InterAcción y PerspectivA

Revista de Trabajo Social

ISSN 2244-808X
D.L. pp 201002Z43506

Octubre-diciembre 2024
Vol. 14 No. 3

50 años
FORMANDO PARA EL BIENESTAR SOCIAL

Universidad del Zulia
Facultad de Ciencias Jurídicas y Políticas
Centro de Investigaciones en Trabajo Social

Interacción y Perspectiva
Revista de Trabajo Social
Vol. 14 Nº3 855-867 pp.
Octubre-diciembre

Dep. Legal pp 201002Z43506
ISSN 2244-808X
Copyright © 2024

ARTÍCULO DE INVESTIGACIÓN

Análisis de los Fundamentos de la Política de Seguridad de la Información de Ucrania: Imperativos Modernos del Desarrollo Sostenible del Estado (Prácticas Internacionales)

DOI: https://doi.org/10.5281/zenodo.11205784

Oleksandr Nazarchuk*, Tetiana Nikolaieva**, Oksana Zaporozhets***,
Nataliia Bielousova**** y Olha Andrieieva*****

Resumen

El objetivo del artículo es analizar los fundamentos de la política de seguridad de la información de Ucrania a partir del estudio de los imperativos modernos pertinentes del desarrollo sostenible del Estado y de las prácticas internacionales existentes. Para lograr su objetivo se utilizan métodos teóricos de investigación científica. Autores también examinan las prácticas existentes en materia de seguridad de la información en los principales países europeos que determinan la política europea actual, incluso en relación con Ucrania en tiempos de guerra (la República de Polonia, la República Federal de Alemania y la República Francesa). Para formar un sistema de seguridad de la información ucraniano de alta calidad, también se propone introducir un equilibrio razonable entre los derechos constitucionales existentes y las libertades de los ciudadanos a la hora de utilizar los recursos de información, apoyar el marco legislativo pertinente, hacer hincapié en el producto cultural e informativo centrado en Ucrania y desarrollar mecanismos para una interacción eficaz con las organizaciones e instituciones públicas. Las conclusiones también destacan la necesidad de mejorar la cultura informativa y digital entre los ucranianos, lo que será clave para superar algunos de los retos asociados a la difusión de propaganda, la ciberdelincuencia.

Palabras clave: seguridad de la información; política; guerra ruso-ucraniana; Ucrania; práctica europea, poder blando.

Abstract

Analysis of the Fundamentals of Ukraine's Information Security Policy: Modern Imperatives of Sustainable State Development

The aim of the article is to research the foundations of Ukraine's information security policy based on a study of the relevant modern imperatives of sustainable development of the state and existing international practices. To achieve this goal, theoretical methods of scientific research are used. Results: the authors examine the existing practices of information security in the leading European countries that determine the current European policy, including in relation to Ukraine in times of war (the Republic of Poland, the Federal Republic of Germany, the French Republic). The main focus is on the introduction of a clear regulatory framework and the establishment of cooperation with civil society institutions. In order to form a high-quality system of Ukrainian information security, it is also proposed to introduce a reasonable balance between the existing constitutional rights and freedoms of citizens when using information resources, support the relevant legislative framework, emphasize the Ukrainian-centered cultural and information product, and develop mechanisms for effective interaction with civil organizations and institutions. The conclusions also highlight the need to improve information and digital culture among Ukrainians, which will be the key to overcoming some of the challenges associated with the spread of propaganda or cybercrime.

Keywords: information security; policy; Russian-Ukrainian war; Ukraine; European practice, soft power

Recibido: 12/02/2024 Aceptado: 29/04/2024

*Ph.D., in Historical Sciences, Doctoral Student of the Department of Political Science, Faculty of Philosophy, Taras Shevchenko Kyiv National University, Kyiv, Ukraine. Email: anazarchuk@ukr.net. ORCID: https://orcid.org/0000-0002-2616-6020

** Ph.D., in Historical Sciences, Professor of the Department of Political Technologies, Institute of Law, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine. Email: n_t_m@ukr.net. ORCID: https://orcid.org/0000-0001-6772-5928

***Ph.D., in Political Sciences, Associate Professor of the Chair of International Information, Educational and Scientific Institute of International Relations, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. Email: xanza@gmail.com. ORCID: https://orcid.org/0000-0003-0784-9253

**** Ph.D.; in Political Sciences, Docent, Associate Professor Department of International Information, Educational and scientific institute of international relations, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. Email: bnnb@ukr.net. ORCID: https://orcid.org/0000-0002-9656-2942

*****Doctor of Political Sciences, Professor, Professor Educational and Scientific Institute of International Relations, Chair of International Information Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. Email: AndreevaOlga@knu.ua. ORCID: https://orcid.org/0000-0003-4587-1267

1. Introduction

The current challenges of the globalized environment pose a considerable danger to society. Possibilities of global terrorism, hybrid threats from authoritarian regimes, transition to open military aggression and establishment of international instability (in the case of the Kremlin regime and its invasion of Ukraine), use and abuse of economic leverage, resort to information warfare, spread of the COVID-19 pandemic and other dangerous diseases are just a small list of potential threats that humanity has faced in the 21st century and which may continue to develop in an unpredictable way. For this reason, models of countering such crises are being updated, and new opportunities for security policy formation are being developed.

In the information society, digital information threats are particularly prominent, which can simultaneously exist as independent vectors of influence and be part of broader threats (Yarmoliuk, 2022). Ensuring information security includes technical, organizational, and social measures that help prevent information security threats and reduce the possibility of harm from their impact. At the same time, Russia's aggression against Ukraine has demonstrated the destructive potential of information warfare capabilities, the dissemination of manipulative and outright false information about Ukrainian realities, which were brutally used to justify open aggression.

Research Problem

Information security is becoming increasingly important in the modern world, where information technology is used in all aspects of life. It includes measures to ensure the confidentiality, integrity, and availability of information, as well as protection against viruses, hacker attacks, and other threats. Information security is important to protect businesses, government agencies, personal data, and financial information. At the same time, Russia's aggression against Ukraine has also demonstrated other dimensions of information security in society. The article focuses on the problem of countering the challenges of Russian propaganda and information warfare, which has been waged against Ukraine and Ukrainian society since at least 2014 and has become especially intense since 2022. Responding to such challenges has led to the formation of certain established algorithms of action that will require additional reflection. Importantly, Russian aggression has also become a serious challenge for all other European countries and the United States, for which Ukraine's experience in countering propaganda campaigns may be useful for further generalization and use.

Research Focus

The main issues of the study are related to the functioning of the information protection mechanism and its use in the Ukrainian context, taking into account the best practices of leading countries. The analysis of digital tools to counter the spread of information aggression, supported by hacker attacks and attempts to seize data, makes it possible to identify the main manifestations of information security policies.

Research Aim and Research Questions

The purpose of the article is to analyze the foundations of Ukraine's information security policy.

Research Questions:

1. Analysis the theoretical substantiation of information security.
2. Study of the relevant modern imperatives of sustainable development of the State.
3. Analysis the existing international practices of the information security policy.

Theoretical Framework

Many contemporary American and European scholars are interested in the study of the multidimensional phenomenon of information security. Nevertheless, the study of the concept of information security has intensified as a result of the Russian-Ukrainian hybrid confrontation, which has covered many areas (information, security, economic, and others) in the international context.

2. Theoretical substantiation of information security

Although there is no unanimous definition of the concept (due to its multidisciplinary nature), modern researchers agree on its main factors and criteria. In particular, Paleri (2022) believes that information security is the ninth element of the national security system. Andersson & Hedström (2022) understand this concept as the state of security of certain information processing and storage systems. The main criteria of this process are the availability, integrity, and confidentiality of data, their use for the benefit of the state and its citizens (Paleri, 2022).

In their experimental study, Tejay & Mohammed (2022) emphasize the importance of the category of "information security culture". In their paper "Cultivating security culture for information security success", it is argued that the development and further transformation of information security culture will contribute to the secure organization of information in general (Tejay & Mohammed, 2022). On the other hand, Van Daalen (2022) understands this concept as the state of security of particularly important information data of society and the state, in which it is important to prevent information damage due to its inaccuracy, incompleteness, and untimeliness. Lam & Lyons (2020) characterized the general aspects of modern data protection.

3. Information security versus cybersecurity

Cybersecurity and information security are both related to data security and its protection from various threats, so in modern scholarship, information security and cybersecurity are often equated. Nonetheless, recent research conducted by Taherdoost (2022) reveals distinct differences within these concepts, emphasizing that they should not be employed interchangeably. Information security, as elucidated in the study, encompasses safeguarding information against a multitude of potential threats. This protective framework is also oriented towards mitigating risks associated with any operational activities.

The foundational criteria for evaluating information security encompass its integrity, confidentiality, and the concurrent availability of essential information resources, as outlined by Paleri (2022). In contrast, cybersecurity possesses a narrower scope, primarily focusing on the safeguarding of data and information and communication technology (ICT). Its core objective is to maintain the confidentiality and availability of data within the realm of cyberspace, a perspective corroborated by Taherdoost (2022). Information security, as articulated by Taherdoost (2022), is a comprehensive approach dedicated to safeguarding not only the information itself but also its critical components, including "the systems and equipment involved in the storage, transmission, and utilization of this information" (Taherdoost, 2022, p. 485).

In contrast, cybersecurity, as perceived by contemporary scholars, encompasses an array of "tools, methodologies, and technologies designed to preserve cyber assets", particularly in the realm of information (Taherdoost, 2022, p. 485). The difference between the two terms is also mentioned in Gushchyn et al. (2022). These conclusions are confirmed by Devanny et al. (2021). They also do not equate these two concepts, because cybersecurity regulates a range of social relations that goes beyond information security, as it covers not only the protection of information but also its carriers, as well as the rights of individuals, society, and the state in this area (Devanny et al., 2021). Therefore, the content of information security is somewhat different from cybersecurity. The issues related to the formation of information security policy in Ukraine remain poorly researched. The Russian aggression has demonstrated a considerable arsenal of hybrid threats, the answers to which still require additional reflection.

4. Methodology

The study was conducted in stages through the prism of a combination of content analysis of theoretical material. The first stage involved a search for theoretical material, scientific sources, and literature. The second stage involved analyzing the data obtained through the prism of comparison, identifying controversial and unexplored points. The third stage was the authors' own interpretation of the importance of information security in the context of the Russian-Ukrainian hybrid war and the identification of the peculiarities of information security as a factor of stable development of the state through the prism of international experience.

The last stage summarizes the results obtained and formulates the authors' own recommendations and conclusions. Through the prism of the analytical method, the role of modern directions of national security policy development in Ukraine is revealed. On the basis of comparative analysis, the authors managed to compare the peculiarities of the implementation of Ukraine's information security policy with European practices.

5. Results

The experience of European countries in shaping information security policy is quite solid. This is due to the long and systematic development and implementation, participation in political associations, including the European Union and NATO, which impose additional requirements on this sensitive area.

The French information security system is an important component of national security. The basic principles of this system are laid down in the White Papers on Defense and National Security. The first White Paper on National Defense was published in 1972 and contained the principles of French defense policy and the foundations of the nuclear deterrence strategy. The second White Paper was published in 1994 and was dedicated to the end of the Cold War and the redirection of the armed forces to military operations outside the country, which led to the professionalization of the armed forces (Manolea, 2021).

Taking into account globalization and the fight against terrorism, a new concept of national security strategy was developed, which combines defense, internal security, foreign policy, and economic policy. This concept was enshrined in the third White Paper on Defense and National Security, which was published in 2008. The latest version of the White Paper (2017) pays special attention to information threats and measures to counter them (Manolea, 2021). It is noted that due to the scale and severity, some cyber-attacks can be classified as armed aggression. Difficulties with the distribution of actions and the combination of direct actions with methods of influence and propaganda make possible many scenarios of instrumentalization to destabilize or support simpler operations.

Accounting for cyber threats and their evolution is complex, as it cannot be limited to the perimeter of defense due to the complexity of issues and the involvement of public and private actors. Therefore, it is emphasized that armed forces should fully plan and conduct operations in digital environment, including the tactical level in the chain of planning and conducting kinetic operations. Operations in digital environment expand the range of traditional effects available to political power and exploit the growing digitization of France's opponents. This capability requires enhanced and sufficiently flexible hum a resource, as well as the continuous development of specific technical solutions.

The main law on information security in Germany is the Law on Strengthening the Security of Information Technology Systems. According to this law, the Federal Office for Information Technology Security (BSI) plays a central role in protecting Germany's critical infrastructures. Critical infrastructures include facilities, installations, or parts thereof that belong to the energy, information technology and telecommunications, transportation, road traffic, healthcare, water supply, food, finance, and insurance sectors (Cherniaieva, Orlenko & Ashcheulova, 2023).

Stopping or disrupting the operation of such facilities can lead to significant problems for the functioning of society, as these facilities ensure security and stability in the economy and public safety. At the same time, in 2019, the Federal Ministry of the Interior proposed an updated version of the law on guaranteeing the security of information technology. This initiative was designed to develop and implement a new holistic concept for the security of this industry, concept of using soft power in security system.

This project proposed the use of easy-to-consume IT security labels for commercial use, strengthening of relevant regulatory authorities, an increase in the list of cybersecurity-related offenses, and the introduction of new rules for investigating alleged offenders (Andersson et al., 2022). This practice has had some negative consequences, in particular, in terms of increasing the number of recipients of reports and obligations. However, despite such discomfort and the creation of additional administrative and economic difficulties, the updated system of information security assurance has received wide international recognition.

In the Republic of Poland, information policy standards are aimed at building an open society with free access to information for all interested and law-abiding citizens, the formation of pluralistic media, free exchange of opinions, etc. The basics of such a policy are regulated by the Law on Television and Radio Broadcasting, the Law on State Relations with the Roman Catholic Church in the Republic of Poland, etc. These and other acts establish the rules for attracting non-state funding to invest in information projects, licensing regulations, and the possibility of clerical representatives influencing information (which is extremely relevant for Polish society).

At the same time, the leading role in ensuring information security is played by the Internal Security Agency, whose functions also include close cooperation with the Ministry of Defense. The Agency is responsible for conducting offensive digital operations and developing appropriate cryptological initiatives to protect national data. ABW has become the main developer of the doctrine of countering threats and challenges to Poland's critical infrastructure.

This doctrine also lists escalation in the international sphere, soft power sphere, spreading propaganda and information damage to Poland's image at the European and global levels as the main threats. In order to implement this program, it is proposed to identify friendly, neutral and hostile parties, which is the responsibility of the highest state authorities. To improve the work of the ABW and other special structures, civil society is also actively involved.

Taherdoost (2022) Central and Eastern European countries (Poland, the Czech Republic, and Slovakia) also have special laws related to the secrecy of NATO information. Thanks to this framework, information related to the internal affairs of this military and political alliance is under special control. The adoption of such initiatives became a condition for joining the North Atlantic Alliance (Van Daalen, 2022). The involvement of this additional independent controlling factor reduces the risk of danger to the information field.

6. Discussion

In the following years Ukrainian government organized several information campaigns to present Ukraine to the world and to counter Russian disinformation about the country. In 2021 the Center for Countering Disinformation was established under the auspices of National Security and Defense Council of Ukraine. The aim of the Center is to monitor threats to Ukraine's information security, respond promptly to them, and deliver truthful information to the public.

The Center’s reports and articles are available on its website as well as in social media. The Center for Strategic Communications and Information Security was created within the Ministry of Information Policy and Culture. The Center is responsible for development of strategic communication, countering disinformation and increasing public awareness about hybrid threats. In this context the Ministry of Information Policy and Culture of Ukraine launched media literacy project “Filter”. It is online platform with a collection of the best educational projects of state authorities, non-governmental organizations, and international partners in the field of media literacy.

At the end of 2021, President of Ukraine approved new Information Security Strategy of Ukraine, that defined the term “information security of Ukraine” and outlined the challenges and key priorities of the country in the field of information security. According to this document the key challenge for Ukraine is the disruptive information influence of Russian Federation on Ukrainian society and the lack of integral disinformation countering system. The Strategy sets such policy priorities as combating disinformation and information operations, promoting Ukrainian culture and strengthening national identity, increasing media literacy of citizens, developing strategic communications, informational reintegration of Ukrainian citizens living in temporarily occupied territories, etc.

The overview of the latest developments in information security policy of Ukraine shows that Ukrainian government makes considerable efforts to strengthen information security of the country. The basic conceptual documents that define policy priorities are adopted. The legal framework is being adapted to the new information threats and challenges.

In comparison to European countries Ukraine has its peculiarities. The notion of information security is very broad and covers all activities aimed to protect national information environment and ensure civil rights and freedoms in information sphere. Many government institutions are involved in information security policy. Some institutions have partly overlapped responsibilities. This situation sometimes creates problems with coordination and consistency of actions.

Based on the developments of specialists operating in European countries (Piumatti *et al.,* 2017; Paleri, 2022; Tejay & Mohammad, 2022), the main directions of Ukrainian state policy in the field of information security can be improved, especially in the field of soft power. These directions include the best practices of democratic countries in improving countering information and hybrid threats that are characteristic of the present and are complemented by the relevant experience of confronting Russian challenges (see Fig. 1). Taking into account the Information Security Strategy of Ukraine, other official documents and implemented actions of Ukrainian government the authors consider necessary to emphasize on the following aspects of information security policy.

a. Finding a reasonable balance between the mandatory observance of the constitutional rights and freedoms of citizens when using information resources (in particular, these rights include freedom of speech) and the exercise of control functions to timely identify, prevent, stop, and neutralize threats in the information sector to Ukrainian citizens, and society, state institutions, etc. At the stage of the Russian military invasion, partial measures to restrict information freedom are a natural response to the military challenge and allow to limit the spread of propaganda (extremist, hateful) and other hybrid threats (Davis, 2020; Matviienkiv&Shmalenko, 2022). However, once most of the hybrid threats have been overcome, regulation should be abandoned.

b. Development and subsequent evolution of a legal framework to regulate the processes in information environment development and its protection from external threats, as well as harmonization with international law. Taking these requirements into account will allow for the future to take into account modern requirements for national security in the information environment and bring it to the level generally accepted among democratic countries. At the same time, the introduction of additional sanctions for "subversive" activities in the field of information influence may become a special feature of the Ukrainian system, at least for some time after the end of the Russian-Ukrainian war. After all, even a victory on the battlefield can have negative consequences if the opportunities for Russian influence on the means of disseminating knowledge, news, and other information remain at the same level.

c. Developing and implementing an effective state information policy in order to develop the national information environment and harmonize the system of management and coordination between the entities implementing the state information policy and the state policy in the field of information security (Gushchyn et al*.,* 2022; Kaplina, 2022). Currently, there is only a draft of such a program, which, although detailed, needs to be finalized due to the military challenge, information protection in extreme situations, agreements with governments and companies of democratic countries on the possible temporary storage of digital information on foreign servers, etc. Taking these possible reactions into account will strengthen Ukraine's position in the field of national information security. These principles have already been partially implemented in practice. For example, the digital documents and information of the state-owned Privatbank were moved to foreign servers to protect it from Russian hackers and digital criminals. It is imperative to take this experience into account in the further elaboration of national development programs.

d. Establishing cooperation between the state and the civil and private sectors, promoting international cooperation to implement the state information policy and ensure information security, creating a high-quality national information product (Park, 2019; Davis, 2009; Kunath & Winkler, 2019), recognizing its priority, providing comprehensive support and state support for its creation. For a long time, Russian influence on Ukrainian society was based on the dominance of Russian and Russian-language products in television, radio, cinema, music, and cultural life. It was only after the occupation of Crimea by Russian troops in 2014 that the processes of gradual prioritization of Ukrainian cultural products began. Along with official orders, public demand for Ukrainian-language digital products has also increased (Sofilkanych, 2022). After 2022, these trends can only be expected to intensify. This line of work would also be useful for developing soft power.

e. Further improvement of digital competencies among the Ukrainian population, developing media literacy skills (Devanny et al., 2022; Hrynchyshyn, 2021). In the future, Ukraine's information security policy should include programs to improve the digital literacy of Ukrainians. Obviously, such measures will be most effective if they are launched at school or higher education institutions, so that young people can acquire the skills to develop this competence on their own and prevent hybrid information threats at the initial stage of their spread.

However, attention should also be paid to representatives of the older and middle generations. As a result of the outbreak of hostilities, a whole campaign of fraudsters was launched, who sent messages about the provision of humanitarian or financial aid through popular messengers, phishing messages about access to money transfers, etc. The threat of obtaining personal information was especially relevant for those who did not know how to behave in such remote communication with fraudsters. Therefore, the organization of additional courses or at least the dissemination of appropriate algorithms for action when falling into digital traps would significantly reduce the damage caused by fraudsters.

The proposed innovations are based on the developed theoretical material and some experiences of the Russian-Ukrainian war of 2022 and were partly implemented by the

President of Ukraine in 2021. Undoubtedly, the inclusion of such provisions in the future line of information security will not provide absolute guarantees for avoiding information threats. As practice shows, fraudsters are quite insidious and actively use human weaknesses to make a profit (Johnson, 2022; Nikolenko, 2022). Unfortunately, there are frequent cases of extortion of money from the families of killed, captured, or missing Ukrainian soldiers. For this purpose, fraudsters use personal information and contacts of mobilized soldiers obtained illegally from their social media accounts or even from physical media (for example, from civilian jobs).

Another effective Russian information campaign was the dissemination of false information about special markings that only recruited Ukrainian citizens placed on buildings at the beginning of the aggression in February-April 2022. According to widespread propaganda, these markings were intended to adjust missile and air strikes. Although this possibility was too fantastic, the panic among the Ukrainian population caused by the general uncertainty of the situation caused significant damage. The development of appropriate digital competencies will help to maintain calm and concentration even in times of high emotional stress.

7. Conclusions and Implications

Therefore, the formation of an information security policy against global challenges, hybrid threats, propaganda, and direct military aggression by the Russian autocratic regime is one of the urgent tasks of the Ukrainian authorities. An important aspect of this process is the use of the latest experience of European countries, which can be combined with the knowledge gained during the war. First of all, we are talking about effective elements of using civil society, the adoption of proper laws and clear mechanisms of its implementation, the use of highly qualified specialists, and secure channels of information transmission.

At the same time, special attention will also be required to counteract hostile propaganda, which can be considered an effective counteraction to information campaigns to incite hatred and enmity. To create a high-quality information security system, it is proposed to introduce a reasonable balance between the mandatory observance of constitutional rights and freedoms of citizens when using information resources, adopt relevant laws, develop an effective state information policy, establish state cooperation with the civil and private sectors, and improve digital competencies among the Ukrainian population.

Some of the proposed changes to the security policy are already being implemented. Military operations have accelerated their implementation, which will lead to improved ways of countering hybrid challenges in the future. At the same time, the use of NATO capabilities and experience for Ukraine's information security is an issue that requires further research in view of the country's Euro-Atlantic aspirations.

Bibliographic references

- Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security – a structurational analysis”. *Information & Management*, *59*(3), 103623. doi:10.1016/j.im.2022.103623
- Cherniaieva, O., Orlenko, O., & Ashcheulova, O. (2023). The infrastructure of the Internet services market of the future: analysis of formation problems. *Futurity Economics&Law, 3*(1), 4–16. https://doi.org/10.57125/FEL.2023.03.25.01
- Davis, A. (2009). New media and fat democracy: the paradox of online participation1. *New Media & Society*, *12*(5), 745–761. doi:10.1177/1461444809341435
- Davis, A., Freedman, D., Fenton, N., & Khiabany, G. (2020). *Media, Democracy and Social Change: Re-Imagining Political Communications*. SAGE Publications. https://research.gold.ac.uk/id/eprint/28251/
- Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, *6*(3), 429–450. doi:10.1080/23738871.2021.2000628
- Gushchyn, O., Kotliarenko, O., Panchenko, I., Rezvorovych, K. (2022). Cyberlaw in Ukraine: current status and future development. *Futurity Economics&Law, 2*(1). https://doi.org/10.57125/FEL.2022.03.25.01
- Hrynchyshyn, Y. (2021). The infrastructure of the Internet services market of the future: analysis of the problems of formation. *Futurity Economics&Law, 1*(2), 12–16. https://doi.org/10.57125/FEL.2021.06.25.2
- Johnson, R. (2022). Dysfunctional Warfare: The Russian Invasion of Ukraine. *The US Army War College Quarterly: Parameters*, *52*(2), 5–20. doi:10.55540/0031-1723.3149
- Kaplina, O. (2022). Prisoner of war: Special status in the criminal proceedings of ukraine and the right to exchange. *Access to Justice in Eastern Europe*, *5*(4-2), 8–24. doi:10.33327/ajee-18-5.4-a000438
- Kunath, M., & Winkler, H. (2019). Usability of information systems to support decision making in the order management process. *Procedia CIRP*, *81*, 322–327. doi:10.1016/j.procir.2019.03.056
- Lam, W. M. W., & Lyons, B. (2020). Does data protection legislation increase the quality of internet services? *Economics Letters*, *195*, 109463. doi:10.1016/j.econlet.2020.109463
- Manolea, A. (2021). The Transpersonal War – Constituent of the Hybrid War. *Land Forces Academy Review*, *26*(4), 372–376. doi:10.2478/raft-2021-0048
- Matviienkiv, S., & Shmalenko, I. (2022). Mass media of national minorities as a means of national reconciliation in society. *Studia Europaea Gnesnensia*, *24*(24), 29–48. doi:10.14746/seg.2022.24.2
- Nikolenko, K. (2022). Artificial Intelligence and Society: Pros and Cons of the Present, Future Prospects. *Futurity Philosophy, 1*(2), 54–67. https://doi.org/10.57125/FP.2022.06.30.05
- Paleri, P. (2022). Informational Security (Infosec). У *Revisiting National Security* (c. 705–740). Singapore: Springer Nature Singapore. doi:10.1007/978-981-16-8293-3_17
- Park, C. S. (2019). The mediating role of political talk and political efficacy in the effects of news use on expressive and collective participation. *Communication and the Public*, *4*(1), 35–52. doi:10.1177/2057047319829580
- Piumatti, G., Magistro, D., Zecca, M., & Esliger, D. W. (2017). The mediation effect of political interest on the connection between social trust and wellbeing among

older adults. *Ageing and Society*, *38*(11), 2376–2395. doi:10.1017/s0144686x1700071x

- Sofilkanych, M. (2022). The formation of a new information culture of the future: the socio-philosophical content. *Futurity Philosophy, 1*(1), 56–67. https://doi.org/10.57125/FP.2022.03.30.05
- Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483–487. doi:10.1016/j.procs.2022.12.050
- Tejay, G. P. S., & Mohammed, Z. A. (2022). Cultivating Security Culture for Information Security Success: A Mixed-Methods Study Based on Anthropological Perspective. *Information & Management*, 103751. doi:10.1016/j.im.2022.103751
- van Daalen, O. (2022). In defense of offense: information security research under the right to science. *Computer Law & Security Review*, *46*, 105706. doi:10.1016/j.clsr.2022.105706
- Yarmoliuk, O. (2022). Information support of enterprises: problems, challenges, prospects. *Futurity Economics & Law, 2*(1), 12–22. https://doi.org/10.57125/FEL.2022.03.25.02