerabilities and bugs in the "Diia" application.

Virtual security of children occupies a prominent place in the information security system: if uncontrolled, as sad practice shows, cyberspace can become a real threat to children's lives. "National Strategy for Child Safety on the Internet for 2020-2025" is gradually being implemented. This vector is implemented through the system of combating and preventing harmful online materials, cyberbullying, suicidal online communities, sexual violence, etc. (preventive measures are based on a risk-based approach). Within the framework of this direction, for instance, the exhibition "Sexual Abuse of Children: Online Dimension" has already been held.

Improving the level of children's information security can be achieved, for instance, through an educational line, namely:

- the Concept and Action Plan for the development of children's digital rights has been developed, based on the policy of securing the child online;

- recommendations on protection of children in the digital environment have been structured; their popularization takes place;
- a special Report IWF feedback line is in operation, through which you can inform about violence by reporting unwanted content online depicting sexual abuse of children;
- an educational series for parents “Child safety on the Internet” has been launched (11 episodes lasting 8-10 minutes);
- an educational series about cyberbullying for teenagers has been published;
- an information and educational campaign #Stop_sexting with parallel launching chatbot project in Telegram has been started;
- COVID-19 online guide with online safety tips for parents and guardians has been issued;
- online child safety courses are available for parents and teachers.

In addition to the activities of the Ministry of Digital Transformation, as part of the analysis of the public governance system in the direction of information security implementation, it is worth mentioning the EMA Association project “Cybersecurity School” launched in October 2017 and active until now. It is implemented with the support of the National Bank of Ukraine, EMA member banks, NPU Cyberpolice Department, EC3 Europol targeting Ukrainian citizens who own payment instruments, as well as in order to improve the culture of non-cash payments among Ukrainians by disseminating knowledge about the security of non-cash transactions.

Introducing preventive measures to avert cyber threats within the information security policy implementation through the prism of public governance should be carried out through the integration of risk-oriented approach. In this context, special mention should be made about one of the most recent rounds in the development of the competence issue of cybersecurity subjects, namely the draft law on amendments to the Law of Ukraine adopted in the first reading on January 28, 2021 “On the Security Service of Ukraine” concerning improving the organizational and legal framework of the Security Service of Ukraine [18]. The specified bill is lobbied by the President of Ukraine, in particular, by the Decree of the President of Ukraine №307 / 2021 “On the decision of the National Security and Defense Council of Ukraine” as of June 4, 2021 “On Urgent Measures to Deepen Ukraine’s Integration into the North Atlantic Treaty Organization”. According to paragraph 10 of this document, SSU has been ordered to continue support the draft of the above legal act in the Verkhovna Rada of Ukraine; along with this, the preparation and submission in the prescribed manner of the draft Law of Ukraine “On Security of Classified Information” (new version of the Law of Ukraine “On State Secrets”) has been initiated [19]. The draft law on the Security Service of Ukraine, in comparison with the previous version of the document, has already entrenched the goals of the Security Service of Ukraine regarding counterintelligence support of “information and scientific and technical potential, cyber security and information security of the state” [18]. The adoption of this bill in the second reading, therefore, is an urgent requirement of the time, correlating with the modern realities of public life in Ukraine and other steps of the state towards

developing an information security system of public governance in the context of digitalization.

Conclusions. The philosophy of digitalization in general, and information security policy, in particular, is developing in a citizen-friendly direction; it is determined to be a service that allows, on the one hand, quick receipt of services, and on the other hand, honest work fulfillment. The slogan of the system is “Diia. Digital State”; it provides for the unification of all departments into a single convenient and effective online system. Document management in the system itself requires serious data protection and confidentiality of the user’s actions. The implementation of “Diia” places the public governance system before the necessity of overcoming challenges, and a successful response to these challenges elaborates a network of state developments in information security. One of the highest priorities is the development of mechanisms towards protecting children on the Internet.

Despite significant efforts towards ensuring the information security of the public governance system in the context of digitalization, the range of work in this niche is still expanding - with the deepening of the digitalization process and the emergence of new threats to information security and, consequently, the need to promptly respond to them. In particular, this is confirmed by the very recent nationwide study “Internet Security”, which has been initiated by the Ministry of Digital Transformation, the Ministry of Interior and with the support of the European Union Advisory Mission (EUMC) and the results of which have been presented on July 15, 2021. As part of a study conducted by Kyiv International Institute of Sociology, which covered 903 settlements, it was revealed that 23% of citizens had precedents of violation of private information security due to the annoying experience of hacking their account in social networks or instant messengers.

The key to strengthening the information security of the public governance system in the context of digitalization is the policy of cyber protection and digital hygiene as a competent consumption of information in compliance with the basic principles of cyber security.

Further investigations on the topic of the present academic paper can be carried out in the areas updated in the plans of the Ministry of Digital Transformation of Ukraine for 2021 and in accordance with similar releases for the next calendar years, as well as the development and implementation of other necessary legislation in the information security sphere.

References:

1. Rapier, G. (2019). 'If you can't beat them join them': Elon Musk says our best hope for competing with AI is becoming better cyborgs. Aug 29. Retrieved from: <https://www.businessinsider.com/elon-musk-humans-must-become-cyborgs-to-compete-with-ai-2019-8> [in Ukrainian].
2. Fostolovych, V. A. (2019). Tsyfrovizatsiia v suchasni systemi upravlinnia [Digitization in a modern management system]. *Ekonomika, finansy, menedzhment: aktualni pytannia nauky i praktyky: zb. nauk. pr. VNAU*, 7, 154-168. [in Ukrainian].
3. United Nations. (2015). The 2030 Agenda for Sustainable Development. Retrieved from: <https://sustainabledevelopment.un.org/post2015/transformingourworld>

4. Ukraina 30 [Ukraine 30]. (2019) Tsyfrovizatsiia. 17-19 travnia. Retrieved from: <https://ukraine30.com/digitalization/> [in Ukrainian]
5. Informatsiina bezpeka i kiberbezpeka – v chomu riznytsia [Information security and cybersecurity – what's the difference]? (2019). 4 zhovtnia. Retrieved from: <https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/> [in Ukrainian]
6. von Solms, B., & von Solms, R. (2018). Cybersecurity and information security—what goes where?. *Information & Computer Security*, 26(1), 2–9. Retrieved from: <https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2017-0025/full/html> (дата звернення: 28.07.2021).
7. Voronkova, V. H. Administrativna diialnist yak ob'ekt informatsiino-komunikatyvnoho menedzhmentu [Administrative activity as an object of information and communication management]. *Publichne upravlinnia ta administruvannia v umovakh informatsiinoho suspilstva: vitchyzniani i zarubizhnyi dosvid: monohrafiia* / za zah. red. S. Chernova, V. Voronkovi, V. Banakha, O. Sosnina, P. Zhukauskasa, Y. Vvainkhardt, R. Andriukaitene. Zaporizhzhia: ZDIA, 2016. S. 24–51. [in Ukrainian]
8. UN. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General. Retrieved from: <https://digitallibrary.un.org/record/799853> [in Ukrainian]
9. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the basic principles of cybersecurity of Ukraine: Law of Ukraine of 05.10.2017 № 2163-VIII]. (2017). *Vidomosti Verkhovnoi Rady*, 45, 403. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2163-19#top> [in Ukrainian]
10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» : Ukaz Prezidenta Ukrainy; Doktryna vid 25.02.2017 № 47/2017 [On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine": Decree of the President of Ukraine; Doctrine from 25.02.2017 № 47/2017]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> [in Ukrainian]
11. DSTU ISO/IEC 27032:2016 Informatsiini tekhnolohii. Metody zakhystu. Nastanovy shchodo kiberbezpeky [ISO / IEC 27032: 2016 Information technologies. Methods of protection. Cybersecurity guidelines] (ISO/IEC 27032:2012, IDT). [in Ukrainian]
12. Fursin, O. O. (2016). Publichna sfera – yednist ekonomichnoi, sotsialnoi i politychnoi sfer [Public sphere - the unity of economic, social and political spheres]. *Publichne upravlinnia ta administruvannia v umovakh informatsiinoho suspilstva: vitchyzniani i zarubizhnyi dosvid: monohrafiia* / za zah. red. S. Chernova, V. Voronkovi, V. Banakha, O. Sosnina, P. Zhukauskasa, Y. Vvainkhardt, R. Andriukaitene. Zaporizhzhia: ZDIA. S. 53–59. [in Ukrainian]
13. Karpenko, O. V. (2019). Tsyfrovi transformatsii komunikatyvnoho upravlinnia: hlobalni здобутки, tendentsii rozvytku ta aktualni zahrozy. Tsyrovizatsiia publichnoho vriaduvannia [Digital transformations of communicative management: global achievements, development trends and current threats. Circulation of public governance]. *Instytutsionalizatsiia publichnoho upravlinnia v Ukraini v umovakh yevrointehratsiinykh ta hlobalizatsiinykh vyklykiv : materialy shchorich. Vseukr. nauk.-prakt. konf. za mizhnaron. uchastiu* (Kyiv, 24 trav. 2019 r.) : u 5 t. / za zah. red. A. P. Savkova, M. M. Bilynskoi, O. M. Petroie. Kyiv: NADU. Vol. 4. [in Ukrainian]
14. Sosnin, O. V. (2016). Problemy zrostaiuchoi roli informatsiinokomunikatyvnoi funksii derzhavy ta shliakhy vyrishennia problem natsionalnoi bezpeky [Problems of the growing role of the information and communication function of the state and ways to solve the problems of national security]. *Publichne upravlinnia ta administruvannia v umovakh informatsiinoho suspilstva: vitchyzniani i zarubizhnyi dosvid: monohrafiia* / za zah. red. S. Chernova, V. Voronkovi, V. Banakha, O. Sosnina, P. Zhukauskasa, Y. Vvainkhardt, R. Andriukaitene. Zaporizhzhia: ZDIA. S. 288-317. [in Ukrainian]
15. LexInform – Yurydychni novyny Ukrainy. (2020). Tsyfrovizatsiia yak nova realnist Ukrainy. Retrieved from: <https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/> [in Ukrainian]

16. Ministerstvo ta Komitet tsyfrovoyi transformatsii Ukrainy. (2021). Pro nas [About us]. Retrieved from: <https://thedigital.gov.ua/ministry> [in Ukrainian]
17. Pro zatverdzhennia planu roboty Ministerstva tsyfrovoyi transformatsii Ukrainy na 2021 rik : Nakaz Ministerstva tsyfrovoyi transformatsii Ukrainy vid 09.04.2021 №49 [On approval of the work plan of the Ministry of Digital Transformation of Ukraine for 2021: Order of the Ministry of Digital Transformation of Ukraine dated 09.04.2021 №49]. Retrieved from: <http://surl.li/wbwu> [in Ukrainian]
18. Proiekt Zakonu pro vnesennia zmin do Zakonu Ukrainy «Pro Sluzhbu bezpeky Ukrainy» shchodo udoskonalennia orhanizatsiino-pravovykh zasad diialnosti Sluzhby bezpeky Ukrainy [Draft Law on Amendments to the Law of Ukraine “On the Security Service of Ukraine” on Improving the Organizational and Legal Principles of the Security Service of Ukraine]. 2021. Retrieved from: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243 [in Ukrainian]
19. Ukaz Prezydenta Ukrainy №307/2021 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 chervnia 2021 roku «Pro nevidkladni zakhody shchodo pohlyblennia intehtatsii Ukrainy do Orhanizatsii Pivnichnoatlantychnoho dohovoru» [Decree of the President of Ukraine №307 / 2021 "On the decision of the National Security and Defense Council of Ukraine of June 4, 2021 “On urgent measures to deepen Ukraine's integration into the North Atlantic Treaty Organization”]. Retrieved from: <https://www.president.gov.ua/documents/3072021-39461> [in Ukrainian]

Література:

1. Rapiet G. 'If you can't beat them join them': Elon Musk says our best hope for competing with AI is becoming better cyborgs. Aug 29, 2019. URL: <https://www.businessinsider.com/elon-musk-humans-must-become-cyborgs-to-compete-with-ai-2019-8> (дата звернення: 20.07.2021).
2. Фостолович В. А. Цифровізація в сучасній системі управління. *Економіка, фінанси, менеджмент: актуальні питання науки і практики: зб. наук. пр. ВНАУ*. 2019. № 7. С. 154–168.
3. United Nations. The 2030 Agenda for Sustainable Development. 2015. URL: <https://sustainabledevelopment.un.org/post2015/transformingourworld> (дата звернення: 20.07.2021).
4. Україна 30. Цифровізація. 17-19 травня 2021 року. URL: <https://ukraine30.com/digitalization/> (дата звернення: 20.07.2021).
5. Інформаційна безпека і кібербезпека – в чому різниця? 4 жовтня 2019. URL: <https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/> (дата звернення: 20.07.2021).
6. von Solms B., von Solms R. Cybersecurity and information security–what goes where?. *Information & Computer Security*. 2018. Vol. 26 No. 1. Pp. 2–9. URL: <https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2017-0025/full/html> (дата звернення: 28.07.2021).
7. Воронкова В. Г. Адміністративна діяльність як об'єкт інформаційно-комунікативного менеджменту. *Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід: монографія / за заг. ред. С. Чернова, В. Воронкової, В. Банаха, О. Сосніна, П. Жукаускаса, Й. Ввайнхардт, Р. Андрюкайтене. Запоріжжя : ЗДІА, 2016. С. 24–51.*
8. UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General. 2015. URL: <https://digitallibrary.un.org/record/799853> (дата звернення: 20.07.2021).
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#top> (дата звернення: 20.07.2021).
10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України; Доктрина від 25.02.2017 № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 28.07.2021).
11. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

12. Фурсін О. О. Публічна сфера – єдність економічної, соціальної і політичної сфер. *Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід: монографія* / за заг. ред. С. Чернова, В. Воронкової, В. Банаха, О. Сосніна, П. Жукаускаса, Й. Ввайнхардт, Р. Андрюкайтене. Запоріжжя : ЗДІА, 2016. С. 53–59.
13. Карпенко О. В. Цифрові трансформації комунікативного управління: глобальні здобутки, тенденції розвитку та актуальні загрози. Цифровізація публічного врядування. *Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаційних викликів : матеріали щоріч. Всеукр. наук.-практ. конф. за міжнародн. участю (Київ, 24 трав. 2019 р.)* : у 5 т. / за заг. ред. А. П. Савкова, М. М. Білинської, О. М. Петроє. Київ: НАДУ, 2019. Т. 4.
14. Соснін О. В. Проблеми зростаючої ролі інформаційнокомунікативної функції держави та шляхи вирішення проблем національної безпеки. *Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід: монографія* / за заг. ред. С. Чернова, В. Воронкової, В. Банаха, О. Сосніна, П. Жукаускаса, Й. Ввайнхардт, Р. Андрюкайтене. Запоріжжя : ЗДІА, 2016. С. 288-317.
15. LexInform – Юридичні новини України. Цифровізація як нова реальність України. 2020. URL: <https://lexinform.com.ua/dumka-eksperta/tsyvrovizatsiya-yak-nova-realnist-ukrayiny/> (дата звернення: 28.07.2021).
16. Міністерство та Комітет цифрової трансформації України. Про нас. 2021. URL: <https://thedigital.gov.ua/ministry> (дата звернення: 28.07.2021).
17. Про затвердження плану роботи Міністерства цифрової трансформації України на 2021 рік : Наказ Міністерства цифрової трансформації України від 09.04.2021 №49. URL: <http://surl.li/wbwu>
18. Проект Закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України. 2021. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243 (дата звернення 29.07.2021)
19. Указ Президента України №307/2021 «Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Про невідкладні заходи щодо поглиблення інтеграції України до Організації Північноатлантичного договору». URL: <https://www.president.gov.ua/documents/3072021-39461> (дата звернення 29.07.2021)