

Formation of an Information (Digital) Society in Ukraine Under Martial Law: Political and Legal Aspects*

Yurii Kyrychenko,¹ Olena Postol,² Natalia Riezanova,³

Pavlo Nazarenko,⁴ Liliia Baieva⁵

^{1,2,3,4,5} National University Zaporizhzhia Polytechnic, Ukraine.



[10.15408/jch.v14i1.50470](https://doi.org/10.15408/jch.v14i1.50470)

Abstract.

In addition to analyzing the political and legal frameworks for guaranteeing the digital transformation of the state in the face of military aggression, the paper looks at the characteristics of the development of an information (digital) society in Ukraine under martial law. The topic is relevant because information and communication technologies are rapidly permeating every aspect of public life in the modern stage of society's development, creating a new model of socioeconomic and political development known as the information or digital society. In order to maintain the stability of state administration, the continuation of administrative services, and efficient communication between the state and its citizens, the Russian Federation's full-scale war against Ukraine created new difficulties for the operation of state institutions. This made the active use of digital technologies necessary. The dominance of knowledge and information as strategic resources for development, the extensive use of digital technologies, the expansion of information access, and the active use of electronic services in the field of public administration are found to be characteristics of the information society. In this sense, digitalization is viewed as a complicated process that uses contemporary information technologies to change public communications, economic interactions, and state institutions. The study also takes into account cyber and information security as a crucial element in the development of a digital society.

Keywords: Political System; Legal System; Sustainable Development; Information Society; Digital Society; Information Security; Cybersecurity

* Received: January 12, 2026; revised: February 24, 2026; accepted: March 22, 2026; published: March 30, 2026.

¹ **Yurii Kyrychenko** - Doctor of legal sciences, Professor, head of the department "Political Science and General Law Disciplines", National University of Zaporizhzhia Polytechnic, Ukraine. ORCID ID: <https://orcid.org/0000-0002-1212-1622>. E-mail: kyrychenko_yuriy84@ukr.net.

² **Olena Postol** - Doctor of political sciences, Professor, Professor of the Department of "Political Science and General Legal Disciplines", National University of Zaporizhzhia Polytechnic, Ukraine. ORCID ID: <https://orcid.org/0000-0003-4603-8955>. E-mail: elepostol2017@gmail.com

³ **Natalia Riezanova** - Candidate of philosophical sciences, Associate Professor, Associate Professor of the Department of "Political Science and General Law Disciplines", National University of Zaporizhzhia Polytechnic, Ukraine. ORCID ID: <https://orcid.org/0000-0003-3094-4881>. E-mail: reznat120@gmail.com

⁴ **Pavlo Nazarenko** - Candidate of Sciences in Law, Associate Professor, Associate professor of the department "Criminal, Civil and International Law", National University of Zaporizhzhia Polytechnic, Ukraine. ORCID ID: <https://orcid.org/0000-0002-6569-0845>. E-mail: pavelnazarenkoo@gmail.com

⁵ **Liliia Baieva** - Candidate of Sciences in Law, Associate Professor, Associate professor of the Department of "Constitutional, Administrative and Labor Law", National University of Zaporizhzhia Polytechnic, Ukraine. ORCID ID: <https://orcid.org/0000-0001-8161-9005>. E-mail: baeva_liliya@ukr.net

**Corresponding Author: kyrychenko_yuriy84@ukr.net.

A. INTRODUCTION

The current stage of development of the world community is characterized by the rapid spread of information and communication technologies, which significantly affect all spheres of public life - economic, political, social, and legal. As a result of these processes, a new type of social development is being formed, which in the scientific literature is defined as an information or digital society. Its main feature is the dominance of information and knowledge as key resources of socio-economic progress, the widespread use of digital technologies in public administration, economic activity and public communications, as well as the active introduction of electronic services in the interaction between the state and citizens (Kulinich *et al.*, 2023).

The development of the information society is one of the priority areas of state policy of many countries of the world. International organizations, in particular the United Nations, the European Union and the Council of Europe, pay significant attention to the issues of digital transformation of public administration, the development of e-government and ensuring citizens' access to information resources. Thus, within the framework of the World Summit on the Information Society, the main principles of building a global information space based on openness, accessibility of information and the use of modern technologies to increase the efficiency of public administration were formulated (Vitvitskyi *et al.*, 2020).

Ukraine is also actively involved in global processes of digital transformation. The formation of an information society has been identified as one of the strategic directions of state development, which is reflected in several program documents and regulatory legal acts, in particular in the Laws of Ukraine "On Information", "On Electronic Trust Services", "On Electronic Communications", "On the Basic Principles of Ensuring Cybersecurity in Ukraine", as well as in the Concept of Development of the Digital Economy and Society of Ukraine. An important step in this direction was the creation of the Ministry of Digital Transformation of Ukraine, whose activities are aimed at the development of electronic governance, digital state services, and the formation of a modern digital infrastructure (Leheza *et al.*, 2023).

The processes of digitalization have acquired particular importance in the conditions of martial law introduced in Ukraine in connection with the full-scale armed aggression of the Russian Federation. In accordance with the Decree of the President of Ukraine No. 64/2022 "On the Introduction of Martial Law in Ukraine" dated February 24, 2022, state institutions were forced to operate in conditions of significant security risks, destruction of infrastructure, population

displacement, and limited access of citizens to traditional administrative services. In these conditions, digital technologies have become one of the key tools for ensuring the continuity of the public administration system, the provision of state and administrative services, and effective communication between the state and society (Sinkevych *et al.*, 2024).

In conditions of martial law, digital tools have acquired new significance as an element of ensuring the stability of the state. The use of electronic registers, digital platforms, and online services has made it possible to provide a prompt response to the challenges of wartime, in particular in the field of social security, support for internally displaced persons, recording damaged or destroyed property, providing humanitarian assistance, and coordinating the activities of state bodies (Chorna *et al.*, 2023).

At the same time, the development of a digital society in conditions of martial law is accompanied by new political and legal challenges. These include issues of ensuring information and cybersecurity, protecting state information resources, preventing disinformation and information operations, as well as ensuring a balance between national security needs and respecting human rights and freedoms in the digital environment. In addition, the issue of improving the regulatory and legal framework for digital processes, adapting legislation to European standards, and ensuring an adequate level of personal data protection remains relevant (Kobrusieva *et al.*, 2021).

Scientific understanding of the processes of forming an information society was carried out in the works of domestic and foreign scientists. However, the new realities of the functioning of the state in wartime require further scientific research aimed at a comprehensive analysis of the political and legal aspects of the development of a digital society.

In view of the above, the relevance of the research topic is due to the need for a comprehensive analysis of the political and legal mechanisms of forming an information (digital) society in Ukraine under martial law, identifying the main trends in the digital transformation of public administration and outlining the prospects for the further development of digital institutions in the face of modern security challenges (Zadyraka *et al.*, 2023).

B. METHODS

The comparative legal method is of great importance in the study of political and legal aspects of the formation of an information (digital) society in Ukraine, as it allows comparing national legislation with the legal systems of

other states and international standards in the field of digitalization, e-government, information protection and cybersecurity. The use of this method helps to identify common and distinctive features of the legal regulation of digital processes, as well as to determine the prospects for improving national legislation taking into account international experience.

Comparative legal analysis makes it possible not only to assess the effectiveness of existing legal mechanisms, but also to determine the possibilities of implementing advanced international practices into the national legal system. This is especially relevant for Ukraine, which is at the stage of active digital transformation and at the same time is carrying out the process of harmonizing legislation with European Union law.

One example of the application of the comparative legal method is the comparison of Ukrainian legislation in the field of electronic trust services with the legal regulation of the European Union. Thus, the Law of Ukraine “On Electronic Trust Services” is largely based on the provisions of Regulation (EU) No. 910/2014 of the European Parliament and of the Council (eIDAS), which defines the legal framework for the use of electronic identification, electronic signatures and other trust services in the EU countries. A comparison of these regulatory acts allows us to establish that Ukrainian legislation is gradually adapting to European standards in the field of electronic identification and digital services.

Another example of the use of the comparative legal method is the analysis of the e-government system in Ukraine and the countries of the European Union, in particular Estonia, which is considered one of the world leaders in the field of digital transformation of the state. Estonia operates a comprehensive e-government system that includes digital identification of citizens, electronic voting, electronic medical systems and digital state registers. Comparing this model with the Ukrainian e-government system allows us to identify promising areas for the development of digital services, in particular, expanding the functionality of electronic government platforms, integrating state registers, and increasing the level of digital interaction between government agencies.

Comparative legal analysis is also used in the study of legal regulation of cybersecurity. For example, Ukrainian legislation in the field of cybersecurity, in particular the Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity of Ukraine”, can be compared with the European Union Directive on the Security of Network and Information Systems (NIS Directive). Such analysis allows us to determine the level of compliance of the Ukrainian cyber defense system with

European standards and identify areas for further improvement of legal regulation in this area.

In addition, the comparative legal method is used to analyze legal mechanisms for the protection of personal data. In this context, a comparison of the provisions of Ukrainian legislation, in particular the Law of Ukraine "On the Protection of Personal Data", with the General Data Protection Regulation of the European Union (GDPR), is of particular importance. Conducting such an analysis allows us to determine the level of harmonization of Ukrainian legislation with European standards in the field of privacy protection and information security.

A separate direction of application of the comparative legal method is the study of digital tools of public administration used in crises or military conflicts. In particular, the analysis of the experience of Israel and some European Union countries in using digital platforms for crisis management allows us to identify effective mechanisms for ensuring information interaction between state bodies and citizens in emergencies. Thus, the application of the comparative legal method in the study allows us to comprehensively assess the state of legal regulation of digital transformation in Ukraine, identify gaps in national legislation, and identify promising areas for its improvement, taking into account international experience and European standards for the development of a digital society.

C. RESULTS AND DISCUSSION

In today's conditions of rapid technological development, an important place in the system of state policy is occupied by the processes of digitalization and the introduction of information technologies in the sphere of public administration. One of the key areas of state activity in this context is the modernization of mechanisms for the provision of administrative services, the improvement of management procedures, and the creation of more convenient conditions for interaction between citizens and state institutions. A significant contribution to the implementation of these tasks has been made through the introduction of modern digital tools, in particular the state platform "Diya", which provides the possibility of using electronic documents, receiving state services remotely and access to a wide range of administrative services via the Internet. At the same time, the development of digital transformation involves not only the creation of new electronic services, but also the improvement of

digital infrastructure, strengthening cyber defense systems and increasing the level of digital competence of the population.

An important component of state information policy is also the development of the education system and the formation of media literacy. In modern conditions, this direction is of particular importance, given the active spread of information manipulations and propaganda influences characteristic of information warfare. The formation of skills for critical analysis of information, the ability to detect unreliable messages, and recognize manipulations and propaganda is a necessary condition for ensuring the information stability of society. To this end, elements of media education are gradually integrated into the curricula of general secondary and higher education institutions, and various educational and educational programs are being implemented aimed at improving the information culture of the adult population.

A separate role in the implementation of information policy is played by higher education institutions, whose information activities are focused primarily on education seekers and other consumers of educational services. In conditions of martial law, ensuring safe and uninterrupted access to educational resources and digital platforms of universities, regardless of the location of users, becomes of great relevance. In this case, compliance with the requirements of the legislation on the protection of personal data, as well as ensuring an adequate level of protection of intellectual property rights for educational materials (Nesteryak, 2021), is of particular importance. An important communication tool in this area is the functioning of official websites of universities and their pages on social networks, which allows for prompt information to the public and supports effective interaction with the academic community.

At the same time, one of the defining areas of state information policy, which covers all spheres of public life, remains ensuring information security. This concept refers to a set of organizational, legal, and technical measures aimed at protecting the national information space from internal and external threats. Information security issues have become particularly relevant in the context of hybrid aggression by the Russian Federation, which actively uses tools of disinformation, cyberattacks, and information and psychological operations.

In this regard, the key areas of state activity in the field of information security are ensuring cyber protection of information systems, countering propaganda influence, protecting critical information infrastructure, and creating effective mechanisms for secure storage and processing of information. At the same time, activities in the field of information security are aimed not only at protecting the information space of the state, but also at guaranteeing citizens

the right to access reliable information and ensuring objective information of society. Considerable attention is also paid to countering the spread of disinformation, strengthening social unity, protecting the information sovereignty of the state, and neutralizing negative information influences of both propaganda and psychological nature (Kochubey & Nekryach, 2025).

Specialized state bodies that perform the functions of coordination, control, and implementation of information protection measures play an important role in ensuring the information security of the state. In particular, the State Service for Special Communications and Information Protection of Ukraine organizes and practically implements measures to protect information with limited access, including in information and telecommunications systems. The main areas of activity of this body include the development of regulatory legal acts in the field of technical and cryptographic information protection, monitoring compliance with information security requirements, certification of appropriate means of protection, as well as coordination of actions of cyber defense entities in the event of cyber incidents or other threats (Matvienkiv & Lushagina, 2023).

A significant role in the cybersecurity system is also played by the Ministry of Internal Affairs of Ukraine, whose activities are aimed at combating cybercrime, protecting state information resources and ensuring the security of information systems. The powers of this body include the detection, prevention and investigation of offenses related to the use of information technologies, ensuring the protection of its own information systems, as well as interaction with other state authorities in the field of cyber defense. At the same time, the National Security and Defense Council of Ukraine performs the function of coordinating and controlling the activities of executive authorities in the field of ensuring the information security of the state. Its competence includes the formation of strategic directions of cybersecurity, determining priority measures for the protection of critical information infrastructure and making binding decisions on responding to information threats (Matvienkiv & Lushagina, 2023). Along with state institutions, public organizations and independent initiatives play an important role in countering disinformation. One example is the StopFake project, launched by public activists to identify and refute false information messages. Thanks to the activities of such initiatives, a prompt response to manifestations of disinformation and the dissemination of verified and reliable information among citizens is ensured (Gudz & Makovii, 2019).

In general, the state information policy of Ukraine is an important component of the general socio-economic strategy of the state and is aimed at

countering threats to national security. Its implementation is carried out on the basis of the principles of a democratic legal state, in particular, ensuring freedom of speech, preventing censorship, guaranteeing the right to access public information and protecting personal data. The practical implementation of such a policy is carried out through the relevant regulatory and legal system of the state.

The legal regulation of information security covers a set of legal norms that regulate social relations in the field of information use and determine the procedure for applying the relevant legal mechanisms in law enforcement practice. The regulatory and legal framework in this area includes a wide range of legislative and subordinate acts, including the provisions of the Constitution of Ukraine, doctrines, state strategies and programs that regulate the legal, institutional, socio-communicational and financial and economic aspects of information policy (Constitution of Ukraine, 1996).

An important element of this system is the Law of Ukraine “On Access to Public Information”, which is aimed at ensuring the openness of the activities of government bodies and increasing the level of transparency of public administration. This regulatory and legal act guarantees citizens the opportunity to obtain information that is at the disposal of state authorities, local governments, and other administrators, which contributes to the harmonization of national legislation with European standards of openness and democratic governance (On access to Public Information, 2011).

At the same time, the Law of Ukraine “On Information” establishes the basic principles of information activity and regulates relations related to access to information, its use and protection, ensuring a balance between the openness of information and the need for its protection. This is an important element of ensuring the information security of the state and the development of a democratic society (About Information, 1992).

In the context of countering modern information threats, the Law of Ukraine “On National Security of Ukraine” is also of great importance, as it forms the legal foundations of a comprehensive approach to protecting state sovereignty, including in the information sphere (On the Basic Principles of Ensuring Cybersecurity in Ukraine, 2017). At the same time, the Information Policy Strategy of Ukraine defines the main directions of forming an open, safe and informationally sovereign society, providing for ensuring freedom of speech, access to information, protection of the information space and countering information threats (Vitvitskyi *et al.*, 2022).

An essential element of modern legal regulation of the information sphere is also the Law of Ukraine “On Media”, which is aimed at creating a balanced and safe media environment, ensuring pluralism of opinions, democratic control over the activities of the mass media and protecting citizens from harmful information content. In the context of hybrid aggression and information influence from the Russian Federation, this law acquires special significance (On the Media, 2022).

The formation of a digital society in Ukraine is accompanied by significant transformational processes in the field of public administration, economy and legal regulation. Along with the positive results of the digitalization of the state, a number of political and legal challenges arise that require proper regulatory regulation, institutional support, and systemic management decisions. These issues have become especially relevant in the conditions of martial law, when digital technologies are actively used to ensure the functioning of the state, the provision of administrative services, and support for public communication (Farynnyk *et al.*, 2025).

One of the key challenges for the development of a digital society is the imperfection of the regulatory and legal framework in the field of digitalization. Despite the significant number of legislative acts regulating information relations, cybersecurity, electronic communications and electronic services, legislation in this area is often characterized by fragmentation and an insufficient level of systematicity. Individual norms do not fully correspond to modern technological realities and also require harmonization with European Union law. Another drawback is the lack of coherence between various regulatory and legal acts, which complicates their practical application

The solution to this problem should be to further improve the legislation in the field of digital transformation, in particular by developing a comprehensive codification of information legislation, harmonizing national norms with European Union law, as well as introducing modern legal mechanisms for regulating digital technologies, artificial intelligence, big data and electronic identification (Vitvitskyi *et al.*, 2022).

Another important challenge is ensuring an adequate level of cybersecurity and protection of the state's information infrastructure. The expansion of the use of digital technologies is accompanied by an increase in the number of cyber threats, in particular cyber attacks on state information systems, critical infrastructure, and electronic registries. In the context of armed aggression by the Russian Federation, cyberspace has become one of the key

areas of confrontation, which significantly increases the risks to national security (Leheza *et al.*, 2024).

Among the shortcomings in this area, one can single out the insufficient level of technical support of individual state bodies, limited resources for the development of cyber defense, as well as insufficient coordination between the subjects of the national cybersecurity system.

Overcoming these problems requires strengthening the institutional capacity of state bodies in the field of cybersecurity, developing a national cyber defense system, improving interdepartmental coordination mechanisms, and intensifying international cooperation in the field of countering cyber threats.

A significant challenge to the development of a digital society is the problem of digital inequality. Not all citizens have the same access to modern information and communication technologies, which can lead to restrictions on their ability to use electronic government services. This problem is especially acute in rural areas, as well as among socially vulnerable groups of the population (Filatov *et al.*, 2025).

The shortcomings in this area include the insufficient development of digital infrastructure in some regions, limited access to high-speed Internet, and low digital literacy among certain categories of the population. (Leheza *et al.*, 2025).

To overcome these problems, it is necessary to expand access to digital infrastructure, develop programs to improve citizens' digital competence, and provide alternative ways to receive public services for people who do not have the opportunity to use electronic services.

An important political and legal challenge is also ensuring an adequate level of protection of personal data and privacy in the digital environment. The expansion of the use of electronic services and digital platforms involves the processing of significant amounts of personal information, which requires effective mechanisms for its protection.

Among the shortcomings in this area are the insufficient harmonization of national legislation with European standards for the protection of personal data, in particular with the EU General Data Protection Regulation (GDPR), as well as insufficient awareness among citizens about their rights in the field of information protection (Leshchenko *et al.*, 2025).

Solving this problem involves improving legislation in the field of personal data protection, creating effective mechanisms for controlling information

processing, and raising the level of legal culture of citizens in the field of information security.

A separate challenge is the problem of countering disinformation and information manipulation. In the digital environment, information spreads extremely quickly, which creates favorable conditions for the spread of fake news, propaganda, and other forms of information influence.

The shortcomings in this area are the insufficient effectiveness of mechanisms for monitoring the information space, the complexity of legal regulation of the activities of digital platforms, and the need to ensure a balance between countering disinformation and respecting the principle of freedom of speech.

The ways to solve this problem are to develop the system of media literacy of the population, improve legislative mechanisms for countering disinformation, as well as expand cooperation between state bodies, civil society and international partners. Thus, the development of a digital society in Ukraine is accompanied by a number of political and legal challenges related to improving legislation, ensuring cybersecurity, overcoming digital inequality, protecting personal data and countering disinformation. Overcoming these problems requires a comprehensive approach that involves the modernization of legal regulation, the development of digital infrastructure, increasing the level of information security and the active participation of the state, civil society and international partners in the processes of digital transformation. (Bobkova *et al.*, 2021).

D. CONCLUSIONS

The formation of an information (digital) society in Ukraine is an important direction of modernization of public administration and development of democratic institutions. The conditions of martial law became a catalyst for the digital transformation of the state, which contributed to the accelerated development of e-government and the introduction of new digital services.

Digitalization made it possible to ensure the continuity of the functioning of state institutions, citizens' access to administrative services and effective communication between the state and society even in wartime.

At the same time, the further development of a digital society requires a comprehensive political and legal approach aimed at improving regulatory and legal regulation, increasing the level of information and cyber security, as well as

harmonizing Ukrainian legislation with European standards.

REFERENCES:

- About information: Law of Ukraine dated 02.10.1992 No. 2657-XII. Bulletin of the Verkhovna Rada of Ukraine. No. 48. P. 650
- Bobkova, A., Vitvitskyi, S., Zakharchenko, A., Nikolenko, L., & Katrych, A. (2021). Formation of scientific research competencies of law students. society. integration. education. *Proceedings of the International Scientific Conference, 1*, 38-49. <https://doi.org/10.17770/sie2021vol1.6484>
- Chorna, Alina. Leheza, Yevhen. Merdova, Olha. Vlasenko, Denys. Davlatov, Shavkat. 2023. Peculiarities of the principles of criminal and administrative law during the provision of the right to education in the conditions of the introduction of martial law: legal regulation and international standards. *Jurnal cita hukum indonesian law journal*. Vol. 11 No. 2, pp. 243-254, DOI: <https://doi.org/10.15408/jch.v11i2.32140>
- Constitution of Ukraine dated 28.06.1996 No. 254k/96-VR. Bulletin of the Verkhovna Rada of Ukraine. 1996. No. 30. P. 141.
- Farynnyk, V., Vitvitskyi, S., & Ponomarova, T. (2025). Improving the sanctions of the norms establishing criminal liability for criminal offences against property as a measure to ensure economic security of Ukraine. *Baltic journal of economic studies*, 11(1), 293-300. [HTTPS://DOI.ORG/10.30525/2256-0742/2025-11-1-293-300](https://doi.org/10.30525/2256-0742/2025-11-1-293-300)
- Filatov, V., Zuieva, O., Yefimova, I., Pylypenko, A., & Leheza, Y. (2025). Problems of legal protection of civilian persons deprived of personal liberty as a result of the armed aggression of the Russian Federation against Ukraine. *DIXI*, 27(1), 1-13. <https://doi.org/10.16925/2357-5891.2025.01.04> URL.: <https://revistas.ucc.edu.co/index.php/di/article/view/5212>
- Gudz O., Makovii V. Conceptual foundations of the formation of information policy of enterprises.
- Kobrusieva, Yevheniia. Leheza, Yevhen. Rudoi, Kateryna. Shamara, Oleksandr. Chalavan, Viktor. 2021. International standards of social protection of internally displaced persons: administrative and criminal aspects. *Jurnal cita hukum indonesian law journal*. Vol 9, No 3, 461-484. DOI: <https://doi.org/10.15408/jch.v9i3.23752>

- Kochubey L., Nekryach A. State information policy of Ukraine in the context of European integration. *Public Administration and Politics*. 2025. No. 4 (8). 1–9.
- Kulinich, Olha. Leheza, Yevhen. Zadyraka, Nataliia. Taranenko, Kseniia, Kostyuk, Tetiana. 2023. Electronic Judicial Procedure as an Element of Access to Justice Regarding Protection of Rights of Individuals: Legal, administrative, Theoretical and Informational Aspects. *Jurnal cita hukum indonesian law journal*. 11 (3), 443-456. DOI: <https://doi.org/10.15408/jch.v11i3.36298>
- Leheza, Y., Korniienko, M. ., Berezhniak, V., Mariienko A., & Radchuk, A. (2024). Legal Regulation of Liability for Illegal Deportation of Children: Administrative, Criminal Aspects, Experience of Ukraine and International Standards. *Revista Jurídica Portucalense*, 257–274. [https://doi.org/10.34625/issn.2183-2705\(36\)2024.ic-11](https://doi.org/10.34625/issn.2183-2705(36)2024.ic-11)
- Leheza, Y., Shcherbyna, Bogdan. Leheza, Yulia. Pushkina, Olena & Marchenko O. (2023). “Features of Applying the Right to Suspension or Complete/ Partial Refusal to Fulfill a Duty in Case of Non-Fulfilment of the Counter Duty by the Other Party According to the Civil Legislation of Ukraine.” *Revista Jurídica Portucalense*, 340–359. Retrieved from <https://revistas.rcaap.pt/juridica/article/view/29662>
- Leheza, Yevhen. Pisotska, Karina. Dubenko, Oleksandr. Dakhno, Oleksandr. Sotskyi, Artur. “The essence of the principles of ukrainian law in modern jurisprudence”. *Revista jurídica portucalense*, december, (2022): 342-363. [https://doi.org/10.34625/issn.2183-2705\(32\)2022.ic-15](https://doi.org/10.34625/issn.2183-2705(32)2022.ic-15).
- Leheza, Yuliia. Kuzmenko, Anatolii. Pashchenko, Oleksandr Tulyantseva, Valeriya. Leheza Yevhen. 2025. Sources of environmental law: National legislation of Ukraine and international legal documents. *Asian Journal of Water, Environment and Pollution*, 025160118 DOI: <https://doi.org/10.36922/AJWEP025160118> URL. https://accscience.com/journal/AJWEP/articles/online_first/5057
- Leshchenko, O., Krahlevych, V., Borysenko, A. , Leheza, Y. and Riabchynska, O. 2026. Legal definition of the cryptocurrency in Ukraine in international comparison. *Intersections. East European Journal of Society and Politics*. 11, 2 (Jan. 2026), 226–242. DOI:<https://doi.org/10.17356/ieejsp.v11i2.1311>. Available at: <https://intersections.tk.hu/index.php/intersections/article/view/1311>

- Matvienkiv S., Lushagina T. Information policy of higher education institutions in the context of the Russian-Ukrainian war. Scientific journal "Politicus". 2023. No. 5. 61–68. http://politicus.od.ua/5_2023/9.pdf
- Nesteryak Yu. Analysis of models of information policy and state regulation of mass media. Public administration and customs administration. 2016. No. 2 (15). 65–70.
- On access to public information: Law of Ukraine dated 13.01.2011 No. 2939-VI. Bulletin of the Verkhovna Rada of Ukraine. 2011. No. 32. P. 314
- On the Basic Principles of Ensuring Cybersecurity in Ukraine: Law of Ukraine dated 05.10.2017. № 2163-VIII. Bulletin of the Verkhovna Rada of Ukraine. 2017. № 45. P. 403.
- On the media: Law of Ukraine dated 13.12.2022 No. 2849-IX. Bulletin of the Verkhovna Rada of Ukraine. 2023. No. 47–50. P. 120
- Scientific Bulletin of Uzhhorod National University. 2019. No. 23. 65–69
- Sinkevych, O., Yurovska V., Komissarova, N., Tkachenko, O., & Leheza, Y. (2024). Subjects of public authority in matters of combating terrorism: legal regulation, administrative and criminal aspect. *Ius Humani. Law Journal*, 13(1), 1-14. <https://doi.org/10.31207/ih.v13i1.332>
- Vitvitskyi S., Andrieieva S., M., Stychynska, O., B. Karashchuk A., G., & Polovko, O. (2020). Social communication of public authorities in the system of potential manifestations of corruption. *Revista San Gregorio*, 1(42). <https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1547>
- Vitvitskyi, S., Nazymko, O., & Ponomarova, T. (2023). Economic component of the judicial career development system. *Baltic Journal of Economic Studies*, 9(4), 72-78. <https://doi.org/10.30525/2256-0742/2023-9-4-72-78>
- Vitvitskyi, S., Syzonenko, A., & Titochka, T. (2022). Peculiarities of corruption risk management in economic activity. *Baltic Journal of Economic Studies*, 8(3), 42-47. <https://doi.org/10.30525/2256-0742/2022-8-3-42-47>
- Zadyraka, Nataliia. Leheza, Yevhen. Bykovskyi, Mykola. Zheliezniak, Yevhenii. Leheza, Yulia. 2023. Correlation of Legal Concepts of Administrative Procedure and Administrative Liability in the Sphere of Urban Planning. *Jurnal cita hukum indonesian law journal*. Vol. 11 No. 1, pp. 33-44, DOI: <https://doi.org/10.15408/jch.v11i1.31784>