Zahoruiko Valerii, Postgraduate Student, National University of Civil Defence of Ukraine, Cherkasy, Ukraine, ORCID: https://orcid.org/0009-0009-1348-4503

STATE-ADMINISTRATION MECHANISMS FOR ENSURING THE SECURITY OF THE DIGITAL SPACE OF UKRAINE: MODEL AND INSTRUMENTS

Abstract

The article substantiates an integrated model of state-administration mechanisms for ensuring the security of the digital space of Ukraine. The relevance of the topic is determined by the transformation of digital space into an independent sphere of public administration, national resilience, critical infrastructure protection and interaction between the state, digital platforms, business actors and civil society. The paper proceeds from the premise that the security of digital space should be considered not only as a technical or cyber-protection task but also as a complex public-administration category connected with the stability, orderliness and controllability of digital relations under martial law and during post-war recovery.

The proposed model combines doctrinal, normative-legal, institutional, organizational-coordination, information-analytical, communication, personnel, control and international-cooperation mechanisms. It is based on the idea that digital space cannot be effectively governed by one centralized actor alone. Therefore, the model links strategic decision-making by state authorities with operational coordination, cooperation with owners of digital platforms, public-private partnership, civic participation, analytical monitoring of threats and international interaction. Particular attention is paid to the protective logic of public administration: state response must be oriented toward the defence of

public interests, digital sovereignty, critical information infrastructure, rights of citizens and the democratic order.

The practical value of the study lies in the development of recommendations for Ukrainian public administration: the formation of a unified state concept of digital-space security; the clarification of powers of responsible institutions; the creation of a stable coordination mechanism; the development of a digital-threat monitoring system; the institutionalization of cooperation with platforms and civil society; the strengthening of personnel capacity; and the use of transparent criteria for assessing proportionality and effectiveness of state response. The results may be used in public-administration research, strategic planning, cybersecurity policy and the preparation of practical recommendations for strengthening Ukraine's resilience in the digital environment.

Keywords: digital space, security of digital space, public administration, state-administration mechanisms, cybersecurity, digital platforms, public interests, Ukraine.

Problem statement. The full-scale war has radically changed the role of digital space in the functioning of the Ukrainian state and society. Digital platforms, electronic public services, communication networks, registers, information systems, cloud infrastructure and online interaction have become not auxiliary tools but essential conditions for the continuity of governance, defence, public services, economic activity and civic communication. At the same time, the same digital environment has become a field of hostile influence, cyberattacks, disinformation, manipulation of public opinion, attacks on critical infrastructure and attempts to undermine trust in public institutions.

Under such conditions, the security of the digital space of Ukraine becomes a direct criterion of state capacity. It shows whether public authorities can not only react to separate incidents but also create a stable system of prevention,

coordination, protection, recovery and communication. The traditional understanding of cybersecurity as a sectoral technical task is no longer sufficient. Digital threats affect public administration, national security, social stability, access to services, economic continuity, rights and freedoms of citizens and international cooperation. Therefore, the problem must be studied through the category of state-administration mechanisms.

In the context of this article, state-administration mechanisms for ensuring the security of digital space are understood as a coordinated set of normative-legal, institutional, organizational, analytical, communication, personnel, control and international instruments through which public authorities identify threats, organize interaction between actors, protect public interests, ensure the resilience of digital infrastructure and maintain the safe functioning of digital relations. This definition emphasizes that the security of digital space cannot be ensured by one ministry, one law, one technical system or one emergency response unit. It requires a cycle of strategic planning, operational coordination, data-based decision-making, cooperation with non-state actors and feedback from society.

The Ukrainian case is especially complex because the state has to combine rapid wartime response with long-term institutional modernization. On the one hand, public authorities must protect digital infrastructure and information resources in conditions of constant external aggression. On the other hand, Ukraine continues digital transformation, develops electronic services, integrates with the European digital space and prepares for recovery. This creates a practical contradiction: the digital environment must remain open, innovative and citizen-oriented, but at the same time it must be protected, resilient and controllable. The development of an integrated model of state-administration mechanisms is therefore both a theoretical and practical task.

Analysis of recent research and publications. The theoretical basis for studying digital space as an object of public administration is provided by research

on the legal order of digital space, digital platforms and models of regulation. T. E. Mehdiiev's dissertation is important because it demonstrates that digital space is characterized by transboundary communication, network interaction, technical complexity, high dynamics and the growing role of non-state regulation. This approach is relevant for public administration because it shows that the state cannot rely exclusively on centralized command methods when governing digital relations.

The protective dimension of the study is supported by A. V. Brutskiy's research on public order as a mechanism for protecting fundamental values of legal order. Although the present article does not use public order as a branch-law category, its logic is useful for defining the public-administration meaning of digital-space security. State intervention in digital space must be connected with the protection of fundamental public interests rather than with abstract expansion of administrative control. This makes it possible to distinguish necessary protective measures from excessive, fragmented or politically inconsistent reactions.

The doctrinal dimension is grounded in O. M. Kazakevich's research on legal doctrine in the development of national order. Its key value for this article is the idea that doctrines, concepts, strategic documents and scientific approaches form the intellectual basis of regulation and public policy. Applied to the digital sphere, this means that Ukraine needs not only separate legal acts on cybersecurity, information security or digital transformation but also a coherent doctrinal framework that explains how the state understands digital space, which interests it protects and how mechanisms of governance should interact.

Ukrainian normative and strategic documents also form an important background for the analysis. The Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine defines legal and organizational foundations for the protection of vital interests of individuals, society and the state in cyberspace. The

Cybersecurity Strategy of Ukraine for 2021-2025 emphasizes cyber resilience, deterrence and interaction, while the Information Security Strategy focuses on protection against information threats and hostile influence. These documents demonstrate that Ukraine already has significant components of the mechanism, but their practical integration remains a challenge.

International approaches confirm the need for multi-level and multi-actor governance. European cybersecurity policy, the NIS2 logic, ENISA analytical materials and NATO-oriented resilience approaches underline that cybersecurity is connected with governance, risk management, incident reporting, protection of essential services, cooperation with private operators and public trust. For Ukraine, this international context is not external; it is part of the practical environment in which the state builds interoperability, receives assistance, exchanges threat intelligence and moves toward European integration.

Despite the growing number of studies and strategic documents, there remains a need for an applied public-administration model that connects digital-space security with mechanisms, subjects, procedures and instruments. A considerable part of the literature focuses either on technical cybersecurity or on general digital transformation. The present article therefore concentrates on the question of how public administration should be organized: what mechanisms are necessary, how they interact, who is responsible for them and how state response can be made systematic, proportionate and effective.

Purpose of the article. The purpose of the article is to substantiate an integrated model of state-administration mechanisms for ensuring the security of the digital space of Ukraine and to define practical instruments for improving public administration in this sphere.

Presentation of the main material of the study. The proposed model is based on a transition from fragmented reaction to a full public-administration cycle. The starting point is the recognition of digital space as an independent object of state

administration. It includes not only networks and technologies but also digital platforms, data flows, public electronic services, online communication, digital markets, critical information infrastructure, activities of state bodies, private operators, citizens and civil society organizations. Security in this context means the protected, stable and ordered functioning of this environment in the interests of the state and society.

The first element of the model is the doctrinal block. It provides conceptual unity for the entire system. Without a doctrinal basis, different institutions may interpret digital threats, public interests and acceptable forms of intervention differently. The doctrinal block should define the meaning of the security of digital space, its relation to national security, cybersecurity, information security, digital transformation and protection of rights. It should also establish the value framework of governance: digital sovereignty, resilience, human dignity, public trust, continuity of services and democratic accountability.

The second element is the normative-legal mechanism. It creates the formal framework for action and defines powers, duties, procedures, standards and responsibility. This mechanism includes laws, presidential decrees, government resolutions, strategies, sectoral regulations, standards of critical infrastructure protection, rules for incident reporting, data-protection requirements and procedures for cooperation with private actors. Its effectiveness depends not only on the number of legal acts but also on their coherence. Fragmentation of definitions, overlapping competences and unclear procedures weaken administrative capacity.

The third element is the institutional mechanism. It determines who acts and how institutions interact. The strategic level includes the President of Ukraine, the National Security and Defence Council, the Verkhovna Rada and the Cabinet of Ministers. The sectoral and operational level includes bodies responsible for cybersecurity, digital transformation, communications, intelligence, law

enforcement, defence, protection of critical infrastructure and emergency response. Regional and local authorities are also important because digital services, public communication and infrastructure resilience are implemented in territories and communities.

A special feature of institutional security in digital space is the role of non-state actors. Owners of digital platforms, telecommunications providers, cloud-service providers, banks, energy companies, media organizations, IT companies, volunteer initiatives and civil society organizations possess resources and information without which the state cannot ensure security. Therefore, the institutional mechanism should not be reduced to a hierarchy of public authorities. It must include stable formats of public-private cooperation, information exchange, joint exercises, crisis communication and participation of expert communities.

The fourth element is the organizational-coordination mechanism. It transforms formal powers into practical interaction. Its instruments include interagency coordination groups, permanent working bodies, protocols of response to digital incidents, operational communication channels, procedures for escalation of threats, joint situational centres and coordination between national, regional and local levels. The main task is to prevent a situation in which each institution sees only its own sector while digital threats move across sectors, platforms and administrative borders.

The fifth element is the information-analytical mechanism. Digital-space security requires constant monitoring, early warning and evidence-based decision-making. This mechanism should include collection and analysis of information about cyber incidents, disinformation campaigns, vulnerabilities of digital services, threats to critical infrastructure, behaviour of hostile actors, public trust and the quality of institutional response. Analytical products must support both

strategic planning and operational decisions. They should be understandable for decision-makers and connected with clear response procedures.

The sixth element is the communication mechanism. In digital space, communication is itself a security instrument. Public authorities must explain risks, provide timely information during incidents, counter disinformation, inform citizens about protective behaviour and maintain trust in digital public services. Communication should be coordinated, transparent and adapted to different audiences. During war, silence, delay or contradictory messages may create panic, reduce trust and amplify hostile narratives. Therefore, communication cannot be separated from administrative coordination.

The seventh element is the personnel mechanism. The security of digital space depends on the competence of public officials, technical specialists, managers, analysts, communicators and local administrators. Ukraine needs not only cyber specialists but also public servants who understand digital risks, platform governance, data protection, crisis coordination and international cooperation. Personnel instruments should include professional training, certification, interagency exercises, reserve expert networks, cooperation with universities and mechanisms for attracting specialists from the private sector.

The eighth element is the control and evaluation mechanism. It ensures accountability and learning. Control should not be limited to formal inspection after incidents. It should include regular assessment of institutional readiness, audits of digital infrastructure, testing of continuity plans, evaluation of implementation of strategies, monitoring of response time and analysis of citizen feedback. The purpose of control is not punishment alone but improvement of the system. A mature mechanism identifies weaknesses before they turn into large-scale failures.

The ninth element is the mechanism of international cooperation. Digital space is transboundary, and many threats cannot be localized within the borders of

one state. Ukraine needs cooperation with the European Union, NATO partners, international organizations, foreign cybersecurity agencies, technology companies and donor programmes. This cooperation should cover threat intelligence, technical assistance, harmonization of standards, training, protection of critical infrastructure, countering disinformation and development of interoperable procedures. International cooperation strengthens national capacity but should be aligned with Ukrainian priorities.

The mechanisms described above should operate together. The doctrinal block defines meanings and values; the normative mechanism establishes rules; the institutional mechanism allocates roles; the organizational mechanism coordinates action; the information-analytical mechanism provides evidence; the communication mechanism maintains trust; the personnel mechanism creates capacity; the control mechanism ensures accountability; and international cooperation expands resources and interoperability. If one of these elements is weak, the whole model becomes vulnerable.

A key principle of the model is the combination of centralized strategic leadership with distributed implementation. In wartime conditions, the state must preserve the capacity for rapid decisions and unified priorities. At the same time, digital space is too dynamic and dispersed to be administered only through centralized commands. Effective governance requires a mixed democratic-security model in which the state defines strategic goals and protective standards, while platforms, private operators, communities and civil society participate in implementation, monitoring and feedback.

The protective logic of the model can be expressed through an administrative algorithm. First, the responsible actor identifies a digital threat or vulnerability. Second, the significance of the threat is assessed in relation to public interests, rights of citizens, critical infrastructure, state sovereignty and social stability. Third, the competent institution is determined. Fourth, possible response

instruments are compared according to effectiveness, proportionality, legality and impact on rights. Fifth, implementation is coordinated with relevant actors. Sixth, results are evaluated and the mechanism is adjusted.

This algorithm prevents both passivity and excessive intervention. It is not enough to say that digital space is threatened; public administration must identify what exactly is threatened, why the threat is significant, who must respond and which instrument is adequate. For example, a cyberattack on a public register, a disinformation campaign during an emergency and a vulnerability in a private platform require different combinations of legal, technical, communication and coordination measures. A proportional response strengthens security without destroying trust or innovation.

The model also requires differentiation of instruments according to the type of digital risk. Cyber incidents affecting critical infrastructure require technical response, emergency coordination and continuity of services. Disinformation campaigns require analytical monitoring, strategic communication and cooperation with media and platforms. Threats to public electronic services require service-resilience planning, backup solutions and user communication. Risks connected with digital platforms require cooperation with owners, transparency of moderation procedures and protection of users. Personnel deficits require training and institutional incentives.

For Ukraine, the regional and local levels deserve special attention. Communities increasingly depend on digital tools for administrative services, humanitarian coordination, warning systems, education, health care and communication with displaced persons. Regional authorities can identify local vulnerabilities, organize cooperation with infrastructure operators and communicate with citizens. Therefore, national mechanisms should be connected with regional digital-security plans, local incident protocols, training of municipal

officials and channels for reporting digital problems from communities to central institutions.

The practical application of the model can be illustrated by the security of digital public services. Electronic services increase accessibility and reduce administrative barriers, but they also create dependence on data protection, authentication, continuity of platforms and public trust. The normative mechanism defines rules; the institutional mechanism allocates responsibility; the organizational mechanism ensures response to failures; the analytical mechanism monitors incidents; the communication mechanism informs users; and the control mechanism evaluates resilience. Only the combination of mechanisms makes the service secure as a public-administration instrument.

Another example is interaction with global digital platforms. These platforms influence information flows, public debate, business communication and civic mobilization in Ukraine. The state cannot simply command them as subordinated institutions, but it also cannot ignore their role. An effective mechanism should include contact points, protocols for urgent requests, cooperation on disinformation and harmful content, transparency requirements where possible, and involvement of civil society experts. This reflects the mixed model of governance in which state authority is combined with negotiated and network forms of regulation.

An important requirement for the model is digitalization of governance itself. Public authorities need secure systems for data exchange, incident registration, monitoring of implementation, dashboards for decision-makers and channels for citizen feedback. However, digitalization should not be interpreted as a universal solution. It must be accompanied by clear procedures, responsible institutions, trained personnel and protection of personal data. Otherwise, new digital tools may reproduce old administrative fragmentation in a technological form.

Transparency and accountability are also necessary. Security policy often operates with sensitive information, but excessive secrecy can weaken public trust and reduce the quality of oversight. The state should distinguish between operational information that must remain protected and strategic information that should be publicly explained. Citizens and partners need to understand priorities, responsible institutions, general results of implementation and channels for reporting problems. This is especially important when digital-space security measures affect access to information, communication or public services.

The model changes the understanding of public administration in the digital sphere. The state is not only a regulator of technologies and not only a provider of electronic services. It is an organizer of a secure digital environment in which many actors interact. Its role is to set strategic priorities, protect public interests, coordinate participants, support resilience, ensure accountability and maintain balance between security, rights, innovation and openness. This balance is the central administrative challenge of Ukraine's digital development.

For practical implementation, the article proposes seven steps. First, Ukraine should develop a unified state concept or doctrine of digital-space security that connects cybersecurity, information security, digital transformation and public-administration resilience. Second, powers of key actors should be clarified in order to reduce duplication and gaps. Third, a permanent interagency coordination mechanism should be strengthened or created with clear procedures for ordinary monitoring and crisis response. Fourth, cooperation with digital platforms, telecommunications providers, critical infrastructure operators and civil society should be institutionalized.

Fifth, a national system of digital-threat monitoring and analytical support should be developed. It should combine technical indicators, administrative information, platform-related risks, communication threats and regional signals. Sixth, personnel capacity should be strengthened through specialized training for

public officials, regional administrators and managers of critical digital services. Seventh, control and evaluation should be linked with measurable indicators: response time, continuity of services, quality of communication, number of coordinated exercises, level of institutional readiness and public trust. This flexibility should also be institutionalized through periodic lessons-learned reports after major incidents, annual review of interagency protocols, and public discussion of non-sensitive results. In this way, adaptation becomes not an informal reaction of individual officials but a regular management procedure. Such an approach is important for Ukraine because wartime experience produces unique practical knowledge about cyber resilience, platform cooperation, digital public services and civic mobilization. If this knowledge is collected, assessed and converted into updated rules, the state will be able to strengthen digital-space security while preserving the advantages of innovation, decentralization and citizen-oriented digital transformation.

Finally, the proposed model should remain flexible. The digital environment changes rapidly: technologies, hostile tactics, platform policies, legal standards and social expectations evolve. A mechanism that is effective today may become insufficient tomorrow. Therefore, the model should include feedback, periodic revision of strategic documents, scenario planning and experimental instruments. Flexibility, however, should not mean randomness. It should be based on doctrine, clear public interests, institutional responsibility and evidence-based assessment.

Conclusion. The article substantiates an integrated model of state-administration mechanisms for ensuring the security of the digital space of Ukraine. The model is based on the understanding of digital space as an independent object of public administration and security as a state of protection, resilience, orderliness and controllability of digital relations in the interests of the state and society. The study shows that digital-space security cannot be reduced to technical cybersecurity or separate legal regulation.

The classification of mechanisms includes doctrinal, normative-legal, institutional, organizational-coordination, information-analytical, communication, personnel, control and international-cooperation components. Their combined use makes it possible to move from fragmented reaction to a full public-administration cycle. The model is built as a mixed democratic-security model: the state preserves strategic leadership and protective responsibility, while digital platforms, private operators, civil society, expert communities and international partners participate in implementation and feedback.

The practical recommendations include forming a unified doctrine or concept of digital-space security, clarifying institutional powers, strengthening interagency coordination, developing digital-threat monitoring, institutionalizing cooperation with platforms and civil society, improving personnel capacity and introducing evaluation indicators for effectiveness and proportionality of state response. Further research should focus on testing the proposed model in specific sectors and regions, developing measurable indicators of digital-space security and analysing how Ukrainian mechanisms can be harmonized with European standards while preserving national resilience priorities.

References

1. Verkhovna Rada of Ukraine. (2017). Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine No. 2163-VIII of 5 October 2017. https://zakon.rada.gov.ua/laws/show/en/2163-19

2. President of Ukraine. (2021). Decree No. 447/2021 On the Cybersecurity Strategy of Ukraine. https://www.president.gov.ua/documents/4472021-40013

3. National Security and Defence Council of Ukraine. (2021). Cybersecurity Strategy of Ukraine for 2021-2025. https://www.rnbo.gov.ua/en/Diialnist/4838.html

4. President of Ukraine. (2021). Decree No. 685/2021 On the Information Security Strategy. https://www.president.gov.ua/documents/6852021-41069

5. Verkhovna Rada of Ukraine. (2020). Decree of the President of Ukraine No. 392/2020 On the National Security Strategy of Ukraine. https://zakon.rada.gov.ua/laws/show/392/2020

6. Cabinet of Ministers of Ukraine. (2024). Ukraine Plan. https://me.gov.ua/Documents/Detail?lang=en-GB&id=8f3cae3c-10f7-4a5a-bf1f-6d9fc3f6b987

7. Ministry of Digital Transformation of Ukraine. (n.d.). Diia: Digital State. https://diia.gov.ua/

8. European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union.

9. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

10. NATO Cooperative Cyber Defence Centre of Excellence. (2024). National Cybersecurity Governance: Ukraine. https://ccdcoe.org/library/publications/

11. European Commission. (n.d.). Supporting Ukraine through digital. https://digital-strategy.ec.europa.eu/en/policies/support-ukraine

12. OECD. (2022). Public Governance in Ukraine: Implications of Russia's War. OECD Policy Responses. https://www.oecd.org/en/publications/public-governance-in-ukraine_c8cbf0f4-en.html

13. Mehdiiev, T. E. (2023). Legal order of digital space: dissertation for the degree of Candidate of Legal Sciences. Moscow State Law University named after O. E. Kutafin.

14. Brutskiy, A. V. (2026). Public order as a protective mechanism of fundamental values of legal order: dissertation for the degree of Candidate of Legal Sciences. Institute of Legislation and Comparative Law under the Government of the Russian Federation.

15. Kazakevich, O. M. (2024). Legal doctrine in the context of the development of legal order: dissertation for the degree of Candidate of Legal Sciences. Institute of Legislation and Comparative Law under the Government of the Russian Federation.

16. Goldsmith, J., & Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. Oxford University Press.