Vol. 08, No. 2 (2026) 1179-1190, doi: 10.24874/PES08.02B.008

Proceedings on Engineering Sciences

www.pesjournal.net

DIGITAL SYSTEMS ENGINEERING FOR MODERNIZING NATIONAL SECURITY MANAGEMENT FRAMEWORKS UNDER EUROPEAN STANDARDS

Anatolii Rachynskyi [1]
Vadym Torichnyi
Maksym Makarenko
Dmytro Tkachuk
Halyna Zavoritnya

Received 12.01.2026.
Revised 04.05.2026.
Accepted 21.05.2026.

Keywords:

Digital systems engineering, National security management, Critical infrastructure protection, Cyber defense systems, Institutional digital adaptation, European standards, Resilience engineering

A B S T R A C T

This study explores the application of digital systems engineering principles for modernizing national security management frameworks in alignment with European Union standards. The research focuses on the digital transformation of institutional and legal structures in public administration for national security, with particular emphasis on critical infrastructure protection and cyber defense systems.

Using formal-logical methods, including analysis, synthesis, modeling, and systematization, the study evaluates current frameworks and proposes pathways for integrating advanced digital technologies into security management processes. The analysis highlights the importance of multi-level institutional interaction and the adoption of EU digital standards to enhance system resilience and operational effectiveness.

The findings underscore the need for a comprehensive digital engineering approach that combines regulatory adaptation with technological integration to strengthen national security systems, especially in the context of post-conflict recovery. Practical recommendations are provided for developing integrated regulatory frameworks that enable effective participation of various institutions in digital security ecosystems.

© 2026 Published by Faculty of Engineering

1. INTRODUCTION

In a world where every independent country has the absolute right to independently formulate and implement its national security policy, a contradictory situation is emerging. In such a scenario, a mere allegation of a threat, even without convincing evidence, may be enough to justify any protective measures that the authorities deem necessary. European Union legislation includes a set of legal restrictions governing the cooperation of national legal systems of member states in the field of national security, and such norms require the unification

[1] Corresponding author: Rachynskyi
Email: l.hetmanenko@kubg.edu.ua

of public administration methods with an emphasis on the protection of human rights, combating discrimination and the formation of reliable institutional mechanisms against abuse of power (Riddervold & Rieker, 2024). For Ukraine, which is on the path of European integration, the application of these principles is not only a political commitment, but also a key component of building a modern, stable and technologically advanced national security system.

For Ukraine, this issue has become particularly acute due to the war started by the Russian Federation, which has radically transformed the country's security space and necessitated the immediate activation of defense mechanisms (Solovyov, 2025). They identified the need for rapid mobilization of resources and institutional capabilities, but at the same time revealed the urgent need to form a systematic, standardized, focused model of legal and institutional support for national security governance that meets the latest EU standards and requirements.

2. LITERATURE REVIEW

Studies by Barbou des Places (2024) and Ostapiak (2024) demonstrate that the harmonization of the legal framework of public administration with the EU legal acquis requires a comprehensive approach that combines institutional reforms with the technological modernization of public authorities, and the authors have identified a critical dependence of the effectiveness of such adaptation on the level of coordination between different sectors of public administration and the ability of national institutions to respond quickly to changes in the European legal framework. However, the issue of specific mechanisms for integrating digital technologies into the national security system remains insufficiently addressed, especially in the context of the simultaneous implementation of EU cybersecurity standards and the need to maintain sovereignty in making critical security decisions. Later on, Perotto (2023), Makedon et al. (2025), Vasiliauskienė et al. (2025) found in their studies that the introduction of digital technologies in the national security sphere requires the creation of new legal institutions capable of regulating the interaction between state and non-state actors in cyberspace. However, their findings did not address the issue of coordination between different levels of public administration in the process of implementing digital security standards, which leaves the problem of creating a unified national security management system in the context of decentralization and European integration unresolved. A significant contribution to the understanding of European approaches to security was made by Bywater et al. (2023), Groussot and Petursson (2024), Krap (2025), who analyzed the evolution of EU security policy and identified the principles of forming supranational mechanisms for coordinating national security systems However, scientists focus mainly on the experience of EU member states and do not consider the specific challenges faced by candidate countries.

Studies by Colombi Ciacchi et al. (2025) and Van Pinxteren (2024) on the development of a European cybersecurity strategy have identified key principles for the formation of common approaches to protecting the EU's digital infrastructure, including the creation of early warning mechanisms, coordination of incident response, and exchange of threat information. However, their work does not take into account the dynamics of threats and the evolution of technological capabilities of attackers, which leaves unresolved the issue of adapting European standards to the rapidly changing nature of modern cyberattacks and the need to ensure the flexibility of legal response mechanisms.

A comprehensive analysis of institutional reforms in the field of national security conducted by Ukrainian researchers Bazychenko (2024), Bondarenko et al. (2025), Oliinyk et al. (2024) showed that adapting the national security system to modern challenges requires a fundamental rethinking of the structure and functions of security institutions, the creation of new mechanisms for coordination between different agencies, and the introduction of modern information management technologies. However, scholars have insufficiently considered the practical implementation of European digital standards in the national security system and do not take into account the specific challenges associated with the simultaneous implementation of institutional reforms.

The analysis of the processes of digital transformation of public administration in the context of national security by Byelova and Goncharenko (2024), Pidbereznykh (2022) demonstrated that the introduction of digital technologies in the public administration sector creates new opportunities for increasing the efficiency of public services and improving coordination between different levels of government. However, their studies hardly take into account the specifics of adapting digital technologies in the field of national security in the context of the need to ensure simultaneous compliance with national security interests and international obligations to European partners.

In general, the analysis shows significant achievements in the study of certain aspects of the adaptation of legal and institutional mechanisms of public administration to digital challenges, but a comprehensive approach to the integration of European digital standards into the national system of national security remains insufficiently researched.

The aim of the article is to substantiate the ways of convergence and combination of legal and institutional practices of public administration in the field of national security of Ukraine with digital achievements and EU standards.

3. MATERIALS AND METHODS

The methodological framework is based on the use of a number of scientific tools, which ensured a comprehensive analysis of the issues under study and contributed to the formation of scientifically sound recommendations and theoretical generalizations. First of all, the methods of formal logic (decomposition, synthetic generalization, deductive conditions, inductive generalization, comparative analogy) were used for a detailed study of theoretical achievements and current scientific developments in the field of digitalization of public administration and national security.

Logical and semantic analysis was used for a detailed study and clarification of the terminological base of the scientific work. This made it possible to specify the content of a number of fundamental concepts, which guaranteed the conceptual transparency of the scientific presentation and excluded the possibility of terminological inconsistencies in substantiating theoretical positions and practical recommendations. Conceptual modeling and prospective analysis were also used to formulate practical recommendations for the modernization of the administrative and legal framework of the system of ensuring the national security of Ukraine in the context of digital transformation.

4. RESEARCH RESULTS

4.1 Legal framework and institutional constructs in the field of national security of Ukraine

In today's realities, when Ukraine is at the stage of active European integration and at the same time faces the need to modernize the national security infrastructure under the influence of digital transformations, the system of national security actors is considered not only as an institutional set of bodies, but also as a complex, symbiotically interconnected legal entity. The authors believe that its structure should be aimed at two strategic directions: first, achieving an adequate level of protection of all spheres of the state and society, and second, fulfilling the obligations arising from the process of approximation to the legal, institutional and technological standards of the European Union (Makedon et al., 2020).

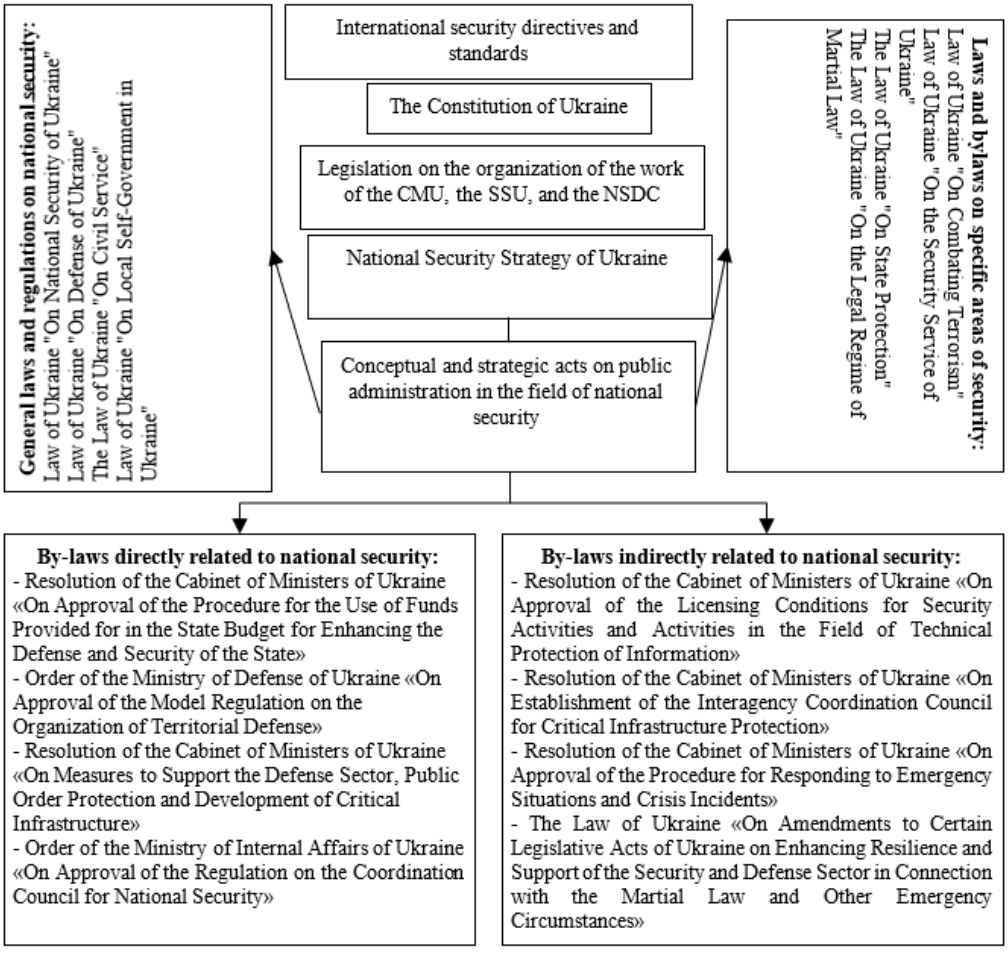


Figure 1. Legal and institutional framework of public administration of national security of Ukraine
Source: developed by the authors

The legal framework that determines both Ukraine's strategic course of integration into the European and Euro-Atlantic space and the subjective composition of the national security system is the Constitution of Ukraine. Its preamble emphasizes the strengthening of civil harmony, confirmation of the European identity of the Ukrainian people and the irreversibility of the course toward membership in the European Union and NATO. The constitutional provisions enshrine the role of the President of Ukraine as the guarantor of the implementation of this strategic course and define the key institutions that ensure national security: The Ukrainian people, military formations, law enforcement agencies, the Verkhovna Rada of Ukraine, the President, the Cabinet of Ministers, and the National Security and Defense Council (Bobro, 2024).

A study of the evolution of legislation shows that the Law of Ukraine "On the Fundamentals of National Security of Ukraine" contains a clear list of security actors, including supreme authorities, law enforcement and intelligence agencies, local governments, judicial institutions, specialized bodies and even citizens. In contrast, the current Law on National Security of Ukraine does not provide for a separate article dedicated exclusively to security actors, but indirectly outlines the range of relevant institutions through the definition of security and defense forces, their tasks and competencies. To clearly define and analyze the institutional composition of the system of security actors in the context of European integration, the authors should refer to a set of basic legal acts: The Constitution of Ukraine, the current laws "On National Security of Ukraine" and "On the National Security and Defense Council of Ukraine", the National Security Strategy of Ukraine, the State Security Strategy, which already provide the basis for the list of subjects by functional areas: lawmaking (Verkhovna Rada of Ukraine, the President), coordination (NSDC, the Cabinet of Ministers), control (NSDC, the Cabinet of Ministers, civil society institutions), executive (central bodies of executive power, security forces, special services).

After the decision of the European Council on June 23, 2022, to grant Ukraine the status of a candidate for membership in the European Union, there was a need to urgently form a comprehensive mechanism for the implementation of additional obligations of the state, which include not only the harmonization and full adaptation of national legislation to the EU acquis (Bazychenko, 2024). The adoption on July 29, 2022, of the Verkhovna Rada Resolution No. 2483-IX "On Certain Measures to Fulfill Ukraine's Obligations in the Field of European Integration" should be considered a regulatory step that prioritizes the tasks of bringing Ukrainian legislation in line with the provisions of EU law (Table 1) (Byelova & Goncharenko, 2024).

Table 1. Ensuring the National Security of Ukraine in the Leveled Format of Interaction of Public Administration Institutions

Level of interaction	Institutions	Tasks	Tools	Expected results
Strategic	Cabinet of Ministers, National Security and Defense Council	Identification of national security priorities	Strategic planning, legislative initiatives	Unified security policy synchronized with the EU
Operational	Ministry of Internal Affairs, Security Service, Ministry of Defense	Coordination of response to threats	Digital platforms, secure communication channels	Rapid response to crises, cyberattacks
Regional	Regional administrations, local councils	Adaptation of national strategies to local conditions	Interagency working groups, local plans	Strengthening regional resilience
International	MFA, missions to the EU	Integration with European security structures	Diplomatic agreements, participation in EU programs	Integration into European security mechanisms
Public	Public organizations, media	Ensuring transparency and engagement of citizens	Information campaigns, public monitoring	Increasing trust in security institutions

The authors propose an expanded vision of the system of security sector actors that includes three interrelated groups: 1) bodies of strategic and managerial activities, 2) performers of practical tasks, and 3) institutions and individual actors involved in ensuring national security. The approach itself forms the basis for a clearer distinction between the political, managerial and operational levels of the system's functioning. At the strategic level, the political foundations of national interests are formed, which are reflected in documents, programs and digital roadmaps for the development of the security sector, and transformed into specific goals and objectives. At the executive level, there are both specialized actors (e.g., the Security Service of Ukraine, the State Service for Special Communications and Information Protection) and general actors (courts, local self-government bodies), and many of them, especially line ministries, may simultaneously belong to several levels depending on the nature and content of their powers.

4.2 EU experience in developing standards and principles of group security

As part of the adaptation to EU digital standards, a special place is occupied by the implementation of norms and

technical requirements set out in documents such as Directive (EU) 2022/2555 (NIS 2 Directive) on measures for a high common level of cybersecurity, Regulation (EU) 2016/679 (GDPR) on the protection of personal data, Directive (EU) 2016/1148 on the security of network and information systems, as well as other regulations that define requirements for the protection of critical infrastructure, incident response and the establishment of national cyber threat exchange centers. Their implementation in Ukrainian legislation involves not only the adoption of new laws and amendments to existing ones, but also the creation of institutional structures to technically ensure the implementation of these norms, including national computer incident response teams (CERT-UA), cyber defense centers in government agencies, and a system of state monitoring of cyber threats (Mader et al, 2024). This set of reasons leads to a significant increase in the burden on the budget system and an increase in public debt, when the situation itself requires a fundamental revision of the mechanisms for forming the revenue base and redistribution of EU budget expenditures, as well as the search for new, more innovative tools and sources of funding, including digital administration tools (Figure 2).

Nevertheless, in 2014-2024, there was a relative stability in the dynamics of own resources and national contributions of the Member States to the EU budget. The revision of the budgetary architecture, driven by pandemic and military factors, has led to a significant change in the EU's financial priorities for 2021-2027 (European Commission, 2024).

The relationship between adaptation and reforms in Ukraine's security and defense sector is direct and mutually reinforcing. The reforms carried out as part of the European integration course, in particular, the implementation of the Law of Ukraine "On National Security", reform of the defense forces management system, and creation of a modern cyber defense system, are aimed at integration with the European security system. NATO and EU-compatible command, control and data exchange standards should be implemented, which, in turn, requires synchronization of national procedures with European digital security protocols (Organization for Economic Co-operation and Development, 1999).

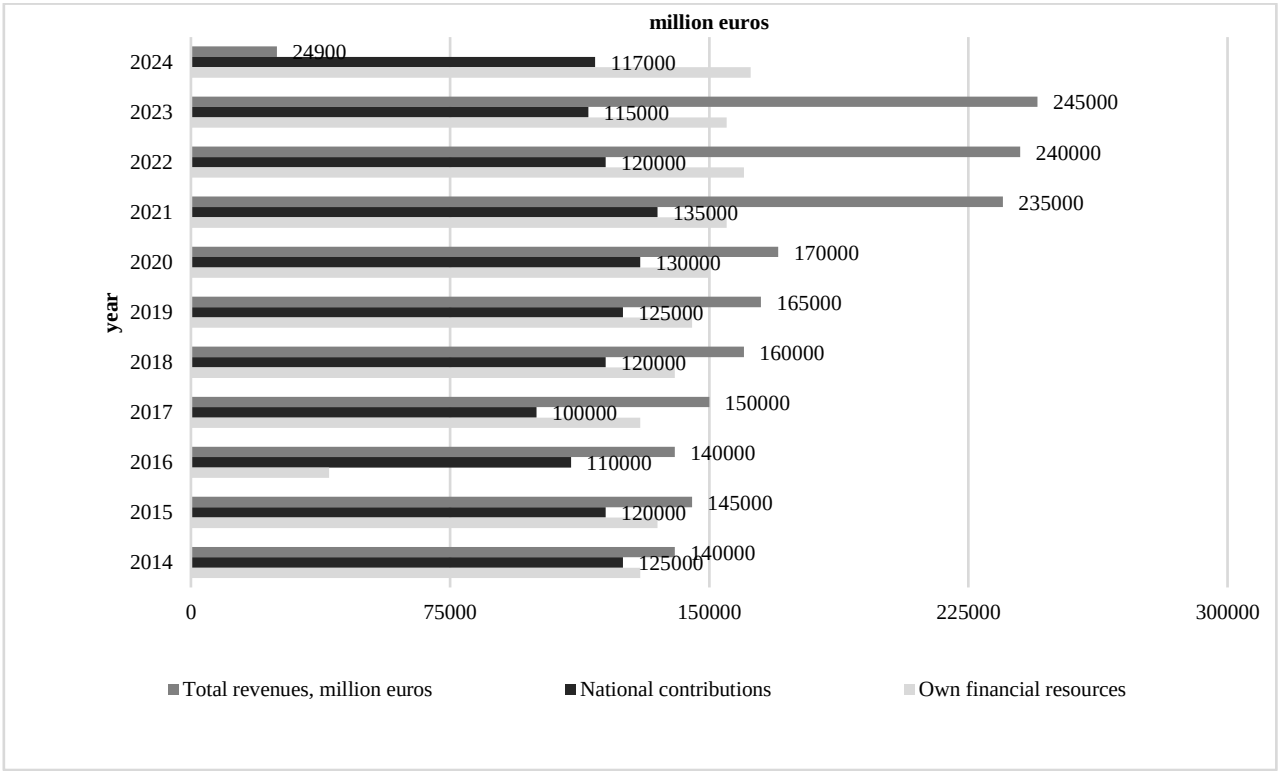


Figure 2. Dynamics of the formation of own financial resources of the EU member states to ensure their own security in 2014-2024, million euros

Source: based on (European Commission, 2025)

The legal framework of Ukraine should enshrine a comprehensive definition of the term "civil society institutions" as associations of citizens, organizations or individuals that voluntarily participate in ensuring national security, including activities in the cybersphere, critical infrastructure protection, information security, countering disinformation and hybrid threats, as well as in civil and territorial defense, taking into account the EU experience, where non-state actors are integrated into the security sector at the institutional level through regulatory frameworks.

The adaptation of the institutional model should be carried out through the process of forming a unified legal mechanism for involving public and private entities in the implementation of digital security and cyber defense tasks that meets EU standards, in particular Directive (EU) 2022/2555 (NIS 2) (Directive (EU) 2022/2555, 2022) and Regulation (EU) 2016/679 (GDPR) (Regulation 2016/679, 2016), which provides for the implementation of unified procedures for incident reporting, personal data protection, information exchange between authorized bodies and critical infrastructure entities, as well as standardization of cyber threat response protocols to be applied by both state and non-state actors in the security sector. To this end, it is advisable to create a centralized coordinating body in Ukraine – the National Center for National Security Cooperation Management – that would combine the functions of risk analysis, threat forecasting, coordination of joint operations, as well as management of resources and technological platforms to ensure the continuity of critical systems (Weerts, 2025).

In the context of the digital transformation of the security sector, it is necessary to envisage the adaptation of European standards of strategic communications to Ukrainian realities, including the development and implementation of a single national standard for training specialists in the field of security and defense communications, similar to STANAG (Standardization Agreement) and STANREC (Standardization Recommendation), which are used in NATO. It is necessary to legislate the principles of information interaction between government agencies and public institutions in the context of crisis communications, including countering disinformation and information attacks, defining response algorithms, communication channels and the procedure for coordinating public statements, which will create an integrated information and communication response system compatible with European protocols (European Commission, Directorate-General for Structural Reform Support, 2021).

In practical terms, the adaptation of the legal and institutional framework for the interaction of state and public institutions to the EU's digital challenges involves: 1) creation of mechanisms for collective cyber risk management, in particular through joint incident monitoring and response centers; 2) implementation of a system for assessing critical infrastructure vulnerabilities with the involvement of independent auditors and public experts; 3) integration of public structures into the planning and implementation of national and regional security programs; 4) formation of a regulatory framework for digital information exchange between state and non-state actors in the security sector; 5) ensuring transparent procedures for public-private.

Table 2. Digital Convergence of the Legal and Institutional Framework of Ukraine and the EU for the Development of Ukraine's National Security System

Strategic vector	**Institutional task**	**Measures implemented**	**Result for the public sector**	**Compliance with EU standards**
Cybersecurity	Ensuring cyber resilience	Establishment of CERT-UA, implementation of NIS 2 and GDPR standards	Secure digital infrastructure, rapid response to incidents	Compliance with Directives (EU) 2022/2555 and 2016/679
Legal harmonization	Unification of terminology	Enshrining the term “legislative approximation” in regulations	Elimination of legal conflicts, clarity in the implementation of international obligations	Compatibility with the acquis communautaire
Institutional coordination	Establishment of a coordination center	Establishment of the National Center for Interaction Management	Unified system for monitoring and responding to threats	Integration with European cybersecurity centers
Public institutions	Involvement of non-governmental organizations	Normative regulation of participation of civil society organizations in security	Transparent distribution of competencies, public-private partnership	Compliance with EU practices on integration of non-state actors
Civil-military cooperation	Promotion of the private sector	Legislative regulation of companies' participation in defense technologies	Development of digital defense technologies, transparent procurement	Compatibility with EU directives on defense procurement
Strategic communications	Countering disinformation	Implementation of communication standards based on the example of the STANAG platform	Integrated system of response to information attacks	Compliance with European crisis communication protocols

Source: based on (Dermine, 2024, European Civic Forum & Civic Space Watch, 2021)

The proposed measures need to be enshrined in a comprehensive legal act, such as the Law of Ukraine on the Participation of Non-Governmental Institutions in National Security, which would define the legal status, powers, responsibilities and guarantees of such institutions, as well as the conditions for their integration into the national security management system, including digital components, mechanisms of communication and interaction with state authorities, international partners and the public.

4.3 Ways to develop the legal and institutional framework for public administration of national security based on the implementation of the EU digital experience

The interconnected concept of "mutual resilience" in the modern sense of the European Union should be considered as a key basis for building a new partnership architecture in the field of global preparedness, which directly relates to the tasks of public administration of national security of Ukraine to digital challenges and EU standards. Supporting mutual resilience also involves expanding and diversifying the diplomatic and security formats in which Ukraine can participate with the EU, including mechanisms for collective response to cyberattacks, hybrid threats, information operations, and other manifestations of digital aggression. This requires not only institutionalizing the relevant forms of coordination, but also integrating digital data analysis tools and automated early warning systems into the public administration of national security.

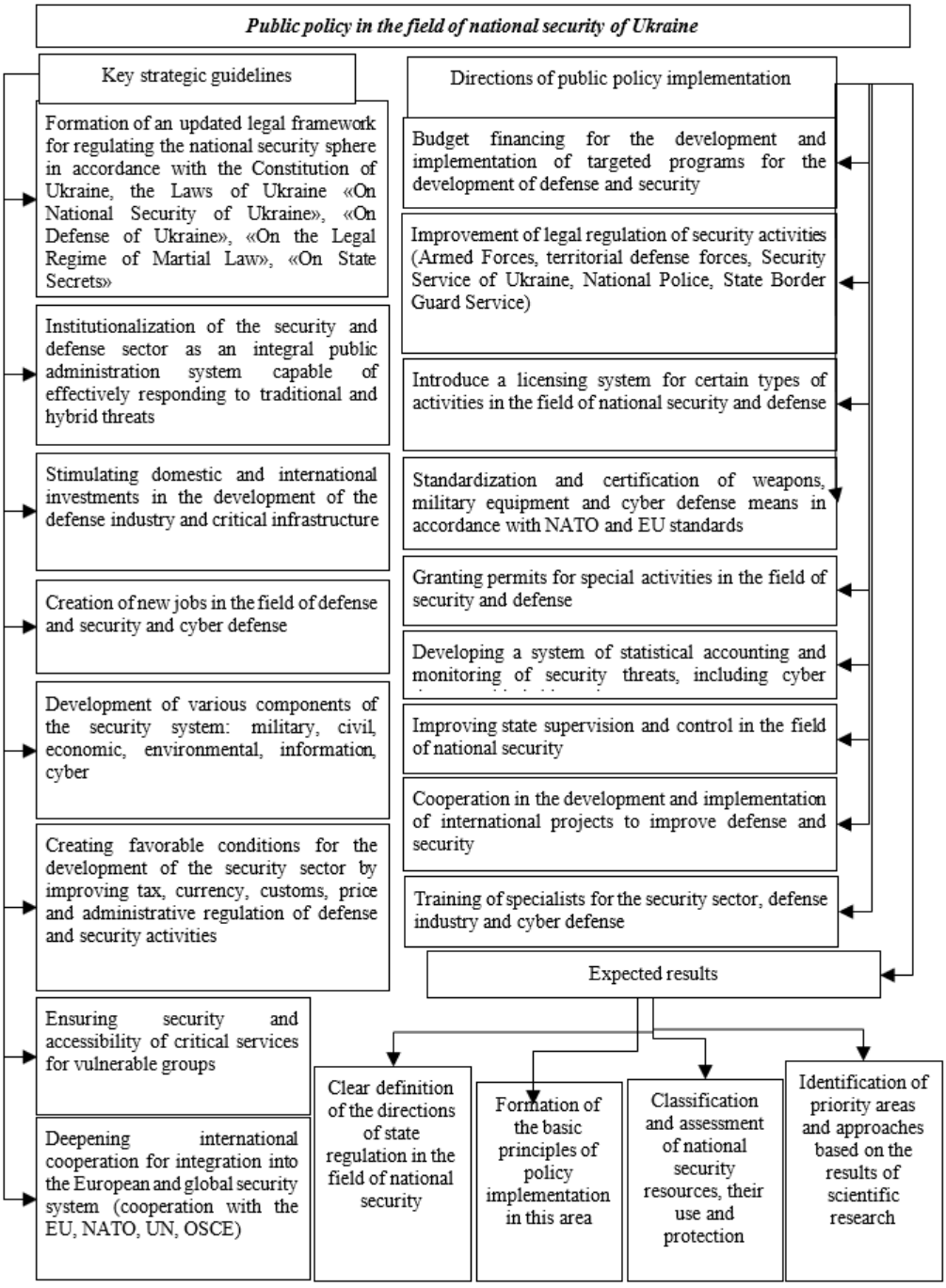


Figure 2. A new structural and functional model of public policy development in the sphere of national security of Ukraine for interaction with the EU
Source: developed by the authors

Examples of specific instruments that can be adapted to the Ukrainian context are the new EU Migration and Asylum Pact, which introduces a binding but flexible system of solidarity between member states in cases of migration crises, and the European Food Security Crisis Preparedness and Response Mechanism (EFSCM), which functions as a monitoring and coordination platform. Further adaptation to Ukrainian conditions involves the creation of integrated digital migration and food risk management systems that would meet European data protection standards and ensure interaction with relevant EU structures (Groussot & Petursson, 2024).

Table 2. Measures to ensure Ukraine's national security based on EU achievements

Area of implementation	**Strategic goal**	**Specific measures**	**Expected public results**	**Compliance with EU standards**
Digital security	Ensuring cyber resilience	Implementation of EUCCS-compliant digital crisis management platforms and secure communication channels	Resilient information infrastructure, protection against cyber attacks	Compliance with European cyber legislation, integration with EuroQCI
Crisis management	Improving preparedness for complex crises	Establishment of a national coordination center based on the ERCC model	Rapid response to crises, integration with European structures	Compatibility with IMERA, rescEU
Strategic planning	Synchronization with European standards	Adaptation of the legal framework to EU norms in the field of strategic planning	Full compatibility with European information exchange mechanisms	Compliance with the EU principles of mutual sustainability
Cross-sectoral coordination	Strengthening cooperation with the EU	Participation in programs of collective response to hybrid threats	Effective counteraction to information operations and cyber attacks	Integration with European digital platforms
Infrastructure resilience	Modernization of critical infrastructure	Implementation of Global Gateway elements for digital and energy infrastructure	Ensuring business continuity in key sectors	Compliance with EU technical regulations
Humanitarian security	Support for vulnerable groups	Adaptation of the EU Migration Pact and EFSCM to manage migration and food risks	Protection of human rights, effective crisis response	Compliance with EU humanitarian aid policy

Source: developed by the authors

Special attention should be paid to the Global Gateway initiative, which focuses on the development of digital, energy, transport and educational infrastructure, which directly correlates with the task of modernizing Ukraine's national security system based on digital technologies and in accordance with EU norms and technical regulations. Other instruments that can be used in the process of adapting Ukrainian legislation include the EU's Internal Market Emergency and Resilience Act (IMERA), which establishes coordination and crisis management mechanisms to maintain the functioning of the single market even in the face of large-scale disruptions. In the Ukrainian context, the implementation of a similar model could mean the creation of a single digital coordination center for managing the supply chains of critical goods and services, integrated with European systems and capable of ensuring their continuity in crisis situations (Figure 2) (Koshykov, 2021).

The European Commission's Emergency Response Coordination Center should be considered as an exemplary model of an integrated institutional and digital platform, the adaptation of functional and technological principles of which to the national conditions of Ukraine can ensure the creation of a highly effective, round-the-clock and multi-level coordination center for public administration of national security, capable of providing prompt interagency response to complex crises using digital management tools.

The structure of the national center should reflect the key elements of the ERCC (Emergency Response Coordination Center) model, including the ability to coordinate responses to multi-component crises, both long and protracted (including the consequences of military aggression and internally displaced persons) and short-lived (floods, large-scale fires, power grid failures, etc.). Using digital platforms for logistics management and real-time information exchange, as well as interaction with counterparts in the EU to jointly manage cross-border challenges and coordinate consular protection of Ukrainian citizens abroad by combining the functions of diplomatic missions and digital crisis response services (Krap, 2025).

The implementation of the national European Critical Communications System in a format compatible with the EUCCS (European Union Common Criteria-based cybersecurity certification scheme) requires the creation of an integrated, resilient and secure telecommunications environment that will guarantee the continuity of key sectors of public administration, defense, healthcare, energy and transport in the event of large-scale emergencies, cyberattacks or physical destruction of infrastructure. For this purpose, it is advisable to envisage the following use of the IRIS satellite constellation with low- and medium-orbit channels that will ensure stable

and secure connection of government agencies and military units in any circumstances, as well as support coordination between government agencies and the population in areas where ground-based communication infrastructure is out of order (Table 2) (Barbou des Places, 2024).

In addition, the integration of elements of the European Quantum Communications Infrastructure (EuroQCI) into the national system will create opportunities to ensure the highest level of data protection, prevent interception and increase the resilience of communication channels between government agencies, data centers, medical institutions and critical infrastructure operators. This platform will be used to implement digital security services that are compatible with European ones and will ensure compliance with EU requirements in the field of cyber defense and critical information infrastructure protection.

5. DISCUSSION

In general, the study confirmed and in a number of aspects clarified and expanded the scientific achievements of the researchers who studied the issue in accordance with the goal. In particular, common positions were found with the works of Barbou des Places (2024) and Ostapiak (2024), where the emphasis was on combining institutional changes with technological innovations to harmonize Ukrainian legislation with European legislation. The findings emphasized the relevance of aligning lawmaking, coordination and executive institutions with European standards, and specified that this can be achieved through clear functional division of security actors and the creation of a specialized National Center for Interaction Management.

At the same time, the results of the study developed the previous ideas of Perotto (2023) and Makedon et al. (2025), supplementing their proposals for the legal consolidation of the role of non-state institutions in the national security system through a separate comprehensive legislative act. In contrast to approaches that focus exclusively on government agencies, the paper highlights the effectiveness of involving NGOs, research centers, and the private sector in cyber defense and crisis response, which is in line with the European model of public-private partnership. A comparative analysis with the studies of Groussot and Petursson (2024), Colombi Ciacchi et al. (2025) revealed a specific similarity of views on the need to harmonize technical standards and legal instruments for cybersecurity. However, the model of integration of European digital standards into the system of multilevel institutional interaction in Ukraine proposed in this paper introduces an element of novelty. The scientific originality lies in the concept of “mutual resilience” as a basic principle for creating a common European-Ukrainian security architecture.

The practical significance of the study is manifested in the development of mechanisms for the implementation of European digital tools, from crisis communication protocols to quantum-secure communication systems in the Ukrainian practice of national security management. These positions are in line with current trends in the digital transformation of public administration (Byelova & Goncharenko, 2024), but also offer specific organizational and legal solutions for their effective implementation in wartime and post-war conditions. Thus, the results obtained not only confirm the relevance of existing scientific approaches, but also fill them with new theoretical and applied developments that expand the boundaries of scientific discourse and can become the basis for reforming the Ukrainian security sector in accordance with European standards.

6. CONCLUSION

It is found that the system of legal and institutional support for public administration of national security of Ukraine is a complex, multi-level structure that unites constitutionally established strategic management bodies, coordination, control, executive and scientific and analytical institutions. The analysis of the evolution of the regulatory framework in the field of national security has shown a clear trend of transition from a formal list of security agencies to a functionally oriented model, in which the institutional architecture is determined not so much by the presence of certain structures as by their powers, competencies and real contribution to security. To increase the efficiency of management, it is proposed to clearly delineate competencies between different levels and actors of the security system, which will help to avoid duplication of functions, increase responsibility and promote Ukraine's deeper integration into the European security space.

Proposals have been developed to harmonize Ukrainian legislation with European standards in the field of cyber defense. In particular, it is proposed to create a unified national system for responding to cyber incidents, standardize procedures for exchanging threat data, and implement European crisis communication protocols to ensure a rapid and coordinated response to emergencies. The study found that the successful adaptation of Ukraine's legal and institutional system of national security management to digital challenges and European standards requires the introduction of the concept of “mutual resilience”.

The potential for integration of the Ukrainian national security system into European platforms for crisis communications, cyber defense and strategic planning is assessed. It is established that these steps should form not only technical compatibility, but also the unification of procedures, data exchange standards and response algorithms in line with EU requirements. It is also proposed to develop a comprehensive legal act that would systematize the requirements for digital security, crisis management and intersectoral coordination in accordance with European standards.

References:

Barbou des Places, S. (2024). Introduction: Public order and public security in EU law. Time for reappraisal. *European Papers*, *9*(3), 1316–1328. Retrieved from https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2024_SS4_1_S%C3%A9gol%C3%A8ne_Barbou_des_Places_00811.pdf

Bazychenko, V. (2024). Basic principles of ensuring public administration in the field of national security at the present stage. *Scientific Collection "InterConf"*, 109–116. Retrieved from https://archive.interconf.center/index.php/conferenceproceeding/article/view/6466

Bobro, N. (2024). Key factors and structures of the development of the digital transformation of the economy. *Věda a Perspektivy*, *1*(32), 9–14. https://doi.org/10.52058/2695-1592-2024-1(32)-9-14

Bondarenko, S., Niziaieva, V., Kravchenko, M., Kaliuha, Y., Kolisnichenko, R., & Tsumariev, M. (2025). Modernization of administrative control over the legality of decisions of local selfgovernment bodies of Ukraine. *Evropský Politický a Právní Diskurz*, *12*(1), 31–44. https://doi.org/10.46340/eppd.2025.12.1.4

Byelova, L., & Goncharenko, G. (2024). Administrative and legal framework of public administration under martial law and emergency situations: Challenges and reform prospects. *Theory and Practice of Public Administration*, *2*(79), 421–441. https://doi.org/10.26565/1727-6667-2024-2-22

Bywater, M., Jefferies, I., & Kitchener, M. (2023). *Civil society landscape in the European Union: Research in support of the Citizens, Equality, Rights and Values (CERV) Programme* (Report to Directorate-General for Justice and Consumers, European Commission). Publications Office of the European Union. https://doi.org/10.2838/884239

Colombi Ciacchi, A., Lane, L., Nowak, T., & Flórez Rojas, L. (Eds.). (2025). *AI and public administration: The (legal) limits of algorithmic governance* [Final JuLIA Handbook]. JuLIA Project / European Commission. Retrieved from https://www.julia-project.eu/sites/default/files/2025-05/Final%20Handbook_%20AI%20and%20Public%20Administration_%20The_%28legal%29_limits_of_algorithmic_governance.docx.pdf

Dermine, P. (2024). EU fiscal capacity - Legal integration after COVID-19 and the war in Ukraine. *Journal of Contemporary European Studies*, *32*(1), 301–302. https://doi.org/10.1080/14782804.2023.2254643

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). (2022). *Official Journal of the European Union*, *L 333*, 80–152. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

European Commission, Directorate General for Structural Reform Support. (2021). *Supporting public administrations in EU Member States to deliver reforms and prepare for the future* (Commission Staff Working Document No. SWD(2021) 101). Publications Office of the European Union. Retrieved from https://commission.europa.eu/system/files/2022-12/supporting_public_administrations_in_eu_ms_to_deliver_reforms_0.pdf

European Commission. (2024). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2024 Rule of Law Report – The rule of law situation in the European Union* (COM(2024) 800 final). Retrieved from https://commission.europa.eu/document/download/27db414358b44b61a021a215940e19d0_en?filename=1_1_58120_communication_rol_en.pdf

European Commission. (2025). *EU spending and revenue 2021–2027* [Interactive chart]. Retrieved from https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/2021-2027/spending-and-revenue_en

Groussot, X., & Petursson, G. T. (2024). Public security and public order in EU law: Adjudicative challenges in the laws of the internal and digital markets. *European Papers*, *9*(3), 1386–1406. Retrieved from https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2024_3_24_SS4_4_Xavier_Groussot_Gunnar_Thor_Petursson_00814.pdf

Koshykov, D. (2021). Place of administrative law provisions in legal framework for implementing public policy on economic security of the state. *Entrepreneurship, Economy and Law*, (10), 43–49. https://doi.org/10.32849/2663-5313/2021.10.07

Krap, A. (2025). Modern concepts of national security: A comparative analysis of the US, EU and Ukraine models. *Public Management and Policy*, *2*(6). https://doi.org/10.70651/3041-2498/2025.2.03

Mader, M., Gavras, K., Hofmann, S. C., Reifler, J., Schoen, H., & Thomson, C. (2024). International threats and support for European security and defence integration: Evidence from 25 countries. *European Journal of Political Research*, *63*(2), 433–454. https://doi.org/10.1111/1475-6765.12605

Makedon, V. V., Valikov, V. P., & Koshlyak, Y. Y. (2020). The global labor market in the coordinates of the digital economy. *Academic Review*, *1*(52), 91–104. https://doi.org/10.32342/2074-5354-2020-1-52-9

Makedon, V., Trachova, D., Myronchuk, V., Opalchuk, R., & Davydenko, O. (2024). The development and characteristics of sustainable finance. In A. Hamdan (Ed.), *Achieving sustainable business through AI, technology education and computer science* (Studies in Big Data, Vol. 163, pp. 373–382). Springer. https://doi.org/10.1007/978-3-031-73632-2_31

Oliinyk, S., Kovalevska, I., Leschynsky, V., Kroitor, V., & Adamovsky, V. (2024). The influence of European integration processes on safeguarding human rights and basic rights in Ukraine. *Evropský Politický a Právní Diskurz*, *11*(5), 15–23. https://doi.org/10.46340/eppd.2024.11.5.2

Ostapiak, V. (2024). Effective public administration and national security in the context of the deep state. *Coordinates of Public Administration*, *1*, 402–419. https://doi.org/10.62664/cpa.2024.01.18

Perotto, G. (2023). The legal framework of the EU defence industry and the pursuit of strategic autonomy. *European Papers*, *8*(1), 475–486. Retrieved from https://www.europeanpapers.eu/europeanforum/legal-framework-eu-defence-industry-and-pursuit-strategic-autonomy

Pidbereznykh, I. (2022). Administrative and legal framework for the national security of the United States with Southeast Asian countries during B. Obama's presidency. *Entrepreneurship, Economy and Law*, (2), 71–75. https://doi.org/10.32849/26635313/2022.2.11

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union*, *L 119*, 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Riddervold, M., & Rieker, P. (2024). Finally coming of age? EU foreign and security policy after Ukraine. *European Security*, *33*(3), 497–516. https://doi.org/10.1080/09662839.2024.2376616

Solovyov, Y. (2025). From parallel trajectories to joint strategy: Models of effective integration of military and civilian security expertise. *Pressing Problems of Public Administration*, *1*(66), 363–382. https://doi.org/10.26565/1684-8489-2025-1-17

Van Pinxteren, I. (2024). *The AI Act: Key impacts for the public sector* [Master's thesis, European Online Academy]. Retrieved from https://www.euonlineacademy.org/EOA/Ressources/FCK/files/Master%20Thesis%20Final%20Paper/2024%20Van%20Pinxteren%20The%20AI%20Act%20Key%20impacts%20for%20the%20Public%20Sector.pdf

Vasiliauskienė, V., Banevičienė, A., & Stumbrys, V. (2025). Business actions posing threat to national security. *Environment. Technology. Resources*, *5*, 329–340. https://doi.org/10.17770/etr2025vol5.8505

Weerts, S. (2025). Generative AI in public administration in light of the regulatory awakening in the US and EU. *Cambridge Forum on AI: Law and Governance*, *1*, Article e3. https://doi.org/10.1017/cfl.2024.10

Anatolii Rachynskyi
Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv
Kyiv,
Ukraine
anatolii.rachynskyi@knu.ua
ORCID 0000-0001-9888-6978

Vadym Torichnyi
Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine
Khmelnytskyi,
Ukraine
thetorik@gmail.com
ORCID 0000-0003-3336-6386

Maksym Makarenko
CEO, MMDental Clinic
Kyiv,
Ukraine
dr.maksymmakarenko@gmail.com
ORCID 0000-0001-8677-8670

Dmytro Tkachuk
Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine
Khmelnytskyi,
Ukraine
tdv30041102@gmail.com
ORCID 0009-0001-1127-5742

Halyna Zavoritnya
Educational and Scientific Institute of Public Administration and Public Service, Taras Shevchenko National University of Kyiv
Kyiv,
Ukraine
galka.zavor@knu.ua
ORCID 0000-0002-0974-9013