4.3. Institutional architecture of information and cybersecurity as the basis of digital resilience of Ukraine: European experience and directions of implementation

Alina HLUSHKO,
Stanislav BILKO
National University "Yuri Kondratyuk Poltava Polytechnic"

The deepening of the digital transformation of the national economy and the growing functional dependence of critical infrastructure, financial systems, government services and business processes on digital technologies highlight the need to apply a systemic approach to strengthening the security of the digital environment (Onyshchenko S. et al., 2024). Under such conditions, the security of individual information resources, networks or digital systems is no longer a sufficient characteristic of the safe digital development of the state. Instead, the ability of the digital ecosystem to maintain functionality under the influence of destabilizing factors, adapt to changes in the security environment and restore critical processes after the implementation of threats becomes crucial.

This necessitates the clarification of the relationship between the categories of 'information security', 'cybersecurity' and 'digital resilience', which in modern scientific discourse and in regulatory and legal regulation are often used in an interrelated context, but have different content, subject orientation and functional purpose. Their identification narrows the analytical capabilities of the study and complicates the formation of a holistic model of security-oriented digital development of the state.

Information security has traditionally been understood through the key principles of confidentiality, integrity and availability of information. These principles are reflected in the ISO/IEC 27000 family of standards and constitute the fundamental basis for the protection of information resources and the functioning of information security management systems (ISO/IEC. Information security management systems – Overview, 2026). At the same time, the contemporary understanding of information security extends beyond the technical protection of data. It also covers the resilience of the information environment, the safeguarding of socially important information

processes, as well as resistance to disinformation, manipulative practices and other manifestations of information aggression (Onyshchenko S. et al., 2022).

This approach is reflected in the domestic regulatory and legal framework. Thus, according to the Information Security Strategy of Ukraine, information security is defined as a component of national security directly related to the protection of sovereignty, territorial integrity, democratic constitutional order and ensuring the right of citizens to reliable information (President of Ukraine. Information Security Strategy, 2021). Thus, information security encompasses both information protection and the ability of society and state institutions to function in conditions of information confrontation.

Cybersecurity is characterised by a distinct functional orientation, as its scope primarily covers cyberspace, digital networks, information systems, software and hardware infrastructure, and the processes associated with their operation (Yanko A. et al., 2025). Within the regulatory framework of the European Union, cybersecurity is interpreted as a set of measures aimed at protecting network and information systems, their users, as well as other entities potentially exposed to cyber threats (European Parliament and Council of the EU. Cybersecurity Act, 2019). This understanding was further expanded in the NIS2 Directive, which moves beyond a narrowly protective approach and incorporates cybersecurity risk management, incident reporting requirements, measures to ensure business continuity, and mechanisms for coordination among relevant entities and EU Member States (European Parliament and Council of the EU. Directive (EU) 2022/2555 – NIS2, 2022).

In Ukrainian legislation, cybersecurity is also associated not only with the state of security, but also with the ability to timely detect, prevent and neutralize cyber threats, while ensuring the sustainable development of the information society (Verkhovna Rada of Ukraine. On the Basic Principles of Ensuring Cybersecurity in Ukraine, 2017). The Cybersecurity Strategy of Ukraine defines cyber resilience as one of the key guidelines for the development of the national cybersecurity system, as the ability to quickly adapt to internal and external threats in cyberspace, to support and restore the sustainable functioning of the national information infrastructure, primarily critical information infrastructure facilities, as well as with the development of

interaction between cybersecurity entities. At the same time, the Strategy directly links strengthening cyber resilience with ensuring the socio-economic development of Ukraine in the digital environment (President of Ukraine. Cybersecurity Strategy of Ukraine, 2021).

Thus, it is inappropriate to consider information security and cybersecurity as identical concepts. Information security has a broader content and communication dimension and covers information regardless of its form of existence, social information processes and information impact. Cybersecurity, in turn, focuses primarily on the digital environment, network systems, software and hardware infrastructure and risks arising in cyberspace. Their relationship is formed through a common object of protection – the digital ecosystem of the state.

At the same time, in this context, the limitations of the security approach are revealed. Even a high degree of protection of individual systems does not guarantee the ability of the state's digital infrastructure to support the performance of critical functions in the event of a large-scale or prolonged violation (Onyshchenko S. et al., 2023). As a result, the category of resilience is becoming increasingly important in the European regulatory field, shifting the emphasis from the prevention of threats to the ability of the system to function in the conditions of their actual implementation.

The concept of digital operational resilience is most explicitly institutionalized in the EU Regulation on Digital Operational Resilience for the Financial Sector – DORA. In this regulatory framework, resilience is linked to an entity’s capacity to preserve operational integrity and reliability by sustaining the ICT capabilities required for the uninterrupted provision of services, including under conditions of disruption or security incidents (European Parliament and Council of the EU. Digital Operational Resilience Act – DORA, 2022). Although DORA is sector-specific, the methodological logic underpinning it extends beyond the financial sphere. It reflects a broader transformation of the security paradigm, in which emphasis is gradually shifting from incident prevention alone towards the capacity to manage disruptions, mitigate their consequences and maintain continuity of critical operations.

A comparable approach is embodied in the Cyber Resilience Act, which broadens cybersecurity requirements to products with digital elements and introduces

the principle of continuous vulnerability management throughout their lifecycle (European Parliament and Council of the EU. Cyber Resilience Act, 2024). Considered together, these regulatory developments demonstrate that the European approach increasingly prioritizes not merely a static condition of protection, but the dynamic capacity of digital systems to preserve essential functions, respond effectively to disruptive events and restore their operation afterwards.

Within this conceptual framework, digital resilience can be understood as an integrated systemic property formed by a set of interdependent capabilities: anticipating potential threats, withstanding destructive impacts, absorbing their consequences, adapting to altered operating conditions and restoring critical functions. Importantly, recovery should not be reduced to returning the system to its pre-disruption state. A resilient digital system is expected to transform the experience gained from crisis events into further improvement by addressing revealed vulnerabilities, reassessing backup and continuity mechanisms, and strengthening institutional coordination.

Generalizing the above gives grounds to consider information security as a category that characterizes the security of information and the information environment, cybersecurity as a state of security of digital systems, networks and processes in cyberspace, while digital resilience reflects the integrated ability of the state's digital ecosystem to counteract destabilizing influences, maintain functionality, adapt to changes and restore critically important processes. It is this ratio of categories that forms the basis of the author's model of their relationship, shown in Figure 4.4.

The full-scale war demonstrated that digital resilience directly affects the continuity of government, the functioning of the financial system, the provision of public services, the operation of businesses, and the provision of critical communications, and cannot be the result of the activities of a single government agency or regulatory initiative (Krasnobayev V. et al., 2023).

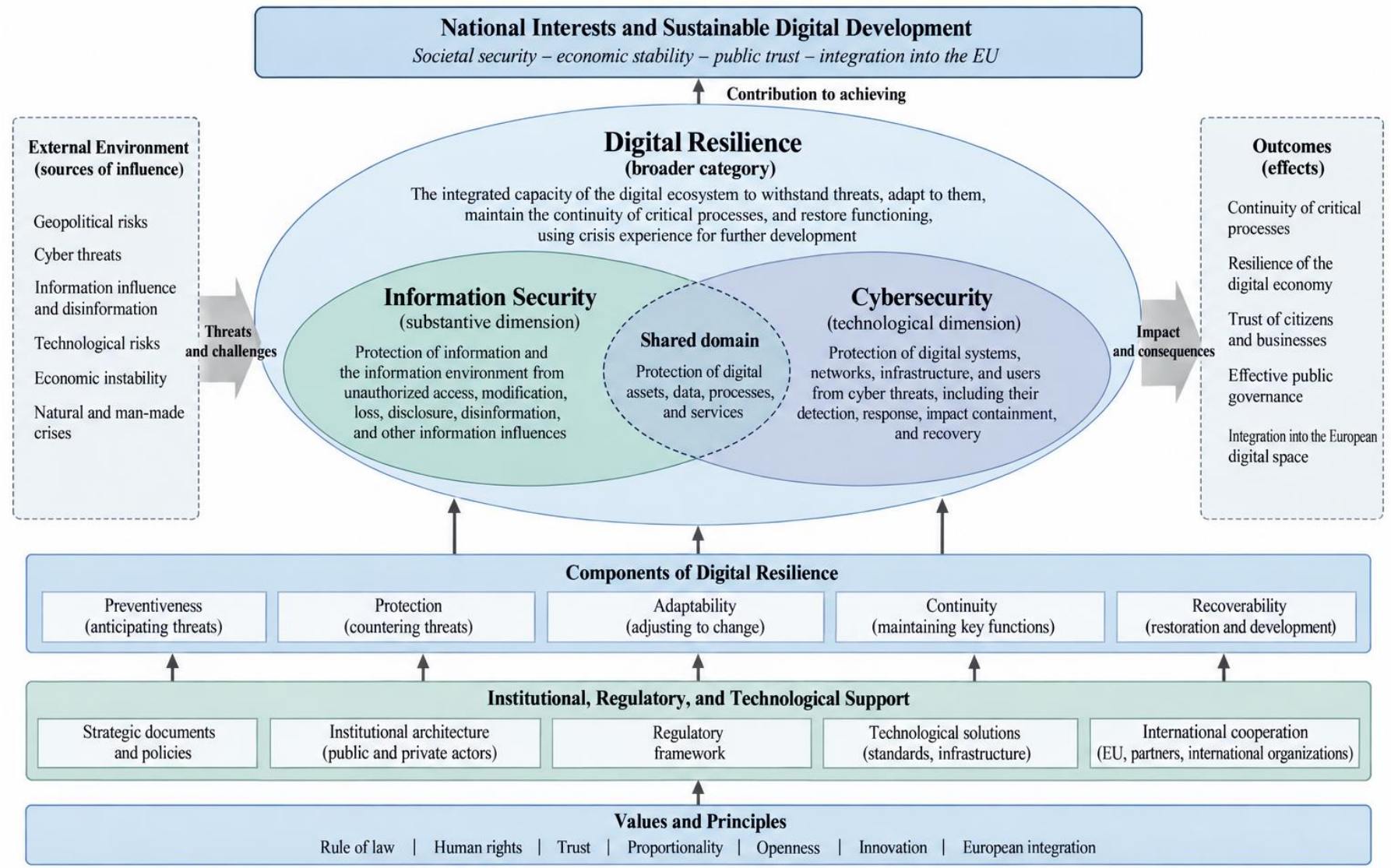


Fig. 4.4. Model of the relationship between the categories ‘information security’, ‘cybersecurity’ and ‘digital resilience’
Source: developed by the authors

Ensuring digital resilience requires a multi-level institutional framework in which strategic, regulatory, coordination and operational mechanisms function as interconnected components of a unified system for responding to cyber threats and digital disruptions. This logic is clearly reflected in the European Union model, where cybersecurity governance is based on the distribution of responsibilities among EU institutions, competent national authorities, incident response networks and specialized crisis-management structures.

A central institutional actor within this framework is the European Union Agency for Cybersecurity – ENISA, whose mandate was substantially strengthened following the adoption of the Cybersecurity Act and NIS2. The Agency's role extends beyond expert, analytical and advisory activities and includes organizational and technical support for key mechanisms of cross-border cybersecurity cooperation. ENISA provides secretariat support to the CSIRTs Network and EU-CyCLONe, facilitates information exchange, contributes to the development of common procedures, supports coordinated incident response and promotes situational awareness at the EU level (ENISA, 2025a; ENISA, 2025b).

An important feature of the European institutional architecture is that it does not concentrate all cybersecurity functions within a single governing centre. Instead, it is structured around the functional differentiation of interaction levels and the distribution of responsibilities among specialized mechanisms. At the strategic level, the NIS Cooperation Group ensures political and strategic coordination among Member States, supports the exchange of experience and good practices, and contributes to the development of coordinated approaches to implementing NIS2 requirements. At the operational and technical level, these functions are complemented by the CSIRTs Network, which brings together the incident response teams designated by Member States and CERT-EU. Its activities include exchanging information on incidents, risks and vulnerabilities, coordinating responses, disseminating relevant technologies, procedures and good practices, and strengthening operational cooperation among national teams (ENISA. CSIRTs Network, 2026).

A separate link is formed by CERT-EU, which acts as a hub for information exchange and coordination of cyber incident response for the institutions, bodies and

agencies of the European Union. Its interaction with ENISA is formalized and covers capacity development, operational cooperation, knowledge exchange and coordination during incidents. Such institutional interaction provides a link between the Union-wide cybersecurity system and the internal cyber resilience of the EU institutions (ENISA. Cooperation with CERT-EU, 2026).

The growing scale and complexity of cyber threats have necessitated the development of a dedicated mechanism for coordinating responses to major cyber crises – the European Cyber Crises Liaison Organisation Network (EU-CyCLONe). In contrast to the CSIRTs Network, which primarily focuses on technical coordination and the exchange of operational information, EU-CyCLONe operates at the operational crisis-management level. Its purpose is to support coordinated management of large-scale cyber incidents, develop a shared situational picture and facilitate interaction among national authorities responsible for cyber crisis management. The network was established in 2020, while its legal foundation was subsequently formalized through NIS2 in 2023 (ENISA. EU CyCLONe, 2026).

Accordingly, the defining feature of the European institutional model lies not merely in the existence of multiple bodies and networks, but in the way their functions complement one another. The strategic level is responsible for aligning policies and common approaches; the technical level supports operational information exchange and incident response; and the crisis-management level coordinates actions during large-scale and cross-border disruptions. Within this architecture, ENISA performs an important integrative role by supporting interaction among the relevant networks and maintaining institutional continuity of cooperation. This multi-level logic has been further consolidated in the updated EU cyber crisis response architecture, which explicitly differentiates between the technical, operational and political levels of cyber crisis management (Council of the European Union. EU Cybersecurity Crisis Management Blueprint, 2025).

The Cyber Solidarity Act, which entered into force in 2025 and strengthened the EU's joint capabilities to detect, prepare for and respond to cyber threats, is also of great importance for the development of this architecture. The document envisages the formation of a European Cybersecurity Alert System based on national and cross-

border cyber centers, as well as mutual assistance mechanisms and reserve response capacities. These developments demonstrate a gradual shift from a predominantly coordination-based model towards a model of collective digital resilience, in which Member States move beyond information exchange and increasingly rely on shared capacities and joint mechanisms for detecting, containing and responding to large-scale cyber incidents (European Parliament and Council of the EU. Cyber Solidarity Act, 2025).

Such a transformation also changes the logic of institutional interaction within the EU cybersecurity framework. As cooperation expands from information exchange to the joint use of resources and coordinated response mechanisms, the institutional architecture increasingly acquires the characteristics of a network-based system. It combines vertical and horizontal links among supranational institutions, Member States, national competent authorities and operational response teams, thereby ensuring the integration of strategic coordination, operational cooperation and collective response capacities within a single institutional framework. Its effectiveness is determined not so much by the number of institutions as by the presence of clearly distributed competencies, stable information exchange mechanisms, coordination procedures and common response tools. It is this property that makes the European model relevant for Ukraine, where further strengthening of digital resilience should be associated not only with the improvement of individual elements of the cybersecurity system, but also with increasing the coherence of interaction between them.

From a methodological perspective, the European experience makes it possible to identify at least four functional levels within the institutional architecture of digital resilience: strategic-regulatory, coordination, operational-technical and crisis-recovery (Fig. 4.5). Such structuring allows the institutional mechanisms of the EU to be considered as an integrated system through which the capacity to anticipate, detect, respond to and recover from digital crises is ensured. At the same time, this framework may serve as an analytical reference for evaluating the Ukrainian system of information security and cybersecurity, particularly in terms of the coherence of institutional functions, the distribution of responsibilities and the interaction between different levels of response.

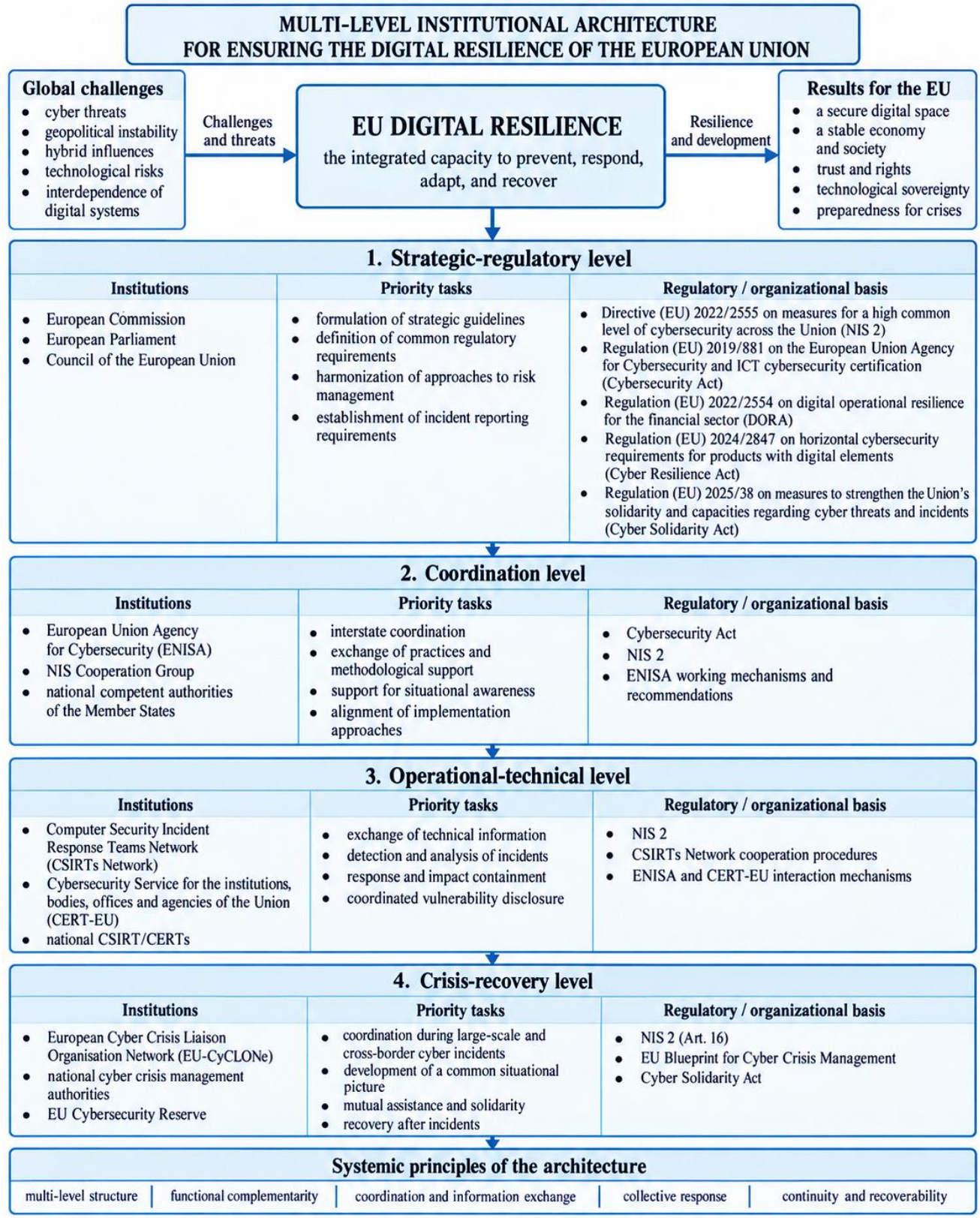


Fig. 4.5. Multi-level institutional architecture for ensuring digital resilience of the European Union

Source: author's development based on EU acts and institutional mechanisms

After all, it allows us to identify not only the presence or absence of individual institutions, but also the degree of functional coherence between management levels,

the effectiveness of information exchange mechanisms, incident response and recovery of digital infrastructure.

The presented multi-level architecture demonstrates that the digital resilience of the European Union is formed not only through the regulatory consolidation of competences or the functioning of specialized institutions, but through their coordinated interaction at different levels of prevention, detection, response and recovery.

At the same time, the functional capacity of the European Union's institutional architecture in the field of information and cybersecurity is most clearly manifested in the practice of responding to complex threats that are cross-border, cross-sectoral and combined in nature. This is not only about cyber incidents in the technological sense, but also about an interconnected spectrum of destabilizing influences, which include foreign information manipulation and interference, disinformation, hybrid operations, economic and technological espionage, attacks on critical infrastructure, disruption of digital supply chains and exploitation of technological dependencies (Onyshchenko S. et al., 2025). It is the multidimensionality of such threats that has led to the EU's transition from a predominantly sectoral model of protection to a comprehensive system of prevention, coordination, response and recovery.

One of the most characteristic areas of this transformation is countering foreign information manipulation and interference (Foreign Information Manipulation and Interference – FIMI). In the European approach, FIMI is viewed not as a set of individual cases of the spread of unreliable information, but as a purposeful and coordinated activity capable of influencing democratic processes, public trust, state decisions and the stability of the information environment. The European Commission notes the growth of coordinated inauthentic behavior, the use of bots, networks of fake accounts and algorithmic amplification of manipulative content, which necessitates the combination of regulatory, technological and communication response tools (European Commission. State of the Digital Decade 2025, 2025).

It is significant that the European model for countering FIMI is increasingly based not on the removal of individual content, but on building capacities for early detection, situational awareness, verification of information and coordination of responses. The European Democracy Shield envisages further strengthening the EU’s

capacities to prevent, detect, analyse and respond to FIMI and disinformation, as well as developing early warning systems and increasing societal resilience (European Commission and High Representative. European Democracy Shield, 2025), which confirms the relevance of managing the vulnerability of the information environment itself.

The EU's experience in responding to hybrid threats is important. The EU Strategic Compass views them as a combination of diverse means of pressure – cyberattacks, information operations, economic coercion, interference in democratic processes, and influence on energy and other critical infrastructure. To counter such threats, the EU Hybrid Toolbox has been created, which integrates preventive, cooperative, stabilizing, restrictive, and restorative measures (EEAS. A Strategic Compass for Security and Defence, 2022). The intersectoral nature of the response is fundamental in this context. The European External Action Service directly emphasizes that hybrid campaigns can combine cyberattacks, information manipulation, sabotage, influence on critical infrastructure, and other destabilizing tools, and therefore cannot be neutralized within the framework of a single policy or the competence of a single body (EEAS. Countering Hybrid Threats, 2026). That is why the EU Hybrid Toolbox interacts with the Cyber Diplomacy Toolbox and the FIMI Toolbox, forming a multi-channel response mechanism in which information, cyber, diplomatic and economic tools are used in a coordinated manner.

Countering economic and technological espionage is of particular importance, as digital transformation significantly increases the value of intangible assets, critical technologies, data, research results and know-how. In European policy, this issue is increasingly linked to the concept of economic security and research security. The EU Council Recommendation of 23 May 2024 on enhancing research security focuses on the risks of unwanted transfers of critical knowledge and technologies, foreign interference and the use of research results in a way that could harm the security of the EU or its Member States (Council of the European Union. Recommendation on Enhancing Research Security, 2024).

This direction is of particular importance for understanding digital resilience as a component of economic security. Protecting digital infrastructure without

simultaneously protecting critical knowledge, technological developments, and research results does not ensure the full sustainability of the economic system (Onyshchenko S. et al., 2024; Yanko A., Glushko A., 2019). Accordingly, the European approach does not involve the isolation of the scientific and innovative environment, but the introduction of risk-based mechanisms for assessing international cooperation, strengthening interagency coordination, developing support services for universities and research institutions, and applying the principle of "as open as possible, and as closed as necessary" (Council of the European Union. Recommendation on Enhancing Research Security, 2024).

No less significant direction is the protection of critical digital and physical infrastructure (Hlushko A.D., 2022). The European approach here also demonstrates a transition from the logic of protecting individual objects to ensuring the resilience of critical functions. Directive (EU) 2022/2557 on the resilience of critical entities forms a general framework for preventing, countering, absorbing the consequences, adapting to and recovering from incidents, covering both natural and anthropogenic, including hybrid, threats (European Parliament and Council of the EU. Directive (EU) 2022/2557 on the Resilience of Critical Entities, 2022).

It is particularly important that the Directive explicitly provides for consistency with NIS2, which allows combining cyber resilience with the physical and organizational resilience of critical entities. This is of fundamental importance for the digital economy, as the functioning of energy, transport, banking, healthcare, water supply, digital infrastructure and public administration is characterized by high interdependence. Disruption of one segment can cause cascading effects in other sectors, which necessitates coordinated risk management and cross-sectoral interaction (European Parliament and Council of the EU. Directive (EU) 2022/2557 on the Resilience of Critical Entities, 2022).

The relevance of this approach is also confirmed by the current cyber threat landscape. ENIS A in its 2025 report analyzed 4,875 incidents over the period from July 2024 to June 2025 and recorded an increase in the complexity of attacks, the active exploitation of vulnerabilities, interdependencies in supply chains and the spread of new attack models (ENISA. Threat Landscape 2025, 2025). ENISA data also shows

that data breaches significantly affected digital infrastructure and public administration, while ransomware attacks remained a significant risk for the manufacturing sector (ENISA. Threat Landscape 2025, 2025).

Generalizing the European experience gives grounds to assert that countering modern information and cyber threats in the EU is not based on the isolated use of individual tools, but on a combination of several interrelated approaches: monitoring and early detection, inter-institutional coordination, risk-based regulation, protection of critical assets, building social and organizational resilience, joint crisis response and recovery. It is their integration that ensures the transition from the model of countering individual threats to the model of maintaining the functional viability of the digital environment.

In this context, the relationship between types of threats and corresponding response mechanisms can be summarized according to the following logic: information manipulation - stability of the information environment; hybrid threats – cross-sectoral coordination; technological and economic espionage – protection of critical knowledge and technologies; attacks on critical infrastructure – continuity and resiliency of critical functions. Thus, European experience confirms that digital resilience is formed not as a result of the implementation of one direction of security policy, but as the overall ability of the institutional system to ensure the continuity of the functioning of the state, economy and society in conditions of complex destabilizing influence.

It is this logic that creates a methodological basis for further analysis of the Ukrainian information and cybersecurity system. At the same time, it is appropriate to compare not individual EU and Ukrainian institutions as formal analogues, but the functional capabilities they provide (strategic regulation, interdepartmental coordination, rapid response, crisis management and recovery) towards strengthening the digital resilience of the state.

The modern institutional model of cybersecurity in Ukraine has been formed as a multi-subject system, the core of which is enshrined in the Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity in Ukraine”. In the current version of the Law, the national cybersecurity system is defined as a set of cybersecurity entities and interconnected political, scientific and technical, informational, educational, legal, organizational, defense, intelligence, counterintelligence and engineering and technical

measures aimed, in particular, at protecting national information resources and critical information infrastructure facilities (Verkhovna Rada of Ukraine. On the Basic Principles of Ensuring Cybersecurity in Ukraine, 2017).

It is important that in 2025 the regulatory structure of this system was significantly updated. The Law of Ukraine No. 4336-IX of March 27, 2025 clarified the composition of the main subjects of the national cybersecurity system and expanded their functions. These include the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine and the Ministry of Foreign Affairs of Ukraine. At the same time, the mechanisms of national response, the functioning of the national SIRT, systems for exchanging information about cyber incidents and assessing the state of cyber defense were specified (Verkhovna Rada of Ukraine. On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Defense of State Information Resources, Critical Information Infrastructure Objects, 2025).

From the standpoint of the proposed four-level model, the first, strategic and regulatory level, in Ukraine is represented primarily by the system of strategic planning and legislative regulation of cybersecurity. Its basic elements are the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", the Cybersecurity Strategy of Ukraine 2021, the Information Security Strategy and the Law of Ukraine "On Critical Infrastructure". In Together, these documents form the legal basis for determining national interests, strategic goals, subject composition, cyber defense priorities, and critical infrastructure resilience requirements. The Cybersecurity Strategy directly orients the national system toward cyber resilience, interaction of subjects, and the ability to adapt to changes in the security environment (President of Ukraine. Cybersecurity Strategy of Ukraine, 2021).

Additional significance is given to this level by the Law of Ukraine 'On Critical Infrastructure', in which the security of critical infrastructure is defined by ensuring functionality, continuity of work, recoverability, integrity and resilience. This definition actually brings national regulatory and legal regulation closer to the

European resilience approach, where the object of protection is not only the infrastructure element as such, but also the ability of critical systems to maintain vital functions in conditions of destabilizing influences (Verkhovna Rada of Ukraine. On Critical Infrastructure, 2021).

The second, coordination level, is centered around the National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine. The NCSC performs the function of interdepartmental coordination, analyzes the state of cybersecurity, the readiness of entities to respond, the state of protection of critical infrastructure and state information resources, and also coordinates the functioning of the national cyber incident response system. In 2026, the NSDC directly characterizes the NCSC as a body designed to ensure coordinated work of state bodies in the field of cybersecurity and strengthen their ability to counter cyber threats (NSDC of Ukraine. NCSC: functions, composition and projects, 2026).

At the same time, it is the coordination level that is most sensitive to problems of institutional coherence. The Cybersecurity Strategy of Ukraine, analyzing the previous stage of its implementation, directly indicated the insufficient involvement of other state bodies, scientific institutions, the public and the private sector, as well as the lack of an established model of public-private partnership and systematicity in the development of cyber training. This indicates that the problem of digital Ukraine's resilience lies not only in the formal distribution of competencies, but also in the density and regularity of horizontal interaction between entities (President of Ukraine. Cybersecurity Strategy of Ukraine, 2021).

The third, operational and technical level, is the most developed in Ukraine in terms of subject matter. Its key element is CERT-UA - the national team for responding to cyber incidents, cyber attacks and cyber threats, which operates as part of the State Service for Special Communications and Information Protection of Ukraine. Its tasks include the accumulation and analysis of data on cyber incidents, providing practical assistance to cyber defense entities, developing recommendations for countering modern cyber attacks, interacting with Ukrainian and international response teams, and assisting state bodies and businesses in countering cyber threats (CERT-UA. About CERT-UA, 2026). The 2025 legislative update further strengthened this level. Law No.

4336-IX provides for the functioning of a national cyber incident response system, a national information exchange system on cyber incidents, cyber attacks and cyber threats, a national CSIRT, sectoral and regional CSIRTs, as well as mechanisms for assessing the state of cyber defense. From an institutional point of view, this means a transition from a model in which response was concentrated mainly in separate central structures to a more network architecture, functionally approaching the European CSIRTs Network model.

The fourth, crisis-recovery level, is being formed in Ukraine at the intersection of the cybersecurity system, critical infrastructure protection, and mechanisms for reserving state information resources. At the regulatory level, the categories of resiliency, continuity, and resilience of critical infrastructure have already been established, and in the legislation on cyber defense, the functioning of the National Center for Reserving State Information Resources and Mechanisms for Recovering After Incidents. At the same time, a comparison with the European architecture shows that it is the crisis-recovery component that remains the least institutionally isolated. In the EU, its functional content is supported by specialized network mechanisms such as EU-CyCLONe and Cybersecurity Reserve, while in Ukraine the corresponding functions are distributed across multiple actors and tools. This does not mean that there is a lack of relevant capabilities, but it makes it difficult to identify them as a holistic level of digital crisis management.

A separate direction of transformation is the gradual institutional rapprochement of Ukraine with the European cybersecurity system. Resolution of the Cabinet of Ministers of Ukraine dated April 8, 2025 No. 393 regulated the representation of Ukraine in the European Union Agency for Cybersecurity ENIS A, which creates a permanent channel of professional and institutional interaction between the national cybersecurity system and the European agency (Cabinet of Ministers of Ukraine. Some issues of representation in the European Union Agency for Cybersecurity ENISA, 2025). The Ukraine Facility provides for the approximation of Ukrainian legislation to the NIS/NIS2 framework and the implementation of EU approaches to 5G security, and the European Commission in its enlargement materials records Ukraine's support in approaching NIS2 and other elements of the digital acquis (European Commission.

Ukraine Plan / Digital Transformation, 2024; European Commission. Ukraine Report 2025, 2025).

The development of international coordination is also based on the continuation of the Ukraine-EU cyber dialogue, supporting the rapprochement with NIS2 and exploring the possibility of Ukraine's access to the European Cybersecurity Reserve established under the Cyber Solidarity Act. This shows that Ukraine's integration into the European cybersecurity space is gradually moving from political partnership to mutual inclusion in institutional and operational mechanisms of digital resilience.

Ukraine is on the path of forming a multi-level architecture of digital resilience, which is accompanied by the expansion of the subject composition, the detailing of functions, the formation of the CSIRT network, the development of information exchange mechanisms, the reservation of state resources, risk-oriented management of critical infrastructure and the deepening of interaction with ENIS A and other EU structures. At the same time, the presence of regulatory and organizational elements does not yet mean the achievement of full functional integrity of the system. According to the proposed four-level model, the most formed in Ukraine has a strategic-regulatory and operational-technical levels, while the coordination and crisis-recovery levels require further institutional strengthening. It is at the border of these levels that the main problems of interaction, duplication or dispersion of powers, uneven capabilities of individual sectors, limited integration of the private sector, and the absence of a fully formed mechanism for joint management of large-scale digital crises arise.

It is advisable to systematize the identified imbalances not only based on the fact of the presence of individual institutional shortcomings, but also taking into account the degree of formation of the corresponding level, the nature of functional gaps and their impact on the system's ability to ensure continuity, adaptability and resilience of the digital environment. Diagnostics of the institutional capacity of the national information and cybersecurity system will allow identifying those elements that require priority strengthening in the context of approaching the European model of digital resilience. A summary of the results of the analysis is presented in Table 4.4.

Table 4.4

Matrix of institutional gaps in the system for ensuring digital resilience in Ukraine

Level of institutional architecture	Current status and formed elements	Key institutional gap	Implications for digital resilience	Priority of institutional strengthening
1	2	3	4	5
Strategic and regulatory	The basic regulatory and strategic basis has been formed: the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", the Cybersecurity Strategy of Ukraine, the Information Security Strategy, the Law of Ukraine "On Critical Infrastructure", the mechanisms of cyber protection, response and functioning of the CSIRT updated in 2025. Gradual approximation to NIS2 and other elements of the EU digital acquis is being observed.	The gap between the regulatory consolidation of strategic guidelines and the completeness of their organizational and resource implementation.	Delay in transition from regulatory changes to real institutional capacities; risk of fragmented reforms; uneven implementation of strategic objectives; difficulty in assessing policy effectiveness.	Ensuring vertical coherence 'strategy → program → resource provision → indicators → monitoring of results'; synchronization of strategic documents; gradual formation of a single framework for the state's digital resilience.
Coordination	The National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine is functioning; the main subjects of the national cybersecurity system have been legally defined; mechanisms for interagency interaction, information exchange, international cooperation, and cyber dialogue with the EU are being developed.	Insufficient institutionalization of horizontal interaction between government agencies, sectoral regulators, critical infrastructure operators, business, the scientific and educational sector, and civil society.	Slowing down the exchange of critical information; risk of inconsistent decisions; difficulty in forming a common situational awareness; reduced speed of response to combined information and cyber threats.	Transition from interagency coordination to a network model of interaction ; formalization of public-private partnerships; standardization of information exchange protocols; development of permanent intersectoral coordination mechanisms.
Operational and technical	CERT-UA is operational; national, industry and regional CSIRTs are envisaged; a national system for exchanging information on cyber incidents, cyber attacks and cyber threats is being developed; significant monitoring, detection and response capabilities have been formed at the central level.	Unevenness of operational, human and technological capabilities between levels and sectors.	Formation of 'weak links' in the digital ecosystem; uneven speed of incident detection and localization; increased risk of cascading attacks; dependence of system stability on the level of the least protected segment.	Alignment of capabilities between central, sectoral and regional levels; development of the CSIRT network; training and retention of human resources; regular joint cyber training; development of testing, modeling and technical data exchange systems.

1	2	3	4	5
Crisis and recovery	The legislation provides for mechanisms for responding to crisis situations in the field of cybersecurity, reserving state information resources, restoring critical infrastructure, and coordinating the actions of entities. Separate continuity and redundancy tools have been formed.	Insufficient integration of crisis management, continuity and post-incident recovery into a single institutional system.	Difficulties in coordination during large-scale and cross-border crises; risk of delayed recovery; incomplete use of incident lessons for structural improvement of the system; weaker link between response and further resilience building.	Formation of a single crisis management cycle ; standardization of procedures for interdepartmental digital crisis management; strengthening of backup and recovery mechanisms.
Cross-level system dimension	All the basic elements of the institutional architecture are in place: strategic regulation, coordination, rapid response, and recovery mechanisms.	Insufficient functional integration of individual levels into a single digital sustainability cycle.	Reducing the synergistic effect of the entire system; digital resilience is formed as the sum of individual capabilities, rather than as a holistic mechanism; the transition from a reactive to a proactive risk management model is complicated.	Building a closed loop of digital resilience , in which strategic planning, coordination, rapid response, recovery, and institutional learning complement each other.

Source: systematized by the authors

The presented matrix allows us to draw a well-founded conclusion that the main problem in the development of the institutional architecture of digital resilience in Ukraine is not the absence of its basic elements, but their uneven level of maturity and insufficient functional integration. The Ukrainian system already contains most of the components characteristic of the modern European model, in particular, strategic regulation, central coordination, a response network, information exchange mechanisms, a critical infrastructure protection system and tools for international interaction. At the same time, the connections between these components require further institutionalization. This is especially important given that the results of the implementation of the Cybersecurity Strategy of Ukraine demonstrate both significant progress and the preservation of systemic limitations. According to the assessment of the NCCC, the overall level of implementation of the Strategy increased from 32% in 2022 to 86% in 2025, and the direction of 'Improving Interaction' was estimated at 88% (NCCC under the NSDC of Ukraine. Review of the National Cybersecurity System of Ukraine 2025, 2026). Among the reasons for incomplete implementation, insufficient budget funding, inconsistency of strategic planning and government plans, personnel limitations, and a number of unresolved organizational issues were identified (N CCC under the NSDC of Ukraine. Review of the National Cybersecurity System of Ukraine 2025, 2026).

Therefore, the identified institutional gaps indicate that further modernization of the national information and cybersecurity system should occur by strengthening the functional connections of already formed elements, which corresponds to the modern European model, within which digital resilience is ensured not by the concentration of powers in one center, but by the interaction of the strategic, coordination, operational and crisis levels.

The first direction is to identify the coordination of strategic and regulatory regulation. For Ukraine, the task of synchronizing strategic documents, their implementation plans, budgetary mechanisms and a system of performance indicators remains relevant. European experience shows that the effectiveness of regulatory regulation of cybersecurity largely depends on its integration with mechanisms for control, reporting, risk assessment and crisis response. The NIS2 Directive, the Cyber Solidarity Act and the updated EU Cybersecurity Crisis Management Blueprint

actually form a single regulatory framework within which risk management, incident response and recovery are considered as interrelated elements of the full cycle of cyber resilience (European Parliament and Council of the EU. Directive (EU) 2022/2555 – NIS2, 2022; Council of the European Union. EU Blueprint for Cyber Crisis Management, 2025).

The second direction is the institutionalization of horizontal coordination. The European model demonstrates that it is network-based mechanisms of interaction that ensure the transition from a formal division of powers to a joint operational capability. The CSIRTs Network, for example, functions as a network of response teams and CERT-EU designated by Member States, and ENISA provides its secretariat, coordination and support for cooperation during incidents. In this context, the Ukrainian system requires further development of permanent mechanisms of interaction between state authorities, industry regulators, critical infrastructure operators, private companies, and the scientific and educational sector. It is advisable to establish unified information exchange protocols, joint threat assessment procedures, incident escalation algorithms, and the formation of joint situational awareness.

The third direction should be the development of an integrated situational awareness and early warning system. In the EU, ENISA provides information exchange between the CSIRTs Network, EU-CyCLONe, CERT-EU, the European External Action Service and other structures, forming a holistic picture of the nature and scale of cyber threats. Such a system makes it possible to combine technical information about incidents with a broader political and strategic context. For Ukraine, a relevant direction for implementation is the development of a single information and analytical circuit that would combine operational data from CERT-UA and other CSIRTs, information from critical infrastructure, the private sector, law enforcement and intelligence agencies and ensure the transformation of this data into a common risk picture.

The fourth direction is related to the formation of a full-fledged crisis management mechanism for digital incidents. The European model clearly distinguishes between the technical, operational and political levels of response. EU-CyCLONe provides coordination at the level of national bodies responsible for cyber crisis management, while Cyber Blueprint 2025 extends this logic to the entire life cycle of a crisis - from preparation and detection to response and recovery. Therefore,

in Ukraine, it is advisable to form a standardized interdepartmental crisis management mechanism that would clearly define: criteria for transition from an incident to a crisis situation; the procedure for activating relevant structures; the distribution of functions between the technical, coordination and political levels; mechanisms for involving the private sector; the procedure for post-crisis analysis and policy adjustments.

The fifth direction should be to strengthen public-private cooperation. A high proportion of digital infrastructure, telecommunications, financial systems, cloud services and technology platforms is outside the direct control of the state, therefore digital sustainability objectively depends on the integration of the private sector. The European approach is increasingly focused on such interaction, in particular through the Cyber Partnership Programme ENISA and the mechanisms of the Cyber Solidarity Act, which provide for joint detection, preparedness and recovery capabilities.

The sixth area is the development of human and technological capacity. The European cyber resilience system relies heavily on the maturity of national CSIRTs, professional training of personnel and the ability to quickly scale up the response. The Cyber Solidarity Act directly links strengthening cyber resilience to the development of skills, knowledge and competences of specialists. At the same time, the task is to strengthen not only central, but also regional and sectoral capabilities, the development of cyber training grounds, a system of certification and training of specialists, regular interdepartmental and intersectoral exercises, as well as mechanisms for retaining highly qualified personnel in the public sector.

The seventh direction is to integrate post-incident analysis into the strategic management cycle. The European approach focuses on the full life cycle of crisis management, where recovery is not a final technical procedure, but a source of new knowledge for improving the system. This aspect is of fundamental importance for the transition to a digital resilience model.

The systematization of the identified areas allowed us to form a conceptual model for the modernization of the institutional architecture of digital resilience in Ukraine, in which the adaptation of European experience is carried out not through the mechanical reproduction of EU organizational structures, but through the implementation of the principles of functional interaction, network coordination, shared situational awareness, multi-level crisis response, and institutional learning (Fig. 4.6).

The proposed model systematizes the key areas of modernization of the institutional architecture of digital resilience of Ukraine and determines the priorities of its approximation to the European model, which are especially relevant given the role of information and cybersecurity in the post-war reconstruction and shaping of the digital future of Ukraine.

Ukraine's post-war recovery will require more than just reconstruction physical infrastructure and restoration of production potential, but also formation of a digital environment capable of ensuring the continuity of state administration, the stability of economic processes, the security of critical services and trust in digital institutions. In this context, information and cybersecurity become basic conditions for the economic and institutional viability of the state. Therefore, the security dimension of digital development must be integrated directly into the architecture of post-war recovery.

Digital resilience directly impacts economic recovery in several interrelated ways. First, it ensures the continuity of economic activity by minimizing losses from digital disruptions and cyberattacks. Second, it creates the prerequisites for investment confidence, as a secure digital environment reduces risks for investors, financial institutions, and technology companies. Third, it increases the resilience of critical infrastructure and digital public services, which is of particular importance in the context of post-war reconstruction. Fourth, it contributes to Ukraine's integration into the European digital space, where security requirements are increasingly linked to the functioning of the single digital market.

That is why the future strategy for Ukraine’s digital development should be shaped not only around technological renewal, business digitalization or expansion of electronic services, but around the combination of digital transformation and security capacity. From a methodological point of view, this gives grounds to consider Ukraine’s digital future as the result of the interaction of four basic components – technological modernization, institutional capacity, economic resilience and digital security.

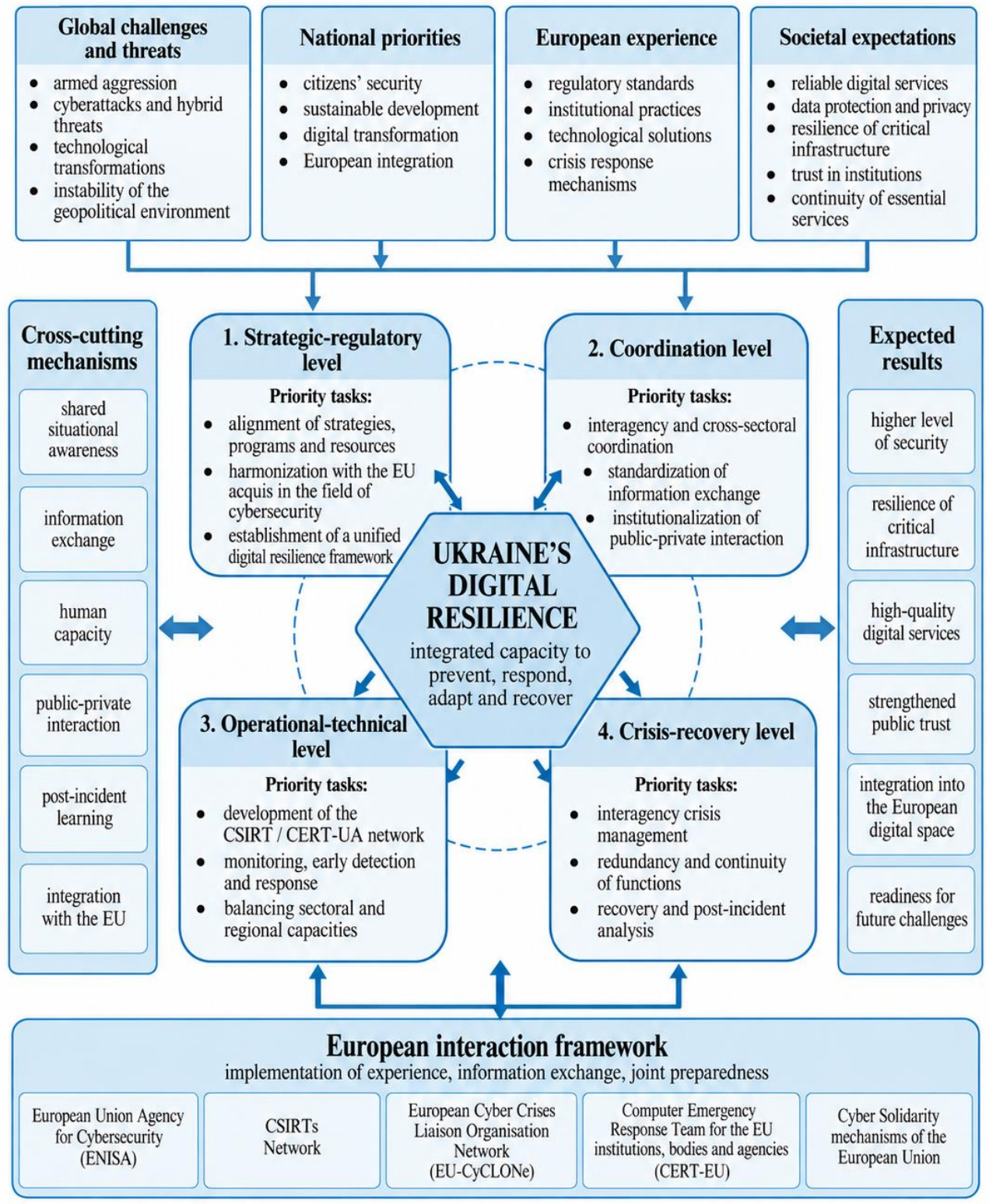


Fig. 4.6. Conceptual model for modernizing the institutional architecture of digital resilience in Ukraine, taking into account European experience

Source: developed by the authors

The absence of any of them violates the integrity of the system. Technological renewal without proper protection increases the surface of digital risks; security without modernization limits innovative development; digitalization without institutional coordination generates fragmentation; economic recovery without digital

resilience remains vulnerable to large-scale technological and cyber disruptions.

The post-war reconstruction of Ukraine should take place according to the principle of ‘security by design’, when information and cybersecurity requirements are laid down at the stage design of digital platforms, infrastructure systems, public services and technological solutions (Hlushko A. et al., 2025). This will avoid a situation in which security mechanisms are integrated after the creation of a digital system, which significantly increases the cost of modernization and leaves vulnerabilities unaccounted for. At the same time, the prospects for Ukraine's digital future directly depend on deepening cooperation with the EU, taking into account and successful implementation of European experience in strengthening information and cybersecurity.

Therefore, the conducted research allows us to assert that information and cybersecurity in the context of digital transformation should not be considered as separate areas of state policy, but as interconnected components of the digital resilience system, which determines the state's ability to prevent information and cyber threats, maintain the continuity of critical functions, adapt to destabilizing influences, respond to them in a coordinated manner, and restore the functioning of the digital ecosystem.

European experience confirms that such a capability is formed through a multi-level institutional architecture, functional complementarity of its elements, standardized mechanisms of coordinat

ion, information exchange and crisis response. For Ukraine, the key task is not to mechanically reproduce individual EU institutional models, but to adapt the principles of their interaction taking into account national conditions, military risks and post-war recovery tasks. The identified institutional gaps indicate that further strengthening of digital resilience should be aimed primarily at increasing coherence between the strategic-regulatory, coordination, operational-technical and crisis-recovery levels.

In this context, digital resilience acquires significance not only in terms of security, but also in terms of economy, as it directly affects the continuity of public administration, the functioning of critical infrastructure, the stability of business processes, investment confidence, and the state's ability to technologically upgrade. That is why it is appropriate to consider it as one of the basic prerequisites for shaping Ukraine's digital future and sustainable post-war development.

REFERENCES FOR SUBSECTION 4.3

1. Onyshchenko S., Hlushko A., Maslii O., Chumak O. Digital transformation of the national economy in the context of information environment development in Ukraine. In: Transformations of national economies under conditions of instability. 2024. P. 169-197. DOI: https://doi.org/10.21303/978-9916-9850-6-9.ch6
2. ISO/IEC 27000:2026. Information security, cybersecurity and privacy protection — Information security management systems — Overview. Geneva : International Organization for Standardization, 2026. URL: https://www.iso.org/standard/27000 (date of application: 10.08.2026).
3. Onyshchenko CB, Hlushko A.D., Masliy O.A. Cyber resilience as a basis for the national security of Ukraine. Innovations and prospects of world science. Proceedings of the 11th International scientific and practical conference. Perfect Publishing. Vancouver, Canada. 2022. Pp. 551-556 (635 p.). URL: https://sci-conf.com.ua/ximezhdunarodnayanauchno-prakticheskaya- konfere ntsiya-innovations-and-prospects-ofworld-science-22-24-iyunya-2022-goda-vankuver-kanada-arhiv (date of application: 10.08.2026).
4. On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 “On the Information Security Strategy”: Decree of the President of Ukraine dated December 28, 2021 No. 685/2021. Legislation of Ukraine / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.Ua/laws/show/685/2021#Text (date of application: 10.08.2026).
5. Yanko A., Krasnobayev V., Hlushko A., Myziura M. Implementation of Cryptographic Transformations for Digital Security Using the Residue Number System. Information Control Systems & Technologies (ICST-2025): proceedings of the 13th International Scientific and Practical Conference, Odesa, Sept. 24-26. 2025. CEUR Workshop Proceedings. 2025. Vol. 4048. P. 55-67. URL: https://ceur-ws.org/Vol-4048/paper05.pdf (date of application: 08/10/2026).
6. European Parliament and Council of the European Union. Regulation (EU) 2019/881 of 17 April 2019 on ENIS A (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the

European Union. 2019.L151.P.15-69. URL: https://eur- lex.europa.eu/eli/reg/2019/881 /oj/eng (date of application: 08/10/2026).

7. European Parliament and Council of the European Union. Directive (EU) 2022/2555 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). Official Journal of the European Union. 2022. L 333. P. 80-152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (date of application: 08/10/2026).

8. On the Basic Principles of Ensuring Cybersecurity in Ukraine: Law of Ukraine dated 05.10.2017 No. 2163-VIII. Legislation of Ukraine / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2 163-19#T ext (date of application: 10.08.2026).

9. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. Legislation of Ukraine / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.Ua/laws/show/447/2021#Text (date of application: 08/10/2026).

10. Onyshchenko S., Yanko A., Hlushko A., Sabelnikova R. Assessment of information protection level against unauthorized access. ScienceRise. 2023. No. 2. C. 36^44. DOI: https://doi.org/10.21303/2313-841 6,2023.003211

11. European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act - DORA). Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (date of application: 08/10/2026).

12. European Parliament and Council of the European Union. Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (date of application: 10.08.2026).

13. Krasnobayev V., Yanko A., Hlushko A., Kruk O., Kruk O., Gakh V., Onyshchenko S., Maslii O., Hrashchenko I. Economic and cyber security. Ternopil:

Medy chna Knyha, 2023. DOI: https://doi.Org/l 0, 15587/978-6 17-73 19-98-5

14. European Union Agency for Cybersecurity (ENISA). ENISA Single Programming Document 2025-2027. Athens : ENISA, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-02/MB%20Decision%202024-16%20on%20 adopting%20ENISA%20SPD%202025-2027%20with%20annexes.pdf (date of application: 08/12/2026).

15. European Union Agency for Cybersecurity (ENISA). ENISA Single Programming Document 2025-2027: Condensed Version. ENISA, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-02/ENISA%20Single%20Programming%20Document %202025-2027%20-%20Condensed%20version.pdf (date of application: 08/12/2026).

16. European Union Agency for Cybersecurity (ENISA). CSIRTs Network. URL: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network (date of application: 08/12/2026).

17. European Union Agency for Cybersecurity (ENISA). Cooperation with CERT-EU. URL: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/cooperation-with-cert-eu (date of application: 08/12/2026).

18. European Union Agency for Cybersecurity (ENISA). EU CyCLONE - European Cyber Crises Liaison Organization Network. URL: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone (date of application: 08/12/2026).

19. Council of the European Union. Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management (C/2025/3445). Official Journal of the European Union. 2025. C/2025/3445. URL: https://eur-lex.europa.eu/eli/C/2025/3445/oj/eng (date of application: 08/12/2026).

20. European Parliament and Council of the European Union. Regulation (EU) 2025/3 8 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). Official Journal of the European Union. 2025. URL: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng (date of application: 08/12/2026).

21. Onyshchenko S., Maslii O., Hlushko A. Digital and Economic Security of the State Under Global Threats. Applied Innovations in Information and Communication Technology. ICAIIT 2024. Lecture Notes in Networks and Systems. Vol. 1338. Cham : Springer, 2025. DOI: https://doi.org/10.1 007/978-3-03 1 -89296-7 29

22. European Commission. State of the Digital Decade 2025. Brussels, 2025. URL: https://digital-strategv.ec.europa.eu/en/policies/2025-s tate-digital-decade-package (date of application: 08/12/2026).

23. European Commission. European Democracy Shield. 2025. URL: https://commission.europa.eu/publications/eu ropean-democracy-shield-documents en (date of application: 08/12/2026).

24. European External Action Service (EEAS). A Strategic Compass for Security and Defense. Brussels, 2022. URL: https://www.eeas.europa.eu /sites/default/files/documents/strategic compass en3 web.pdf (date of application: 08/12/2026).

25. European External Action Service (EEAS). Countering Hybrid Threats. 2026. URL: https://www.eeas.europa.eu/eeas/eu-action-countering-hybrid-threats_en (date of application: 08/12/2026).

26. Council of the European Union. Council Recommendation of 23 May 2024 on enhancing research security (C/2024/3510). Official Journal of the European Union. 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/23/council-adopts-a-recommendation-to-enhance-research-security/ (date of application: 08/12/2026).

27. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. Cyber risk management technology to strengthen the information security of the national economy. Naukovyi Visnyk

National University of Agriculture. 2024. Vol. 5. P. 136-142. DOI: https://doi.org/10.33271/nvngu/2024-5/136

28. Yanko AS, Glushko AD Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. Economics and Region. 2019. Vol. 4 (75). P. 36-44. DOI: https://d0i.0rg/l 0.26906/eip.2019.4(75). 1814

29. Hlushko A.D. Deregulation of the business environment in Ukraine under

martial law. Economic security: state. region, enterprise: Materials of the International Scientific and Practical Internet Conference, September 29, 2022. Poltava: NUPP, 2022. P. 24-27 (215 p.) . URL: https://reposit.nupp.edu.ua/item/9632 (date of application: 08/15/2026).

30. European Parliament and Council of the European Union. Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (date of application: 08/15/2026).

31. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. Athens : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (date of application: 08/15/2026).

32. On Amendments to Certain Laws of Ukraine on Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure Objects: Law of Ukraine dated 27.03.2025 No. 4336-IX. Bulletin of the Verkhovna Rada of Ukraine. 2025. No. 35. Art. 134. URL: https://zakon.rada.gov.ua/laws/show/43 3 6-20#Text (date of application: 08/15/2026).

33. On critical infrastructure: Law of Ukraine dated 16.11.2021 No. 1882-IX. Legislation of Ukraine / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/ 1882-20#T ext (date of application: 08/15/2026).

34. National Security and Defense Council of Ukraine. NKCC: we tell about the functions, composition and projects. 2026. URL: https://rnbo .gov.ua/ua/Diialnist/7801.html (date of application: 08/15/2026).

35. CERT-UA. About CERT-UA. URL: https://cert.gov.ua/about-us (date of application: 08/15/2026).

36. Some issues of representation in the European Union Agency for Cybersecurity ENISA : Resolution of the Cabinet of Ministers of Ukraine dated 08.04.2025 No. 393. Legislation of Ukraine / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/3 93-2025 -%D0%BF#Te xt (date of application: 08/16/2026).

37. European Commission. Ukraine Plan. Digital Transformation. 2024. URL: https://enlargement.ec.europa.eu/document/download/128f83e6-11 fe-494a-867b-bda5177b62dd_ en (date of application: 08/16/2026).

38. European Commission. Ukraine Report 2025. Brussels, 2025. URL: https://enlargement.ec.europa.eu/ukraine-report-2025 en (date of application: 08/16/2026).

39. National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine. Overview of the National Cybersecurity System of Ukraine 2025. Kyiv, 2026. URL: https://www.rnbo.gov.ua/files/2026/NATIQNAL CYBER SCC/kiber 2025.pdf (date of application: 08/16/2026).

40. Hlushko A., Yanko A., Bilko S. Digital transformation of business processes: security aspect. Digital economy and economic security. 2025. 2 (17). 160-166. DOI: https://d0i.0rg/l 0.32782/dees. 17-26