DOI: 10.31866/2616-745X.14.2024.319359
UDC 341.232

INFORMATION STATE IN THE CONTEXT OF INTERNATIONAL SECURITY AND GLOBAL IDENTITY: CHALLENGES AND PROSPECTS

Nataliia Likarchuk

Doctor of Political Sciences,
Professor at the Department of Public Administration,
ORCID: https://orcid.org/0000-0001-7119-439X,
e-mail: n.likarchuk@gmail.com,
Educational and Scientific Institute of Public Administration
and Civil Service of Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine, 04050

Received:
01.09.2024
Reviewed:
12.09.2024
Accepted:
14.09.2024

For citation:

Likarchuk, N., 2024. Information State in the Context of International Security and Global Identity: Challenges and Prospects. *International Relations: Theory and Practical Aspects,* 14, pp.107-121. doi: 10.31866/2616-745X.14.2024.319359.

This research aimed to analyse and conceptualise the phenomenon of the information state through the lens of national security and political identity. Accordingly, the study examines contemporary approaches to the concept of the information state within the framework of national security and political identity. The research methodology encompasses analytical modelling of the relationships between information security and political identity and qualitative and quantitative analyses, which identify critical challenges and further evolve the information state concept. The research results demonstrate that the information state plays a significant role in ensuring national security and safeguarding political identity. It has been established that, according to Eurostat data, by 2024, 94.7% of European Union member states had implemented information state standards into their national systems. The study also confirms the challenges and risks associated with information attacks, terrorism, and cybercrime, including using advanced social engineering techniques to manipulate public opinion and compromise critical infrastructure due to vulnerabilities in network protocols and cybersecurity systems. With the proliferation of information technologies, the term "electronic state" has emerged in the academic sphere, though it still lacks a clear definition. The electronic state is a concept that envisions the development of a modern state in such a way that all spheres of public life, including legislation, governance, and the economy, are reflected in an electronic format. The study concludes that the concept of the electronic state is understood as an ontology of state-building and functioning, state governance, and policy. In turn, this ontology encompasses the study of digital government, e-democracy, digital justice, electronic voting technologies, and public oversight in digitalisation. Ultimately, the primary characteristics of an information state include the blurring of territorial boundaries, the provision of information sovereignty both technically and legally, the adequate protection of citizens' rights through digital mechanisms, and the integration of law into the informatisation process.

Keywords: cybersecurity; digital technologies; digital infrastructure; analytical modelling; transnational cooperation; digital literacy.

Introduction

The rapid development of information and communication technologies, along with the widespread adoption of computerisation and electronic document management in daily practice, is setting the stage for a transformation in the principles of public administration. Information and communication technologies enhance the mechanisms of interaction among participants in societal relations, streamline the procedures for providing public services and self-governance, reduce the costs of maintaining state apparatuses, improve the quality of governmental decisions, and ensure the principles of transparency and openness. The concept of an "information state" represents a developmental direction for countries that necessitates legal recognition in light of the new "information reality" (McGowan, Phinnemore and Haastrup, 2024, p.84, p.97). Given current trends, it is advisable to enshrine the concept of an "information state" in the constitutions of certain countries, similar to the recognition of a legal, social, and democratic state. These proposals are supported by the idea that specific characteristics of the state (legal, social, democratic) are not only descriptions of the current status but also normative goals to be pursued. In this context, the information state will result from transitioning all spheres of social life into a digital format, a process that requires significant time.

The transition to an information state demands continuous monitoring of the informatisation processes at the national, regional, and economic entity levels, impacting national security and political identity. The institutional structure for forming and implementing state information policy includes governing and coordinating bodies, analytical units, databases, information security centres, standards development centres for information interaction, public relations services, and research organisations. These components form a complex network that aligns information policy with society's needs and the state's goals. The importance of studying information security issues is increasing due to several unresolved challenges in establishing an information state. Among the main challenges are the difficulties in adapting the state information security system, which, due to objective and subjective reasons, has rigid boundaries and is difficult to change; the problems with the practical utilization of the potential of information security in various state systems for their effective functioning and integration into the global system, mainly due to contradictions in the research, generalization, and implementation of information security practices in developed countries; and the use of national information security structures for free exchange of information and knowledge, as well as cooperation in various fields, faces specific challenges, driven by the need to ensure effective exchange that fosters mutual understanding and trust among participants; and the necessity to shift the priorities of information security structures from protecting national consciousness to developing global consciousness as a critical condition for the preservation of civilization and the survival of humanity.

Strategic and technological tasks related to national security and preserving political identity must be addressed to establish a comprehensive information state. Transitioning from paper-based to digital document management will allow citizens to interact more efficiently with government bodies, creating an internal security framework. Such a system will enhance the ability to monitor financial flows and eliminate transaction costs, thus helping to preserve state identity. The information state enables the creation of "smart" platforms for users, accelerating the resolution of various societal issues.

According to data provided by the European Commission, approximately 91% of EU citizens consider cybercrime to be one of the most significant threats within an information state and 79% note that data leaks and breaches of personal information are also substantial concerns. For instance, in 2023, over 67,000 incidents related to cybersecurity were recorded, a 51% increase compared to 2022. Consequently, several initiatives have been introduced, including the Single Digital Market and the Digital Europe Programme (Hammerschmid et al., 2024, p.417).

Analysis of recent research and publications

In their research on digital technologies in public administration, various authors analyse various aspects. B. Raduchel (2023) examines how digital technologies lead to societal crises and proposes solutions for overcoming them. A. R. Gohdes (2023) explores how states use digital tools for surveillance, censorship, and violence. K. Wone (2024) investigates the role of e-government in state development, while G. Hammerschmid et al. (2024) analyse the impact of national digitalisation strategies on public administration. O. Pakhnenko and Z. Kuan (2023) discuss the ethical aspects of digital innovations in public administration, and A. Svintsytskyi et al. (2023) consider the fight against fake news as a means of ensuring state information security. A. Fazil et al. (2024) study the practical aspects of e-government in the context of digitalisation. Z. Huang analyses how digital technologies shape national identity and patriotism, emphasising the importance of an information state for political identity. E. Chachko and K. Linos (2022) examine changes in international law following events in Ukraine, which also relate to information security and national identity.

Several aspects of the research require further study. First, the economic impact of information security measures on the state budget and the business sector has not been sufficiently explored. Specifically, how spending on cybersecurity and information security affects economic development and the competitiveness of national economies remains under-researched. Second, there is a lack of detailed analysis of the social consequences of implementing digital technologies, such as the digital divide between different social groups and regions. Additionally, international cooperation in the field of information security requires thorough consideration, particularly regarding the various strategies and practices employed by countries with different levels of technological development. Moreover, further research is needed on the impact of information security on cultural identities, specifically how digital technologies and information security policies might influence the preservation of cultural heritage and national identity in globalisation.

Formulation of the objectives of the article

Accordingly, the study aimed to analyse the challenges and prospects for ensuring national security and political identity in the context of recent technological changes on the international stage.

Presentations of the primary material of the study

The modern global information society and the new challenges of the 21st century underscore the importance of legal regulation of information security at all levels: individual, societal, and state. The concept of an information state encompasses two main directions: the social use of information technologies, the protection of national security, and the modernisation of state structures based on political identity (*Cambridge Dictionary*, n.d.).

The increasing number of studies and public statements (Likarchuk et al., 2023, p.771) dedicated to this conceptual transformation reflects a trend toward new terminology and the necessity of developing and understanding an adequate conceptual framework. This can serve as a foundation for implementing digital technologies in government institutions.

The term "digital era" was first introduced in 2000 by M. Castells (1999, p.523), who noted that: "…the process of technological change is rapidly accelerating as it can unite various technological fields through a common digital language by which information is generated, stored, retrieved, processed, and transmitted. We are in the era of digitalisation…". Subsequently, in 2006, scholars P. Dunleavy and H. Margetts (2010) began using the term DeG (digital-era governance), which refers to: "…a complex set of changes in public administration, based on improved information processing and the rapid 'multi-sectoral' spread of information technologies…".

To define certain conceptual foundations of the information state, it is necessary to clarify its understanding. For example, A. Svintsytskyi et al. (2023, p.431) define this term as a set of tools aimed at the implementation of state authority in the provision of services, as well as the direct interaction between government bodies and the protection of national security. According to A. Fazil et al. (2024, p.521), the term in question, characterises the state as a whole, incorporating modern communication and international information technology standards while preserving its political independence and identity. J. Harris (2021, p.42) argues that the information state represents a state power organisation based on the application of information and communication technologies and the protection of national security. According to B. Raduchel (2023, p.106), the information state is a distinctive interaction between citizens and government bodies. A. Gohdes (2023, p.83) offers an exciting perspective, defining the "information state" as an information-technical organisation of politico-legal interaction between subjects of law and public authorities to ensure the participation of the former in governance and provide them with state services using digital technologies.

It should be noted that information security is based on national interests; thus, national security involves protecting citizens residing within the country. The issue of information security, taking into account strategic national priorities, is of great importance, as digitalisation is one of the critical characteristics of modernity. The development of information technologies has led to significant expansion and increased competitiveness in many sectors. The political leadership of countries also implies dominance in the information sphere: whereas in the 1990s and early 2000s, informatisation was seen as a source of radical changes in the economy, today it is a fundamental infrastructure necessary for the development of various sectors of business, society, and the state (Wang and Eldemerdash, 2023, p.749). Progress in information and communication technologies, including state, personal, and big data (Big Data), is now at the forefront of impact.

Accordingly, their importance far exceeds that of software solutions and technical infrastructure. Consequently, protecting information becomes one of the critical aspects of national security.

Analysing the views of European and American scholars, researchers define the mechanism for ensuring information security as a system of various tools (political, personnel, managerial, informational, legal) through which authorised entities protect the information interests of the country, community, and citizens from internal and external threats (Beti, 2024, p.107).

The legal policies of central states such as the USA, China, Germany, and France vividly demonstrate the significant attention these governments pay to information security. The information state is a modern concept that integrates information technologies into all aspects of public administration, including the provision of services to citizens, ensuring transparency, and enhancing the efficiency of governmental processes (Wone, 2023, p.53). This interpretation implies the use of electronic resources for interaction between government bodies and citizens, as well as for internal administration. In such a state, conditions are created for effective data-driven decision-making, which contributes to increasing public trust in state institutions and improving the quality of life for citizens.

Accordingly, assessing an information state's development level is based on several critical indicators. The E-Government Development Index, developed by the United Nations, is one of the main tools for this purpose. It comprises three components: online services, telecommunications infrastructure, and human capital. A high E-Government Development Index indicates a well-developed e-government infrastructure and the effective integration of IT solutions into public administration (Hamidi, 2023, p.63). The Networked Readiness Index is also an important indicator for assessing the information state. It measures a country's readiness to apply information and communication technologies in various areas, such as business, public administration, and personal life. A high Networked Readiness Index demonstrates that the country has the necessary infrastructure, legal framework, and human resources to effectively implement information and communication technologies (Hamidi, 2023, p.71).

In this context, it is worth noting that implementing the principles of an information state requires a systematic approach and active government support. This includes technical infrastructure, educational programs to improve the population's IT literacy, legislative initiatives to ensure data security, and incentives for innovation. As a result, the information state enhances the country's competitiveness in the global market and provides the sustainability of economic development.

One example of a prosperous information state is Estonia. Estonia has gained recognition for its innovations in e-government and digital services. The e-Estonia system, implemented in 2001, has enabled the country to become a leader in this field. According to the UN, in 2022, Estonia ranked third in the world on the E-Government Development Index with a score of 0.9472, significantly higher than the global average (Profiroiu, Negoiță and Costea, 2024, p.337). Estonia has also achieved high results on the Networked Readiness Index. In 2022, the country ranked 8th out of 130 countries with a score of 81.05 points, reflecting a high level of infrastructure readiness and a robust legal framework for using information and communication technologies. Notably, 99% of public services in Estonia are available online, providing citizens with convenient and fast access to administrative services and enhancing the efficiency of public administration (Beti, 2024, p.110).

Another example of a prosperous information state is Singapore, which actively implements digital technologies in public administration and provides services to citizens. In 2022, Singapore ranked first in the world on the E-Government Development Index with a score of 0.9150, reflecting the quality of online services, developed telecommunications infrastructure, and significant human capital (Pakhnenko and Kuan, 2023, p.117). Singapore also performs exceptionally well on the Networked Readiness Index, ranking second globally in 2022 with a score of 84.00 points (Fazil et al., 2024, p.525). This indicates a high level of readiness for integrating and using information and communication technologies across all aspects of public life. The Singaporean government actively invests in developing digital technologies, such as the “Smart Nation” project, which involves the implementation of the Internet of Things and Big Data to improve citizens’ quality of life and governance efficiency.

In light of the above, the most accessible form of information security for scientific analysis is state information security. Strategies, doctrines, and other similar programmatic documents adopted by states in the field of information security clearly define the goals, scope, directions, and methods of its provision. For instance, American and Ukrainian legal scholars view the information environment as the material and technical foundation of the information state and a part of the noosphere (Chachko and Linos, 2022, p.127). In the modern world, there is a close relationship between security, the conditions for development and the level of protection of the information state. The main threats to the vital interests of citizens and the state are realised through the information component. As a result, the significance of the information component is increasing, prevailing in all aspects of national security.

Political identity undergoes significant transformations in the context of the information state. The accessibility of information, digital literacy, and the integration of new technologies into daily life foster the formation of civic consciousness and active citizen participation in political processes. The development of information technologies allows citizens to access a wide range of information sources, promoting pluralistic viewpoints and shared national values. At the same time, legal regulation and collaboration between state and private entities help maintain national identity amidst rapidly changing global dynamics. The informatisation of society and the development of digital technologies are transforming the principles of state functioning, leading to the emergence of the information state. This state actively uses information technologies to deliver public services. It integrates them into all spheres of social life, ensuring effective national security management and the preservation of political identity. For instance, information security becomes a critical element of national security in the information state, which includes digital sovereignty—state control over the national information space, ensuring its integrity and protection from external threats; cybersecurity—a system of measures to protect information resources and infrastructure from cyberattacks, including the development of response strategies and countering cybercrime; and information hygiene—educating citizens on safe use of information technologies to reduce the risk of social engineering and cybercrime.

Political identity, which defines national uniqueness and societal resilience to internal and external challenges, also includes information pluralism—ensuring access to diverse information sources that contribute to a multifaceted political culture and reduce the risk of information manipulation; media literacy—developing critical thinking among citizens, enabling them to analyse and evaluate information, thus countering fake news and propaganda; and e-democracy—using digital technologies to increase government transparency and foster civic engagement in the political process. In the national security realm, the information state faces numerous challenges requiring deep analysis and strategic approaches. One key challenge is intensifying cyber threats, which can have catastrophic consequences for a state's critical infrastructure. The increasing number of state and non-state actors and the complexity of cyberattacks underscore the need to develop advanced defence and monitoring systems. Modern technologies like artificial intelligence and machine learning can significantly enhance a state's ability to detect and neutralise cyber threats, ensuring national security.

The information state contends with public opinion manipulation and disinformation challenges in political identity. Globalisation, accompanied by the widespread use of information technologies, contributes to the erosion of national identity and heightens the risk of external actors interfering in domestic politics. Thus, the state must focus on increasing public media literacy and developing strategies to protect national identity. Implementing innovative educational programs and supporting independent media can substantially strengthen citizens' political awareness and counteract destructive informational influences.

The prospects for developing the information state include harmonising legislation on information security, enhancing international cooperation, and investing in technological advancement. A crucial aspect is the formation of international alliances and participation in global initiatives aimed at combating cybercrime. This approach will allow various countries to unite to address transnational threats.

The development of the information state is an integral part of national security strategies. However, along with opportunities, this development also brings significant challenges that require appropriate responses from the state. Cyberattacks, cyber espionage, and information wars are the main threats to the information state. They disrupt the operation of critical infrastructures, undermine trust in state institutions, and spread disinformation. For example, cyberattacks on government systems in the United States (such as the OPM breach in 2015) and the European Union (such as the cyberattack on Estonia in 2007) demonstrate the scale of these threats. Using big data and monitoring citizens infringes on privacy rights, and the misuse of such technologies can lead to authoritarianism. For instance, China's social credit system uses vast amounts of personal data to monitor and control citizen behaviour. Additionally, using disinformation and propaganda to influence public opinion and political processes destabilises the internal situation within a state. Russia's interference in the 2016 U.S. elections through social media to spread disinformation is an example of how such actions can polarise society and undermine trust in democratic institutions.

Implementing advanced cybersecurity systems, enhancing international cooperation in cybersecurity to analyse and detect threats, and strengthening legislative measures are necessary to combat cybercrime and protect democratic processes from interference. For example, the United States and the EU have established cybersecurity agencies, such as the Cybersecurity and Infrastructure Security Agency. Cybersecurity is becoming an essential element of national security, as cyberattacks result in significant losses and disruptions to critical infrastructures. States use information resources to control and manage public opinion, affecting citizens' political identity. Statistics show a growing investment in cybersecurity and an increase in cyberattacks. Over the past five years, global cybersecurity spending has risen from $106 billion in 2017 to $173 billion in 2022. The number of cyberattacks in 2022 reached 2.8 billion, a 40% increase compared to 2017 (Beti, 2024, p.109). This underscores the importance of developing the information state to safeguard national security. Simultaneously, the mass media and social networks have become platforms for political manipulation and propaganda, impacting citizens' political identity.

Using information and communication technologies to enhance government transparency and accountability and encourage citizen participation in political life through electronic platforms helps create a more open and democratic societal system. For example, Estonia has implemented e-governance and e-voting, significantly boosting citizen trust in state institutions. Over 99% of public services are available online, and e-voting has been implemented nationally since 2005. In the 2019 parliamentary elections, 44% of votes were cast online, reflecting high public trust in the e-voting system.

Fostering innovation, developing the digital economy, and creating favourable conditions for technological startups lead to economic growth, job creation, and strengthening of a country's international standing. Accordingly, Israel actively develops its high-tech sector, contributing to economic growth and national security. The government is home to over 6,000 startups, and venture capital investment in 2022 reached approximately $10 billion (Beti, 2024, p.107). High-tech industries, such as cybersecurity, secure Israel's leading position in the global market and significantly enhance its defence capabilities. In the context of national security and political identity in the information society, the primary threats to the vital interests of individuals, society, and the state in the information sphere may come from countries or their alliances and special services, international terrorist and criminal organisations, and groups, as well as national and global information and communication systems.

The influence of harmful information factors reduces or distorts the awareness of government agencies. Individuals and social groups may develop a false perception of surrounding events and processes, affecting their behaviour, development, knowledge, upbringing, mental state, and health, ultimately impacting their existence within society. The impact of destructive information on societal consciousness lowers general culture, fosters spiritual emptiness, and spreads inhumane ideas. This leads to negative phenomena such as corruption, monopolies, theft, and blackmail. Utilising these factors can trigger internal political unrest, strikes, ethnic conflicts, armed clashes, and civil wars.

In various areas of the information state, threats and dangers may manifest differently. However, a misunderstanding of reality by those making state decisions can negatively impact national security and political identity. Information distortion and disinformation can lead to erroneous conclusions that threaten political stability, economic development, and state security. Overcoming and preventing these threats requires improving the state's information security system, fostering the innovative development of the information technology sector, eliminating dependence on foreign information technologies, and creating and using information technologies inherently protected against various influences.

Conclusions

Information security is critical to national security, as protecting the informational interests of the state, society, and citizens from internal and external threats is paramount. Legal, political, personnel, administrative, and informational measures form the mechanism for ensuring information security, enabling states to respond to the challenges of a globalised world effectively. The development of the information state involves the integration of digital technologies into all aspects of state governance, which enhances the efficiency of service delivery, transparency, and citizen trust in government institutions. The E-Government Development Index and the Networked Readiness Index are critical indicators of the level of information state development, reflecting a country's readiness to utilise information and communication technologies.

The conducted research established that the concept of the information state is crucial for ensuring national security and shaping political identity. In particular, it was found that integrating digital technologies into state governance enhances the efficiency of administrative processes, transparency, and citizen participation in political life. Protecting information systems and cybersecurity was confirmed as essential for maintaining state resilience against external and internal threats.

Further research within the framework of the information state in the context of national security and political identity should focus on developing new methods for protection against cyber threats. The continuous evolution of cybercrime requires the creation of innovative technologies to detect and neutralise new threats, the analysis of the impact of information security on social stability, the investigation of the relationship between the protection of personal data and citizens' trust in government institutions, integration of information technologies into various areas of government, assessing the effectiveness of using information and communication technologies in health care, education, law enforcement, and other sectors to improve the quality of public services; international cooperation in information security, and examining the practices of different countries and developing joint strategies to combat global cyber threats.

Qualitative indicators were obtained, demonstrating the positive impact of digital technologies on the functioning of the state. Specifically, implementing information systems has reduced the time and costs associated with providing public services and increased citizens' trust in government institutions. The results showed that effective management of information security and political identity is achievable by adhering to transparency, data protection, and digital identification principles. Examples of successful information states, such as Estonia and Singapore, demonstrate that an innovative approach to implementing electronic resources and developing telecommunications infrastructure contributes to increased competitiveness and sustainable development. These countries have achieved high results on the EGDI and NRI indicators, indicating the effectiveness of their digitalisation strategies.

The information state also significantly influences political identity, contributing to forming civic consciousness and active citizen participation in political processes. Ensuring access to diverse information sources, developing critical thinking, and promoting media literacy are essential elements in supporting national identity and countering informational manipulation.

At the same time, it is essential to note the limitations of this research, which may affect its results. One of the main limitations is the rapid development of information technologies, which complicates the prediction and analysis of long-term trends. The obtained results significantly impacted the understanding of the role of information technologies in state governance and national security. They underscore the need for continuous monitoring and adaptation of state strategies to new technological challenges. In the future, the results could be improved by expanding the database, involving additional resources, and conducting comparative studies in other countries. Another important direction is the development of interdisciplinary approaches, which will allow for a more comprehensive assessment of the impact of information technologies on society and the state.

REFERENCES

Beti, E., 2024. National security as a comprehensive notion, state security from the aspect of international law and its political manifesto. *Balkan Journal of Interdisciplinary Research,* [e-journal] 10 (1), pp.105-113. https://doi.org/10.2478/bjir-2024-0010

Cambridge Dictionary, n.d. [online] Available at: <https://dictionary.cambridge.org/dictionary/english/> [Accessed 25 May 2024].

Castells, M., 1999. *The Information Age. Volumes 1-3: Economy, Society, and Culture.* Oxford: Blackwell.

Chachko, E. and Linos, K., 2022. International Law After Ukraine: Introduction to the Symposium. *American Journal of International Law Unbound,* [e-journal] 116, pp.124-129. https://doi.org/10.1017/aju.2022.18

Dunleavy, P. and Margetts, H., 2010. The Second Wave of Digital Era Governance. In: *American Political Science Association (APSA)* Annual Conference, Washington, DC, 2-5 September. [online] American Political Science Association, pp.1-32. Available at: <https://core.ac.uk/download/pdf/95777.pdf> [Accessed 25 May 2024].

Fazil, A.W., Hakimi, M., Aslamzai, S. and Quchi, M.M., 2024. A Review of E-Government Practices in the Age of Digitalization. *International Journal of Multidisciplinary Approach*

Research and Science, [e-journal] 2 (02), pp.511-527. https://doi.org/10.59653/ijmars.v2i02.568

Gohdes, A.R., 2023. *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence.* [e-book] New York: Oxford University Press. https://doi.org/10.1093/oso/9780197743577.001.0001

Hamidi, A., 2023. *Auswirkungen von E-Government in Entwicklungsländer.* Verlag Unser Wissen.

Hammerschmid, G., Palaric, E., Rackwitz, M. and Wegrich, K., 2024. A shift in paradigm? Collaborative public administration in the context of national digitalization strategies. *Governance,* [e-journal] 37 (2), pp.411-430. https://doi.org/10.1111/gove.12778

Harris, J., 2021. Effective strategies for changing public opinion: A literature review*. Sentience Institute*, [online] 08 November. Available at: <https://www.sentienceinstitute.org/downloads/Effective%20strategies%20for%20changing%20public%20opinion.pdf> [Accessed 25 May 2024].

Likarchuk, N., Velychko, Z., Andrieieva, O., Lenda, R. and Vusyk, H., 2023. Manipulation as an element of the political process in social networks. *Cuestiones Políticas*, [e-journal] 41 (76), pp.769-779. https://doi.org/10.46398/cuestpol.4176.45

McGowan, L., Phinnemore, D.A. and Haastrup, T., 2024. *A Dictionary of the European Union.* 11th ed. [e-book] London: Routledge. https://doi.org/10.4324/9781003476863

Pakhnenko, O. and Kuan, Z., 2023. Ethics of Digital Innovation in Public Administration. *Business Ethics and Leadership,* [e-journal] 7 (1), pp.113-121. https://doi.org/10.21272/bel.7(1).113-121.2023

Profiroiu, C., Negoiță, C. and Costea, A., 2024. Digitalization of public administration in EU member states in times of crisis: the contributions of the national recovery and resilience plans. *International Review of Administrative Sciences,* [e-journal] 90 (2), pp.336-352. https://doi.org/10.1177/00208523231177554

Raduchel, B., 2023. *The New Technology State: How Our Digital Dreams Became Societal Nightmares—and What We Can Do about It.* Reston: Amplify Publishing.

Svintsytskyi, A.V., Semeniuk, O.H., Ufimtseva, O.S., Irkha, Y.B. and Suslin, S.V., 2023. Countering fake information as a guarantee of state information security. *Security Journal,* [e-journal] 36 (3), pp.427-442. https://doi.org/10.1057/s41284-022-00347-0

Wang, A. and Eldemerdash, N., 2023. National identity, willingness to fight, and collective action. *Journal of Peace Research,* [e-journal] 60 (5), pp.745-759. https://doi.org/10.1177/00223433221099058

Wone, K., 2023. *E-government: Digital governance, a solution for development*. Independently published.

INTERNATIONAL RELATIONS: THEORY AND PRACTICAL ASPECTS
Issue 14 (2024)
ISSN (print) 2616-745X;   ISSN (online) 2616-7794

ІНФОРМАЦІЙНА ДЕРЖАВА В КОНТЕКСТІ МІЖНАРОДНОЇ БЕЗПЕКИ ТА ГЛОБАЛЬНОЇ ІДЕНТИЧНОСТІ: ВИКЛИКИ І ПЕРСПЕКТИВИ

Лікарчук Наталія Василівна

Докторка політичних наук, професорка кафедри державного управління,
ORCID: https://orcid.org/0000-0001-7119-439X,
e-mail: n.likarchuk@gmail.com,
Навчально-науковий інститут публічного управління
та державної служби Київського національного
університету імені Тараса Шевченка, Київ, Україна, 04050

Метою дослідження було провести аналіз та концептуалізацію феномену інформаційної держави крізь призму національної безпеки та політичної ідентичності. Відповідно, у дослідженні розглядаються сучасні підходи до концепції інформаційної держави в рамках національної безпеки та політичної ідентичності. Методологія дослідження охоплює аналітичне моделювання взаємозв’язків між інформаційною безпекою і політичною ідентичністю та якісний і кількісний аналізи, що дозволяє визначити основні виклики та подальшу генезу становлення концепції інформаційної держави. Результати дослідження доводять, що інформаційна держава має велику вагу, передусім у гарантуванні національної безпеки, але водночас і у забезпеченні політичної ідентичності. Встановлено, що, за даними Eurostat, до 2024 року 94,7 % держав-членів Європейського Союзу впровадили стандарти інформаційної держави у свої національні системи. Також пропоноване дослідження підтверджує, що існують виклики та ризики, які пов’язані з інформаційними атаками, тероризмом і кіберзлочинністю, зважаючи на використання передових методів соціальної інженерії для маніпуляції суспільною думкою, а також компрометацію критично важливої інфраструктури через уразливості в мережевих протоколах і системах кібербезпеки. З поширенням інформаційних технологій у науковій сфері з’явився термін «електронна держава», проте він досі не має чіткого визначення. Електронна держава – це концепція, яка передбачає розвиток сучасної держави таким чином, що всі сфери суспільного життя, включаючи законодавство, управління та економіку, відображаються в електронному форматі. У дослідженні робиться висновок, що концепція електронної держави зводиться до її розуміння як онтології державного будівництва та функціонування, державного управління і політики. Зі свого боку, подібна онтологія включає вивчення цифрового уряду, електронної демократії, цифрового правосуддя, електронних виборчих технологій, громадського контролю з урахуванням цифровізації. У підсумку, основними ознаками інформаційної держави є розмитість територіальних меж, забезпечення інформаційного суверенітету як із технічної, так і з правової сторони, ефективний захист прав громадян за допомогою цифрових механізмів та інтеграція права у процес інформатизації.

Ключові слова: кібербезпека; цифрові технології; цифрова інфраструктура; аналітичне моделювання; транснаціональна співпраця; цифрова грамотність.